



Documentação do NetApp Ransomware Resilience

NetApp Ransomware Resilience

NetApp
February 17, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/data-services-ransomware-resilience/index.html> on February 17, 2026. Always check docs.netapp.com for the latest.

Índice

Documentação do NetApp Ransomware Resilience	1
Notas de lançamento	2
Novidades na NetApp Ransomware Resilience	2
16 de fevereiro de 2026	2
19 de janeiro de 2026	2
12 de janeiro de 2026	2
08 de dezembro de 2025	3
10 de novembro de 2025	3
06 de outubro de 2025	3
12 de agosto de 2025	5
15 de julho de 2025	5
9 de junho de 2025	5
13 de maio de 2025	6
29 de abril de 2025	6
14 de abril de 2025	7
10 de março de 2025	8
16 de dezembro de 2024	8
7 de novembro de 2024	9
30 de setembro de 2024	10
2 de setembro de 2024	10
5 de agosto de 2024	11
1 de julho de 2024	11
10 de junho de 2024	12
14 de maio de 2024	12
5 de março de 2024	14
6 de outubro de 2023	14
Limitações conhecidas do NetApp Ransomware Resilience	15
Problema com a opção de reinicialização do exercício de prontidão	15
Limitações do Amazon FSx for NetApp ONTAP	15
Limitações do Azure NetApp Files	15
Começar	16
Saiba mais sobre a NetApp Ransomware Resilience	16
Resiliência do Ransomware na camada de dados	16
O que você pode fazer com a resiliência do Ransomware	17
Benefícios do uso do Ransomware Resilience	18
Custo	18
Licenciamento	19
NetApp Console	19
Como funciona a resiliência do ransomware	19
Destinos de backup, sistemas e fontes de dados de carga de trabalho suportados	21
Termos-chave	22
Pré-requisitos de NetApp Ransomware Resilience	23
Sistemas suportados	23

Requisitos do NetApp Console	23
Requisitos do ONTAP	24
Backups de dados	24
Requisitos de comportamento suspeito do usuário	24
Atualizar permissões de usuários não administradores em um sistema ONTAP	24
Início rápido para NetApp Ransomware Resilience	25
Configurar a NetApp Ransomware Resilience	26
Preparar o destino do backup	26
Configurar o NetApp Console	27
Acesse a NetApp Ransomware Resilience	27
Configurar licenciamento para NetApp Ransomware Resilience	28
Tipos de licença	29
Outras licenças	29
Experimente o Ransomware Resilience com um teste gratuito de 30 dias	29
Assine pelo AWS Marketplace	30
Assine pelo Microsoft Azure Marketplace	32
Assine pelo Google Cloud Platform Marketplace	34
Traga sua própria licença (BYOL)	36
Atualize sua licença do Console quando ela expirar	37
Encerrar a assinatura do PAYGO	38
Mais informações	38
Descubra cargas de trabalho no NetApp Ransomware Resilience	38
Selecione cargas de trabalho para descobrir e proteger	39
Descubra cargas de trabalho recém-criadas para sistemas selecionados anteriormente	41
Descubra novos sistemas	41
Excluir cargas de trabalho	41
Realizar um exercício de preparação para ataques de ransomware no NetApp Ransomware Resilience	43
Configurar um exercício de preparação para ataque de ransomware	43
Iniciar um exercício de prontidão	46
Responder a um alerta de exercício de prontidão	46
Restaurar a carga de trabalho de teste	48
Alterar o status dos alertas após o exercício de prontidão	49
Relatórios de revisão sobre o exercício de prontidão	50
Configurar as definições de proteção no NetApp Ransomware Resilience	50
Acesse a página Configurações diretamente	51
Simule um ataque de ransomware	51
Configurar descoberta de carga de trabalho	51
Adicionar um destino de backup	51
Conecte NetApp Ransomware Resilience ao sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças	58
Dados de eventos enviados para um SIEM	58
Configurar o AWS Security Hub para detecção de ameaças	59
Configurar o Microsoft Sentinel para detecção de ameaças	60
Configurar o Splunk Cloud para detecção de ameaças	62
Conecte o SIEM na resiliência do ransomware	62

Configurar detecção de atividade do usuário	63
Aprenda sobre detecção de atividade do usuário em NetApp Ransomware Resilience	64
Requisitos para detecção de comportamento do usuário em NetApp Ransomware Resilience	66
Configurar agentes e coletores para detecção de atividade do usuário em NetApp Ransomware Resilience	70
Use a resiliência do ransomware	76
Monitore a integridade da carga de trabalho usando o NetApp Ransomware Resilience Dashboard	76
Revise a integridade da carga de trabalho usando o Pannel	76
Revise as recomendações de proteção no Pannel	77
Exportar dados de proteção para arquivos CSV	79
Acessar documentação técnica	80
Proteja as cargas de trabalho	80
Proteja cargas de trabalho com estratégias de proteção de NetApp Ransomware Resilience	80
Procure informações de identificação pessoal com a NetApp Data Classification no Ransomware Resilience	95
Gerencie alertas no NetApp Ransomware Resilience	99
Ver alertas	100
Responder a um e-mail de alerta	101
Detecte atividades maliciosas e comportamento anômalo do usuário	102
Marcar incidentes de ransomware como prontos para recuperação (após os incidentes serem neutralizados)	103
Descartar incidentes que não sejam ataques potenciais	104
Ver uma lista de arquivos afetados	106
Recupere-se de um ataque de ransomware (após a neutralização dos incidentes) com a NetApp Ransomware Resilience	107
Exibir cargas de trabalho que estão prontas para serem restauradas	108
Restaurar uma carga de trabalho gerenciada pelo SnapCenter	108
Restaurar uma carga de trabalho não gerenciada pelo SnapCenter	109
Baixe relatórios no NetApp Ransomware Resilience	117
Conhecimento e suporte	119
Registre-se para obter suporte	119
Visão geral do registro de suporte	119
Registre o NetApp Console para suporte ao NetApp	119
Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP	121
Obter ajuda	123
Obtenha suporte para um serviço de arquivo de provedor de nuvem	123
Use opções de autoapoio	123
Crie um caso com o suporte da NetApp	123
Gerencie seus casos de suporte	126
Perguntas frequentes sobre a NetApp Ransomware Resilience	127
Implantação	127
Acesso	127
Interoperabilidade	128
Cargas de trabalho	128
Políticas de proteção	129

Avisos legais	131
Direitos autorais	131
Marcas Registradas	131
Patentes	131
Política de Privacidade	131
Código aberto	131

Documentação do NetApp Ransomware Resilience

Notas de lançamento

Novidades na NetApp Ransomware Resilience

Saiba o que há de novo no NetApp Ransomware Resilience.

16 de fevereiro de 2026

Suporte do Azure NetApp Files

O Ransomware Resilience agora oferece suporte a sistemas Azure NetApp Files, permitindo que você detecte e responda a ameaças de ransomware no Azure NetApp Files com eficiência. Ao descobrir cargas de trabalho, o Ransomware Resilience agora apresenta Azure NetApp Files e as exibe no painel de proteção. O suporte do Ransomware Resilience para Azure NetApp Files inclui estratégias de detecção e proteção apenas com snapshots. O suporte para Azure NetApp Files está atualmente em versão prévia.

Para obter mais informações, consulte o xref:./para obter mais informações, consulte ["Saiba mais sobre resiliência ao ransomware"](#).

Excluir usuários dos alertas de comportamento do usuário

Ransomware Resilience agora permite que você exclua usuários específicos dos alertas de comportamento do usuário. Excluir usuários confiáveis pode evitar falsos positivos e alertas desnecessários.

Para obter mais informações, consulte o xref:./Para obter mais informações, consulte ["Excluir usuários dos alertas"](#).

Suporte de grupo de proteção para atividade de comportamento do usuário

Os grupos de proteção Ransomware Resilience agora oferecem suporte a políticas de detecção para detecção de comportamento suspeito do usuário. Ao aplicar uma estratégia de proteção contra ransomware a um grupo de proteção, ela aplica uma política em todas as cargas de trabalho, simplificando o gerenciamento da sua postura de cibersegurança.

Para mais informações, consulte ["Crie um grupo de proteção"](#).

19 de janeiro de 2026

Volumes não suportados

Os relatórios de Resiliência a Ransomware agora capturam informações sobre volumes suportados e não suportados no relatório **Resumo**. Utilize essas informações para diagnosticar por que os volumes de um sistema podem não ser elegíveis para proteção contra ransomware.

Para mais informações, consulte ["Baixe relatórios em Resiliência a Ransomware"](#).

12 de janeiro de 2026

Replicar snapshots para o ONTAP

Ransomware Resilience agora oferece suporte à adição de replicação de snapshots para um site ONTAP secundário. Com grupos de proteção que utilizam uma política de replicação, você pode replicar para o

mesmo destino ou para destinos diferentes para cada carga de trabalho. Você pode criar uma estratégia de proteção contra ransomware que inclua replicação ou usar a estratégia predefinida.

Para mais informações, consulte ["Proteja as cargas de trabalho com resiliência contra ransomware."](#)

Excluir cargas de trabalho da resiliência a ransomware

O Ransomware Resilience agora permite excluir cargas de trabalho específicas de um sistema da proteção, além de oferecer suporte ao painel de controle do Ransomware Resilience. Você pode excluir cargas de trabalho após a descoberta e incluí-las novamente se desejar adicionar proteção contra ransomware. Você não será cobrado por cargas de trabalho excluídas.

Para mais informações, consulte ["Excluir cargas de trabalho"](#).

Alertas de marcação como em revisão

A Resiliência contra Ransomware agora permite que você marque alertas como "Em análise". Use a etiqueta "Em análise" para melhorar a clareza em toda a sua equipe ao priorizar e gerenciar ameaças ativas de ransomware.

Para mais informações, consulte ["Gerencie alertas em Resiliência a Ransomware"](#).

08 de dezembro de 2025

O bloqueio de extensões está habilitado no nível da carga de trabalho.

Ao ativar o bloqueio de extensão, ele passa a ser ativado no nível da carga de trabalho, e não no nível da máquina virtual de armazenamento.

Editar o status de alerta de comportamento do usuário

O recurso Resiliência a Ransomware agora permite editar o status dos alertas de comportamento do usuário. Você pode descartar e resolver alertas manualmente.

Para mais informações, consulte ["Gerencie alertas em Resiliência a Ransomware"](#).

Suporte para vários agentes de console

O Ransomware Resilience agora suporta o uso de vários agentes de console para gerenciar os mesmos sistemas.

Para obter mais informações sobre agentes do Console, consulte ["Criar um agente de console"](#).

10 de novembro de 2025

Esta versão inclui aprimoramentos e melhorias gerais.

06 de outubro de 2025

A BlueXP ransomware protection agora é NetApp Ransomware Resilience

O serviço de BlueXP ransomware protection foi renomeado para NetApp Ransomware Resilience.

BlueXP agora é NetApp Console

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados em ambientes locais e na nuvem em nível empresarial, fornecendo insights em tempo real, fluxos de trabalho mais rápidos e administração simplificada.

Para obter detalhes sobre o que mudou, consulte o ["Notas de versão do NetApp Console"](#).

Detecção de violação de dados

O Ransomware Resilience inclui um novo mecanismo de detecção que pode ser ativado em algumas etapas para detectar leituras anômalas do usuário como um indicador precoce de violação de dados. A resiliência do ransomware coleta e analisa eventos de leitura do usuário criando uma linha de base histórica, que é um perfil de comportamento normal esperado a partir de dados anteriores. Quando uma nova atividade do usuário se desvia significativamente dessa norma estabelecida (como um aumento inesperado de leituras combinado com padrões de leitura suspeitos), um alerta é gerado. O Ransomware Resilience inclui um modelo de IA para detectar padrões de leitura suspeitos.

Diferentemente da detecção de criptografia pelo ARP na camada de armazenamento, a detecção da anomalia de comportamento do usuário é feita no serviço Ransomware Resilience SaaS por meio da coleta de eventos FPolicy.



Você deve usar o novo ["Administrador de comportamento do usuário do Ransomware Resilience e visualizador de comportamento do usuário do Ransomware Resilience"](#) funções para acessar configurações de detecção de comportamento suspeito do usuário.

Para mais informações, consulte ["Habilitar detecção de atividades suspeitas de usuários"](#) e ["Visualizar comportamento anômalo do usuário"](#).

Detecções adicionais de atividades suspeitas de usuários

Além da detecção de violações de dados, o Ransomware Resilience também detecta os seguintes tipos de alerta com base na atividade suspeita observada do usuário:

- **Destruição de dados - ataque potencial** - Um alerta com a gravidade do ataque potencial é criado quando o número de exclusões de arquivos excede a norma histórica.
- **Comportamento suspeito do usuário - ataque potencial** - Um alerta com a gravidade do ataque potencial é criado quando são observadas operações de leitura, renomeação e exclusão em uma sequência semelhante a um ataque de ransomware
- **Comportamento suspeito do usuário - Aviso** - Um alerta com a gravidade do aviso é criado quando o número total de atividades de arquivo (leitura, exclusão, renomeação etc.) excede a norma histórica

Novas funções de usuário para detecção de violação de dados

Para gerenciar alertas de atividades suspeitas do usuário, o Ransomware Resilience introduziu duas novas funções para administradores da organização do Console concederem acesso à detecção de atividades suspeitas do usuário: administrador de comportamento do usuário do Ransomware Resilience e visualizador de comportamento do usuário do Ransomware Resilience.

Você deve ser um administrador de comportamento do usuário para configurar configurações de comportamento suspeito do usuário. A função de administrador do Ransomware Resilience não tem suporte para configurar comportamentos suspeitos do usuário.

Para obter mais informações, consulte ["Acesso baseado em função de NetApp Ransomware Resilience"](#).

12 de agosto de 2025

Esta versão inclui aprimoramentos e melhorias gerais.

15 de julho de 2025

Suporte de carga de trabalho SAN

Esta versão inclui suporte para cargas de trabalho SAN na BlueXP ransomware protection. Agora você pode proteger cargas de trabalho SAN, além de cargas de trabalho NFS e CIFS.

Para mais informações, consulte ["Pré-requisitos de BlueXP ransomware protection"](#) .

Proteção aprimorada da carga de trabalho

Esta versão melhora o processo de configuração para cargas de trabalho com políticas de snapshot e backup de outras ferramentas da NetApp , como SnapCenter ou BlueXP backup and recovery. Em versões anteriores, a BlueXP ransomware protection descobria as políticas de outras ferramentas, permitindo apenas que você alterasse a política de detecção. Com esta versão, agora você pode substituir políticas de snapshot e backup por políticas de BlueXP ransomware protection ou continuar a usar as políticas de outras ferramentas.

Para mais detalhes, consulte ["Proteja as cargas de trabalho"](#) .

Notificações por e-mail

Se a BlueXP ransomware protection detectar um possível ataque, uma notificação aparecerá nas Notificações do BlueXP e um e-mail será enviado para o endereço de e-mail que você configurou.

O e-mail inclui informações sobre a gravidade, a carga de trabalho impactada e um link para o alerta na guia **Alertas** da BlueXP ransomware protection .

Se você configurou um sistema de gerenciamento de segurança e eventos (SIEM) na BlueXP ransomware protection, o serviço envia detalhes de alerta para seu sistema SIEM.

Para mais detalhes, consulte ["Lidar com alertas de ransomware detectados"](#) .

9 de junho de 2025

Atualizações da página de destino

Esta versão inclui atualizações na página inicial da BlueXP ransomware protection, o que facilita o início do teste gratuito e a descoberta.

Atualizações de exercícios de prontidão

Anteriormente, você podia executar um exercício de prontidão para ransomware simulando um ataque em uma nova carga de trabalho de amostra. Com esse recurso, você pode investigar o ataque simulado e recuperar a carga de trabalho. Use este recurso para testar notificações de alerta, resposta e recuperação. Execute e programe esses exercícios sempre que necessário.

Com esta versão, você pode usar um novo botão no Painel de BlueXP ransomware protection para executar um exercício de prontidão para ransomware em uma carga de trabalho de teste, facilitando a simulação de ataques de ransomware, a investigação de seu impacto e a recuperação eficiente de cargas de trabalho, tudo em um ambiente controlado.

Agora você pode executar exercícios de prontidão em cargas de trabalho CIFS (SMB), além de cargas de trabalho NFS.

Para mais detalhes, consulte ["Realizar um exercício de preparação para ataques de ransomware"](#) .

Habilitar atualizações de BlueXP classification

Antes de usar a BlueXP classification no serviço de BlueXP ransomware protection , você precisa habilitar a BlueXP classification para verificar seus dados. Classificar dados ajuda você a encontrar informações de identificação pessoal (PII), o que pode aumentar os riscos de segurança.

Você pode implantar a BlueXP classification em uma carga de trabalho de compartilhamento de arquivos a partir da BlueXP ransomware protection. Na coluna **Exposição de privacidade**, selecione a opção **Identificar exposição**. Se você ativou o serviço de classificação, esta ação identifica a exposição. Caso contrário, com esta versão, uma caixa de diálogo apresenta a opção de implantar a BlueXP classification. Selecione **Implantar** para ir para a página inicial do serviço de BlueXP classification , onde você pode implantar esse serviço. C

Para mais detalhes, consulte ["Implantar a BlueXP classification na nuvem"](#) e para usar o serviço dentro da BlueXP ransomware protection, consulte ["Escaneie informações de identificação pessoal com a BlueXP classification"](#) .

13 de maio de 2025

Relatório de ambientes de trabalho não suportados na BlueXP ransomware protection

Durante o fluxo de trabalho de descoberta, a BlueXP ransomware protection relata mais detalhes quando você passa o mouse sobre Cargas de trabalho suportadas ou não suportadas. Isso ajudará você a entender por que algumas de suas cargas de trabalho não são descobertas pelo serviço de BlueXP ransomware protection .

Há muitos motivos pelos quais o serviço não oferece suporte a um ambiente de trabalho, por exemplo, a versão do ONTAP no seu ambiente de trabalho pode ser inferior à versão necessária. Quando você passa o mouse sobre um ambiente de trabalho sem suporte, uma dica de ferramenta exibe o motivo.

Você pode visualizar os ambientes de trabalho sem suporte durante a descoberta inicial, onde também pode baixar os resultados. Você também pode visualizar os resultados da descoberta na opção **Descoberta de carga de trabalho** na página Configurações.

Para mais detalhes, consulte ["Descubra cargas de trabalho na BlueXP ransomware protection"](#) .

29 de abril de 2025

Suporte para Amazon FSx for NetApp ONTAP

Esta versão oferece suporte ao Amazon FSx for NetApp ONTAP. Este recurso ajuda você a proteger suas cargas de trabalho FSx para ONTAP com a BlueXP ransomware protection.

O FSx for ONTAP é um serviço totalmente gerenciado que fornece o poder do armazenamento NetApp ONTAP na nuvem. Ele fornece os mesmos recursos, desempenho e capacidades administrativas que você usa no local, com a agilidade e escalabilidade de um serviço nativo da AWS.

As seguintes alterações foram feitas no fluxo de trabalho de BlueXP ransomware protection :

- O Discovery inclui cargas de trabalho no FSx para ambientes de trabalho ONTAP 9.15.
- A guia Proteção mostra cargas de trabalho no FSx para ambientes ONTAP . Neste ambiente, você deve executar operações de backup usando o serviço de backup FSx for ONTAP . Você pode restaurar essas cargas de trabalho usando instantâneos de BlueXP ransomware protection .



Políticas de backup para uma carga de trabalho em execução no FSx para ONTAP não podem ser definidas no BlueXP. Todas as políticas de backup existentes definidas no Amazon FSx for NetApp ONTAP permanecem inalteradas.

- Incidentes de alerta mostram o novo ambiente de trabalho do FSx para ONTAP .

Para mais detalhes, consulte ["Saiba mais sobre a BlueXP ransomware protection e ambientes de trabalho"](#) .

Para obter informações sobre as opções suportadas, consulte o ["Limitações da BlueXP ransomware protection"](#) .

Função de acesso BlueXP necessária

Agora você precisa de uma das seguintes funções de acesso para visualizar, descobrir ou gerenciar a BlueXP ransomware protection: administrador da organização, administrador de pasta ou projeto, administrador de proteção contra ransomware ou visualizador de proteção contra ransomware.

["Saiba mais sobre as funções de acesso do BlueXP para todos os serviços"](#) .

14 de abril de 2025

Relatórios de exercícios de prontidão

Com esta versão, você pode revisar relatórios de exercícios de prontidão para ataques de ransomware. Um exercício de prontidão permite simular um ataque de ransomware em uma carga de trabalho de amostra recém-criada. Em seguida, investigue o ataque simulado e recupere a carga de trabalho de amostra. Esse recurso ajuda você a saber se está preparado no caso de um ataque real de ransomware, testando processos de notificação de alerta, resposta e recuperação.

Para mais detalhes, consulte ["Realizar um exercício de preparação para ataques de ransomware"](#) .

Novas funções e permissões de controle de acesso baseadas em funções

Anteriormente, você podia atribuir funções e permissões aos usuários com base em suas responsabilidades, o que ajuda a gerenciar o acesso dos usuários à BlueXP ransomware protection. Com esta versão, há duas novas funções específicas para a BlueXP ransomware protection com permissões atualizadas. As novas funções são:

- Administrador de proteção contra ransomware
- Visualizador de proteção contra ransomware

Para obter detalhes sobre permissões, consulte ["Acesso baseado em função de BlueXP ransomware protection aos recursos"](#) .

Melhorias de pagamento

Esta versão inclui diversas melhorias no processo de pagamento.

Para mais detalhes, consulte ["Configurar opções de licenciamento e pagamento"](#) .

10 de março de 2025

Simule um ataque e responda

Com esta versão, simule um ataque de ransomware para testar sua resposta a um alerta de ransomware. Esse recurso ajuda você a saber se está preparado no caso de um ataque real de ransomware, testando processos de notificação de alerta, resposta e recuperação.

Para mais detalhes, consulte ["Realizar um exercício de preparação para ataques de ransomware"](#) .

Melhorias no processo de descoberta

Esta versão inclui melhorias nos processos seletivos de descoberta e redescoberta:

- Com esta versão, você pode descobrir cargas de trabalho recém-criadas que foram adicionadas aos ambientes de trabalho selecionados anteriormente.
- Você também pode selecionar *novos* ambientes de trabalho nesta versão. Esse recurso ajuda a proteger novas cargas de trabalho adicionadas ao seu ambiente.
- Você pode executar esses processos de descoberta durante o processo de descoberta inicialmente ou na opção Configurações.

Para mais detalhes, consulte ["Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente"](#) e ["Configurar recursos com a opção Configurações"](#) .

Alertas gerados quando alta criptografia é detectada

Com esta versão, você pode visualizar alertas quando alta criptografia for detectada em suas cargas de trabalho, mesmo sem grandes alterações na extensão do arquivo. Este recurso, que usa a IA de proteção autônoma contra ransomware (ARP) do ONTAP , ajuda você a identificar cargas de trabalho que correm risco de ataques de ransomware. Use este recurso e baixe a lista completa de arquivos afetados com ou sem alterações de extensão.

Para mais detalhes, consulte ["Responder a um alerta de ransomware detectado"](#) .

16 de dezembro de 2024

Detecte comportamento anômalo do usuário usando o Data Infrastructure Insights Storage Workload Security

Com esta versão, você pode usar o Data Infrastructure Insights Storage Workload Security para detectar comportamento anômalo do usuário em suas cargas de trabalho de armazenamento. Este recurso ajuda você a identificar potenciais ameaças à segurança e bloquear usuários potencialmente mal-intencionados para proteger seus dados.

Para mais detalhes, consulte ["Responder a um alerta de ransomware detectado"](#) .

Antes de usar o Data Infrastructure Insights Storage Workload Security para detectar comportamento anômalo do usuário, você precisa configurar a opção usando a opção **Configurações** de BlueXP ransomware protection .

Consulte ["Configurar as definições de BlueXP ransomware protection"](#) .

Selecione cargas de trabalho para descobrir e proteger

Com esta versão, agora você pode fazer o seguinte:

- Em cada Conector, selecione os ambientes de trabalho onde você deseja descobrir cargas de trabalho. Você pode se beneficiar desse recurso se quiser proteger cargas de trabalho específicas em seu ambiente e não outras.
- Durante a descoberta de carga de trabalho, você pode habilitar a descoberta automática de cargas de trabalho por Conector. Este recurso permite que você selecione as cargas de trabalho que deseja proteger.
- Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente.

Consulte ["Descubra cargas de trabalho"](#) .

7 de novembro de 2024

Habilitar classificação de dados e busca de informações de identificação pessoal (PII)

Com esta versão, você pode habilitar a BlueXP classification, um componente principal da família BlueXP , para escanear e classificar dados em suas cargas de trabalho de compartilhamento de arquivos. Classificar dados ajuda você a identificar se seus dados incluem informações pessoais ou privadas, o que pode aumentar os riscos de segurança. Esse processo também afeta a importância da carga de trabalho e ajuda a garantir que você esteja protegendo as cargas de trabalho com o nível certo de proteção.

A verificação de dados PII na BlueXP ransomware protection geralmente está disponível para clientes que implantaram a BlueXP classification. A BlueXP classification está disponível como parte da plataforma BlueXP sem custo adicional e pode ser implantada no local ou na nuvem do cliente.

Consulte ["Configurar as definições de BlueXP ransomware protection"](#) .

Para iniciar a verificação, na página Proteção, clique em **Identificar exposição** na coluna Exposição de privacidade.

["Escaneie dados pessoais confidenciais com a BlueXP classification"](#) .

Integração do SIEM com o Microsoft Sentinel

Agora você pode enviar dados ao seu sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças usando o Microsoft Sentinel. Anteriormente, você podia selecionar o AWS Security Hub ou o Splunk Cloud como seu SIEM.

["Saiba mais sobre como configurar as configurações de BlueXP ransomware protection"](#) .

Teste grátis agora por 30 dias

Com este lançamento, novas implantações da BlueXP ransomware protection agora têm 30 dias de teste gratuito. Anteriormente, a BlueXP ransomware protection oferecia 90 dias de teste gratuito. Se você já estiver no teste gratuito de 90 dias, a oferta continuará por 90 dias.

Restaurar a carga de trabalho do aplicativo no nível de arquivo para Podman

Antes de restaurar uma carga de trabalho de aplicativo no nível de arquivo, agora você pode visualizar uma lista de arquivos que podem ter sido afetados por um ataque e identificar aqueles que deseja restaurar. Anteriormente, se os Conectores BlueXP em uma organização (anteriormente uma conta) estivessem usando

o Podman, esse recurso era desabilitado. Agora está habilitado para o Podman. Você pode deixar que a BlueXP ransomware protection escolha os arquivos a serem restaurados, pode enviar um arquivo CSV que lista todos os arquivos afetados por um alerta ou pode identificar manualmente quais arquivos deseja restaurar.

["Saiba mais sobre como se recuperar de um ataque de ransomware"](#) .

30 de setembro de 2024

Agrupamento personalizado de cargas de trabalho de compartilhamento de arquivos

Com esta versão, agora você pode agrupar compartilhamentos de arquivos para facilitar a proteção do seu patrimônio de dados. O serviço pode proteger todos os volumes de um grupo ao mesmo tempo. Anteriormente, você precisava proteger cada volume separadamente.

["Saiba mais sobre o agrupamento de cargas de trabalho de compartilhamento de arquivos em estratégias de proteção contra ransomware"](#) .

2 de setembro de 2024

Avaliação de risco de segurança do Digital Advisor

A BlueXP ransomware protection agora coleta informações sobre riscos de segurança altos e críticos relacionados a um cluster do NetApp Digital Advisor. Se algum risco for encontrado, a BlueXP ransomware protection fornece uma recomendação no painel **Ações recomendadas** do Painel: "Corrigir uma vulnerabilidade de segurança conhecida no cluster <nome>". Na recomendação no Painel, clicar em **Revisar e corrigir** sugere revisar o Digital Advisor e um artigo sobre Vulnerabilidade e Exposição Comuns (CVE) para resolver o risco de segurança. Se houver vários riscos de segurança, revise as informações no Digital Advisor.

Consulte ["Documentação do Digital Advisor"](#) .

Fazer backup no Google Cloud Platform

Com esta versão, você pode definir um destino de backup para um bucket do Google Cloud Platform. Anteriormente, você só podia adicionar destinos de backup ao NetApp StorageGRID, Amazon Web Services e Microsoft Azure.

["Saiba mais sobre como configurar as configurações de BlueXP ransomware protection"](#) .

Suporte para Google Cloud Platform

O serviço agora oferece suporte ao Cloud Volumes ONTAP para Google Cloud Platform para proteção de armazenamento. Anteriormente, o serviço suportava apenas o Cloud Volumes ONTAP para Amazon Web Services e Microsoft Azure, além de NAS local.

["Saiba mais sobre a BlueXP ransomware protection e fontes de dados suportadas, destinos de backup e ambientes de trabalho"](#) .

Controle de acesso baseado em função

Agora você pode limitar o acesso a atividades específicas com o controle de acesso baseado em função (RBAC). A BlueXP ransomware protection usa duas funções do BlueXP: Administrador de conta do BlueXP e Administrador sem conta (Visualizador).

Para obter detalhes sobre as ações que cada função pode executar, consulte ["Privilégios de controle de acesso baseados em funções"](#) .

5 de agosto de 2024

Detecção de ameaças com Splunk Cloud

Você pode enviar dados automaticamente para seu sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças. Com versões anteriores, você podia selecionar apenas o AWS Security Hub como seu SIEM. Com esta versão, você pode selecionar o AWS Security Hub ou o Splunk Cloud como seu SIEM.

["Saiba mais sobre como configurar as configurações de BlueXP ransomware protection"](#) .

1 de julho de 2024

Traga sua própria licença (BYOL)

Com esta versão, você pode usar uma licença BYOL, que é um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas da NetApp .

["Saiba mais sobre a configuração do licenciamento"](#) .

Restaurar a carga de trabalho do aplicativo no nível do arquivo

Antes de restaurar uma carga de trabalho de aplicativo no nível de arquivo, agora você pode visualizar uma lista de arquivos que podem ter sido afetados por um ataque e identificar aqueles que deseja restaurar. Você pode deixar que a BlueXP ransomware protection escolha os arquivos a serem restaurados, pode enviar um arquivo CSV que lista todos os arquivos afetados por um alerta ou pode identificar manualmente quais arquivos deseja restaurar.



Com esta versão, se todos os conectores BlueXP em uma conta não estiverem usando o Podman, o recurso de restauração de arquivo único será habilitado. Caso contrário, ele será desabilitado para essa conta.

["Saiba mais sobre como se recuperar de um ataque de ransomware"](#) .

Baixe uma lista de arquivos afetados

Antes de restaurar uma carga de trabalho de aplicativo no nível de arquivo, agora você pode acessar a página Alertas para baixar uma lista de arquivos afetados em um arquivo CSV e, em seguida, usar a página Recuperação para carregar o arquivo CSV.

["Saiba mais sobre como baixar arquivos afetados antes de restaurar um aplicativo"](#) .

Excluir plano de proteção

Com esta versão, agora você pode excluir uma estratégia de proteção contra ransomware.

["Saiba mais sobre como proteger cargas de trabalho e gerenciar estratégias de proteção contra ransomware"](#) .

10 de junho de 2024

Bloqueio de cópia de instantâneo no armazenamento primário

Habilite isso para bloquear as cópias de instantâneo no armazenamento primário para que elas não possam ser modificadas ou excluídas por um determinado período de tempo, mesmo que um ataque de ransomware chegue ao destino do armazenamento de backup.

["Saiba mais sobre como proteger cargas de trabalho e habilitar o bloqueio de backup em uma estratégia de proteção contra ransomware"](#) .

Suporte para Cloud Volumes ONTAP para Microsoft Azure

Esta versão oferece suporte ao Cloud Volumes ONTAP para Microsoft Azure como um sistema, além do Cloud Volumes ONTAP para AWS e do ONTAP NAS local.

["Início rápido para Cloud Volumes ONTAP no Azure"](#)

["Saiba mais sobre a BlueXP ransomware protection"](#) .

Microsoft Azure adicionado como destino de backup

Agora você pode adicionar o Microsoft Azure como destino de backup junto com o AWS e o NetApp StorageGRID.

["Saiba mais sobre como configurar as definições de proteção"](#) .

14 de maio de 2024

Atualizações de licenciamento

Você pode se inscrever para um teste gratuito de 90 dias. Em breve, você poderá comprar uma assinatura paga conforme o uso no Amazon Web Services Marketplace ou trazer sua própria licença do NetApp .

["Saiba mais sobre a configuração do licenciamento"](#) .

Protocolo CIFS

O serviço agora oferece suporte a ONTAP local e Cloud Volumes ONTAP em sistemas AWS usando protocolos NFS e CIFS. A versão anterior suportava apenas o protocolo NFS.

Detalhes da carga de trabalho

Esta versão agora fornece mais detalhes nas informações de carga de trabalho da Proteção e outras páginas para melhor avaliação da proteção da carga de trabalho. Nos detalhes da carga de trabalho, você pode revisar a política atribuída atualmente e revisar os destinos de backup configurados.

["Saiba mais sobre como visualizar detalhes da carga de trabalho nas páginas de proteção"](#) .

Proteção e recuperação consistentes com aplicativos e VMs

Agora você pode executar proteção consistente com aplicativos com o NetApp SnapCenter Software e proteção consistente com VMs com o SnapCenter Plug-in for VMware vSphere, obtendo um estado quiescente e consistente para evitar possível perda de dados posteriormente, caso seja necessária

recuperação. Se a recuperação for necessária, você pode restaurar o aplicativo ou a VM para qualquer um dos estados disponíveis anteriormente.

["Saiba mais sobre como proteger cargas de trabalho"](#) .

Estratégias de proteção contra ransomware

Se não houver políticas de snapshot ou backup na carga de trabalho, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas neste serviço:

- Política de instantâneo
- Política de backup
- Política de detecção

["Saiba mais sobre como proteger cargas de trabalho"](#) .

Detecção de ameaças

Agora é possível habilitar a detecção de ameaças usando um sistema de gerenciamento de eventos e segurança (SIEM) de terceiros. O Painel agora mostra uma nova recomendação para "Ativar detecção de ameaças", que pode ser configurada na página Configurações.

["Saiba mais sobre como configurar opções de configurações"](#) .

Descartar alertas falsos positivos

Na aba Alertas, agora você pode descartar falsos positivos ou decidir recuperar seus dados imediatamente.

["Saiba mais sobre como responder a um alerta de ransomware"](#) .

Status de detecção

Novos status de detecção aparecem na página Proteção, mostrando o status da detecção de ransomware aplicada à carga de trabalho.

["Saiba mais sobre como proteger cargas de trabalho e visualizar status de proteção"](#) .


Baixar arquivos CSV

Você pode baixar arquivos CSV* nas páginas Proteção, Alertas e Recuperação.

["Saiba mais sobre como baixar arquivos CSV do Painel e de outras páginas"](#) .

Link da documentação

O link para visualizar a documentação agora está incluído na interface do usuário. Você pode acessar esta

documentação na vertical do Painel **Ações***  **opção. Selecione *Novidades** para ver detalhes nas Notas de versão ou **Documentação** para ver a página inicial da documentação de BlueXP ransomware protection .

BlueXP backup and recovery

O serviço de BlueXP backup and recovery não precisa mais estar habilitado no sistema. Ver ["pré-requisitos"](#) .
O serviço de BlueXP ransomware protection ajuda a configurar um destino de backup por meio da opção Configurações. Ver ["Configurar definições"](#) .

Opção de configurações

Agora você pode configurar destinos de backup nas configurações de BlueXP ransomware protection .

["Saiba mais sobre como configurar opções de configurações"](#) .

5 de março de 2024

Gestão de políticas de proteção

Além de usar políticas predefinidas, agora você pode criar políticas. ["Saiba mais sobre o gerenciamento de políticas"](#) .

Imutabilidade no armazenamento secundário (DataLock)

Agora você pode tornar o backup imutável no armazenamento secundário usando a tecnologia NetApp DataLock no armazenamento de objetos. ["Saiba mais sobre como criar políticas de proteção"](#) .

Backup automático para NetApp StorageGRID

Além de usar a AWS, agora você pode escolher o StorageGRID como seu destino de backup. ["Saiba mais sobre como configurar destinos de backup"](#) .

Recursos adicionais para investigar ataques potenciais

Agora você pode visualizar mais detalhes forenses para investigar o possível ataque detectado. ["Saiba mais sobre como responder a um alerta de ransomware detectado"](#) .

Processo de recuperação

O processo de recuperação foi aprimorado. Agora, você pode recuperar volume por volume ou todos os volumes de uma carga de trabalho. ["Saiba mais sobre como se recuperar de um ataque de ransomware \(após os incidentes terem sido neutralizados\)"](#) .

["Saiba mais sobre a BlueXP ransomware protection"](#) .

6 de outubro de 2023

O serviço de BlueXP ransomware protection é uma solução SaaS para proteger dados, detectar ataques potenciais e recuperar dados de um ataque de ransomware.

Na versão de pré-visualização, o serviço protege cargas de trabalho baseadas em aplicativos do Oracle, datastores de máquinas virtuais e compartilhamentos de arquivos em armazenamento NAS local, bem como Cloud Volumes ONTAP na AWS (usando o protocolo NFS) em organizações BlueXP individualmente e faz backup dos dados para o armazenamento em nuvem da Amazon Web Services.

O serviço de BlueXP ransomware protection oferece uso completo de diversas tecnologias da NetApp para que seu administrador de segurança de dados ou engenheiro de operações de segurança possa atingir os

seguintes objetivos:

- Visualize a proteção contra ransomware em todas as suas cargas de trabalho rapidamente.
- Obtenha insights sobre recomendações de proteção contra ransomware
- Melhore a postura de proteção com base nas recomendações de BlueXP ransomware protection .
- Atribua políticas de proteção contra ransomware para proteger suas principais cargas de trabalho e dados de alto risco contra ataques de ransomware.
- Monitore a saúde de suas cargas de trabalho contra ataques de ransomware em busca de anomalias nos dados.
- Avalie rapidamente o impacto de incidentes de ransomware em sua carga de trabalho.
- Recupere-se de incidentes de ransomware de forma inteligente restaurando dados e garantindo que não ocorram reinfecções a partir de dados armazenados.

["Saiba mais sobre a BlueXP ransomware protection"](#) .

Limitações conhecidas do NetApp Ransomware Resilience

Limitações conhecidas identificam plataformas, dispositivos ou funções que não são suportados por esta versão do produto ou que não interoperam corretamente com ele. Revise essas limitações cuidadosamente.

Problema com a opção de reinicialização do exercício de prontidão

Se você selecionar um volume ONTAP 9.11.1 para o exercício de prontidão para ataque de ransomware, o Ransomware Resilience enviará um alerta. Se você recuperar os dados usando a opção "clone-to-volume" e redefinir o drill, a operação de redefinição falhará.

Limitações do Amazon FSx for NetApp ONTAP

O sistema Amazon FSx for NetApp ONTAP é compatível com o Ransomware Resilience. As seguintes limitações se aplicam ao Amazon FSx para ONTAP:

- As políticas de backup não são compatíveis com Amazon FSx for ONTAP. Nesse ambiente, você deve executar operações de backup usando o Amazon FSx for backups. Você pode restaurar essas cargas de trabalho usando Ransomware Resilience.
- As operações de restauração são executadas somente a partir de instantâneos.

Limitações do Azure NetApp Files

Azure NetApp Files é compatível com Ransomware Resilience. As seguintes limitações se aplicam ao Azure NetApp Files:

- Estratégias de proteção contra ransomware com políticas de backup não são compatíveis com o Azure NetApp Files. Em vez disso, você pode usar Azure NetApp Files backup.
- Estratégias de proteção contra ransomware com replicação não são suportadas para Azure NetApp Files.
- Ao selecionar uma estratégia de proteção, certifique-se de que sua programação de snapshots seja compatível com o Azure NetApp Files. A programação de snapshots mais frequente disponível no Azure NetApp Files é a cada hora.

Começar

Saiba mais sobre a NetApp Ransomware Resilience

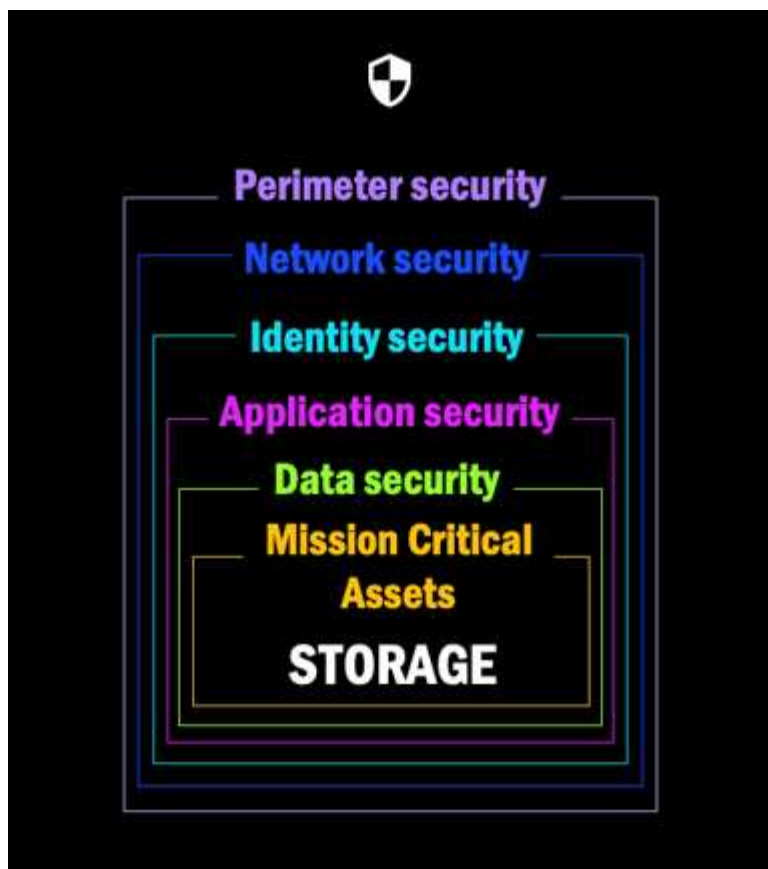
Ataques de ransomware podem bloquear o acesso aos seus dados e os invasores podem pedir resgate em troca da liberação de dados ou descriptografia. De acordo com o IDC, não é incomum que vítimas de ransomware sofram múltiplos ataques de ransomware. O ataque pode interromper o acesso aos seus dados por um dia ou várias semanas.

O NetApp Ransomware Resilience protege seus dados contra ataques de ransomware. Na Resiliência contra Ransomware, a proteção está disponível para cargas de trabalho baseadas em aplicativos do Oracle, datastores de máquinas virtuais e compartilhamentos de arquivos em armazenamento NAS local (usando os protocolos NFS e CIFS) e armazenamento SAN (FC, iSCSI e NVMe), bem como Cloud Volumes ONTAP para Amazon Web Services, Cloud Volumes ONTAP para Google Cloud, Cloud Volumes ONTAP para Microsoft Azure e Amazon FSx for NetApp ONTAP, tudo através do NetApp Console. Você pode fazer backup de dados no Amazon Web Services, Google Cloud, armazenamento em nuvem do Microsoft Azure e NetApp StorageGRID.

Resiliência do Ransomware na camada de dados

Sua postura de segurança normalmente abrange várias camadas de defesa para proteger contra uma série de ameaças cibernéticas.

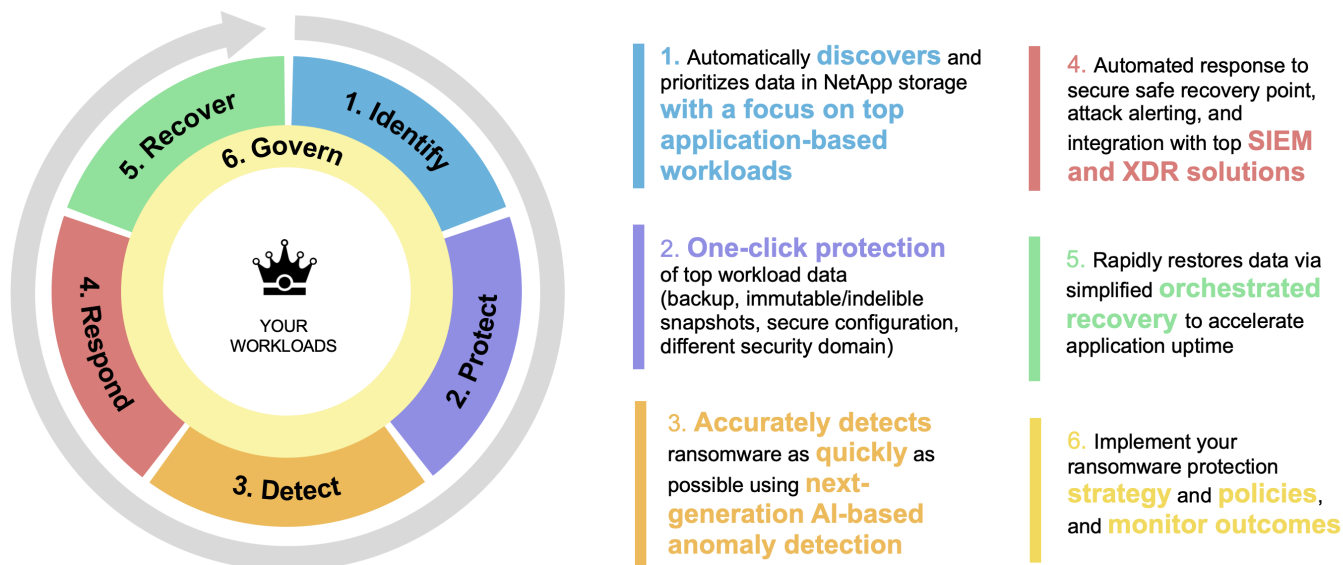
- **Camada mais externa:** Esta é sua primeira linha de defesa usando firewalls, sistemas de detecção de intrusão e redes privadas virtuais para proteger os limites da rede.
- **Segurança de rede:** Esta camada se baseia na base com segmentação de rede, monitoramento de tráfego e criptografia.
- **Segurança de identidade:** usa métodos de autenticação, controles de acesso e gerenciamento de identidade para garantir que somente usuários autorizados possam acessar recursos confidenciais.
- **Segurança de aplicativos:** protege aplicativos de software usando práticas de codificação seguras, testes de segurança e autoproteção de aplicativos em tempo de execução.
- **Segurança de dados:** Proteja seus dados com estratégias de proteção de dados, backups e recuperação. A resiliência do ransomware opera nessa camada.



O que você pode fazer com a resiliência do Ransomware

O Ransomware Resilience oferece uso total de diversas tecnologias da NetApp para que seu administrador de armazenamento, administrador de segurança de dados ou engenheiro de operações de segurança possa atingir os seguintes objetivos:

- **Identificar** todas as cargas de trabalho baseadas em aplicativos, compartilhamento de arquivos ou gerenciadas pelo VMware em sistemas NetApp NAS (NFS ou CIFS) e SAN (FC, iSCSI e NVMe) locais, no NetApp Console, projetos e agentes do Console. O Ransomware Resilience categoriza a prioridade dos dados e fornece recomendações para melhorias na resiliência do ransomware.
- **Proteja** suas cargas de trabalho habilitando backups, cópias de snapshot e estratégias de proteção contra ransomware em seus dados.
- **Detecte** anomalias que podem ser ataques de ransomware. Nota de rodapé: [Embora seja possível que um ataque passe despercebido, nossa pesquisa indica que a tecnologia NetApp resultou em um alto grau de detecção para certos ataques de ransomware baseados em criptografia de arquivos.]
- **Responda** a possíveis ataques de ransomware iniciando automaticamente um instantâneo em um determinado momento, que é bloqueado para que a cópia não possa ser excluída acidentalmente ou maliciosamente. Seus dados de backup permanecerão imutáveis e protegidos de ponta a ponta contra ataques de ransomware, tanto na origem quanto no destino.
- **Recupere** suas cargas de trabalho que ajudam a acelerar o tempo de atividade da carga de trabalho orquestrando diversas tecnologias NetApp. Você pode escolher recuperar volumes específicos. O Ransomware Resilience fornece recomendações sobre as melhores opções.
- **Governar**: implemente sua estratégia de proteção contra ransomware e monitore os resultados.



Benefícios do uso do Ransomware Resilience

O Ransomware Resilience oferece os seguintes benefícios:

- Descobre cargas de trabalho e seus agendamentos de backup e snapshots existentes e classifica sua importância relativa.
- Avalia sua postura de proteção contra ransomware e a exibe em um painel fácil de entender.
- Fornece recomendações sobre as próximas etapas com base na análise de postura de descoberta e proteção.
- Aplica recomendações de proteção de dados orientadas por IA/ML com acesso em um clique.
- Protege dados em cargas de trabalho baseadas em aplicativos, como Oracle, datastores VMware e compartilhamentos de arquivos.
- Detecta ataques de ransomware em dados em tempo real no armazenamento primário usando tecnologia de IA.
- Inicia ações automatizadas em resposta a ataques potenciais detectados, criando cópias instantâneas e iniciando alertas sobre atividades anormais.
- Aplica recuperação selecionada para atender às políticas de RPO. O Ransomware Resilience orquestra a recuperação de incidentes de ransomware usando vários serviços de recuperação da NetApp, incluindo NetApp Backup and Recovery (antigo Cloud Backup) e SnapCenter.
- Usa controle de acesso baseado em função (RBAC) para governar o acesso a recursos e operações.

Custo

Você pode experimentar o Ransomware Resilience com um teste gratuito de 30 dias. A NetApp não cobra pelo uso da versão de teste do Ransomware Resilience.

Se você tiver o Backup and Recovery e o Ransomware Resilience, quaisquer dados comuns protegidos por ambos os produtos serão cobrados somente pelo Ransomware Resilience.

Após adquirir uma licença ou assinatura do PayGo, qualquer carga de trabalho que tenha uma política de detecção de ransomware (Autonomous Ransomware Protection) habilitada (descoberta ou definida pelo Ransomware Resilience) e pelo menos uma política de snapshot ou backup, o Ransomware Resilience a

classifica como "Protegida" e isso é contabilizado na capacidade adquirida ou na assinatura do PayGo. Se uma carga de trabalho for descoberta sem uma política de detecção, mesmo que tenha políticas de backup ou snapshot, ela será classificada como "Em risco" e *não* será contabilizada na capacidade adquirida.

As cargas de trabalho protegidas são contabilizadas na capacidade adquirida ou na assinatura após o término do período de teste de 90 dias. A resiliência contra ransomware é cobrada por GB para os dados associados às cargas de trabalho protegidas antes das eficiências.

Licenciamento

Com o Ransomware Resilience, você pode usar diferentes planos de licenciamento, incluindo um teste gratuito, uma assinatura paga conforme o uso ou trazer sua própria licença.

O Ransomware Resilience requer uma licença NetApp ONTAP One.

A licença do Ransomware Resilience não inclui produtos NetApp adicionais. O Ransomware Resilience pode usar o Backup and Recovery mesmo que você não tenha uma licença para ele.

Para detectar comportamento anômalo do usuário, o Ransomware Resilience usa o NetApp Autonomous Ransomware Protection, um modelo de aprendizado de máquina (ML) dentro do ONTAP que detecta atividades de arquivos maliciosos. Este modelo está incluído na licença Ransomware Resilience.

Para obter detalhes, consulte ["Configurar licenciamento"](#).

NetApp Console

O Ransomware Resilience pode ser acessado por meio do NetApp Console.

O NetApp Console fornece gerenciamento centralizado de serviços de armazenamento e dados da NetApp em ambientes locais e na nuvem em nível empresarial. O Console é necessário para acessar e usar os serviços de dados do NetApp. Como uma interface de gerenciamento, ele permite que você gerencie muitos recursos de armazenamento a partir de uma única interface. Os administradores do console podem controlar o acesso ao armazenamento e aos serviços de todos os sistemas da empresa.

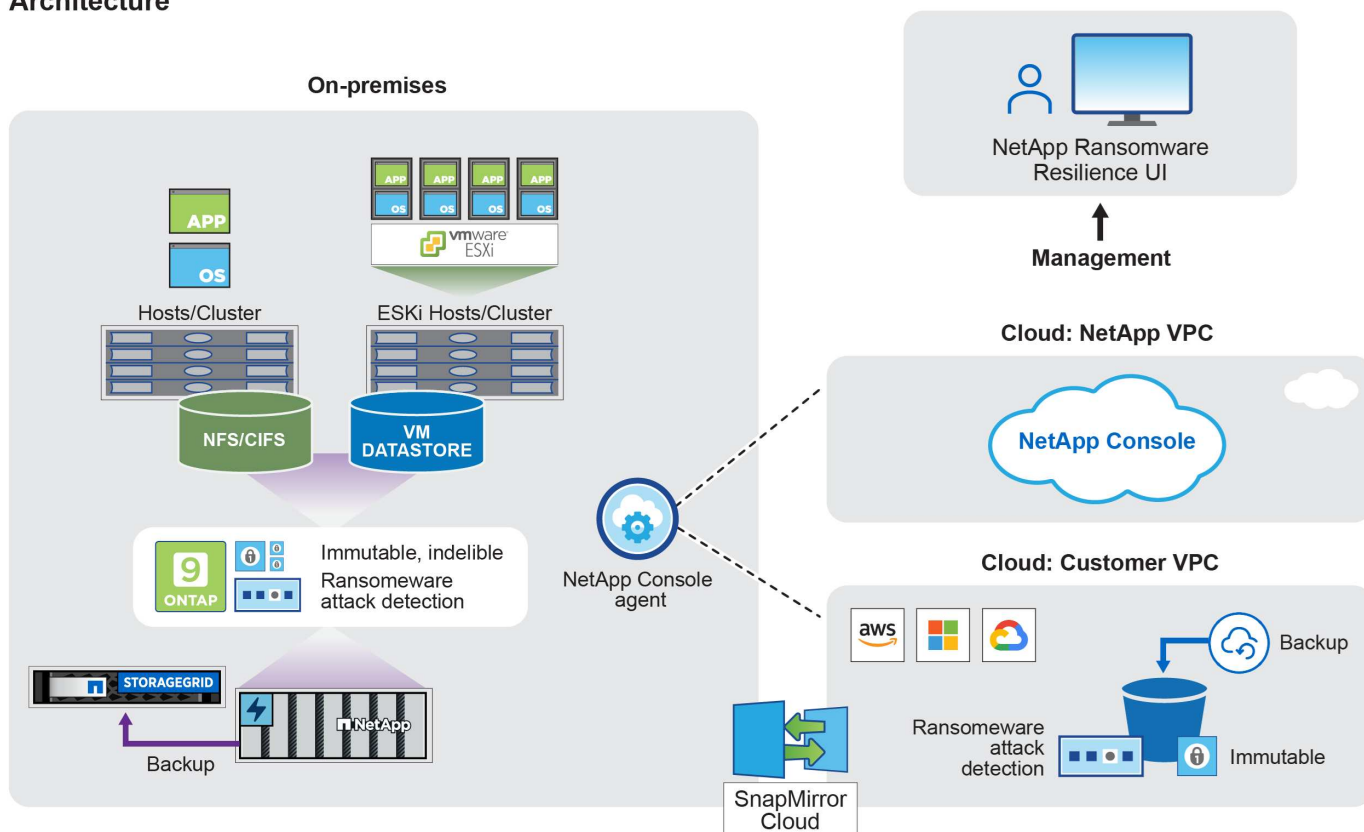
Você não precisa de licença ou assinatura para começar a usar o NetApp Console e só incorre em cobranças quando implanta agentes do Console em sua nuvem para garantir a conectividade com seus sistemas de armazenamento ou NetApp data services. No entanto, alguns NetApp data services acessíveis pelo Console são licenciados ou baseados em assinatura.

Saiba mais sobre o ["NetApp Console"](#).

Como funciona a resiliência do ransomware

O Ransomware Resilience usa o NetApp Backup and Recovery para descobrir e definir políticas de backup e snapshot para cargas de trabalho de compartilhamento de arquivos, e o SnapCenter ou SnapCenter for VMware para descobrir e definir políticas de backup e snapshot para cargas de trabalho de aplicativos e VMs. Além disso, o Ransomware Resilience usa o Backup and Recovery e o SnapCenter / SnapCenter for VMware para executar uma recuperação consistente de arquivos e cargas de trabalho.

Architecture



Recurso	Descrição
IDENTIFICAR	<ul style="list-style-type: none"> Encontra todos os dados NAS (protocolos NFS e CIFS) locais do cliente, SAN (FC, iSCSI e NVMe) e Cloud Volumes ONTAP conectados ao Console. Identifica dados de clientes das APIs de serviço ONTAP e SnapCenter e os associa a cargas de trabalho. Saiba mais sobre "ONTAP" e "Software SnapCenter" . Descobre o nível de proteção atual de cada volume de cópias de snapshots e políticas de backup do NetApp , bem como quaisquer recursos de detecção on-box. A Resiliência contra Ransomware associa essa postura de proteção às cargas de trabalho usando Backup e Recuperação, serviços ONTAP e tecnologias NetApp , como Proteção Autônoma contra Ransomware (ARP ou ARP/AI, dependendo da sua versão do ONTAP), FPolicy, políticas de backup e políticas de snapshot. Saiba mais sobre "Proteção Autônoma contra Ransomware" , "NetApp Backup and Recovery" , e "Política ONTAP" . Atribui uma prioridade empresarial a cada carga de trabalho com base em níveis de proteção descobertos automaticamente e recomenda políticas de proteção para cargas de trabalho com base em sua prioridade empresarial. A prioridade da carga de trabalho é baseada nas frequências de snapshot já aplicadas a cada volume associado à carga de trabalho.
PROTEGER	<ul style="list-style-type: none"> Monitora ativamente as cargas de trabalho e orquestra o uso de APIs de backup e recuperação, SnapCenter e ONTAP aplicando políticas a cada uma das cargas de trabalho identificadas.

Recurso	Descrição
DETECTAR	<ul style="list-style-type: none"> • Detecta ataques potenciais com um modelo integrado de aprendizado de máquina (ML) que detecta criptografia e atividades potencialmente anômalas. • Fornece detecção de camada dupla que começa com a detecção de potenciais ataques de ransomware no armazenamento primário e responde a atividades anormais fazendo cópias instantâneas automatizadas adicionais para criar os pontos de restauração de dados mais próximos. A resiliência ao ransomware oferece a capacidade de investigar mais profundamente para identificar ataques potenciais com maior precisão, sem afetar o desempenho das cargas de trabalho primárias. • Determina os arquivos suspeitos específicos e mapeia os ataques às cargas de trabalho associadas, usando as tecnologias ONTAP, Autonomous Ransomware Protection (ARP ou ARP/AI, dependendo da sua versão do ONTAP) e FPolicy.
RESPONDER	<ul style="list-style-type: none"> • Exibe dados relevantes, como atividade de arquivo, atividade do usuário e entropia, para ajudar você a concluir análises forenses sobre o ataque. • Inicia cópias rápidas de snapshot usando tecnologias e produtos da NetApp , como ONTAP, Autonomous Ransomware Protection (ARP ou ARP/AI, dependendo da versão do ONTAP) e FPolicy.
RECUPERAR	<ul style="list-style-type: none"> • Determina o melhor snapshot ou backup e recomenda o melhor ponto de recuperação real (RPA) usando Backup e Recuperação, ONTAP, Proteção Autônoma contra Ransomware (ARP ou ARP/AI, dependendo da sua versão do ONTAP) e tecnologias e serviços FPolicy. • Orquestra a recuperação de cargas de trabalho, incluindo VMs, compartilhamentos de arquivos, armazenamento em bloco e bancos de dados com consistência de aplicativos.
GOVERNAR	<ul style="list-style-type: none"> • Atribui as estratégias de proteção contra ransomware • Ajuda você a monitorar os resultados.

Destinos de backup, sistemas e fontes de dados de carga de trabalho suportados

O Ransomware Resilience oferece suporte aos seguintes destinos de backup, sistemas e fontes de dados:

Destinos de backup suportados

- Amazon Web Services (AWS) S3
- Plataforma Google Cloud
- Blob do Microsoft Azure
- NetApp StorageGRID

Sistemas suportados

Ambiente	Protocolo	Versões suportadas
Amazon FSx for NetApp ONTAP*	CIFS, NFS e SAN	N / D

Ambiente	Protocolo	Versões suportadas
Azure NetApp Files	CIFS e NFS	N / D
Cloud Volumes ONTAP para AWS	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
Cloud Volumes ONTAP para Google Cloud Platform	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
Cloud Volumes ONTAP para Microsoft Azure	CIFS e NFS	9.12.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
ONTAP (local)	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior

{asterisco} O Amazon FSx for NetApp ONTAP usa a Proteção Autônoma contra Ransomware (ARP) e não o ARP/AI. Para obter mais informações sobre a diferença, consulte ["ARP/AI"](#).



Para usar ARP/AI no ONTAP, é necessário ter o ONTAP 9.16 ou superior. + O ONTAP não oferece suporte à proteção contra ransomware para volumes FabricPool FlexCache, FlexGroup, grupos de consistência, pontos de montagem, caminhos de montagem, volumes offline e volumes de proteção de dados (DP). Certifique-se de revisar ["Configurações suportadas e não suportadas no ONTAP"](#).

Fontes de dados de carga de trabalho suportadas

O Ransomware Resilience protege as seguintes cargas de trabalho baseadas em aplicativos em volumes de dados primários:

- Armazenamento em bloco
- Bancos de dados:
 - Servidor Microsoft SQL
 - Oráculo
 - PostgreSQL
- Compartilhamentos de arquivos NetApp
- Armazenamentos de dados VMware

Se você estiver usando o SnapCenter ou o SnapCenter para VMware, todas as cargas de trabalho compatíveis com esses produtos também serão identificadas no Ransomware Resilience. O Ransomware Resilience pode proteger e recuperar esses dados de maneira consistente com a carga de trabalho.

Termos-chave

Você pode se beneficiar ao entender alguma terminologia relacionada à proteção contra ransomware.

- **Proteção:** Proteção na resiliência de ransomware significa garantir que instantâneos e backups imutáveis ocorram regularmente em um domínio de segurança diferente usando políticas de proteção.
- **Carga de trabalho:** Uma carga de trabalho no Ransomware Resilience pode incluir bancos de dados Oracle, datastores VMware ou compartilhamentos de arquivos.

Pré-requisitos de NetApp Ransomware Resilience

Comece a usar o NetApp Ransomware Resilience verificando se seu ambiente operacional, acesso à rede e navegador da web estão prontos.

Para usar o Ransomware Resilience, certifique-se de atender aos pré-requisitos.

Sistemas suportados

Certifique-se de estar usando um sistema compatível:

Ambiente	Protocolo	Versões suportadas
Amazon FSx for NetApp ONTAP*	CIFS, NFS e SAN	N / D
Azure NetApp Files	CIFS e NFS	N / D
Cloud Volumes ONTAP para AWS	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
Cloud Volumes ONTAP para Google Cloud Platform	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
Cloud Volumes ONTAP para Microsoft Azure	CIFS e NFS	9.12.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior
ONTAP (local)	CIFS e NFS	9.11.1 e posterior
	SAN (FC, iSCSI e NVMe)	9.17.1 e posterior

{asterisco} O Amazon FSx for NetApp ONTAP usa a Proteção Autônoma contra Ransomware (ARP) e não o ARP/AI. Para obter mais informações sobre a diferença, consulte ["ARP/AI"](#).

Requisitos do NetApp Console

A configuração do seu NetApp Console requer:

- Uma conta de usuário do NetApp Console com privilégios de administrador da organização para descobrir recursos.
- Uma organização e sistema de console com pelo menos um agente de console ativo conectado a um ["sistema suportado"](#).
 - Se seus clusters ONTAP locais ou Cloud Volumes ONTAP na AWS ou na nuvem Azure não estiverem configurados no Console, consulte ["Aprenda a configurar um agente de console"](#) e ["requisitos padrão do console"](#).



Se você tiver vários agentes do Console em uma única organização do Console, o Ransomware Resilience verificará os recursos do ONTAP em todos os agentes do Console além daquele que está selecionado no momento na IU do Console.

- O agente do Console deve ter o `cloudmanager-ransomware-protection` contêiner em estado ativo.
- Pelo menos um sistema de console com um cluster ONTAP local da NetApp ou Cloud Volumes ONTAP na AWS ou Azure. O Ransomware Resilience oferece suporte aos protocolos NAS (NFS e SMB) e SAN

(iSCSI, FC e NVMe).

- O Ransomware Resilience é compatível com clusters ONTAP ou Cloud Volumes ONTAP com ONTAP versão 9.11.1 ou superior.



Para usar a Resiliência a Ransomware em cargas de trabalho SAN, você precisa estar executando o ONTAP 9.17.1 ou posterior.

Requisitos do ONTAP

- Você precisa estar executando o ONTAP 9.11.1 ou posterior com uma licença ONTAP One habilitada na instância ONTAP local. Para obter mais informações sobre o suporte do ONTAP, consulte ["Visão geral da proteção autônoma contra ransomware"](#).
- Para aplicar configurações de proteção (como ativar a Proteção Autônoma contra Ransomware), o Ransomware Resilience precisa de permissões de administrador no cluster ONTAP. O cluster ONTAP deveria ter sido integrado usando apenas credenciais de usuário administrador do cluster ONTAP.



Se você conectou um cluster ONTAP ao Console com credenciais não administrativas, [você deve atualizar as credenciais no cluster ONTAP](#update-non-admin-user-permissions-in-an-ontap-system).

Backups de dados

- Uma conta no NetApp StorageGRID, AWS S3, Azure Blob ou Google Cloud Platform para destinos de backup com as permissões de acesso apropriadas configuradas.

Consulte o ["Lista de permissões AWS, Azure ou S3"](#) para mais detalhes.

- O NetApp Backup and Recovery não precisa ser habilitado no sistema.

O Ransomware Resilience ajuda a configurar um destino de backup por meio da opção Configurações. Ver ["Configurar definições"](#).

Requisitos de comportamento suspeito do usuário

Para que o Ransomware Resilience forneça alertas sobre comportamentos suspeitos de usuários, você deve configurar um agente de atividade do usuário. Para instalar um agente de atividade do usuário, certifique-se de que seu sistema atenda ["os requisitos"](#).

Atualizar permissões de usuários não administradores em um sistema ONTAP

Se você precisar atualizar as permissões de usuários não administradores para um determinado sistema, use estas etapas do procedimento.

1. Faça login no Console. No painel, identifique o sistema que precisa ter suas permissões de usuário ONTAP atualizadas.
2. Selecione o sistema para visualizar seus detalhes.
3. Selecione **Exibir informações adicionais** para exibir o nome de usuário.
4. Faça login na CLI do cluster ONTAP como usuário administrador.
5. Exibir as funções existentes para esse usuário:

```
security login show -user-or-group-name <username>
```

6. Alterar a função do usuário. Digitar:

```
security login modify -user-or-group-name <username> -application  
console|http|ontapi|ssh|telnet -authentication-method password -role  
admin
```

7. Retorne ao NetApp Console para usar a Resiliência a Ransomware.

Início rápido para NetApp Ransomware Resilience

Entenda as etapas gerais que você precisa seguir para configurar o Ransomware Resilience e proteger suas cargas de trabalho.

Siga os links em cada etapa para obter informações detalhadas.

1

Revise os pré-requisitos

Essas tarefas exigem a função *Administrador do console*.

- ["Certifique-se de ter instalado um agente do Console"](#)
- ["Certifique-se de que seu sistema atenda aos requisitos"](#)
- ["Revise as funções de usuário do Ransomware Resilience e atribua permissões aos usuários que acessam o Ransomware Resilience"](#)
- ["Configurar licenciamento"](#)

2

Comece com a resiliência contra ransomware

Essas tarefas exigem a função *Administrador de resiliência contra ransomware*.

- ["Descubra cargas de trabalho no Console"](#)
- ["Visualizar a integridade da proteção da carga de trabalho no Painei"](#)
- ["Opcionalmente, realize um exercício de preparação para ataque de ransomware"](#)

3

Configurar proteção e detecção no Ransomware Resilience

Essas tarefas exigem a função *Administrador de resiliência contra ransomware*. Configurar atividades de comportamento suspeito do usuário requer a função adicional *Administrador de comportamento do usuário de resiliência ao ransomware*.

- ["Proteja as cargas de trabalho"](#)
 - Opcionalmente, ["melhorar a proteção configurando a detecção de atividades suspeitas do usuário"](#)

- Opcionalmente, configure destinos de backup:
 - ["Prepare o NetApp StorageGRID, Amazon Web Services, Google Cloud Platform ou Microsoft Azure como destino de backup"](#) .
 - ["Configurar destinos de backup"](#)
- ["Responder à detecção de potenciais ataques de ransomware"](#)
- ["Recuperar-se de um ataque \(após os incidentes serem neutralizados\)"](#)

4

O que vem a seguir?

Depois de configurar a proteção no Ransomware Resilience, veja o que você pode fazer em seguida.

- ["Habilitar a classificação de dados para identificar riscos de governança e segurança"](#)
- ["Enviar alertas para SIEM"](#)
- ["Baixe relatórios de alerta, proteção, treinamento de prontidão, recuperação ou resumo"](#)

Configurar a NetApp Ransomware Resilience

Você pode facilmente implantar o NetApp Ransomware Resilience. Antes de começar, revise ["pré-requisitos"](#) para garantir que seu ambiente esteja pronto.

Preparar o destino do backup

Prepare um dos seguintes destinos de backup:

- NetApp StorageGRID
- Serviços Web da Amazon
- Plataforma Google Cloud
- Microsoft Azure

Depois de configurar as opções no próprio destino de backup, você o configurará posteriormente como um destino de backup no Ransomware Resilience. Para obter detalhes sobre como configurar o destino de backup no Ransomware Resilience, consulte ["Configurar destinos de backup"](#) .

Preparar o StorageGRID para se tornar um destino de backup

Se você quiser usar o StorageGRID como seu destino de backup, consulte ["Documentação do StorageGRID"](#) para obter detalhes sobre StorageGRID.

Prepare a AWS para se tornar um destino de backup

- Crie uma conta na AWS.
- Configurar ["Permissões da AWS"](#) na AWS.

Para obter detalhes sobre como gerenciar seu armazenamento do AWS no Console, consulte ["Gerencie seus buckets do Amazon S3"](#) .

Prepare o Azure para se tornar um destino de backup

- Crie uma conta no Azure.
- Configurar "[Permissões do Azure](#)" no Azure.

Para obter detalhes sobre como gerenciar seu armazenamento do Azure no Console, consulte "[Gerencie suas contas de armazenamento do Azure](#)".

Configurar o NetApp Console

O próximo passo é configurar o Console e a Resiliência contra Ransomware.

Análise "[Requisitos do console para o modo padrão](#)".

Criar um agente de console

Entre em contato com seu representante de vendas da NetApp para experimentar ou usar este serviço. Então, quando você usar o agente do Console, ele incluirá os recursos apropriados para Resiliência de Ransomware.

Para criar um agente do Console usando o Ransomware Resilience, entre em contato com o administrador da organização do Console que tem permissões para criar agentes do Console e consulte a documentação que descreve "[como criar um agente de console](#)".



Se você tiver vários agentes do Console, o Ransomware Resilience verificará os dados de todos os agentes do Console além daquele que é exibido no Console. Este serviço descobre todos os projetos e todos os agentes do Console associados a esta organização.

Acesse a NetApp Ransomware Resilience

Efetue login no NetApp Ransomware Resilience por meio do NetApp Console.

Para fazer login no Console, você pode usar suas credenciais do Site de Suporte da NetApp ou pode se inscrever para um login na nuvem da NetApp usando seu e-mail e uma senha. "[Saiba mais sobre como fazer login](#)".

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Passos

1. Abra um navegador da web e vá para "[o Console](#)".

A página de login do Console é exibida.

2. Efetue login no Console.
3. Na navegação à esquerda do Console, selecione **Proteção > Resiliência a Ransomware**.

Se esta for a primeira vez que você faz login neste serviço, a página de destino será exibida.



Se você não tiver um agente de console ou se ele não for o adequado para esse serviço, será necessário implantar um. "[Aprenda a configurar um agente de console](#)".


Ransomware Resilience

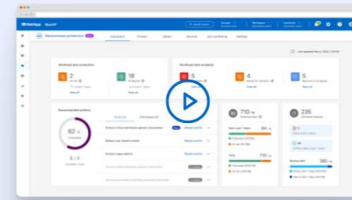
Outsmart ransomware

Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

[Start 30-day free trial](#)

 We won't read the contents of your data or change existing protection.



Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click



Detect and respond

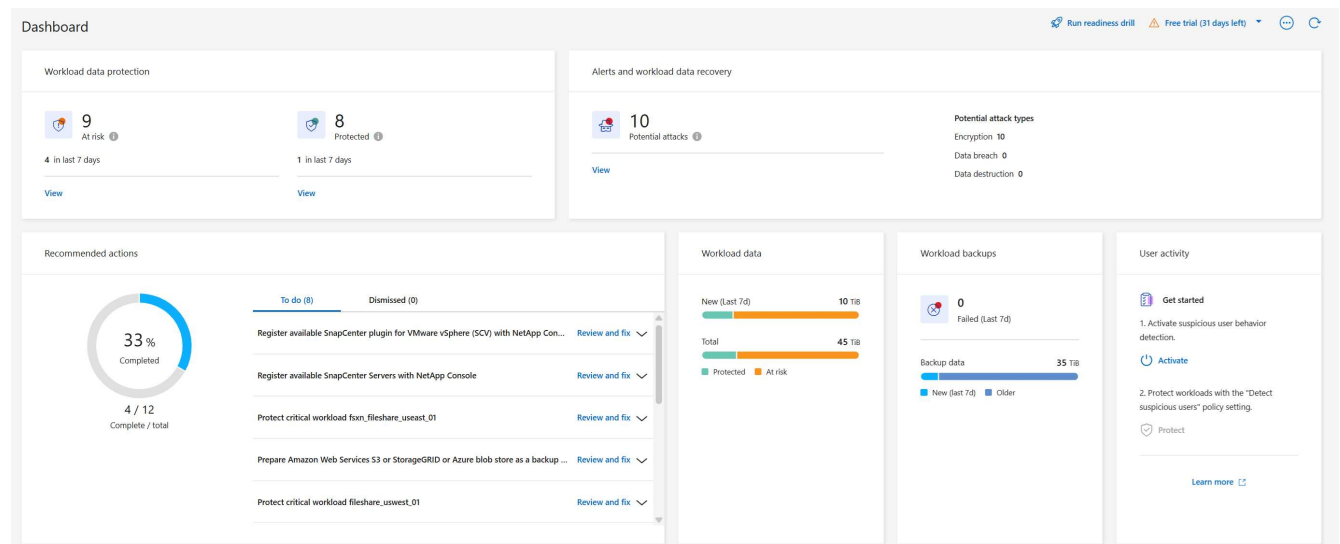
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point



Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

Caso contrário, o painel de resiliência do Ransomware será exibido.



4. Se você ainda não fez isso, selecione a opção **Descobrir cargas de trabalho**.

Consulte "[Descubra cargas de trabalho](#)".

Configurar licenciamento para NetApp Ransomware Resilience

Com o NetApp Ransomware Resilience, você pode usar diferentes planos de licenciamento.

Para executar esta tarefa, você precisa da função de administrador da organização, pasta ou projeto. "[Saiba mais sobre as funções de acesso do Console](#)".

Tipos de licença

A Resiliência contra Ransomware está disponível com os seguintes tipos de licença:

- Teste gratuito de 30 dias
- Adquira uma assinatura pré-paga (PAYGO) com o Amazon Web Services (AWS) Marketplace, Google Cloud Marketplace ou Azure Marketplace
- Traga sua própria licença (BYOL): um arquivo de licença NetApp (NLF) que você obtém do seu representante de vendas da NetApp . Você pode usar o número de série da licença para ativar o BYOL no Console.

Depois de configurar seu BYOL ou comprar uma assinatura PAYGO, você poderá ver a licença na seção Licenses and subscriptions do Console.

Após o término do teste gratuito ou a licença ou assinatura expirar, você ainda poderá:

- Exibir cargas de trabalho e integridade da carga de trabalho
- Excluir recursos como políticas
- Execute todas as operações agendadas criadas durante o período de teste ou sob a licença

Outras licenças

A licença do Ransomware Resilience não inclui produtos NetApp adicionais. No entanto, o Ransomware Resilience pode ser integrado ao NetApp Backup and Recovery, mesmo que você não tenha uma licença separada para Backup and Recovery.



Se você tiver o Backup and Recovery e o Ransomware Resilience, quaisquer dados comuns protegidos por ambos os produtos serão cobrados somente pelo Ransomware Resilience.

Experimente o Ransomware Resilience com um teste gratuito de 30 dias

Você pode experimentar o Ransomware Resilience com um teste gratuito de 30 dias. Você deve ser um administrador da Organização do Console para iniciar o teste gratuito.

Os limites de capacidade de armazenamento não são aplicados durante o teste.

Você pode obter uma licença ou assinar a qualquer momento e não será cobrado até o término do teste de 30 dias. Para continuar após o teste de 30 dias, você precisará comprar uma licença BYOL ou uma assinatura PAYGO.

Durante o teste, você terá funcionalidade total.

Passos

1. Acesse o ["Console"](#) .
2. Efetue login no Console.
3. No NetApp Console, selecione **Proteção > Resiliência contra ransomware**.

Se esta for a primeira vez que você faz login neste serviço, a página de destino será exibida.

Ransomware Resilience

Outsmart ransomware

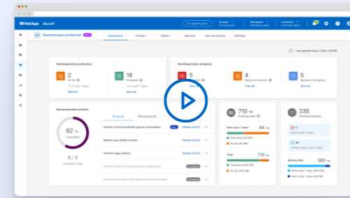
Fortify, safeguard, and quickly recover ONTAP workloads using comprehensive orchestration, AI-driven attack detection, and fast recovery processes in alignment with cybersecurity best practices.

Get **full access** to ransomware resilience with a 30-day free trial.

Start 30-day free trial



We won't read the contents of your data or change existing protection.



Identify and protect

Automatically identifies workloads at risk, recommends fixes, and protects with one-click



Detect and respond

Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point



Recover

Restores workloads in minutes through simplified, orchestrated workload-consistent recovery

- Se você ainda não adicionou um agente do Console para outros serviços, ["adicione um"](#).
- Na página inicial do Ransomware Resilience, selecione **Começar descobrindo cargas de trabalho** para descobrir suas cargas de trabalho.



Esta opção só estará disponível se você tiver instalado com sucesso um agente do Console.

- Para revisar as informações do teste gratuito, selecione a opção suspensa no canto superior direito.

Após o término do teste, obtenha uma assinatura ou licença

Após o término do teste gratuito, você pode assinar por meio de um dos Marketplaces ou comprar uma licença da NetApp.

Se você já tiver uma assinatura PAYGO, a licença será automaticamente transferida para a assinatura após o término do teste gratuito.

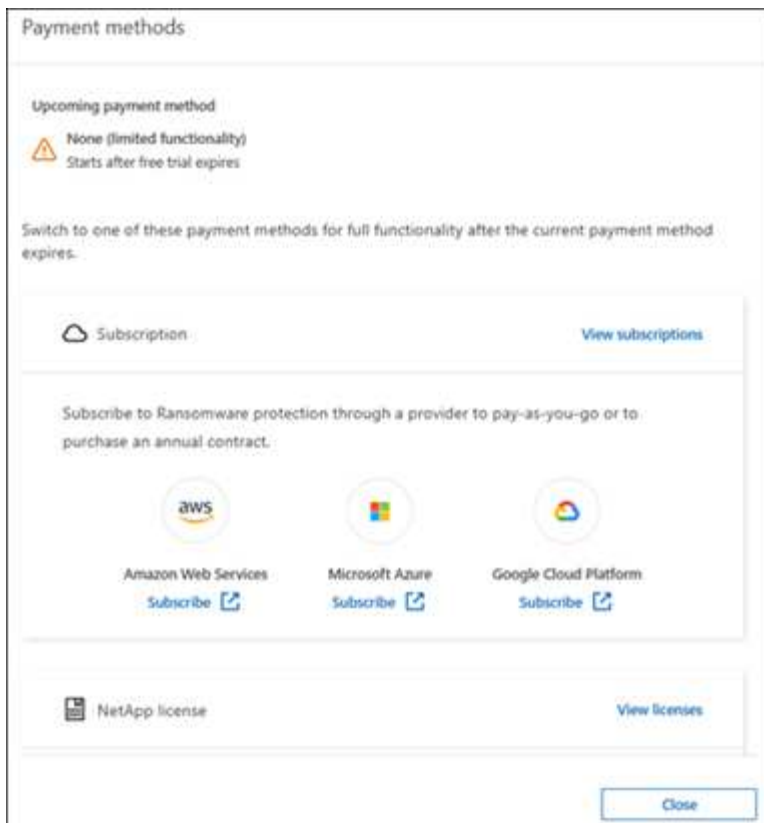
[Assine pelo AWS Marketplace](#) [Assine pelo Microsoft Azure Marketplace](#) [Assine pelo Google Cloud Platform Marketplace](#) [Traga sua própria licença \(BYOL\)](#)

Assine pelo AWS Marketplace

Este procedimento fornece uma visão geral de alto nível de como assinar diretamente no AWS Marketplace.

Passos

- Em Ransomware Resilience, faça um dos seguintes:
 - Se você receber uma mensagem informando que o teste gratuito está expirando, selecione **Ver métodos de pagamento**.
 - Se você ainda não iniciou o teste, selecione o aviso **Teste gratuito** no canto superior direito e depois **Ver métodos de pagamento**.



2. Na página Métodos de pagamento, selecione **Assinar** para **Amazon Web Services**.
3. No AWS Marketplace, selecione **Exibir opções de compra**.
4. Use o AWS Marketplace para assinar o * NetApp Intelligent Services* e o **Ransomware Resilience**.
5. Quando você retorna ao Ransomware Resilience, uma mensagem informa que você está inscrito.



Um e-mail será enviado a você, incluindo o número de série do Ransomware Resilience e indicando que o Ransomware Resilience está inscrito no AWS Marketplace.

6. Retorne à página de métodos de pagamento do Ransomware Resilience.
7. Adicione a licença ao Console selecionando **Adicionar licença**.

8. Na página Adicionar licença, selecione **Inserir número de série**, insira o número de série que foi incluído no e-mail enviado a você e selecione **Adicionar licença**.
9. Para visualizar os detalhes da licença, na navegação à esquerda do Console, selecione **Administração > * Licenses and subscriptions***.
 - Para ver informações sobre a assinatura, selecione **Assinaturas**.
 - Para ver as licenças BYOL, selecione **Licenças de serviços de dados**.
10. Retornar para Resiliência ao Ransomware. Na navegação à esquerda do Console, selecione **Proteção > Resiliência a Ransomware**.

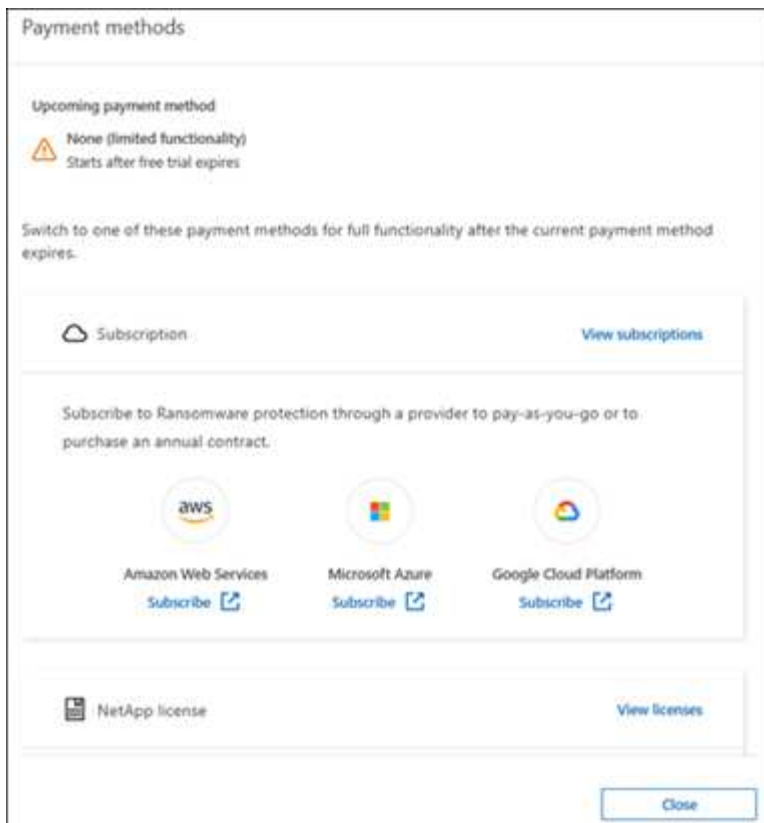
Uma mensagem confirma que uma licença foi adicionada.

Assine pelo Microsoft Azure Marketplace

Este procedimento fornece uma visão geral de alto nível de como assinar diretamente no Azure Marketplace.

Passos

1. Em Ransomware Resilience, faça um dos seguintes:
 - Se você receber uma mensagem informando que o teste gratuito está expirando, selecione **Ver métodos de pagamento**.
 - Se você ainda não iniciou o teste, selecione o aviso **Teste gratuito** no canto superior direito e depois **Ver métodos de pagamento**.



2. Na página Métodos de pagamento, selecione **Assinar no Microsoft Azure Marketplace**.
3. No Azure Marketplace, selecione **Exibir opções de compra**.
4. Use o Azure Marketplace para assinar o * NetApp Intelligent Services* e o **Ransomware Resilience**.
5. Quando você retorna ao Ransomware Resilience, uma mensagem informa que você está inscrito.



Um e-mail será enviado a você, incluindo o número de série do Ransomware Resilience e indicando que o Ransomware Resilience está inscrito no Azure Marketplace.

6. Voltar para a página Métodos de pagamento do Ransomware Resilience.
7. Para adicionar a licença, selecione **Adicionar uma licença**.

8. Na página Adicionar licença, selecione **Inserir número de série** e insira o número de série do e-mail enviado a você. Selecione **Adicionar licença**.
9. Para visualizar detalhes da licença em Licenses and subscriptions, na navegação à esquerda do Console, selecione **Governança** > * Licenses and subscriptions*.
 - Para ver informações sobre a assinatura, selecione **Assinaturas**.
 - Para ver as licenças BYOL, selecione **Licenças de serviços de dados**.
10. Retornar para Resiliência ao Ransomware. Na navegação à esquerda do Console, selecione **Proteção** > **Resiliência a Ransomware**.

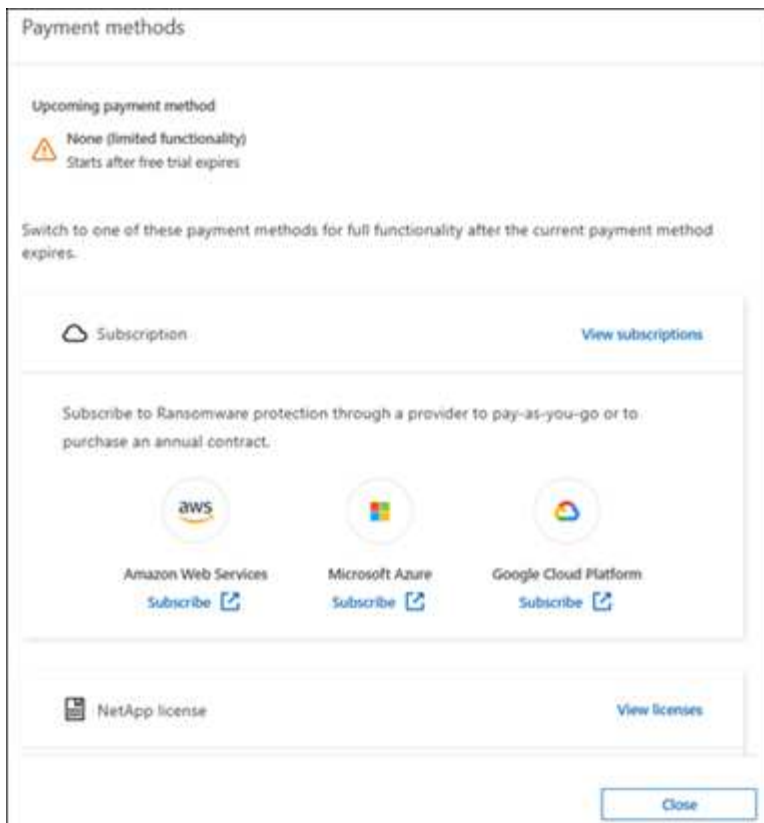
Aparece uma mensagem indicando que uma licença foi adicionada.

Assine pelo Google Cloud Platform Marketplace

Este procedimento fornece uma visão geral de alto nível de como assinar diretamente no Google Cloud Platform Marketplace.

Passos

1. Em Resiliência contra Ransomware, faça um dos seguintes:
 - Se você receber uma mensagem informando que o teste gratuito está expirando, selecione **Ver métodos de pagamento**.
 - Se você ainda não iniciou o teste, selecione o aviso **Teste gratuito** no canto superior direito e depois **Ver métodos de pagamento**.



2. Na página Métodos de pagamento, selecione **Assinar** no Google Cloud Platform Marketplace*.
3. No Google Cloud Platform Marketplace, selecione **Inscrever-se**.
4. Use o Google Cloud Platform Marketplace para assinar o * NetApp Intelligent Services* e o **Ransomware Resilience**.
5. Quando você retorna ao Ransomware Resilience, uma mensagem informa que você está inscrito.



Um e-mail será enviado a você, incluindo o número de série do Ransomware Resilience e indicando que o Ransomware Resilience está inscrito no Google Cloud Platform Marketplace.

6. Voltar para a página Métodos de pagamento do Ransomware Resilience.
7. Para adicionar a licença ao Console, selecione **Adicionar licença**.

8. Na página Adicionar licença, selecione **Inserir número de série**. Digite o número de série no e-mail enviado a você. Selecione **Adicionar licença**.
9. Para visualizar os detalhes da licença, na navegação à esquerda do Console, selecione **Governança** > * Licenses and subscriptions*.
 - Para ver informações sobre a assinatura, selecione **Assinaturas**.
 - Para ver as licenças BYOL, selecione **Licenças de serviços de dados**.
10. Retornar para Resiliência ao Ransomware. Na navegação à esquerda do Console, selecione **Proteção** > **Resiliência a Ransomware**.

Aparece uma mensagem indicando que uma licença foi adicionada.

Traga sua própria licença (BYOL)

Se você quiser trazer sua própria licença (BYOL), precisará comprá-la, obter o arquivo de licença NetApp (NLF) e adicionar a licença ao Console.

Adicione seu arquivo de licença ao Console

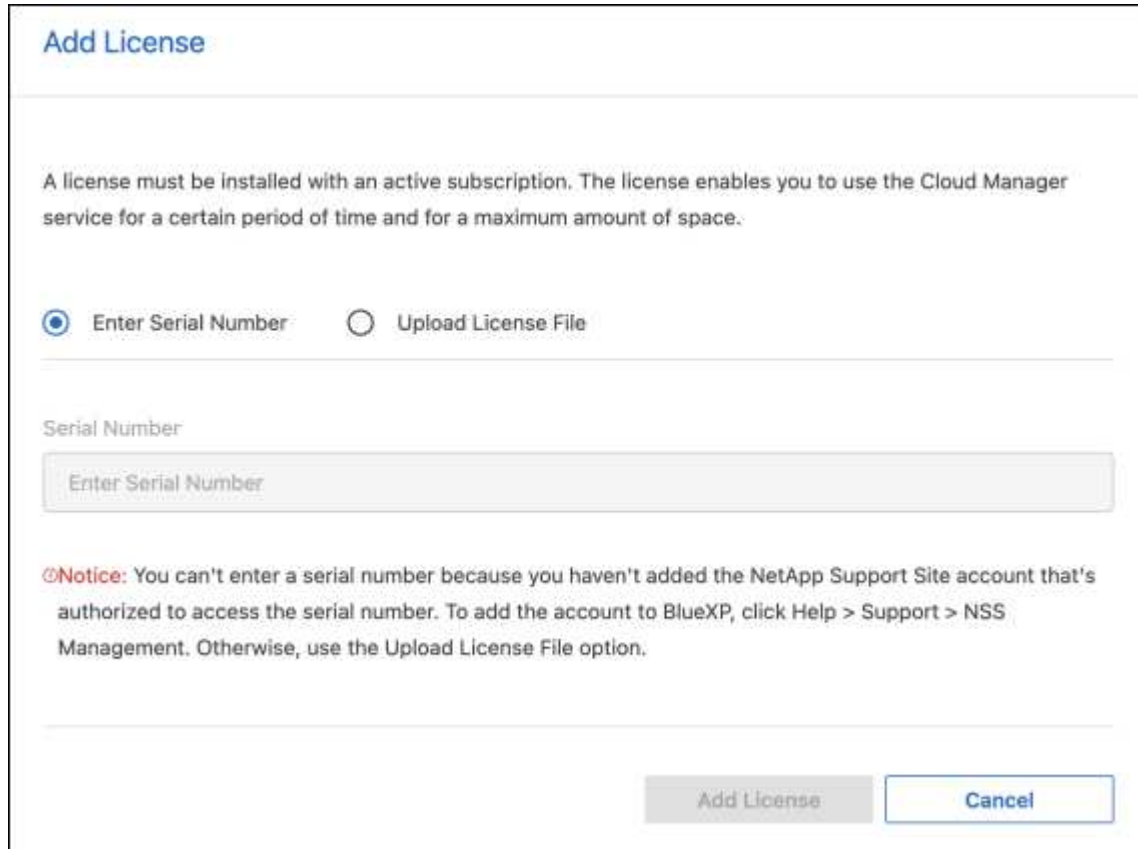
Depois de comprar sua licença do Ransomware Resilience com seu representante de vendas da NetApp, ative a licença inserindo o número de série do Ransomware Resilience e as informações da conta do NetApp Support Site (NSS).

Antes de começar

Você precisa do número de série do Ransomware Resilience. Localize esse número no seu pedido de vendas ou entre em contato com a equipe de contas para obter essas informações.

Passos

1. Depois de obter a licença, retorne ao Ransomware Resilience. Selecione a opção **Ver métodos de pagamento** no canto superior direito. Ou, na mensagem de que o teste gratuito está expirando, selecione **Assinar ou comprar uma licença**.
2. Selecione **Adicionar licença** para ir para a página Licenças e assinaturas do Console.
3. Na aba **Licenças de Serviços de Dados**, selecione **Adicionar licença**.



4. Na página Adicionar licença, insira o número de série e as informações da conta do site de suporte da NetApp .
 - Se você tiver o número de série da licença do Console e souber sua conta NSS, selecione a opção **Inserir número de série** e insira essas informações.

Se sua conta do site de suporte da NetApp não estiver disponível na lista suspensa, "[adicione a conta NSS ao Console](#)".
 - Se você tiver o arquivo de licença zvondolr (necessário quando instalado em um site escuro), selecione a opção **Carregar arquivo de licença** e siga as instruções para anexar o arquivo.
5. Selecione **Adicionar licença**.

Resultado

A página Licenses and subscriptions mostra que o Ransomware Resilience tem uma licença.

Atualize sua licença do Console quando ela expirar

Se o prazo da sua licença estiver próximo da data de expiração ou se a capacidade da sua licença estiver atingindo o limite, você será notificado na interface do usuário do Ransomware Resilience. Você pode

atualizar sua licença do Ransomware Resilience antes que ela expire para que não haja interrupção na sua capacidade de acessar seus dados digitalizados.



Esta mensagem também aparece em Licenses and subscriptions e em "[Configurações de notificação](#)".

Passos

1. Você pode enviar um e-mail ao suporte para solicitar uma atualização da sua licença.

Depois que você paga pela licença e ela é registrada no site de suporte da NetApp, o Console atualiza a licença automaticamente. A página Licenças de Serviços de Dados refletirá a alteração em 5 a 10 minutos.

2. Se o Console não puder atualizar a licença automaticamente, você precisará carregar manualmente o arquivo de licença.
 - a. Você pode obter o arquivo de licença no site de suporte da NetApp.
 - b. No Console, selecione **Administração > Licenses and subscriptions**.
 - c. Selecione a aba **Licenças de Serviços de Dados**, selecione o ícone **Ações...** para o número de série que você está atualizando e então selecione **Atualizar Licença**.

Encerrar a assinatura do PAYGO

Se você quiser encerrar sua assinatura PAYGO, poderá fazê-lo a qualquer momento.

Passos

1. Em Ransomware Resilience, no canto superior direito, selecione a opção de licença.
2. Selecione **Ver métodos de pagamento**.
3. Nos detalhes suspensos, desmarque a caixa **Usar após o vencimento do método de pagamento atual**.
4. Selecione **Salvar**.

Mais informações

- "[Documentação sobre licenças e assinaturas do NetApp Console](#)"

Descubra cargas de trabalho no NetApp Ransomware Resilience

Antes de poder usar o NetApp Ransomware Resilience, ele precisa primeiro descobrir os dados da carga de trabalho. Durante a descoberta, o Ransomware Resilience analisa todos os volumes e arquivos em sistemas em todos os agentes e projetos do Console dentro de uma organização.

No painel de controle Discovery, o Ransomware Resilience exibe as configurações de sistema compatíveis e incompatíveis. A ferramenta de Resiliência a Ransomware avalia aplicativos Oracle, datastores VMware, compartilhamentos de arquivos e armazenamento em blocos.



A Resiliência contra Ransomware não detecta cargas de trabalho com volumes que utilizam FlexGroup.

O Ransomware Resilience verifica sua proteção de backup atual, cópias de snapshots e opções de proteção autônoma contra ransomware da NetApp . O Ransomware Resilience também detecta informações de proteção do SnapCenter for VMware para datastores de máquinas virtuais, do SnapCenter for Oracle e do NetApp Backup and Recovery para compartilhamentos de arquivos e compartilhamentos de arquivos de máquinas virtuais. Em seguida, ele recomenda maneiras de melhorar sua proteção contra ransomware.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

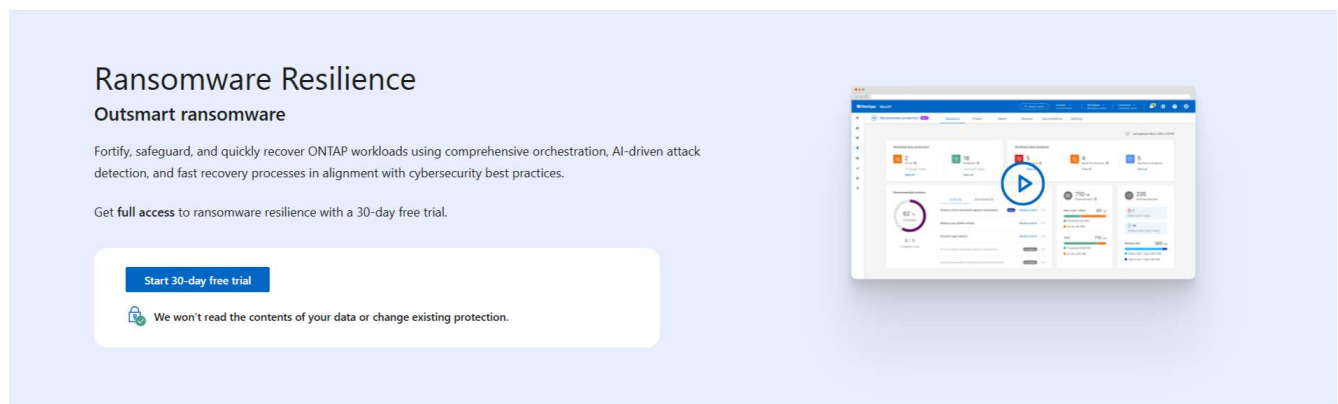
Selecione cargas de trabalho para descobrir e proteger

Em cada agente do Console, selecione os sistemas onde você deseja descobrir cargas de trabalho.

Passos


1. No NetApp Console, selecione **Proteção > Proteção contra ransomware**.

Se este for seu primeiro login, a página de destino será exibida.




Identify and protect
Automatically identifies workloads at risk, recommends fixes, and protects with one-click


Detect and respond
Identifies potential attacks using AI/ML and automatically responds to secure a safe recovery point

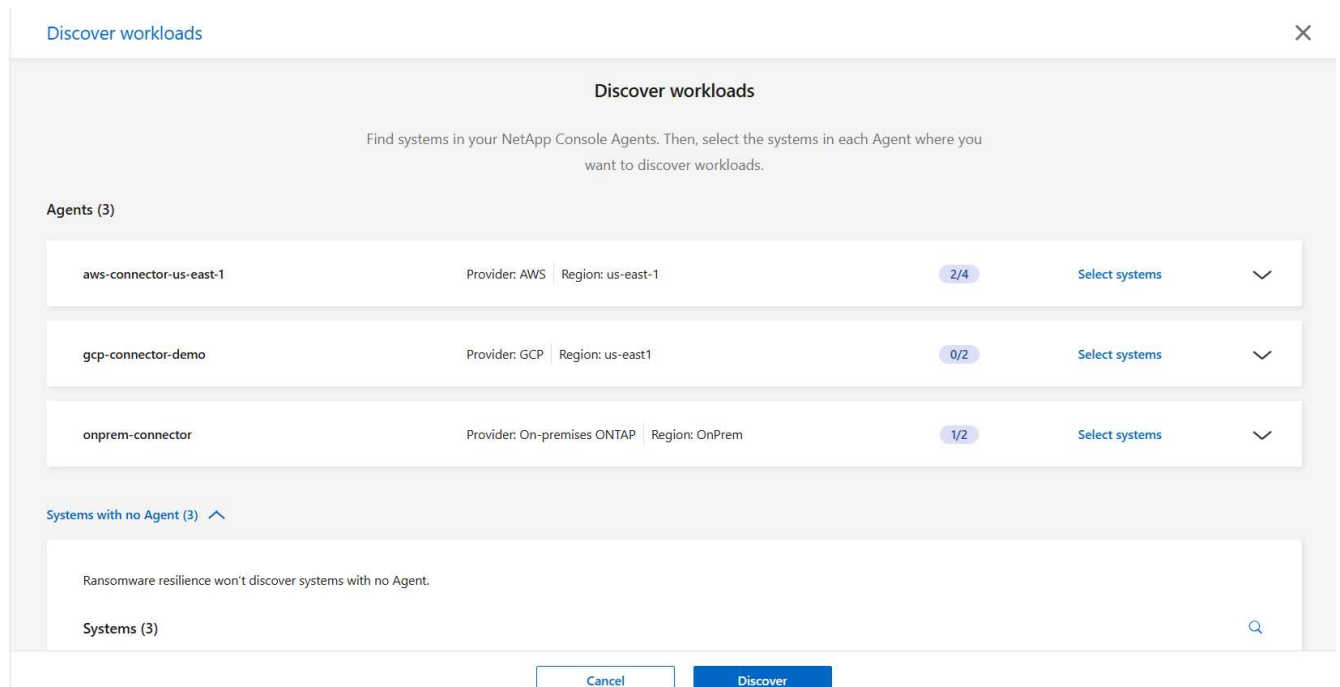

Recover
Restores workloads in minutes through simplified, orchestrated workload-consistent recovery



Se você iniciou o teste gratuito, o rótulo do botão **Iniciar teste gratuito de 30 dias** muda para **Começar descobrindo cargas de trabalho**.

2. Na página inicial, selecione **Começar descobrindo cargas de trabalho**.

O Ransomware Resilience encontra sistemas suportados e não suportados. Este processo pode levar alguns minutos.

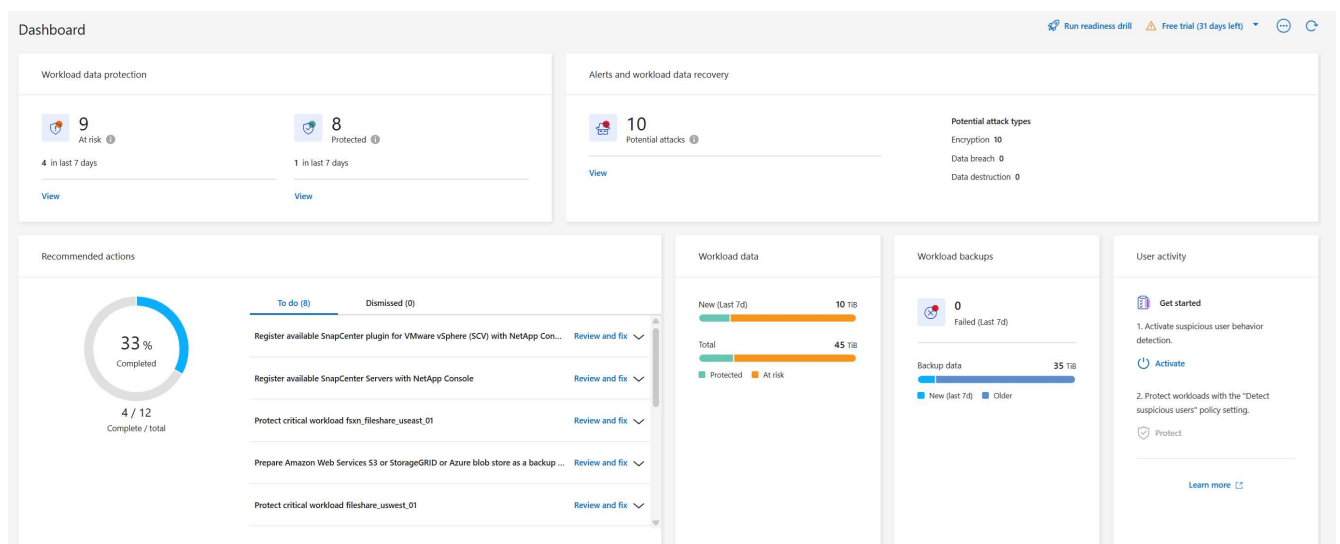


3. Para descobrir cargas de trabalho para um agente de Console específico, selecione **Selecionar sistemas** ao lado do agente de Console onde você deseja descobrir cargas de trabalho.
4. Selecione os sistemas nos quais você deseja descobrir cargas de trabalho.
5. Selecione **Descobrir**.

A Resiliência contra Ransomware só descobre dados de carga de trabalho quando você seleciona o sistema. O processo de descoberta pode levar vários minutos.

6. Para baixar a lista de cargas de trabalho descobertas, selecione **Baixar resultados**.
7. Para exibir o painel de resiliência ao ransomware, selecione **Ir para o painel**.

O Painel mostra a integridade da proteção de dados. O número de cargas de trabalho em risco ou protegidas é atualizado à medida que novas cargas de trabalho são descobertas.



"Saiba o que o Painel mostra para você."

Descubra cargas de trabalho recém-criadas para sistemas selecionados anteriormente

Se você adicionou cargas de trabalho a um sistema previamente descoberto, é necessário reiniciar a descoberta para proteger as novas cargas de trabalho.

Passos

1. Para identificar o momento da última detecção, observe a data e a hora ao lado do ícone **Atualizar** no canto superior direito do painel de controle de Resiliência a Ransomware.
2. No painel de controle, selecione o ícone **Atualizar** para encontrar novas cargas de trabalho.



Se você encontrar volumes que não estão sendo exibidos para o sistema que você descobriu, esses volumes podem não ser compatíveis. Para encontrar uma lista de volumes não suportados, acesse o menu **Configurações** e selecione a opção correspondente no cartão de descoberta de carga de trabalho para baixar um relatório JSON com os volumes suportados e não suportados.

Descubra novos sistemas

Se você já descobriu sistemas, você pode encontrar sistemas novos ou não selecionados anteriormente.

Passos

1. No menu Resiliência a Ransomware, selecione a opção vertical. Opção "category='inline-code'/" no canto superior direito. No menu suspenso, selecione **Configurações**.
2. No cartão Descoberta de carga de trabalho, selecione **Descobrir cargas de trabalho**. A descoberta pode levar alguns minutos. Um ícone de carregamento exibe o progresso.
3. O Ransomware Resilience descobre sistemas suportados e não suportados. Não oferece suporte a um sistema se a versão do ONTAP for inferior à versão exigida. Quando você passa o mouse sobre um sistema não suportado, uma dica de ferramenta exibe o motivo. Selecione os sistemas nos quais você deseja descobrir cargas de trabalho.
4. Selecione **Descobrir**.

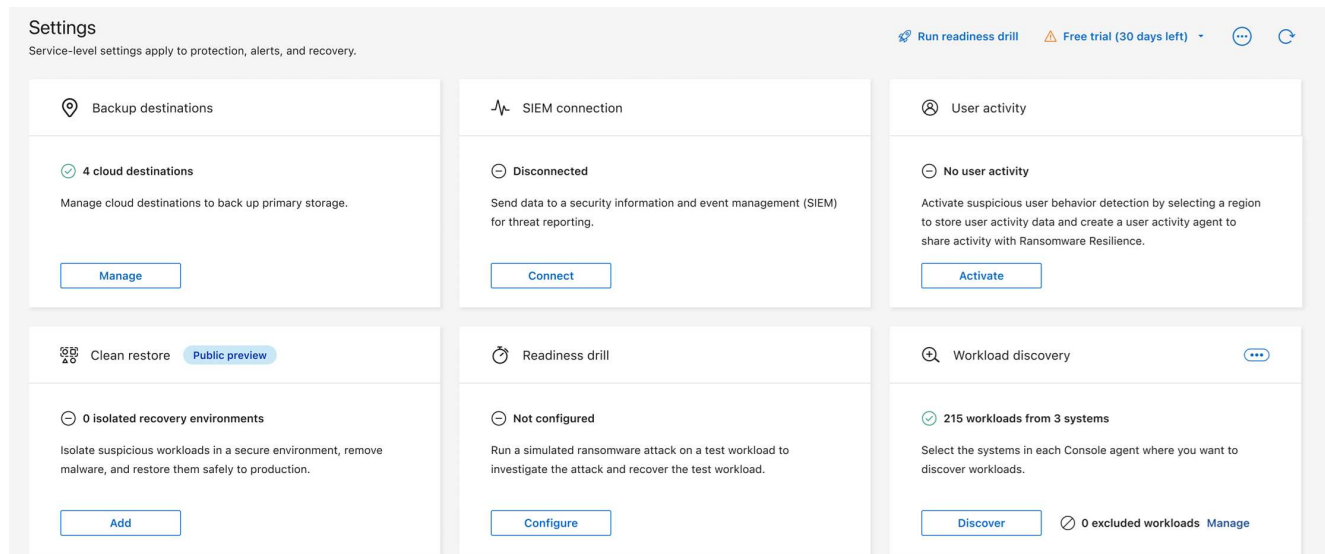
Excluir cargas de trabalho

A Resiliência a Ransomware permite excluir cargas de trabalho específicas de um sistema da proteção e detecção de ransomware.

Você só pode excluir cargas de trabalho que sejam compatíveis e tenham sido detectadas com sucesso. Você pode modificar a lista de cargas de trabalho excluídas a qualquer momento. Você não será cobrado por cargas de trabalho excluídas da Resiliência a Ransomware.

Adicionar cargas de trabalho à lista de cargas de trabalho excluídas

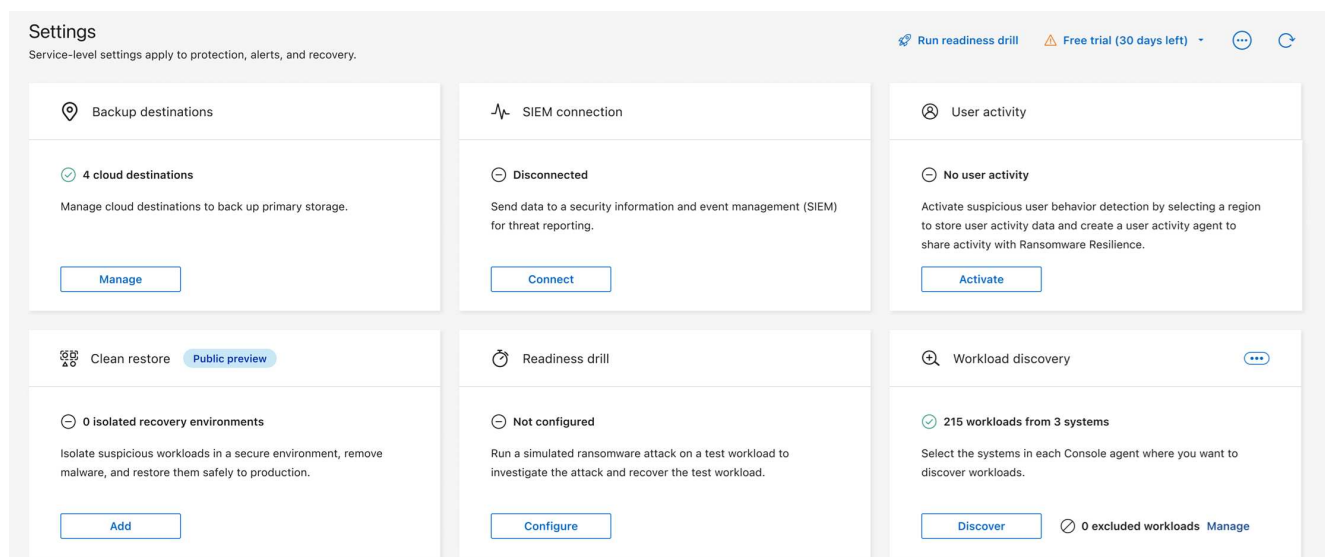
1. Em Resiliência a Ransomware, selecione **Configurações**.
2. No painel de Configurações, localize o painel de descoberta de cargas de trabalho. O cartão identifica o número de cargas de trabalho excluídas. Para adicionar cargas de trabalho, ao lado das cargas de trabalho excluídas, selecione **Gerenciar**.



3. Na página Cargas de trabalho excluídas, selecione **Adicionar**.
4. Selecione as cargas de trabalho que deseja excluir e clique em **Adicionar**.
5. Consulte a lista de cargas de trabalho excluídas na página Cargas de trabalho excluídas. Enquanto a carga de trabalho está sendo adicionada, um indicador de progresso é exibido ao lado do nome dela. Se uma carga de trabalho não for excluída com sucesso, ela não será exibida na página.

Remover cargas de trabalho da lista de cargas de trabalho excluídas

1. Em Resiliência a Ransomware, selecione **Configurações**.
2. No painel de Configurações, localize o painel de descoberta de cargas de trabalho. O cartão identifica o número de cargas de trabalho excluídas. Ao lado das cargas de trabalho excluídas, selecione **Gerenciar**.



3. Para remover uma carga de trabalho individual, selecione a ação correspondente à carga de trabalho que deseja remover da lista de exclusões.

Para remover várias cargas de trabalho, selecione a caixa de seleção ao lado das cargas de trabalho que deseja remover e, em seguida, **Remover da lista de excluídos**.

4. Na caixa de diálogo, selecione **Remover** para confirmar que deseja remover as cargas de trabalho da lista de exclusão.

5. Se a carga de trabalho for removida com sucesso da lista de cargas de trabalho excluídas, uma mensagem de sucesso será exibida na página Cargas de trabalho excluídas e a carga de trabalho não aparecerá mais na lista de cargas de trabalho excluídas. Se a ação falhar, uma mensagem de erro será exibida; tente a operação novamente.

[Settings](#) > Excluded workloads

Excluded workloads

Remove workloads from Ransomware Resilience. You aren't charged for excluded workloads.

Excluded workloads (0)



Add



Excluded workload

Type



No excluded workloads



Removed workload from excluded list Name. [View workload](#)



Realizar um exercício de preparação para ataques de ransomware no NetApp Ransomware Resilience

Execute um exercício de preparação para ataque de ransomware simulando um ataque em uma nova carga de trabalho de amostra. Investigue o ataque simulado e recupere a carga de trabalho. Use este recurso para testar notificações de alerta, resposta e recuperação. Execute a broca sempre que necessário.



Seus dados reais de carga de trabalho não são afetados.

Você pode executar exercícios de prontidão em cargas de trabalho NFS e CIFS (SMB).

Configurar um exercício de preparação para ataque de ransomware

Antes de executar uma simulação, configure um exercício na página Configurações. Acesse a página Configurações na opção Ações no menu superior.

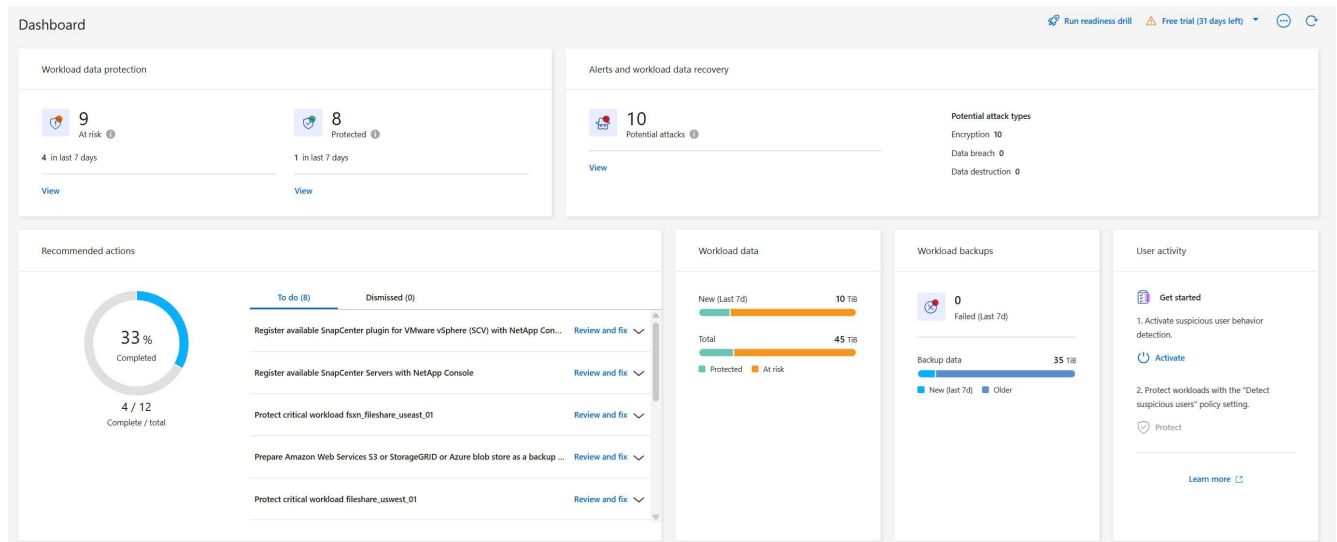
Você precisa inserir um nome de usuário e uma senha para as seguintes situações:

- Se ocorrerem alterações no nome de usuário ou na senha da VM de armazenamento selecionada anteriormente
- Se você selecionar uma VM de armazenamento CIFS (SMB) diferente
- Se você inserir um nome de carga de trabalho de teste diferente

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Passos

1. No menu NetApp Ransomware Resilience, selecione o botão **Executar teste de prontidão** no canto superior direito.




2. No cartão de exercício de prontidão na página Configurações, selecione **Configurar**.

O Console exibe a página Configurar exercício de prontidão.

Readiness drill

Run a simulated ransomware attack on a new test workload that will be saved in the selected system. Then, investigate the simulated attack and recover the test workload. You can run a readiness drill multiple times.

 Your real workload data will not be impacted.

Select a readiness drill test environment where the new test workload will be created.

Console agent

aws-connector-us-east-1 


System

VsaWorkingEnvironment-1 

Storage VM

svm_rps_test_readiness_drill_01 

New test workload

 Requires 10 GiB of storage

rps_test_ drill01

Readiness drill type

Custom recovery 

Save

Cancel

3. Faça o seguinte:

- Selecione o agente do Console que você deseja usar para o exercício de prontidão.
- Selecione um sistema de teste.
- Selecione um SVM de armazenamento de teste.
- Se você selecionou uma VM de armazenamento CIFS (SMB), os campos **Nome de usuário** e **Senha** serão exibidos. Digite o nome de usuário e a senha para a VM de armazenamento.
- Selecione o tipo de exercício de prontidão. Para uma recuperação manual de uma violação de dados de criptografia, escolha **Recuperação personalizada**. Para recuperação de atividades suspeitas de usuários, escolha **Violação de dados**.

f. Insira o nome de uma nova carga de trabalho de teste a ser criada. Não inclua hífen no nome.

4. Selecione **Salvar**.



Você pode editar a configuração do exercício de prontidão mais tarde usando a página Configurações.

Iniciar um exercício de prontidão

Depois de configurar o exercício de prontidão, você pode iniciá-lo.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Quando você inicia o exercício de prontidão, o Ransomware Resilience ignora o modo de aprendizado e inicia o exercício no modo ativo. O status de detecção da carga de trabalho é Ativo.

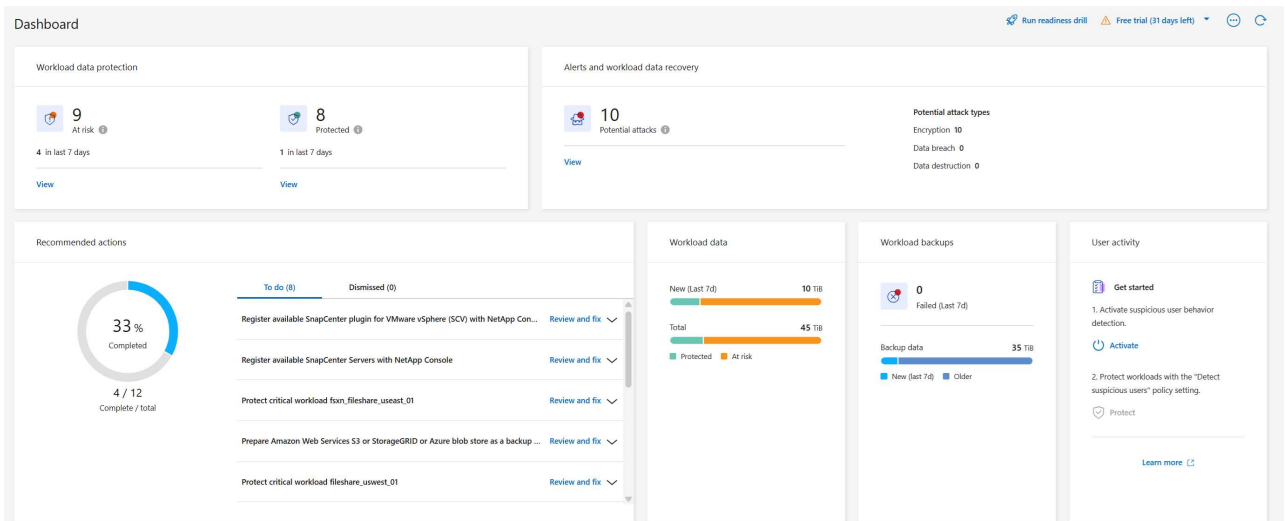


Uma carga de trabalho pode ter um status de detecção de ransomware **Modo de aprendizagem** quando uma política de detecção é atribuída recentemente e o Ransomware Resilience verifica as cargas de trabalho.

Passos

1. Faça um dos seguintes:

- No menu Resiliência contra Ransomware, selecione o botão **Executar teste de prontidão** no canto superior direito.



- OU, na página Configurações, no cartão de exercício de prontidão, selecione **Iniciar**.



Não é possível editar a configuração do exercício de prontidão enquanto o exercício estiver em execução. Você pode reiniciar a broca para pará-la e modificar a configuração.

Responder a um alerta de exercício de prontidão


Teste sua prontidão respondendo a um alerta de treinamento de prontidão.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Passos


- 1. No menu Resiliência contra Ransomware, selecione **Alertas**.

O Console exibe a página Alertas. Na coluna ID do alerta, você vê "Exercício de prontidão" ao lado do ID.

 6 Alerts


12 GiB Impacted data

Automated responses

 9 Snapshot copies

Alerts (6)

Alert ID	Workload	Location	Type	Status	Connector	Incidents	Impacted data	First detected
alert8727	Oracle_8821	10.0.1.193	Oracle	New	aws-connector-us-east-1	2	2 GiB	23 days ago
ws_alert9823	Oracle_9819	10.0.1.193	Oracle	New	aws-connector-us-east-1	1	2 GiB	23 days ago
alert3932	MySQL_9294	10.0.1.10	MySQL	New	aws-connector-us-east-1	2	2 GiB	23 days ago
alert7918	vm_datastore_202_735...	10.195.52.126	VM datastore	New	onprem-connector	1	2 GiB	23 days ago
alert5319	vm_datastore_uswest_...	10.0.1.215	VM file share	New	aws-connector-us-west-1-account-LXtft4X...	1	2 GiB	23 days ago
alert1407 Readiness drill	rps_test_gri	rps_test_readiness_drill_svm	File share	New	aws-connector-us-east-1	1	2 GiB	1 minute ago



Workload rps_test_readiness-drill-workload-test, marked restore needed. [Restore workload](#)

- 2. Selecione o alerta com a indicação "Exercício de prontidão". Uma lista de alertas de incidentes aparece na página de detalhes Alertas.

 7 Alerts

12 TiB Impacted data

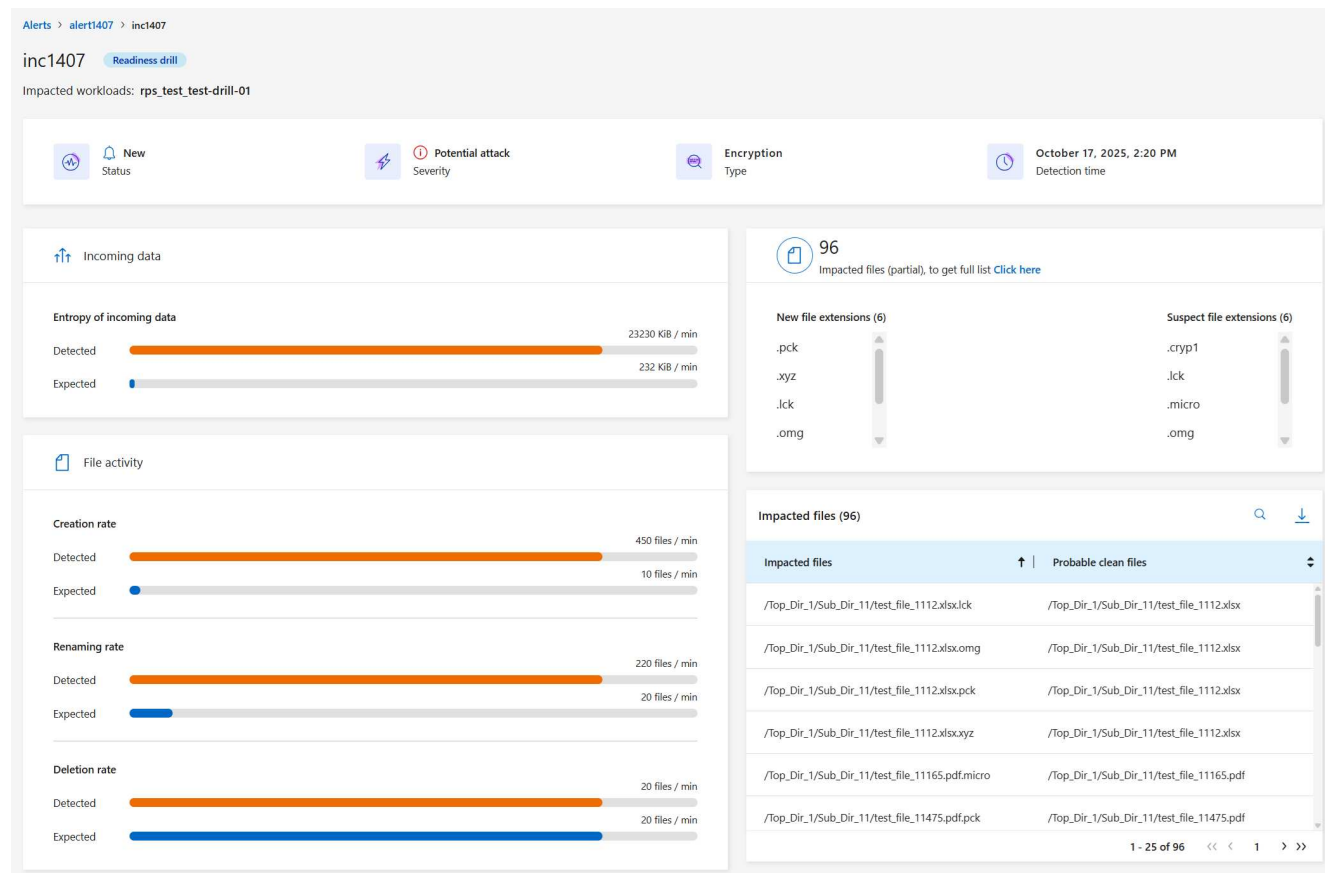
Automated responses

 9 Snapshot copies

Alerts (7)

Alert ID	Workload	Location	Type	Status	Console agent	Incide...	Impacted data	First detected	Most rec
alert1407 Readiness drill	rps_test_awsSystemTest	svm_rps_test_readi...	File share	Active	aws-connector-us-east-1	1	2 GiB	Just now	Just now

- 3. Revise os incidentes de alerta.
- 4. Selecione um incidente de alerta.



Aqui estão algumas coisas que você deve procurar:

- Observe a gravidade potencial do ataque.

Se a gravidade indicar que um usuário é suspeito de atividade maliciosa, revise o nome do usuário. Você também pode **"bloquear o usuário."**

- Observe a atividade do arquivo e os processos suspeitos:
 - Observe os dados detectados recebidos em comparação com os dados esperados.
 - Observe a taxa de criação de arquivos detectada em comparação com a taxa esperada.
 - Observe a taxa de renomeação de arquivos detectada em comparação com a taxa esperada.
 - Observe a taxa de exclusão em comparação com a taxa esperada.
- Veja a lista de arquivos afetados. Veja as extensões que podem estar causando o ataque.
- Determine o impacto e a amplitude do ataque analisando o número de arquivos e diretórios afetados.

Restaurar a carga de trabalho de teste

Após revisar o alerta do exercício de prontidão, restaure a carga de trabalho do teste, se necessário.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. **"Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"**.

Passos

1. Retorne à página de detalhes do alerta.
2. Se a carga de trabalho de teste precisar ser restaurada, faça o seguinte:
 - Selecione **Marcar restauração necessária**.
 - Revise a confirmação e selecione **Marcar restauração necessária** na caixa de confirmação.
 - No menu Resiliência contra Ransomware, selecione **Recuperação**.
 - Selecione a carga de trabalho de teste marcada com "Exercício de prontidão" que você deseja restaurar.
 - Selecione **Restaurar**.
 - Na página Restaurar, forneça informações para a restauração:
 - Selecione a cópia do instantâneo de origem.
 - Selecione o volume de destino.
3. Na página de revisão de restauração, selecione **Restaurar**.

O Console exibe o status da restauração do exercício de prontidão como "Em andamento" na página Recuperação.

Após a conclusão da restauração, o Console altera o status da carga de trabalho para **Restaurada**.

4. Revise a carga de trabalho restaurada.



Para obter detalhes sobre o processo de restauração, consulte ["Recuperar-se de um ataque de ransomware \(após os incidentes serem neutralizados\)"](#).

Alterar o status dos alertas após o exercício de prontidão

Após revisar o alerta do exercício de prontidão e restaurar a carga de trabalho, altere o status do alerta, se necessário.

Função necessária no Console Administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de acesso do Console para todos os serviços"](#).

Passos

1. Retorne à página de detalhes do alerta.
2. Selecione o alerta novamente.
3. Indique o status selecionando **Editar status** e altere o status para um dos seguintes:
 - Descartado: se você suspeitar que a atividade não é um ataque de ransomware, altere o status para Descartado.



Depois de rejeitar um ataque, você não pode alterá-lo de volta. Se você descartar uma carga de trabalho, todas as cópias de snapshot feitas automaticamente em resposta ao possível ataque de ransomware serão excluídas permanentemente. Se você ignorar o alerta, o exercício de prontidão será considerado concluído.

- Resolvido: O incidente foi atenuado.

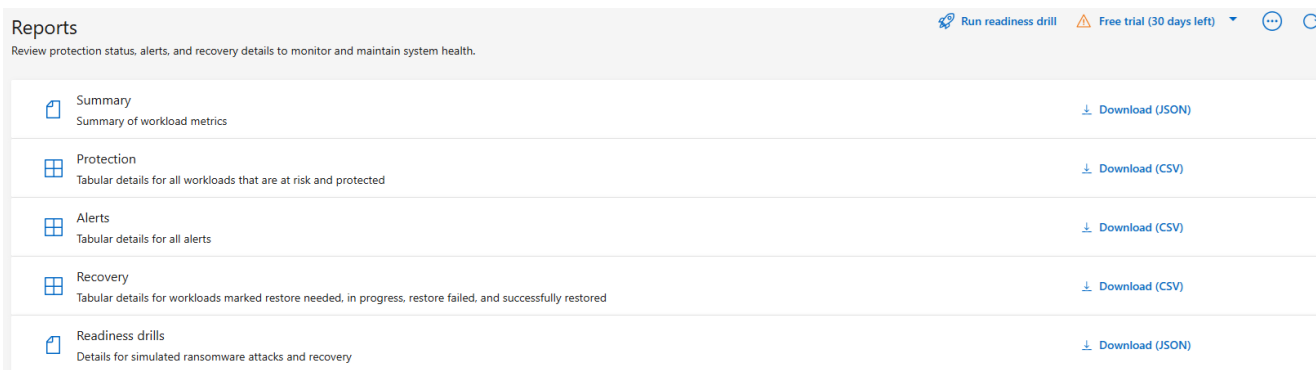
Relatórios de revisão sobre o exercício de prontidão

Após a conclusão do exercício de prontidão, talvez você queira revisar e salvar um relatório sobre o exercício.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Passos

1. No menu Resiliência contra Ransomware, selecione **Relatórios**.



2. Selecione **Exercícios de prontidão** e **Baixar** para baixar o relatório do exercício de prontidão.

Configurar as definições de proteção no NetApp Ransomware Resilience

Na guia de configurações de NetApp Ransomware Resilience, você pode configurar destinos de backup, realizar um exercício de preparação para ataques, configurar a descoberta de cargas de trabalho ou configurar a detecção de atividades suspeitas do usuário.


Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

O que você pode fazer na página Configurações? Na página Configurações, você pode fazer o seguinte:

- Simule um ataque de ransomware realizando um exercício de prontidão e respondendo a um alerta simulado de ransomware. Para obter detalhes, consulte ["Realizar um exercício de preparação para ataques de ransomware"](#).
- Configurar descoberta de carga de trabalho.
- Configure o relatório de atividades suspeitas do usuário. Para mais informações, consulte ["Atividade suspeita do usuário"](#).
- Adicione um destino de backup.
- Conecte seu sistema de gerenciamento de eventos e segurança (SIEM) para análise e detecção de ameaças. Habilitar a detecção de ameaças envia automaticamente dados para o seu SIEM para análise de ameaças. Para mais informações, consulte ["Conecte NetApp Ransomware Resilience a um SIEM"](#).

Acesse a página Configurações diretamente

Você pode acessar facilmente a página Configurações na opção Ações, próxima ao menu superior.

1. Em Resiliência de Ransomware, selecione a vertical  ... opção no canto superior direito.
2. No menu suspenso, selecione **Configurações**.

Simule um ataque de ransomware

Realize um exercício de preparação para ransomware simulando um ataque de ransomware em uma carga de trabalho de amostra recém-criada. Em seguida, investigue o ataque simulado e recupere a carga de trabalho de amostra. Esse recurso ajuda você a saber se está preparado no caso de um ataque real de ransomware, testando processos de notificação de alerta, resposta e recuperação. Você pode executar um exercício de prontidão para ransomware várias vezes.

Para mais detalhes, consulte ["Realizar um exercício de preparação para ataques de ransomware"](#).

Configurar descoberta de carga de trabalho

Você pode configurar a descoberta de carga de trabalho para descobrir automaticamente novas cargas de trabalho em seu ambiente.

1. Na página Configurações, localize o bloco **Descoberta de carga de trabalho**.
2. No bloco **Descoberta de carga de trabalho**, selecione **Descobrir cargas de trabalho**.

Esta página mostra agentes do Console com sistemas que não foram selecionados anteriormente, agentes do Console recentemente disponíveis e sistemas recentemente disponíveis. Esta página não mostra os sistemas que foram selecionados anteriormente.

3. Selecione o agente do Console onde você deseja descobrir cargas de trabalho.
4. Revise a lista de sistemas.
5. Marque os sistemas nos quais você deseja descobrir cargas de trabalho ou selecione a caixa na parte superior da tabela para descobrir cargas de trabalho em todos os ambientes de carga de trabalho descobertos.
6. Faça isso para outros sistemas, conforme necessário.
7. Selecione **Descobrir** para que o Ransomware Resilience descubra automaticamente novas cargas de trabalho no agente do Console selecionado.



No cartão de descoberta de cargas de trabalho em Configurações, selecione o menu de ações. ... Em seguida, **Baixe o relatório (JSON)** para revisar uma lista de cargas de trabalho suportadas e não suportadas em seus sistemas.

Adicionar um destino de backup

O Ransomware Resilience pode identificar cargas de trabalho que ainda não têm backups e também cargas de trabalho que ainda não têm destinos de backup atribuídos.

Para proteger essas cargas de trabalho, você deve adicionar um destino de backup. Você pode escolher um dos seguintes destinos de backup:

- NetApp StorageGRID
- Serviços Web da Amazon (AWS)
- Plataforma Google Cloud
- Microsoft Azure



Os destinos de backup não estão disponíveis para cargas de trabalho no Amazon FSx for NetApp ONTAP nem no Azure NetApp Files. Realize operações de backup usando soluções de backup nativas: FSx for ONTAP backup service ou Azure NetApp Files backupss.

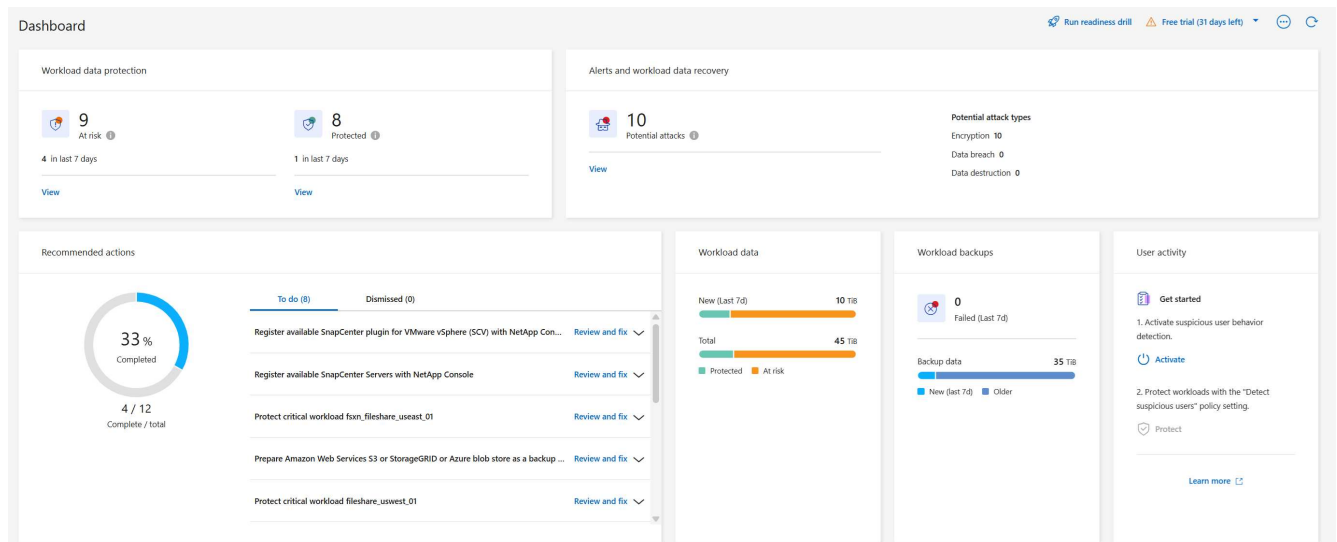
Você pode adicionar um destino de backup com base em uma ação recomendada no Painel ou acessando a opção Configurações no menu.

Acesse as opções de destino de backup nas ações recomendadas do painel

O Painel fornece muitas recomendações. Uma recomendação pode ser configurar um destino de backup.

Passos

1. No painel Resiliência de Ransomware, revise o painel Ações recomendadas.



2. No Painel, selecione **Revisar e corrigir** para a recomendação de "Preparar <provedor de backup> como destino de backup".
3. Continue com as instruções dependendo do provedor de backup.

Adicionar StorageGRID como destino de backup

Para configurar o NetApp StorageGRID como um destino de backup, insira as seguintes informações.

Passos


1. Na página **Configurações > Destinos de backup**, selecione **Adicionar**.
2. Digite um nome para o destino do backup.

Add backup destination


Name
ⓘ Action required
⌵

Provider ⌵


Select a provider to back up to the cloud.




Amazon Web Services



Microsoft Azure



Google Cloud Platform



StorageGRID

3. Selecione * StorageGRID*.

4. Selecione a seta para baixo ao lado de cada configuração e insira ou selecione valores:

◦ **Configurações do provedor:**

- Crie um novo bucket ou traga seu próprio bucket que armazenará os backups.
- Nome de domínio totalmente qualificado do nó do gateway StorageGRID , porta, chave de acesso do StorageGRID e credenciais de chave secreta.

◦ **Rede:** Escolha o IPspace.






- O IPspace é o cluster onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.

5. Selecione **Adicionar**.

Resultado

O novo destino de backup é adicionado à lista de destinos de backup.

Settings > Backup destinations

Backup destinations							
Backup destinations (5)							
Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
	netapp-backup-vsavhok7dpp	us-east-1	n/a	Default	None	VsaWorkingEnvironment-VHAK7DPp	Backup and Recovery
	netapp-backup-vsac2gmsuu	us-east-1	n/a	Default	None	VsaWorkingEnvironment-C2Gmsuu	Backup and Recovery
	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuoO50z	Ransomware Resilience
	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuoO50z	Ransomware Resilience
	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuoO50z	Ransomware Resilience

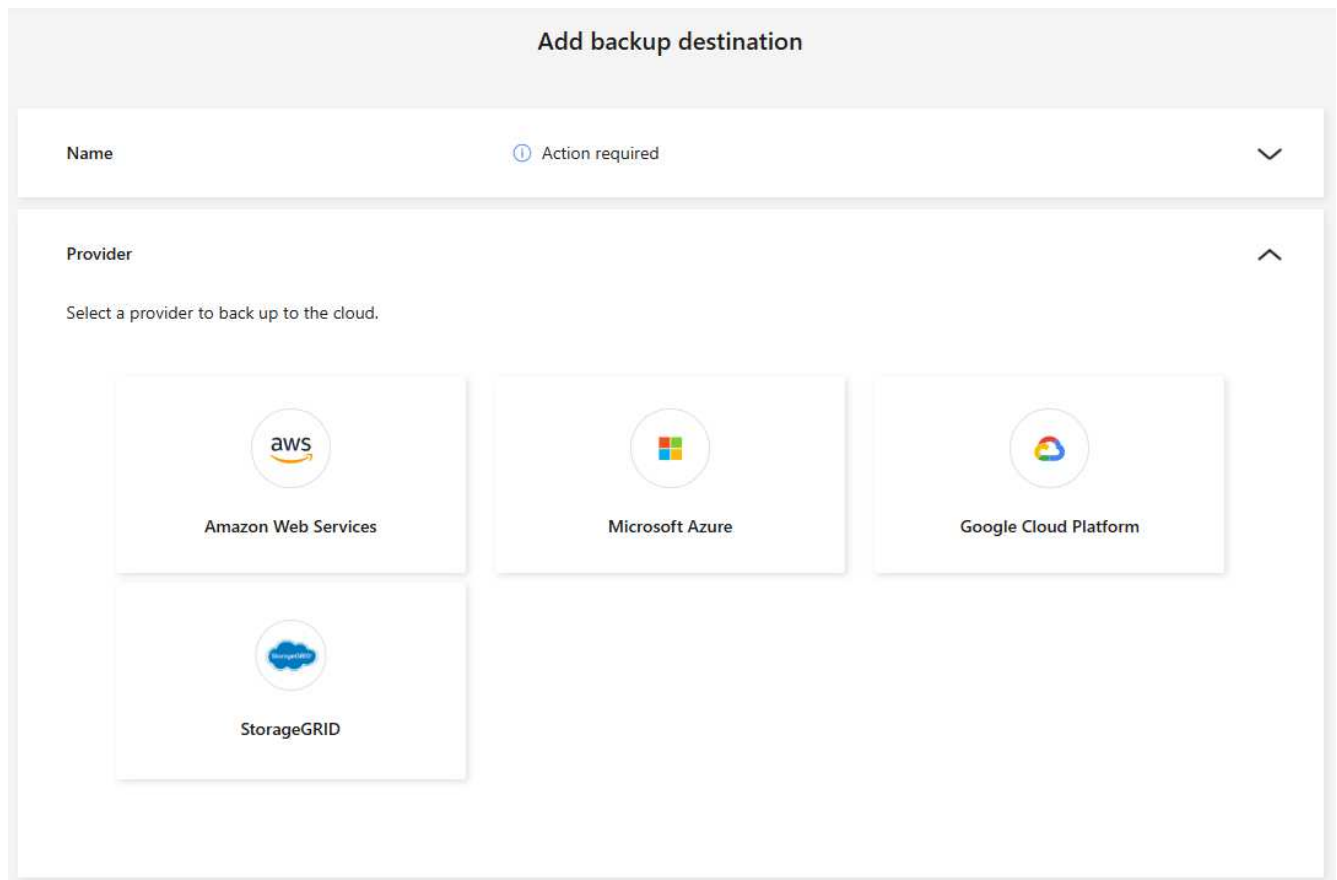
Adicionar Amazon Web Services como destino de backup

Para configurar a AWS como destino de backup, insira as seguintes informações.

Para obter detalhes sobre como gerenciar seu armazenamento do AWS no Console, consulte "[Gerencie seus buckets do Amazon S3](#)".

Passos

1. Na página **Configurações > Destinos de backup**, selecione **Adicionar**.
2. Digite um nome para o destino de backup.



3. Selecione **Amazon Web Services**.
4. Selecione a seta para baixo ao lado de cada configuração e insira ou selecione valores:
 - **Configurações do provedor:**
 - Crie um novo bucket, selecione um bucket existente se já houver um no Console ou traga seu próprio bucket que armazenará os backups.
 - Conta AWS, região, chave de acesso e chave secreta para credenciais AWS
 - **Criptografia:** Se você estiver criando um novo bucket S3, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis.

"Se você quiser trazer seu próprio bucket, consulte [Adicionar buckets S3](#)".

Os dados no bucket são criptografados com chaves gerenciadas pela AWS por padrão. Você pode continuar usando chaves gerenciadas pela AWS ou pode gerenciar a criptografia dos seus dados

usando suas próprias chaves.

- **Rede:** Escolha o espaço IP e se você usará um ponto de extremidade privado.
 - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
 - Opcionalmente, escolha se você usará um endpoint privado da AWS (PrivateLink) que você configurou anteriormente.

Se você quiser usar o AWS PrivateLink, consulte ["AWS PrivateLink para Amazon S3"](#) .

- **Bloqueio de backup:** escolha se deseja que o Ransomware Resilience proteja os backups contra modificações ou exclusão. Esta opção usa a tecnologia NetApp DataLock. Cada backup será bloqueado durante o período de retenção, ou por um mínimo de 30 dias, mais um período de buffer de até 14 dias.



Se você configurar a configuração de bloqueio de backup agora, não poderá alterá-la depois que o destino do backup for configurado.

- **Modo de governança:** Usuários específicos (com permissão s3:BypassGovernanceRetention) podem substituir ou excluir arquivos protegidos durante o período de retenção.
- **Modo de conformidade:** Os usuários não podem substituir ou excluir arquivos de backup protegidos durante o período de retenção.

5. Selecione **Adicionar**.

Resultado

O novo destino de backup é adicionado à lista de destinos de backup.

Backup destinations							
Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by
aws	netapp-backup-vsavrhk7dpp	us-east-1	n/a	Default	None	VisaWorkingEnvironment-VHAK7DPP	Backup and Recovery
aws	netapp-backup-vsac2gmsuu	us-east-1	n/a	Default	None	VisaWorkingEnvironment-C2Gmsuu	Backup and Recovery
aws	netapp-backup-vsajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
aws	netapp-backup-vsajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience
aws	netapp-backup-vsajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience

Adicionar o Google Cloud Platform como destino de backup

Para configurar o Google Cloud Platform (GCP) como destino de backup, insira as seguintes informações.

Para obter detalhes sobre como gerenciar seu armazenamento do GCP no Console, consulte ["Opções de instalação do agente de console no Google Cloud"](#) .

Passos

1. Na página **Configurações > Destinos de backup**, selecione **Adicionar**.
2. Digite um nome para o destino do backup.
3. Selecione **Google Cloud Platform**.
4. Selecione a seta para baixo ao lado de cada configuração e insira ou selecione valores:
 - **Configurações do provedor:**

- Crie um novo bucket. Digite a chave de acesso e a chave secreta.
- Insira ou selecione seu projeto e região do Google Cloud Platform.

Add backup destination

Name
✓ gcp-backup
⌵

Provider
✓ Google Cloud Platform
⌵

Provider settings ⌵

☒ Create new bucket
 ☐ Bring your own bucket

Netapp ransomware resilience will create the bucket in your provider environment.

Google Cloud Platform credentials

Access key

Secret key

Google Cloud Platform details

Project

Region

Encryption
✓ Google-managed key
⌵

Backup lock
⚠ Not supported
⌵

- **Criptografia:** Se você estiver criando um novo bucket, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolher um bucket existente, as informações de criptografia já estarão disponíveis.

Os dados no bucket são criptografados com chaves gerenciadas pelo Google por padrão. Você pode continuar usando as chaves gerenciadas pelo Google.

- **Rede:** Escolha o espaço IP e se você usará um ponto de extremidade privado.
 - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
 - Opcionalmente, escolha se você usará um ponto de extremidade privado do GCP (PrivateLink) que você configurou anteriormente.

5. Selecione **Adicionar**.

Resultado

O novo destino de backup é adicionado à lista de destinos de backup.

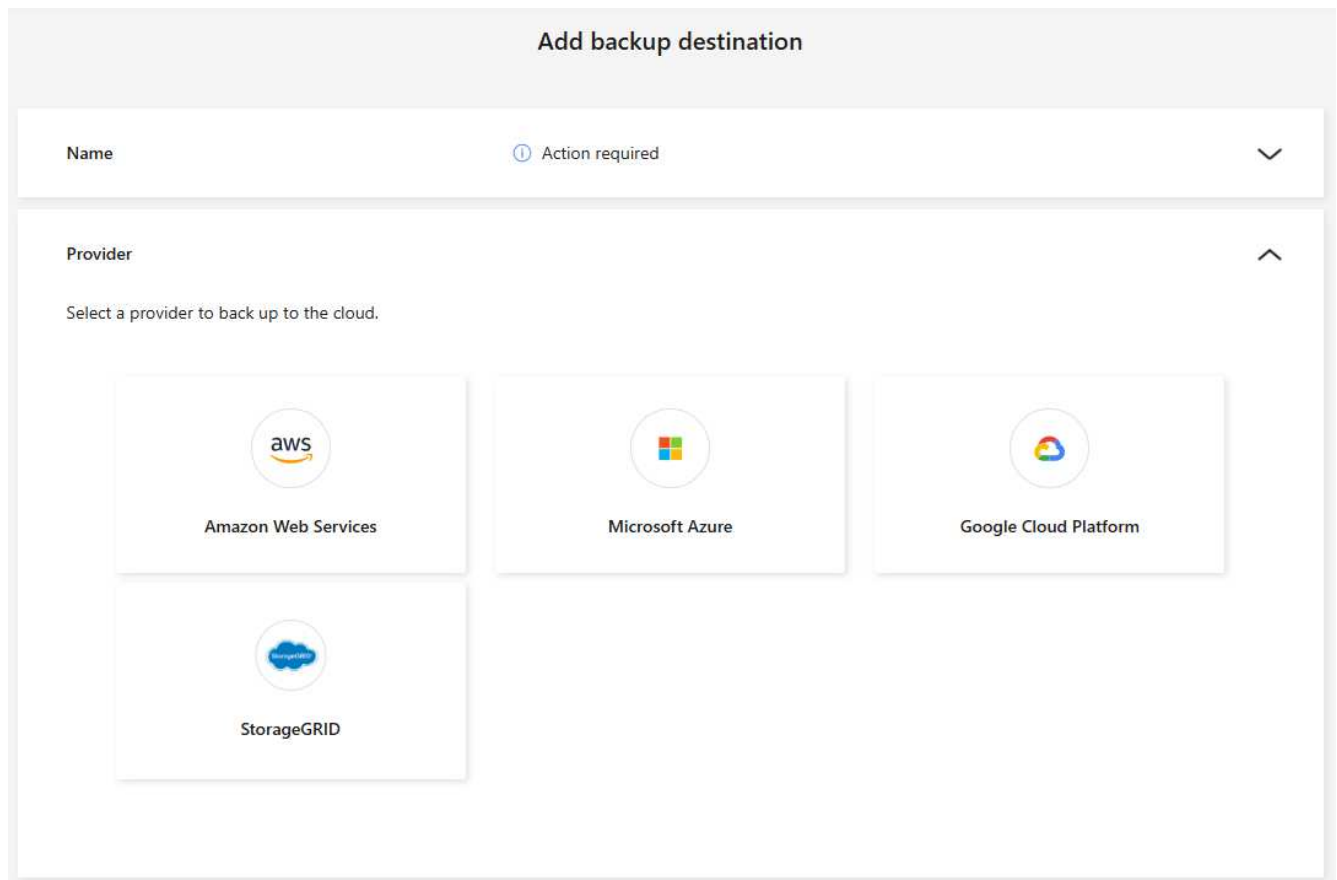
Adicionar o Microsoft Azure como destino de backup

Para configurar o Azure como um destino de backup, insira as seguintes informações.

Para obter detalhes sobre como gerenciar suas credenciais do Azure e assinaturas do marketplace no Console, consulte ["Gerencie suas credenciais do Azure e assinaturas do marketplace"](#).

Passos

1. Na página **Configurações > Destinos de backup**, selecione **Adicionar**.
2. Digite um nome para o destino do backup.



3. Selecione **Azure**.
4. Selecione a seta para baixo ao lado de cada configuração e insira ou selecione valores:
 - **Configurações do provedor:**
 - Crie uma nova conta de armazenamento, selecione uma existente se já houver uma no Console ou traga sua própria conta de armazenamento que armazenará os backups.
 - Assinatura, região e grupo de recursos do Azure para credenciais do Azure

["Se você quiser trazer sua própria conta de armazenamento, consulte Adicionar contas de armazenamento de Blobs do Azure"](#).
 - **Criptografia:** Se você estiver criando uma nova conta de armazenamento, insira as informações da chave de criptografia fornecidas pelo provedor. Se você escolheu uma conta existente, as informações de criptografia já estarão disponíveis.

Os dados na conta são criptografados com chaves gerenciadas pela Microsoft por padrão. Você pode

continuar usando chaves gerenciadas pela Microsoft ou pode gerenciar a criptografia dos seus dados usando suas próprias chaves.






- **Rede:** Escolha o espaço IP e se você usará um ponto de extremidade privado.
 - O IPspace é o cluster onde residem os volumes que você deseja fazer backup. Os LIFs intercluster para este IPspace devem ter acesso de saída à Internet.
 - Opcionalmente, escolha se você usará um ponto de extremidade privado do Azure que você configurou anteriormente.

Se você quiser usar o Azure PrivateLink, consulte "[Link Privado do Azure](#)".

5. Selecione **Adicionar**.

Resultado

O novo destino de backup é adicionado à lista de destinos de backup.

Backup destinations									
Backup destinations (5)									
Provider	Name	Region	Encryption	IP space	Backup lock	Systems	Created by		
	netapp-backup-viaahk7dpp	us-east-1	n/a	Default	None	ViaWorkingEnvironment-VHk7Dpp	Backup and Recovery		
	netapp-backup-viaclgmsusu	us-east-1	n/a	Default	None	ViaWorkingEnvironment-C2Gmsusu	Backup and Recovery		
	netapp-backup-viajgd1	us-east-1	n/a	Default	Compliance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience		
	netapp-backup-viajgd2	us-east-1	n/a	Default	None	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience		
	netapp-backup-viajgd3	us-east-1	n/a	Default	Governance mode	OnPremWorkingEnvironment-uDuo050z	Ransomware Resilience		

Conecte NetApp Ransomware Resilience ao sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças

Você pode enviar automaticamente dados do NetApp Ransomware Resilience para o seu sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças.

Ransomware Resilience é compatível com os seguintes SIEMs:

- AWS Security Hub
- Microsoft Sentinel
- Splunk Cloud

Antes de habilitar o SIEM no Ransomware Resilience, você precisa configurar seu sistema SIEM.

Dados de eventos enviados para um SIEM

O Ransomware Resilience pode enviar os seguintes dados de eventos para o seu sistema SIEM:

- **contexto:**
 - **os:** Esta é uma constante com o valor de ONTAP.
 - **os_version:** A versão do ONTAP em execução no sistema.

- **connector_id**: O ID do agente do Console que gerencia o sistema.
- **cluster_id**: O ID do cluster relatado pelo ONTAP para o sistema.
- **svm_name**: O nome do SVM onde o alerta foi encontrado.
- **volume_name**: O nome do volume no qual o alerta é encontrado.
- **volume_id**: O ID do volume relatado pelo ONTAP para o sistema.
- **incidente**:
 - **incident_id**: O ID do incidente gerado pelo Ransomware Resilience para o volume sob ataque no Ransomware Resilience.
 - **alert_id**: O ID gerado pelo Ransomware Resilience para a carga de trabalho.
 - **gravidade**: Um dos seguintes níveis de alerta: "CRÍTICO", "ALTO", "MÉDIO", "BAIXO".
 - **description**: Detalhes sobre o alerta que foi detectado, por exemplo, "Um possível ataque de ransomware detectado na carga de trabalho arp_learning_mode_test_2630"

Configurar o AWS Security Hub para detecção de ameaças

Antes de habilitar o AWS Security Hub em NetApp Ransomware Resilience, você precisa executar as seguintes etapas gerais no AWS Security Hub:

- Configure permissões no AWS Security Hub.
- Configure a chave de acesso de autenticação e a chave secreta no AWS Security Hub. (Essas etapas não são fornecidas aqui.)

Etapas para configurar permissões no AWS Security Hub

1. Acesse o **console do AWS IAM**.
2. Selecione **Políticas**.
3. Crie uma política usando o seguinte código no formato JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "NetAppSecurityHubFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchImportFindings",
        "securityhub:BatchUpdateFindings"
      ],
      "Resource": [
        "arn:aws:securityhub:*:*:product/*/default",
        "arn:aws:securityhub:*:*:hub/default"
      ]
    }
  ]
}
```

Configurar o Microsoft Sentinel para detecção de ameaças

Antes de habilitar o Microsoft Sentinel em NetApp Ransomware Resilience, você precisa executar as seguintes etapas gerais no Microsoft Sentinel:

- **Pré-requisitos**

- Ativar o Microsoft Sentinel.
- Crie uma função personalizada no Microsoft Sentinel.

- **Inscrição**

- Registre o Ransomware Resilience para receber eventos do Microsoft Sentinel.
- Crie um segredo para o registro.

- **Permissões:** Atribua permissões ao aplicativo.

- **Autenticação:** Insira as credenciais de autenticação para o aplicativo.

Etapas para habilitar o Microsoft Sentinel

1. Acesse o Microsoft Sentinel.
2. Crie um **espaço de trabalho do Log Analytics**.
3. Habilite o Microsoft Sentinel para usar o espaço de trabalho do Log Analytics que você acabou de criar.

Etapas para criar uma função personalizada no Microsoft Sentinel

1. Acesse o Microsoft Sentinel.
2. Selecione **Assinatura > Controle de acesso (IAM)**.
3. Insira um nome de função personalizado. Use o nome **Ransomware Resilience Sentinel Configurator**.
4. Copie o seguinte JSON e cole-o na aba **JSON**.

```
{
  "roleName": "Ransomware Resilience Sentinel Configurator",
  "description": "",
  "assignableScopes": ["/subscriptions/{subscription_id}"],
  "permissions": [

  ]
}
```

5. Revise e salve suas configurações.

Etapas para registrar o Ransomware Resilience para receber eventos do Microsoft Sentinel

1. Acesse o Microsoft Sentinel.
2. Selecione **Entra ID > Aplicativos > Registros de aplicativos**.
3. Para o **Nome de exibição** do aplicativo, digite **"Resiliência ao Ransomware"**.
4. No campo **Tipo de conta compatível**, selecione **Contas somente neste diretório organizacional**.
5. Selecione um **Índice Padrão** onde os eventos serão enviados.
6. Selecione **Revisar**.

7. Selecione **Registrar** para salvar suas configurações.

Após o registro, o centro de administração do Microsoft Entra exibe o painel Visão geral do aplicativo.

Etapas para criar um segredo para o registro

1. Acesse o Microsoft Sentinel.
2. Selecione **Certificados e segredos > Segredos do cliente > Novo segredo do cliente**.
3. Adicione uma descrição para o segredo do seu aplicativo.
4. Selecione uma **Expiração** para o segredo ou especifique um tempo de vida personalizado.



A vida útil do segredo do cliente é limitada a dois anos (24 meses) ou menos. A Microsoft recomenda que você defina um valor de expiração inferior a 12 meses.

5. Selecione **Adicionar** para criar seu segredo.
6. Registre o segredo a ser usado na etapa de Autenticação. O segredo nunca mais será exibido depois que você sair desta página.

Etapas para atribuir permissões ao aplicativo

1. Acesse o Microsoft Sentinel.
2. Selecione **Assinatura > Controle de acesso (IAM)**.
3. Selecione **Adicionar > Adicionar atribuição de função**.
4. Para o campo **Funções de administrador privilegiado**, selecione **Configurador do Ransomware Resilience Sentinel**.



Esta é a função personalizada que você criou anteriormente.

5. Selecione **Avançar**.
6. No campo **Atribuir acesso a**, selecione **Usuário, grupo ou entidade de serviço**.
7. Selecione **Selecionar membros**. Em seguida, selecione **Ransomware Resilience Sentinel Configurador**.
8. Selecione **Avançar**.
9. No campo **O que o usuário pode fazer**, selecione **Permitir que o usuário atribua todas as funções, exceto as funções de administrador privilegiado Proprietário, UAA, RBAC (recomendado)**.
10. Selecione **Avançar**.
11. Selecione **Revisar e atribuir** para atribuir as permissões.

Etapas para inserir credenciais de autenticação para o aplicativo

1. Acesse o Microsoft Sentinel.
2. Insira as credenciais:
 - a. Insira o ID do locatário, o ID do aplicativo cliente e o segredo do aplicativo cliente.
 - b. Clique em **Autenticar**.



Após a autenticação ser bem-sucedida, uma mensagem "Autenticado" será exibida.

3. Insira os detalhes do espaço de trabalho do Log Analytics para o aplicativo.
 - a. Selecione o ID da assinatura, o grupo de recursos e o espaço de trabalho do Log Analytics.

Configurar o Splunk Cloud para detecção de ameaças

Antes de habilitar o Splunk Cloud no Ransomware Resilience, você precisará seguir as seguintes etapas de alto nível no Splunk Cloud:

- Habilite um Coletor de Eventos HTTP no Splunk Cloud para receber dados de eventos via HTTP ou HTTPS do Console.
- Crie um token do Event Collector no Splunk Cloud.

Etapas para habilitar um coletor de eventos HTTP no Splunk

1. Acesse o Splunk Cloud.
2. Selecione **Configurações > Entradas de dados**.
3. Selecione **Coletor de Eventos HTTP > Configurações Globais**.
4. Na alternância Todos os tokens, selecione **Ativado**.
5. Para que o Coletor de Eventos escute e se comunique por HTTPS em vez de HTTP, selecione **Ativar SSL**.
6. Insira uma porta em **Número da porta HTTP** para o Coletor de eventos HTTP.

Etapas para criar um token do Event Collector no Splunk


1. Acesse o Splunk Cloud.
2. Selecione **Configurações > Adicionar dados**.
3. Selecione **Monitor > Coletor de Eventos HTTP**.
4. Digite um nome para o token e selecione **Avançar**.
5. Selecione um **Índice Padrão** onde os eventos serão enviados e, em seguida, selecione **Revisar**.
6. Confirme se todas as configurações do ponto de extremidade estão corretas e selecione **Enviar**.
7. Copie o token e cole-o em outro documento para deixá-lo pronto para a etapa de Autenticação.

Conecte o SIEM na resiliência do ransomware

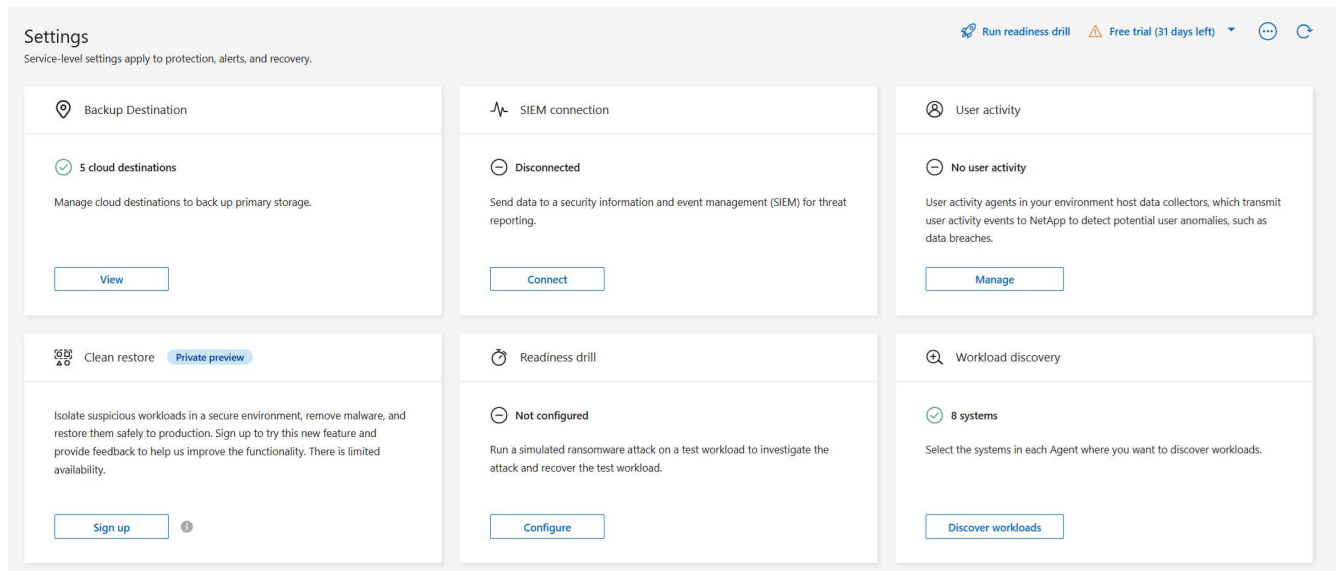
A ativação do SIEM envia dados do Ransomware Resilience para seu servidor SIEM para análise e geração de relatórios de ameaças.

Passos

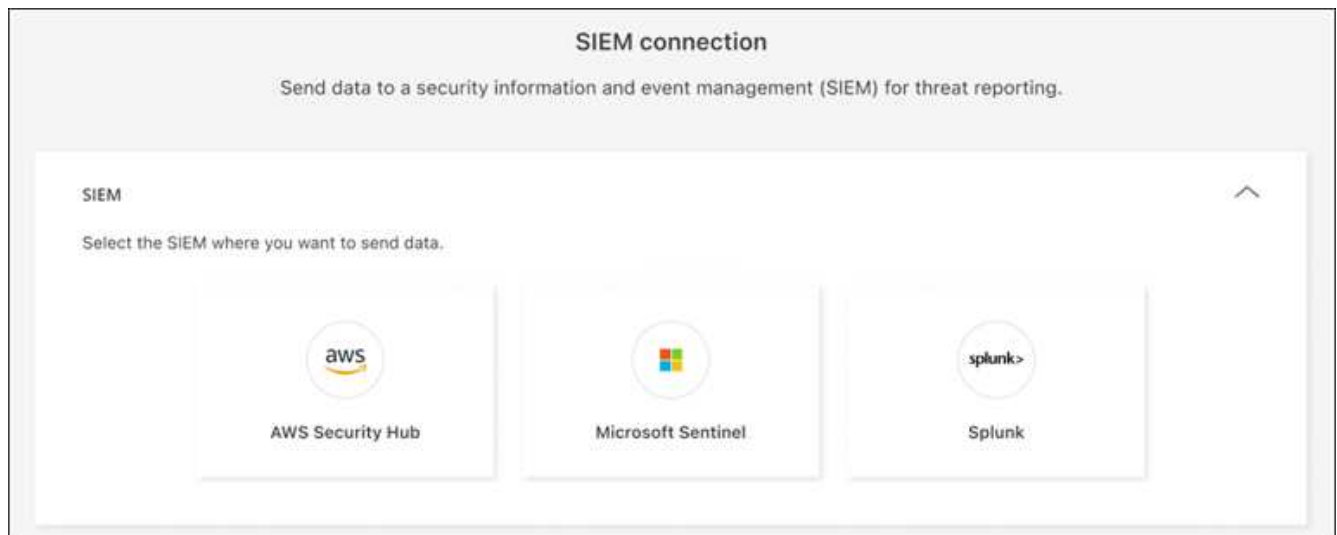
1. No menu Console, selecione **Proteção > Resiliência ao Ransomware**.
2.

No menu Resiliência do Ransomware, selecione a vertical  ... opção no canto superior direito.
3. Selecione **Configurações**.

A página Configurações é exibida.



4. Na página Configurações, selecione **Conectar** no bloco de conexão SIEM.



5. Escolha um dos sistemas SIEM.

6. Insira o token e os detalhes de autenticação que você configurou no AWS Security Hub ou no Splunk Cloud.



As informações inseridas dependem do SIEM selecionado.

7. Selecione **Ativar**.

A página Configurações mostra "Conectado".

Configurar detecção de atividade do usuário

Aprenda sobre detecção de atividade do usuário em NetApp Ransomware Resilience

NetApp Ransomware Resilience oferece suporte à detecção de comportamentos suspeitos do usuário, permitindo que você lide com incidentes de ransomware no nível do usuário.

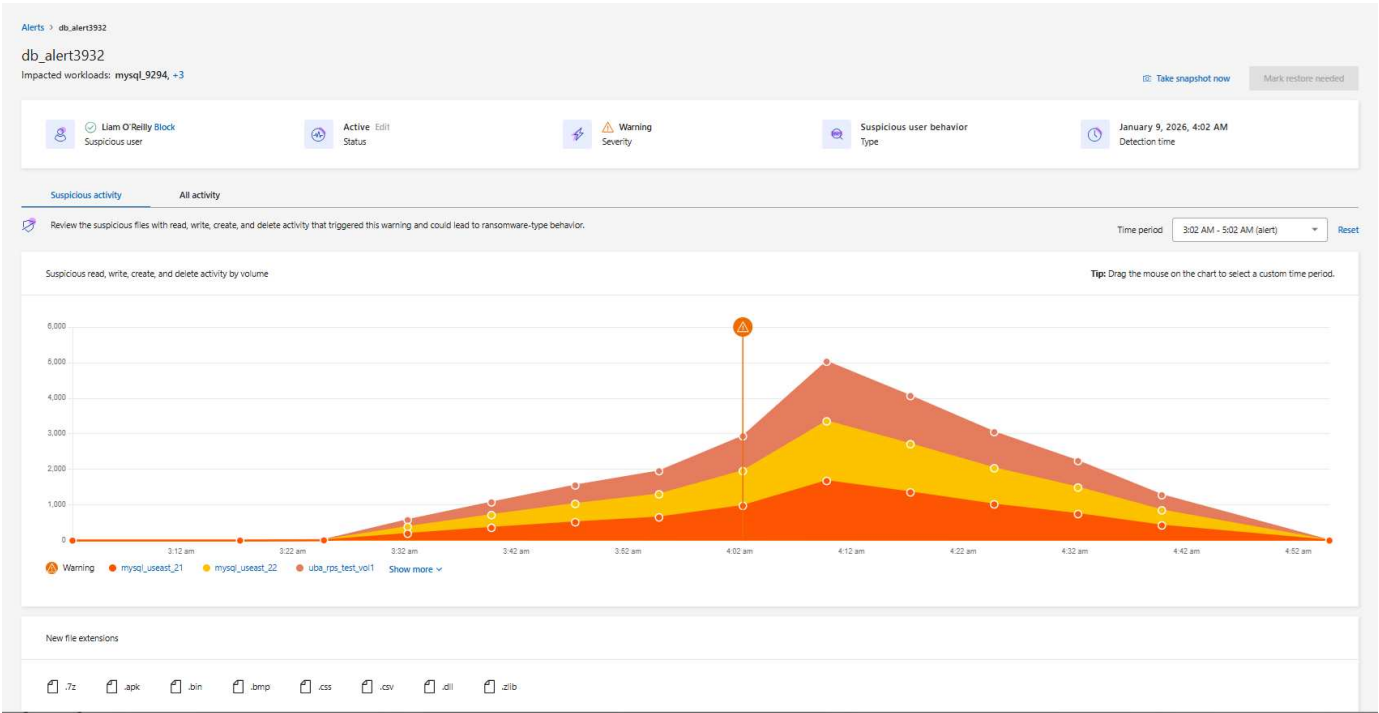
NetApp Ransomware Resilience oferece uma detecção de violação de dados baseada em IA ao monitorar atividades suspeitas do usuário. Aumentos acentuados na atividade de leitura e nos padrões de acesso de leitura são usados para determinar intenção maliciosa. Uma vez detectado, o Ransomware Resilience gera alertas automaticamente no NetApp Console, por e-mail e em qualquer ecossistema de segurança configurado (por exemplo, SIEM).

Com a detecção e alerta de comportamentos suspeitos de usuários, o Ransomware Resilience alerta você sobre tentativas de violação e destruição de dados e padrões que parecem suspeitos. Em cada alerta, o Ransomware Resilience identifica um usuário que você pode bloquear.

O Ransomware Resilience detecta atividades suspeitas do usuário analisando eventos de atividade do usuário gerados pelo FPolicy no ONTAP. Para coletar dados de atividade do usuário, você precisa implantar um ou mais agentes de atividade do usuário. O agente é um servidor Linux ou VM com conectividade com dispositivos no seu localatário.

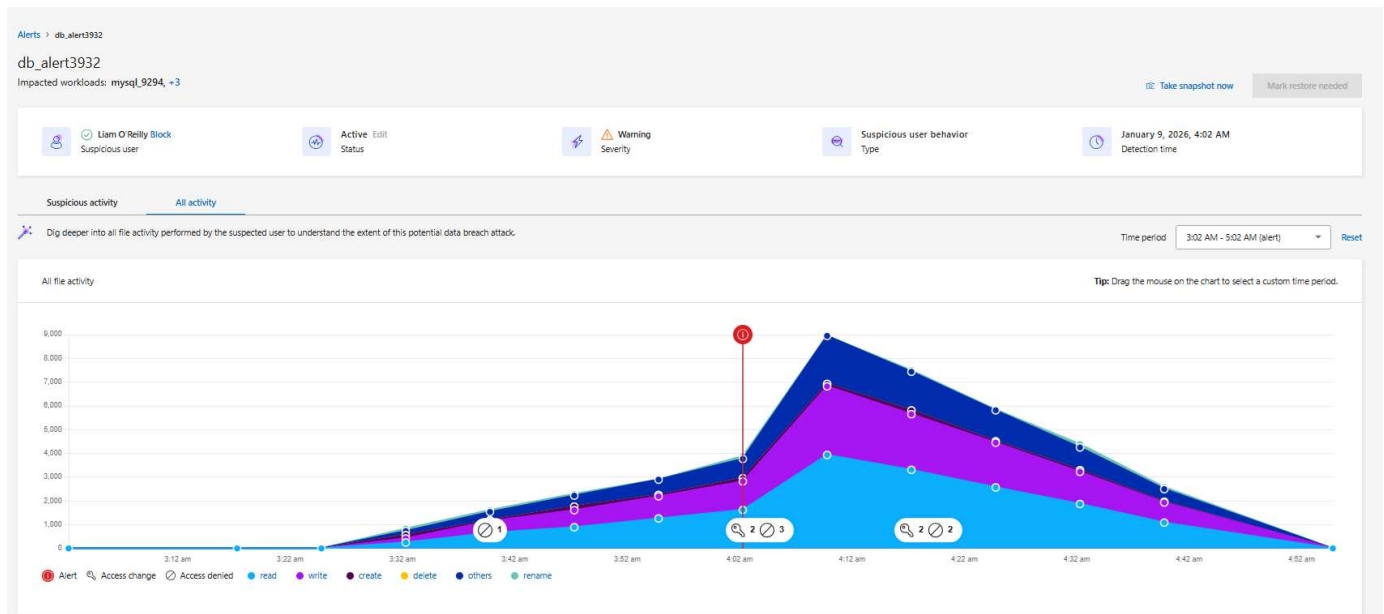
Análise forense de atividades suspeitas de usuário

Ransomware Resilience oferece análises forenses para comportamentos do usuário: listas e gráficos que mostram quando ocorreu atividade suspeita e quando as notificações foram enviadas. Esses detalham a frequência de atividade suspeita em arquivos, diretórios, volumes e cargas de trabalho ao longo do tempo para ajudar a mapear os eventos. Você também pode observar o surgimento de novas extensões de arquivo.



Você pode comparar atividades suspeitas com uma visão de todas as atividades. Na visualização de todas as atividades, você pode observar eventos de leitura, gravação, renomeação, movimentação, criação e exclusão,

além de eventos de alteração de acesso e acesso negado.



Componentes

Existem três componentes principais na detecção de atividades suspeitas de comportamento do usuário em Ransomware Resilience.

- O **agente de atividade do usuário** é um ambiente executável para coletores de dados. Você deve configurar o agente de atividade do usuário.
- O **coletor de dados** compartilha eventos de atividade do usuário com o Ransomware Resilience. O coletor de dados é criado automaticamente quando você [Habilite uma estratégia de proteção contra ransomware com detecção de atividade suspeita do usuário](#).
- O **conector de diretório de usuários** permite o mapeamento entre nomes de usuário e IDs de usuário, proporcionando maior clareza ao responder a comportamentos suspeitos de usuários. Você deve configurar o conector de diretório de usuários.

Ransomware Resilience e Data Infrastructure Insights

A detecção de comportamento suspeito do usuário do Ransomware Resilience é uma integração com Data Infrastructure Insights (DII) Workload Security e utiliza ["Endpoints DII"](#). Você não precisa de nenhuma configuração do DII para habilitar a detecção de comportamento do usuário no Ransomware Resilience. Para habilitar a detecção de comportamento do usuário, ["crie os agentes e coletores necessários e ative a estratégia de proteção contra ransomware adequada"](#).

Se você já utiliza NetApp Data Infrastructure Insights (DII) Workload Security, é recomendável usar os mesmos agentes do Workload Security para Ransomware Resilience. Você não precisa implantar agentes separados do Workload Security para Ransomware Resilience, porém, o uso dos mesmos agentes do Workload Security requer um relacionamento de pareamento entre a organização do Ransomware Resilience Console e o tenant do DII Storage Workload Security. Entre em contato com seu representante de conta para habilitar esse pareamento.

Próximos passos

- ["Requisitos para detecção de atividade de comportamento do usuário"](#)
- ["Configurar agentes e detectores de atividade de comportamento do usuário"](#)

Requisitos para detecção de comportamento do usuário em NetApp Ransomware Resilience

Antes de criar um agente de atividade do usuário e outros coletores, você deve garantir que atende aos requisitos de sistema operacional, servidor e rede descritos.

Suporte do provedor de nuvem

Suporte a provedores de nuvem

Dados suspeitos de atividades do usuário podem ser armazenados na AWS e no Azure nas seguintes regiões:

Provedor de nuvem	Região
AWS	<ul style="list-style-type: none">• Ásia-Pacífico (Sydney) (ap-sudeste-2)• Europa (Frankfurt) (eu-central-1)• Leste dos EUA (Norte da Virgínia) (us-east-1)
Azul	Leste dos EUA

Requisitos do sistema operacional

A detecção de comportamentos suspeitos do usuário é compatível com os seguintes sistemas operacionais:

Sistema operacional	Versões suportadas
Alma Linux	9.4 (64 bits) a 9.5 (64 bits) e 10 (64 bits), incluindo SELinux
CentOS	CentOS Stream 9 (64 bits)
Debian	11 (64 bits), 12 (64 bits), incluindo SELinux
OpenSUSE Leap	15.3 (64 bits) a 15.6 (64 bits)
Oracle Linux	8.10 (64 bits) e 9.1 (64 bits) até 9.6 (64 bits), incluindo SELinux
Chapéu Vermelho	8.10 (64 bits), 9.1 (64 bits) até 9.6 (64 bits) e 10 (64 bits), incluindo SELinux
Rochoso	Rocky 9.4 (64 bits) até 9.6 (64 bits), incluindo SELinux
SUSE Enterprise Linux	15 SP4 (64 bits) a 15 SP6 (64 bits), incluindo SELinux
Ubuntu	20,04 LTS (64 bits), 22,04 LTS (64 bits) e 24,04 LTS (64 bits)



A máquina que você usa para o agente de atividade do usuário não deve estar executando nenhum outro software de nível de aplicativo. Um servidor dedicado é recomendado.

O `unzip` É necessário um comando para a instalação. O `sudo su` - O comando é necessário para instalação, execução de scripts e desinstalação.

Requisitos do servidor

O servidor deve atender aos seguintes requisitos mínimos:

- **CPU:** 4 núcleos
- **RAM:** 16 GB de RAM
- **Espaço em disco:** 36 GB de espaço livre em disco

Recomendações do servidor

- Alocar espaço adicional em disco para permitir a criação do sistema de arquivos. Certifique-se de que haja pelo menos 35 GB de espaço livre no sistema de arquivos. + Se `/opt` É uma pasta montada de um armazenamento NAS; os usuários locais devem ter acesso a esta pasta. A criação do agente de atividade do usuário pode falhar se os usuários locais não tiverem as permissões necessárias.
- Recomenda-se instalar o agente de atividade do usuário em um sistema separado do seu ambiente de Ransomware Resilience. Caso opte por instalá-los na mesma máquina, reserve de 50 a 55 GB de espaço de disco. Para Linux, aloque de 25 a 30 GB de espaço para `/opt/netapp` e 25 GB para `var/log/netapp`.
- Recomenda-se sincronizar a hora tanto no sistema ONTAP quanto na máquina do agente de atividade do usuário usando o Protocolo de Tempo de Rede (NTP) ou o Protocolo de Tempo de Rede Simples (SNTP).

regras de acesso à rede em nuvem

Analise as regras de acesso à rede em nuvem para a sua região geográfica (Ásia-Pacífico, Europa ou Estados Unidos).



Durante a instalação inicial, substitua a `<site_name>` por uma permissão de caractere curinga (*). Após o agente ser ativado e estar totalmente operacional, você pode substituir a permissão pelo nome do site. Entre em contato com seu representante da NetApp para obter o nome do site.



O agente de atividade do usuário utiliza a tecnologia NetApp Data Insights Infrastructure, daí o uso de `cloudinsights` endpoints. Para mais informações, consulte

Implantações de agentes de atividade do usuário baseadas em APAC

Protocolo	Porta	Fonte	Destino	Descrição
HTTPS (TCP)	443	Agente de atividade do usuário	<ul style="list-style-type: none"> • <site_name>.cs01-ap-1.cloudinsights.netapp.com/br/ • <site_name>.c01-ap-1.cloudinsights.netapp.com/br/ • <site_name>.c02-ap-1.cloudinsights.netapp.com/br/ • gentlogin.cs01-ap-1.cloudinsights.netapp.com/br/ 	Acesso à resiliência contra ransomware

Implantações de agentes de atividade do usuário baseadas na Europa

Protocolo	Porta	Fonte	Destino	Descrição
HTTPS (TCP)	443	Agente de atividade do usuário	<ul style="list-style-type: none"> • <site_name>.cs01-eu-1.cloudinsights.netapp.com/br/ • <site_name>.c01-eu-1.cloudinsights.netapp.com/br/ • <site_name>.c02-eu-1.cloudinsights.netapp.com/br/ • agentlogin.cs01-eu-1.cloudinsights.netapp.com/br/ 	Acesso à resiliência contra ransomware

Implantações de agentes de atividade do usuário baseados nos EUA

Protocolo	Porta	Fonte	Destino	Descrição
HTTPS (TCP)	443	Agente de atividade do usuário	<ul style="list-style-type: none"> • <site_name>.cs01.cloudinsights.netapp.com/br/ • <site_name>.c01.cloudinsights.netapp.com/br/ • <site_name>.c02.cloudinsights.netapp.com/br/ • agentlogin.cs01.cloudinsights.netapp.com 	Acesso à resiliência contra ransomware

Regras na rede

Protocolo	Porta	Fonte	Destino	Descrição
TCP	389(LDAP) 636 (LDAPs / start-tls)	Agente de atividade do usuário	URL do servidor LDAP	Conectar ao LDAP

Protocolo	Porta	Fonte	Destino	Descrição
HTTPS (TCP)	443	Agente de atividade do usuário	Endereço IP de gerenciamento do cluster ou SVM (dependendo da configuração do coletor SVM)	Comunicação de API com ONTAP
TCP	35000 - 55000	Dados SVM LIF endereços IP	Agente de atividade do usuário	Comunicação do ONTAP para o agente de atividade do usuário para eventos Fpolicy. Essas portas devem ser abertas para o agente de atividade do usuário para que o ONTAP possa enviar eventos a ele, incluindo qualquer firewall no próprio agente de atividade do usuário (se houver). + NOTA: Não é necessário reservar todas essas portas, mas as portas reservadas devem estar dentro desse intervalo. Recomenda-se começar reservando 100 portas e aumentar esse número se necessário.

Protocolo	Porta	Fonte	Destino	Descrição
TCP	35000-55000	IP de gerenciamento de cluster	Agente de atividade do usuário	Comunicação do endereço IP de gerenciamento do cluster ONTAP para o agente de atividade do usuário para eventos EMS . Essas portas devem ser abertas para o agente de atividade do usuário para que o ONTAP possa enviar eventos EMS para ele, incluindo qualquer firewall no próprio agente de atividade do usuário. + NOTA: Não é necessário reservar todas essas portas, mas as portas reservadas devem estar dentro desse intervalo. Recomenda-se começar reservando 100 portas e aumentar esse número se necessário.
SSH	22	Agente de atividade do usuário	Gerenciamento de cluster	Necessário para bloqueio de usuários CIFS/SMB.

Próximo passo

- ["Configurar agentes de atividade do usuário e coletores"](#)

Configurar agentes e coletores para detecção de atividade do usuário em NetApp Ransomware Resilience

Para habilitar a detecção de comportamento suspeito do usuário no NetApp Ransomware Resilience, você precisa instalar pelo menos um agente de atividade do usuário. Ao ativar o recurso de atividade suspeita do usuário no painel do Ransomware Resilience, você precisa fornecer as informações do host do agente de atividade do usuário.

Um agente pode hospedar vários coletores de dados. Os coletores de dados enviam dados para um local SaaS para análise. Existem dois tipos de coletores:

- O **coletor de dados** coleta dados de atividade do usuário do ONTAP.
- O **conector de diretório de usuários** conecta-se ao seu diretório para mapear IDs de usuários a nomes de usuários.

Os coletores são configurados nas configurações de Resiliência de Ransomware.



Se você já utiliza NetApp Data Infrastructure Insights (DII) Workload Security, é recomendável usar os mesmos agentes do Workload Security para Ransomware Resilience. Você não precisa implantar agentes separados do Workload Security para Ransomware Resilience, porém, o uso dos mesmos agentes do Workload Security requer um relacionamento de pareamento entre a organização do Ransomware Resilience Console e o tenant do DII Storage Workload Security. Entre em contato com seu representante de conta para habilitar esse pareamento.

+ Se você ainda não estiver usando DII, siga as instruções de configuração aqui.

Antes de começar

- Certifique-se de cumprir os ["sistema operacional, requisitos de servidor e de rede"](#).

Função de console necessária Para ativar a detecção de atividades suspeitas do usuário, você precisa da **função de administrador da organização**. Para configurações subsequentes de atividades suspeitas do usuário, você precisa da **função de administrador de comportamento do usuário de resiliência a ransomware**. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Garanta que cada função seja aplicada no nível organizacional.

Crie um agente de atividade do usuário

Os agentes de atividade do usuário são ambientes executáveis para ["coletores de dados"](#); coletores de dados compartilham eventos de atividade do usuário com o Ransomware Resilience. Você deve criar pelo menos um agente de atividade do usuário para habilitar a detecção de atividade suspeita do usuário.

Passos

1. Se esta for a primeira vez que você cria um agente de atividade do usuário, acesse o **Painel**. No bloco **Atividade do usuário**, selecione **Ativar**.

Se você estiver adicionando um agente de atividade de usuário adicional, vá para **Configurações**, localize o bloco **Atividade do usuário** e selecione **Gerenciar**. Na tela Atividade do usuário, selecione a aba **Agentes de atividade do usuário** e depois **Adicionar**.

2. Selecione um **Provedor de nuvem** e depois uma **Região**. Selecione **Avançar**.
3. Forneça os detalhes do agente de atividade do usuário:
 - **Nome do agente de atividade do usuário**
 - **Agente de console** - O agente de console deve estar na mesma rede que o agente de atividade do usuário e ter conectividade SSH com o endereço IP do agente de atividade do usuário.
 - **Nome DNS ou endereço IP da VM**
 - **Chave SSH da VM** - Insira a chave SSH usando este formato:

```
-----BEGIN OPENSSH PRIVATE KEY-----
private-key-contents
-----END OPENSSH PRIVATE KEY-----
```

User activity agent name

Select a Console agent located near the user activity agent to minimize latency when transmitting activity to Ransomware Resilience.

Console agent



Select a Console agent



Provide the VM executable environment with "root" access for collectors in this user activity agent.

VM DNS name or IP address

VM SSH key



4. Selecione **Avançar**.
5. Revise suas configurações. Selecione **Ativar** para concluir a adição do agente de atividade do usuário.
6. Confirme se o agente de atividade do usuário foi criado com sucesso. No bloco Atividade do usuário, uma implantação bem-sucedida é exibida como **Running**.

Resultado

Após a criação bem-sucedida do agente de atividade do usuário, retorne ao menu **Configurações** e selecione **Gerenciar** no bloco **Atividade do usuário**. Selecione a guia **Agentes de atividade do usuário** e selecione o agente de atividade do usuário para visualizar detalhes sobre ele, incluindo coletores de dados e conectores de diretório de usuários.

Adicionar um coletor de dados

Os coletores de dados são criados automaticamente quando você ativa uma estratégia de proteção contra ransomware com detecção de atividades suspeitas de usuários. Para mais informações, consulte [adicionar uma política de detecção](#).

Você pode visualizar os detalhes do coletor de dados. Em Configurações, selecione **Gerenciar** no bloco Atividade do usuário. Selecione a aba **Coletor de dados** e selecione o coletor de dados para visualizar seus detalhes ou pausá-lo.

NetApp

Console

Q Search

Organization Account name

Project Project name

10

?

Ransomware Resilience

Settings > User activity > collector_001

collector_svm_001 Pause

Data collector

Running

Status

1.685.0

Version

10.001.00.001

Cluster or storage VM IP address

svm_001

Storage VM

23 days ago

Last reported

ua_agent_001

User activity agent

Workloads (1)

Workload	Type	Importance	Protection status	Detection status	Detection	Other policy sources	Backup destination
fileshare_uswest_03_...	File share	Critical	Protected	Active	2 / 3 enabled		netapp-backup-aws

Criar um conector de diretório de usuários

Para mapear IDs de usuário para nomes de usuário, você deve criar um conector de diretório de usuário.

Passos

1. Em Ransomware Resilience, vá para **Configurações**.
2. No bloco Atividade do usuário, selecione **Gerenciar**.
3. Selecione a aba **Conectores de diretório do usuário** e depois **Adicionar**.
4. Configure a conexão. Insira as informações necessárias em cada campo.

Campo	Descrição
Nome	Insira um nome exclusivo para o conector do diretório de usuários.
Tipo de diretório de usuário	O tipo de diretório
Endereço IP do servidor ou nome de domínio	O endereço IP ou o Nome de Domínio Totalmente Qualificado (FQDN) do servidor que hospeda a conexão.
Nome da floresta ou nome da pesquisa	Você pode especificar o nível da floresta na estrutura de diretórios como o nome de domínio direto (por exemplo, <code>unit.company.com</code>) ou um conjunto de nomes distintos relativos (por exemplo: <code>DC=unit, DC=company, DC=com</code>). Você também pode inserir um OU filtrar por uma unidade organizacional ou um CN limitar a um usuário específico (por exemplo: <code>CN=user, OU=engineering, DC=unit, DC=company, DC=com</code>).
LIGAR DN	O DN BIND é uma conta de usuário com permissão para pesquisar no diretório, como por exemplo, <code>user@domain.com</code> . O usuário precisa da permissão "Somente leitura" para o domínio.
Senha BIND	A senha do usuário fornecida em BIND DN
Protocolo	O campo de protocolo é opcional. Você pode usar LDAP, LDAPS ou LDAP sobre StartTLS.
Porta	Insira o número da porta escolhida.

User directory
 Connect to your user directories to identify specific users performing potentially suspicious behavior. [Get help](#)

Connection
^

Name

User activity agent

Forest name or search name

Bind password

Port

User directory type

Server IP or DNS name

Bind DN

Protocol
Optional

Attribute mapping
Not set
^

Forneça os detalhes do mapeamento de atributos:

- **Nome de exibição**
- **SID** (se você estiver usando LDAP)
- **Nome de usuário**
- **ID Unix** (se você estiver usando NFS)
- Se selecionar **Incluir atributos opcionais**, você também poderá adicionar um endereço de e-mail, número de telefone, função, estado, país, departamento, foto, nome do gerente ou grupos. Selecione **Avançado** para adicionar uma consulta de pesquisa opcional.

5. Selecione **Adicionar**.

6. Retorne à guia de conectores do diretório do usuário para verificar o status do seu conector do diretório do usuário. Se criado com sucesso, o status do conector do diretório do usuário será exibido como **Em execução**.

Excluir um conector de diretório de usuário

Passos

1. Em Ransomware Resilience, vá para **Configurações**.
2. Localize o bloco Atividade do usuário e selecione **Gerenciar**.
3. Selecione a aba **Conector de diretório do usuário**.
4. Identifique o conector de diretório do usuário que você deseja excluir. No menu de ação no final da linha, selecione os três pontos ... então **Excluir**.
5. Na janela pop-up, selecione **Delete** para confirmar.

Excluir usuários dos alertas

Se houver determinados usuários confiáveis cujo comportamento possa acionar alertas de comportamento do

usuário, você pode excluí-los dos alertas.

Passos

1. Em Resiliência a Ransomware, selecione **Configurações**.
2. No painel de Configurações, localize o cartão Atividade do usuário e selecione **Manage**.
3. Selecione a guia **Usuários excluídos**.
4. Para visualizar usuários individuais na interface do usuário, escolha **Selecionar manualmente**. Para carregar uma lista de usuários excluídos, selecione **Carregar**.
 - a. Se você selecionou **Select manually**, marque a caixa de seleção ao lado dos nomes dos usuários específicos que deseja excluir.
 - b. Se você selecionar **Upload**, primeiro deverá baixar um arquivo CSV que inclui a lista de todos os usuários. Selecione **Download** para acessar a lista.

Analise o arquivo CSV. Remova os nomes de todos os usuários para os quais você deseja manter a detecção. Quando a lista contiver apenas os nomes dos usuários que você deseja excluir da detecção, salve-a. Selecione **Carregar** para localizar o arquivo e, em seguida, escolha-o.

5. Selecione **Adicionar** para concluir a inclusão dos usuários na lista de exclusão.
6. Na aba **Usuários excluídos**, os nomes dos usuários removidos dos alertas de detecção de comportamento do usuário agora são exibidos no dashboard.



Você também pode excluir um usuário diretamente de um alerta. Para mais informações, consulte ["Responder a alertas de ransomware"](#).

Remova usuários da lista de usuários excluídos

Você pode adicionar um usuário de volta à detecção depois.

Passos

1. No painel de Configurações, localize o cartão Atividade do usuário e selecione **Manage**.
2. Selecione a guia **Usuários excluídos**.
3. Localize o nome do usuário que deseja remover da seleção de usuários excluídos. Selecione o menu de ações (...) na linha com o nome do usuário e então **Remove**.
4. Na caixa de diálogo, selecione **Remove** para confirmar que deseja remover os usuários selecionados.

Responder a alertas de atividades suspeitas de usuários

Após configurar a detecção de atividades suspeitas do usuário, você pode monitorar eventos na página de alertas. Para mais informações, consulte ["Detectar atividades maliciosas e comportamentos suspeitos de usuários"](#).

Use a resiliência do ransomware

Monitore a integridade da carga de trabalho usando o NetApp Ransomware Resilience Dashboard

O NetApp Ransomware Resilience Dashboard fornece informações rápidas sobre a integridade da proteção de suas cargas de trabalho. Você pode determinar rapidamente as cargas de trabalho que estão em risco ou protegidas, identificar as cargas de trabalho impactadas por um incidente ou em recuperação e avaliar a extensão da proteção observando quanto armazenamento está protegido ou em risco.

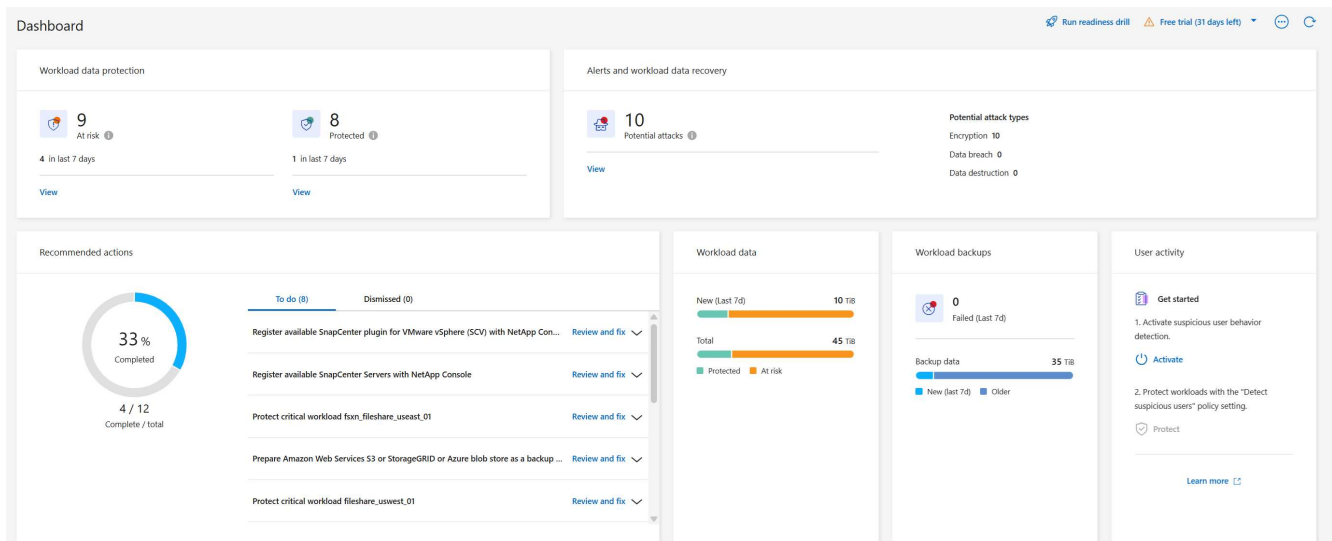
Utilize o Painel de Controle para revisar sugestões de proteção, alterar configurações e baixar relatórios.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Revise a integridade da carga de trabalho usando o Painel

Passos

1. Depois que o Console descobre suas cargas de trabalho, o painel de resiliência contra ransomware exibe a integridade da proteção de dados da carga de trabalho.



2. No Painel, você pode realizar as seguintes ações em cada um dos painéis:

- **Proteção de dados da carga de trabalho:** selecione **Exibir tudo** para ver todas as cargas de trabalho que estão em risco ou protegidas na página Proteção. As cargas de trabalho correm risco quando os níveis de proteção não correspondem a uma política de proteção. Consulte "[Proteja as cargas de trabalho](#)".



Selecione a dica de ferramenta "i" para ver dicas sobre esses dados. Para aumentar o limite de carga de trabalho, selecione **Aumentar limite de carga de trabalho** dentro desta nota. Selecionar isso leva você para a página de Suporte do Console, onde você pode criar um tíquete de caso.

- **Alertas e recuperação de dados de carga de trabalho:** selecione **Exibir tudo** para ver incidentes ativos que impactaram sua carga de trabalho, estão prontos para recuperação após os incidentes serem neutralizados ou estão em recuperação. Consulte ["Responder a um alerta detectado"](#).
 - Um incidente é categorizado em um dos seguintes estados:
 - Novo
 - Demitido
 - Dispensando
 - Resolvido
 - Um alerta pode ter um dos seguintes status:
 - Novo
 - Inativo
 - Uma carga de trabalho pode ter um dos seguintes status de restauração:
 - Restauração necessária
 - Em andamento
 - Restaurado
 - Fracassado
- **Ações recomendadas:** Para aumentar a proteção, revise cada recomendação e selecione **Revisar e corrigir**.

Ver ["Revise as sugestões de proteção no Painel"](#) ou ["Proteja as cargas de trabalho"](#).

O Ransomware Resilience exibe novas recomendações desde sua última visita ao Painel com a tag "Novo" por 24 horas. As ações aparecem em ordem de prioridade, com as mais importantes no topo. Revise, aja ou descarte cada recomendação.

O número total de ações não inclui ações que você descartou.

- **Dados de carga de trabalho:** Monitore as alterações na cobertura de proteção nos últimos 7 dias.
- **Backups de carga de trabalho:** monitore alterações em backups de carga de trabalho criados pelo Ransomware Resilience que falharam ou foram concluídos com sucesso nos últimos 7 dias.

Revise as recomendações de proteção no Painel

O Ransomware Resilience avalia a proteção em suas cargas de trabalho e recomenda ações para melhorar essa proteção.

Você pode revisar uma recomendação e agir de acordo com ela, o que altera o status da recomendação para Concluído. Ou, se quiser agir mais tarde, você pode descartá-la. Descartar uma ação move a recomendação para uma lista de ações descartadas, que você pode revisar mais tarde.

Aqui está uma amostra das recomendações que o Ransomware Resilience oferece.

Recomendação	Descrição	Como resolver
Adicione uma política de proteção contra ransomware.	A carga de trabalho não está protegida no momento.	Atribua uma política à carga de trabalho. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .
Conecte-se ao SIEM para relatórios de ameaças.	Envie dados para um sistema de gerenciamento de segurança e eventos (SIEM) para análise e detecção de ameaças.	Insira os detalhes do servidor SIEM/XDR para habilitar a detecção de ameaças. Consulte "Configurar definições de proteção" .
Habilite proteção consistente com a carga de trabalho para aplicativos ou VMware.	Essas cargas de trabalho não são gerenciadas pelo SnapCenter Software ou pelo SnapCenter Plug-in for VMware vSphere.	Para que eles sejam gerenciados pelo SnapCenter, ative a proteção consistente com a carga de trabalho. Consulte "Proteja a carga de trabalho contra ataques de ransomware" .
Melhore a postura de segurança do sistema	O NetApp Digital Advisor identificou pelo menos um risco de segurança alto ou crítico.	Revise todos os riscos de segurança no NetApp Digital Advisor. Consulte "Documentação do Digital Advisor" .
Fortaleça uma política.	Algumas cargas de trabalho podem não ter proteção suficiente. Fortaleça a proteção das cargas de trabalho com uma política.	Aumente a retenção, adicione backups, imponha backups imutáveis, bloqueie extensões de arquivo suspeitas, habilite a detecção em armazenamento secundário e muito mais. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .
Prepare <provedor de backup> como um destino de backup para fazer backup dos dados da sua carga de trabalho.	A carga de trabalho não tem nenhum destino de backup no momento.	Adicione destinos de backup a esta carga de trabalho para protegê-la. Consulte "Configurar definições de proteção" .
Proteja cargas de trabalho de aplicativos críticos ou altamente importantes contra ransomware.	A página Proteger exibe cargas de trabalho de aplicativos críticas ou altamente importantes (com base no nível de prioridade atribuído) que não estão protegidas.	Atribua uma política a essas cargas de trabalho. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .
Proteja cargas de trabalho de compartilhamento de arquivos críticos ou altamente importantes contra ransomware.	A página Proteção exibe cargas de trabalho críticas ou altamente importantes do tipo Compartilhamento de Arquivos ou Armazenamento de Dados que não estão protegidas.	Atribua uma política a cada uma das cargas de trabalho. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .

Recomendação	Descrição	Como resolver
Registre o plugin SnapCenter disponível para VMware vSphere (SCV) com o Console	Uma carga de trabalho de VM não é protegida.	Atribua proteção consistente de VM à carga de trabalho da VM habilitando o SnapCenter Plugin para VMware vSphere. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .
Registre o SnapCenter Server disponível com o Console	Um aplicativo não está protegido.	Atribua proteção consistente com o aplicativo à carga de trabalho habilitando o SnapCenter Server. Consulte "Proteja cargas de trabalho contra ataques de ransomware" .
Revise novos alertas.	Existem novos alertas.	Revise os novos alertas. Consulte "Responder a um alerta de ransomware detectado" .

Passos

1. No painel Ações recomendadas em Resiliência contra Ransomware, selecione uma recomendação e depois **Revisar e corrigir**.
2. Para descartar a ação até mais tarde, selecione **Descartar**.

A recomendação sai da lista de Tarefas e aparece na lista de Descartados.



Mais tarde, você pode transformar um item descartado em um item de Tarefa. Quando você marca um item como concluído ou transforma um item descartado em uma ação A Fazer, o Total de ações aumenta em 1.

3. Para revisar informações sobre como agir de acordo com as recomendações, selecione o ícone **informações**.

Exportar dados de proteção para arquivos CSV

Você pode exportar dados e baixar arquivos CSV que mostram detalhes de proteção, alertas e recuperação.



Você pode baixar arquivos CSV de qualquer uma das opções do menu principal:

- **Proteção:** Contém o status e os detalhes de todas as cargas de trabalho, incluindo o número total de cargas de trabalho que o Ransomware Resilience marca como protegidas ou em risco.
- **Alertas:** Inclui o status e os detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação:** Inclui o status e os detalhes de todas as cargas de trabalho que precisam ser restauradas, incluindo o número total de cargas de trabalho que o Ransomware Resilience marca como "Restauração necessária", "Em andamento", "Falha na restauração" e "Restaurada com sucesso".

O download de um arquivo CSV de uma página inclui apenas os dados dessa página.

Os arquivos CSV incluem dados para todas as cargas de trabalho em todos os sistemas do Console.


Passos

1. No painel de controle de Resiliência a Ransomware, selecione **Atualizar**.  opção no canto superior direito para atualizar os dados que aparecerão nos arquivos.
2. Faça um dos seguintes:
 - Na página, selecione **Download**.  opção.
 - No menu Resiliência contra Ransomware, selecione **Relatórios**.
3. Se você selecionou a opção **Relatórios**, selecione um dos arquivos nomeados pré-configurados e selecione **Baixar (CSV)** ou **Baixar (JSON)**.

Acessar documentação técnica

Você pode acessar a documentação técnica do Ransomware Resilience em "docs.netapp.com" ou de dentro do Ransomware Resilience.

Passos

1. No painel de Resiliência do Ransomware, selecione a vertical ***Ações***  opção.
2. Selecione uma destas opções:
 - **Novidades** para ver informações sobre os recursos das versões atuais ou anteriores nas Notas de Versão.
 - **Documentação** para visualizar a página inicial da documentação do Ransomware Resilience e esta documentação.

Proteja as cargas de trabalho

Proteja cargas de trabalho com estratégias de proteção de NetApp Ransomware Resilience

Você pode proteger cargas de trabalho contra ataques de ransomware habilitando a proteção consistente da carga de trabalho ou criando estratégias de proteção contra ransomware no NetApp Ransomware Resilience.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Entenda as estratégias de proteção contra ransomware

As estratégias de proteção contra ransomware abrangem *deteção*, *proteção* e *replicação* policies.

- **Políticas de deteção** identificam ameaças de ransomware
- **Políticas de proteção** incluem políticas de snapshot e backup. Políticas de deteção e snapshot são necessárias em uma estratégia de proteção. As políticas de backup são opcionais.

Se você estiver usando outros produtos da NetApp para proteger sua carga de trabalho, o Ransomware Resilience os descobre e oferece a opção de:

- use uma política de detecção de ransomware e continue a usar as políticas de snapshot e backup criadas por outras ferramentas da NetApp ou
- use o Ransomware Resilience para gerenciar detecção, snapshots e backups.
- **As políticas de replicação** permitem replicar snapshots do Ransomware Resilience para um site secundário. Os cronogramas de replicação podem ser definidos para frequências horárias, diárias, semanais ou mensais.

Atualmente, você só pode replicar snapshots para armazenamento ONTAP local.



Se você estiver configurando estratégias de proteção para Amazon FSxN para ONTAP e Azure NetApp Files, consulte "[as limitações para cada serviço](#)".



Para melhor gerenciamento e proteção do seu patrimônio de dados, você pode criar "[compartilhamentos de arquivos em grupo](#)" para proteger coletivamente volumes sob uma estratégia.

Políticas de proteção com outros serviços gerenciados pela NetApp

Além da Resiliência contra Ransomware, os seguintes serviços podem ser usados para gerenciar a proteção:

- NetApp Backup and Recovery para compartilhamentos de arquivos, compartilhamentos de arquivos de VM
- SnapCenter para VMware para datastores de VM
- SnapCenter para Oracle

As informações de proteção desses serviços aparecem em Resiliência de Ransomware. Você pode adicionar políticas de detecção a esses serviços com o Ransomware Resilience. Adicionar uma política de proteção com o Ransomware Resilience substitui as políticas de proteção existentes.

Se uma política de detecção de ransomware estiver sendo gerenciada pelo Autonomous Ransomware Protection (ARP ou ARP/AI, dependendo da versão do ONTAP) e FPolicy no ONTAP, essas cargas de trabalho serão protegidas e continuarão sendo gerenciadas pelo ARP e FPolicy.



Os destinos de backup não estão disponíveis para cargas de trabalho no Amazon FSx for NetApp ONTAP ou Azure NetApp Files. Realize operações de backup usando o serviço de backup do FSx for ONTAP. Você define políticas de backup para cargas de trabalho no FSx for ONTAP na AWS, não no Ransomware Resilience. As políticas de backup aparecem no Ransomware Resilience e permanecem inalteradas em relação à AWS.

Políticas de proteção para cargas de trabalho não protegidas por aplicativos NetApp

Se sua carga de trabalho não for gerenciada pelo Backup and Recovery, Ransomware Resilience, SnapCenter ou SnapCenter Plug-in for VMware vSphere, ela poderá ter instantâneos tirados como parte do ONTAP ou de outros produtos. Se a proteção FPolicy do ONTAP estiver em vigor, você poderá alterar a proteção FPolicy usando o ONTAP.

Visualizar proteção contra ransomware em uma carga de trabalho

Uma das primeiras etapas para proteger cargas de trabalho é visualizar suas cargas de trabalho atuais e seu status de proteção. Você pode ver os seguintes tipos de cargas de trabalho:

- Cargas de trabalho de aplicativos
- Cargas de trabalho em bloco
- Cargas de trabalho de compartilhamento de arquivos
- Cargas de trabalho de VM

Passos

1. Na navegação à esquerda do Console, selecione **Proteção > Resiliência a Ransomware**.
2. Faça um dos seguintes:
 - No painel Proteção de Dados do Painel, selecione **Exibir tudo**.
 - No menu, selecione **Proteção**.

The screenshot displays the 'Protection status' dashboard. At the top, it shows two summary cards: 'At risk' with 9 items and 'Protected' with 9 items. Below this, there are tabs for 'Workloads' and 'Protection groups'. The 'Workloads' tab is active, showing a table of 19 workloads. The table columns include Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions. The workloads listed are FSxN_fileshare_usteast_01 (At risk), LUN_storage_01 (Protected), MySQL_4781 (Protected), MySQL_8009 (At risk), MySQL_9294 (Protected), and Oracle_2115 (At risk). Each row has an action button: 'Protect' for 'At risk' and 'Edit protection' for 'Protected'.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_usteast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

3. Nesta página, você pode visualizar e alterar os detalhes de proteção da carga de trabalho.



Ver "Adicione uma estratégia de proteção contra ransomware" para saber mais sobre como usar o Ransomware Resilience quando houver uma política de proteção existente com o SnapCenter ou Backup and Recovery.

Entenda a página Proteção

A página Proteção mostra as seguintes informações sobre proteção de carga de trabalho:

Status de proteção: Uma carga de trabalho pode mostrar um dos seguintes status de proteção para indicar se uma política é aplicada ou não:

- **Protegido:** Uma política é aplicada. O ARP (ou ARP/AI, dependendo da versão do ONTAP) é habilitado em todos os volumes relacionados à carga de trabalho.
- **Em risco:** Nenhuma política é aplicada. Se uma carga de trabalho não tiver uma política de detecção primária habilitada, ela estará "em risco", mesmo que tenha uma política de snapshot e backup habilitada.
- **Em andamento:** Uma política está sendo aplicada, mas ainda não foi concluída.

- **Falha:** Uma política foi aplicada, mas não está funcionando.

Status de detecção: Uma carga de trabalho pode ter um dos seguintes status de detecção de ransomware:

- **Aprendizado:** Uma política de detecção de ransomware foi recentemente atribuída à carga de trabalho e o Ransomware Resilience está verificando as cargas de trabalho.
- **Ativo:** Uma política de proteção contra detecção de ransomware está atribuída.
- **Não definido:** Uma política de proteção de detecção de ransomware não foi atribuída.
- **Erro:** Uma política de detecção de ransomware foi atribuída, mas o Ransomware Resilience encontrou um erro.



Quando a proteção está habilitada no Ransomware Resilience, a detecção de alertas e os relatórios começam depois que o status da política de detecção de ransomware muda do modo de aprendizagem para o modo ativo.



Atividades suspeitas de comportamento do usuário e atividades relacionadas ao FPolicy (extensões de arquivo suspeitas) são listadas separadamente do status de detecção.

Política de detecção: O nome da política de detecção de ransomware aparece, se uma tiver sido atribuída. Se a política de detecção não tiver sido atribuída, "N/A" aparecerá.

Destino da replicação: Se você configurou a replicação de snapshots, os nomes das VMs e dos sistemas de armazenamento de destino serão listados. Se não houver replicação, este campo exibirá "Nenhum".

Políticas de snapshot e backup: esta coluna mostra as políticas de snapshot e backup aplicadas à carga de trabalho e ao produto ou serviço que está gerenciando essas políticas.

- Gerenciado pelo SnapCenter
- Gerenciado pelo SnapCenter Plug-in for VMware vSphere
- Gerenciado por Backup e Recuperação
- Nome da política de proteção contra ransomware que rege instantâneos e backups
- Nenhum

Importância da carga de trabalho

A resiliência ao ransomware atribui uma importância ou prioridade a cada carga de trabalho durante a descoberta com base em uma análise de cada carga de trabalho. A importância da carga de trabalho é determinada pelas seguintes frequências de snapshot:

- **Crítico:** Mais de uma cópia instantânea é feita por hora (cronograma de proteção altamente agressivo)
- **Importante:** Cópias de snapshots são criadas com menos frequência do que a cada hora, mas com mais frequência do que a cada dia.
- **Padrão:** Cópias instantâneas são tiradas mais de uma vez por dia.

Políticas de detecção predefinidas

Você pode escolher uma das seguintes políticas predefinidas de Resiliência contra Ransomware, que estão alinhadas com a importância da carga de trabalho.



A política **Extensão de usuário de criptografia** é a única política predefinida que oferece suporte à detecção de comportamento suspeito do usuário.

+ A **política de replicação crítica** é a única política predefinida que suporta a replicação de snapshots para o ONTAP.

Nível de política	Instantâneo	Frequência	Retenção (dias)	Número de cópias instantâneas	Número máximo de cópias instantâneas
Política de carga de trabalho crítica	A cada quarto de hora	A cada 15 minutos	3	288	309
	Diário	A cada 1 dia	14	14	309
	Semanalmente	A cada 1 semana	35	5	309
	Mensal	A cada 30 dias	60	2	309
Política importante e de carga de trabalho	A cada quarto de hora	A cada 30 minutos	3	144	165
	Diário	A cada 1 dia	14	14	165
	Semanalmente	A cada 1 semana	35	5	165
	Mensal	A cada 30 dias	60	2	165
Política de carga de trabalho padrão	A cada quarto de hora	A cada 30 minutos	3	72	93
	Diário	A cada 1 dia	14	14	93
	Semanalmente	A cada 1 semana	35	5	93
	Mensal	A cada 30 dias	60	2	93
Extensão de usuário de criptografia	A cada quarto de hora	A cada 30 minutos	3	72	93
	Diário	A cada 1 dia	14	14	93
	Semanalmente	A cada 1 semana	35	5	93
	Mensal	A cada 30 dias	60	2	93

Nível de política	Instantâneo	Frequência	Retenção (dias)	Número de cópias instantâneas	Número máximo de cópias instantâneas
Extensão de usuário de criptografia	A cada quarto de hora	A cada 30 minutos	3	72	93
	Diário	A cada 1 dia	14	14	93
	Semanalmente	A cada 1 semana	35	5	93
	Mensal	A cada 30 dias	60	2	93
Política de replicação crítica	A cada quarto de hora	A cada 15 minutos	3	288	309
	Diário	A cada 1 dia	14	14	309
	Semanalmente	A cada 1 semana	35	5	309
	Mensal	A cada 30 dias	60	2	309

Habilite a proteção consistente com aplicativos ou VMs com o SnapCenter

Habilitar a proteção consistente com aplicativos ou VMs ajuda a proteger suas cargas de trabalho de aplicativos ou VMs de maneira consistente, alcançando um estado quiescente e consistente para evitar possível perda de dados posteriormente, caso seja necessária recuperação.

Este processo inicia o registro do SnapCenter Software Server para aplicativos ou do SnapCenter Plug-in for VMware vSphere para VMs usando Backup e Recuperação.

Depois de habilitar a proteção consistente com a carga de trabalho, você pode gerenciar estratégias de proteção no Ransomware Resilience. A estratégia de proteção inclui políticas de snapshot e backup gerenciadas em outro lugar, juntamente com uma política de detecção de ransomware gerenciada no Ransomware Resilience.

Para saber mais sobre como registrar o SnapCenter ou o SnapCenter Plug-in for VMware vSphere usando Backup e Recuperação, consulte as seguintes informações:

- ["Registrar o software SnapCenter Server"](#)
- ["Registrar o SnapCenter Plug-in for VMware vSphere"](#)

Passos

1. No menu Resiliência contra Ransomware, selecione **Painel**.
2. No painel Recomendações, localize uma das seguintes recomendações e selecione **Revisar e corrigir**:
 - Registre o SnapCenter Server disponível com o NetApp Console
 - Registre o SnapCenter Plug-in for VMware vSphere (SCV) com o NetApp Console

3. Siga as informações para registrar o SnapCenter ou o SnapCenter Plug-in for VMware vSphere usando o Backup and Recovery.
4. Retornar para Resiliência ao Ransomware.
5. No Ransomware Resilience, navegue até o Painel e inicie o processo de descoberta novamente.
6. Em Ransomware Resilience, selecione **Proteção** para visualizar a página Proteção.
7. Revise os detalhes na coluna de políticas de snapshot e backup na página Proteção para ver se as políticas são gerenciadas em outro lugar.

Adicione uma estratégia de proteção contra ransomware

Existem três abordagens para adicionar uma estratégia de proteção contra ransomware:

- **Crie uma estratégia de proteção contra ransomware se você não tiver políticas de snapshot ou backup.**

A estratégia de proteção contra ransomware inclui:

- Política de instantâneo
- Política de detecção de ransomware
- Política de backup
- **Substitua as políticas de backup ou snapshot existentes do SnapCenter ou da proteção de Backup e Recuperação por estratégias de proteção gerenciadas pelo Ransomware Resilience.**

A estratégia de proteção contra ransomware inclui:

- Política de instantâneo
- Política de detecção de ransomware
- Política de backup
- **Crie uma política de detecção para cargas de trabalho com políticas de snapshot e backup existentes gerenciadas em outros produtos ou serviços da NetApp .**

A política de detecção não altera as políticas gerenciadas em outros produtos.

A política de detecção habilita a Proteção Autônoma contra Ransomware e a proteção FPolicy se elas já estiverem ativadas em outros serviços. Saiba mais sobre "[Proteção Autônoma contra Ransomware](#)" , "[Backup e Recuperação](#)" , e "[Política ONTAP](#)" .

Crie uma estratégia de proteção contra ransomware (se você não tiver políticas de snapshot ou backup)


Se não houver políticas de snapshot ou backup na carga de trabalho, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas no Ransomware Resilience:

- Política de instantâneo
- Política de backup
- Política de detecção de ransomware
- Replicação secundária para ONTAP


Etapas para criar uma estratégia de proteção contra ransomware

1. No menu Resiliência contra Ransomware, selecione **Proteção**.

Protection status

 **9**
At risk ⓘ

9 in last 7 days
35 TiB data at risk

 **9**
Protected ⓘ

1 in last 7 days
10 TiB data at risk

[Workloads](#) [Protection groups](#)

Workloads (19) 🔍 ⬇ [Manage protection strategies](#)

Workload	↑	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u:	Actions
FSxN_fileshare_useast_01		At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01		Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781		Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009		At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294		Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115		At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. Na página Proteção, selecione uma carga de trabalho e depois **Proteger**.

3. Na página Estratégias de proteção contra ransomware, selecione **Adicionar**.

[Add Ransomware Resilience strategy](#) ✕

Add Ransomware Resilience strategy

Ransomware Resilience strategy name

Copy from existing Ransomware Resilience strategy

No policy selected 📄 Select

Detection

1 / 3 enabled

▼

Snapshot policy

Action required

▼

Backup policy

None

▼

4. Insira um novo nome de estratégia ou insira um nome existente para copiá-lo. Se você inserir um nome existente, escolha qual deseja copiar e selecione **Copiar**.



Se você optar por copiar e modificar uma estratégia existente, o Ransomware Resilience anexará "_copy" ao nome original. Você deve alterar o nome e pelo menos uma configuração para torná-lo único.

5. Para cada item, selecione a **Seta para baixo**.

- **Política de detecção:**

- **Política:** Escolha uma das políticas de detecção predefinidas.
- **Detecção primária:** Ative a Resiliência a Ransomware para detectar possíveis ataques de ransomware.
- **Detecção de comportamento suspeito do usuário:** habilite a detecção de comportamento do usuário para transmitir eventos de atividade do usuário ao Ransomware Resilience e detectar eventos suspeitos, como violações de dados.
- **Bloquear extensões de arquivo:** Ative a Resiliência a Ransomware para bloquear extensões de arquivo suspeitas conhecidas. O recurso de Resiliência a Ransomware cria cópias instantâneas automáticas quando a detecção primária está ativada.

Se você quiser alterar as extensões de arquivo bloqueadas, edite-as no Gerenciador do Sistema.

◦ **Política de instantâneos:**

- **Nome base da política de instantâneo:** Selecione uma política ou selecione **Criar** e insira um nome para a política de instantâneo.
- **Bloqueio de instantâneo:** ative esta opção para bloquear as cópias de instantâneo no armazenamento primário para que elas não possam ser modificadas ou excluídas por um determinado período de tempo, mesmo que um ataque de ransomware chegue ao destino do armazenamento de backup. Isso também é chamado de *armazenamento imutável*. Isso permite um tempo de restauração mais rápido.

Quando um snapshot é bloqueado, o tempo de expiração do volume é definido como o tempo de expiração da cópia do snapshot.

O bloqueio de cópia de instantâneo está disponível no ONTAP 9.12.1 e posteriores. Para saber mais sobre SnapLock, consulte ["SnapLock no ONTAP"](#).

- **Agendamentos de instantâneos:** escolha opções de agendamento, o número de cópias de instantâneos a serem mantidas e selecione para habilitar o agendamento.
 - **Política de replicação:**
- **Nome base da política de replicação:** Insira um novo nome ou escolha um existente. O nome base é o prefixo adicionado a todos os instantâneos.
- **Agendamentos de replicação:** Alterne as frequências que deseja ativar (por hora, diariamente, semanalmente ou mensalmente) e defina o valor de retenção (o número de snapshots replicados a serem mantidos) para cada agendamento ativado.
 - **Política de backup:**
- **Nome base da política de backup:** insira um novo nome ou escolha um nome existente.
- **Agendamentos de backup:** escolha opções de agendamento para armazenamento secundário e ative o agendamento.



Para habilitar o bloqueio de backup no armazenamento secundário, configure seus destinos de backup usando a opção **Configurações**. Para obter detalhes, consulte ["Configurar definições"](#).

6. Selecione **Adicionar**.

Adicionar uma política de detecção a cargas de trabalho com políticas de backup e snapshot existentes gerenciadas pelo SnapCenter ou Backup and Recovery

O Ransomware Resilience permite que você atribua uma política de detecção ou uma política de proteção a cargas de trabalho com proteção de backup e snapshot existente gerenciada em outros produtos ou serviços da NetApp. Outros serviços, como Backup and Recovery e SnapCenter, usam políticas que controlam snapshots, replicação para armazenamento secundário ou backups para armazenamento de objetos.

Adicionar uma política de detecção a cargas de trabalho com políticas de backup ou snapshot existentes

Se você tiver políticas de backup ou snapshot existentes com o Backup and Recovery ou SnapCenter, poderá adicionar uma política para detectar ataques de ransomware. Para gerenciar a proteção e a detecção com o Ransomware Resilience, consulte [Proteja-se com resiliência contra ransomware](#).

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.

The screenshot displays the 'Protection status' dashboard. At the top, it shows two summary cards: 'At risk' with 9 items and 'Protected' with 9 items. Below these, there are tabs for 'Workloads' and 'Protection groups'. The 'Workloads' tab is active, showing a table of 19 workloads. The table columns include Workload, Protection status, Snapshot and back..., Type, Protec..., Encryption detecti..., Suspected u, and Actions. The table lists several workloads with their respective protection statuses and actions.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. Na página Proteção, selecione uma carga de trabalho e selecione **Proteger**.
3. O Ransomware Resilience detecta se há políticas ativas do SnapCenter ou de Backup e Recuperação.
4. Para deixar suas políticas existentes de Backup e Recuperação ou SnapCenter em vigor e aplicar apenas uma política de *detecção*, deixe a caixa **Substituir políticas existentes** desmarcada.
5. Para ver detalhes das políticas do SnapCenter, selecione a **Seta para baixo**.
6. Selecione as configurações de detecção que você deseja:

Encryption detection
Suspicious user behavior detection
Block suspicious file extensions

7. Selecione **Avançar**.

- Se você selecionou **Deteção de comportamento suspeito do usuário** como uma configuração de detecção, selecione o agente de atividade do usuário ou ["ou criar um"](#).

O agente de atividade do usuário hospeda os novos coletores de dados. O Ransomware Resilience cria o coletor de dados automaticamente para transmitir eventos de atividade do usuário ao Ransomware Resilience para detectar comportamento anômalo do usuário.

- Selecione **Avançar**.
- Reveja suas escolhas. Selecione **Criar** para ativar a detecção.
- Na página Proteção, revise o **Status de detecção** para confirmar se a detecção está Ativa.

Substitua as políticas de backup ou snapshot existentes por uma estratégia de proteção contra ransomware

Você pode substituir suas políticas existentes de backup ou snapshot por uma estratégia de proteção contra ransomware. Essa abordagem remove sua proteção gerenciada externamente e configura a detecção e a proteção no Ransomware Resilience.

Passos

- No menu Resiliência contra Ransomware, selecione **Proteção**.

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

- Na página Proteção, selecione uma carga de trabalho e selecione **Proteger**.
- O Ransomware Resilience detecta se há políticas ativas de Backup e Recuperação ou SnapCenter . Para substituir as políticas existentes do Backup and Recovery ou do SnapCenter , selecione a caixa **Substituir políticas existentes**. Quando você seleciona a caixa, o Ransomware Resilience substitui a lista de políticas de detecção por políticas de detecção.
- Escolha uma política de proteção. Se não houver nenhuma política de proteção, selecione **Adicionar** para criar uma nova política. Para obter informações sobre como criar uma política, consulte [Crie uma política de proteção](#) . Selecione **Avançar**.
- Se sua estratégia incluir replicação, selecione o **Sistema de destino** e a **VM de armazenamento de destino**. Selecione **Próximo**.

6. Selecione um destino de backup ou crie um novo. Selecione **Avançar**.
 - a. Se sua estratégia de proteção incluir detecção de comportamento do usuário, selecione um agente de atividade do usuário em seu ambiente para hospedar os novos coletores de dados. O Ransomware Resilience cria o coletor de dados automaticamente para transmitir eventos de atividade do usuário ao Ransomware Resilience para detectar comportamento anômalo do usuário.
7. Revise a nova estratégia de proteção e selecione **Proteger** para aplicá-la.
8. Na página Proteção, revise o **Status de detecção** para confirmar se a detecção está Ativa.

Atribuir uma política diferente

Você pode substituir a política existente por uma diferente.

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, na linha de carga de trabalho, selecione **Editar proteção**.
3. Se a carga de trabalho tiver uma política de Backup e Recuperação ou SnapCenter existente que você deseja manter, desmarque **Substituir políticas existentes**. Para substituir as políticas existentes, marque **Substituir políticas existentes**.
4. Na página Políticas, selecione a seta para baixo da política que você deseja atribuir para revisar os detalhes.
5. Selecione a política que você deseja atribuir.
6. Selecione **Proteger** para concluir a alteração.

Crie um grupo de proteção


Agrupar compartilhamentos de arquivos em um grupo de proteção facilita a proteção do seu patrimônio de dados. A resiliência ao ransomware pode proteger todos os volumes de um grupo ao mesmo tempo, em vez de proteger cada volume separadamente.

Você pode criar grupos independentemente do status de proteção (ou seja, grupos não protegidos e grupos protegidos). Quando você adiciona uma política de proteção a um grupo de proteção, a nova política de proteção substitui qualquer política existente, incluindo políticas gerenciadas pelo SnapCenter e NetApp Backup and Recovery.


Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.

Protection status

 **9**
At risk ⓘ

9 in last 7 days
35 TiB data at risk

 **9**
Protected ⓘ

1 in last 7 days
10 TiB data at risk

Workloads Protection groups

Workloads (19)

Workload	Protection status	Snapshot and back...	Type	Protec...	Encryption detecti...	Suspected u	Actions
FSxN_fileshare_useast_01	At risk	None	File share	N/A	N/A	N/A	Protect
LUN_storage_01	Protected	NetApp Ransomware...	Block	N/A	Enabled	N/A	Edit protection
MySQL_4781	Protected	NetApp Ransomware...	MySQL	pg_important	Enabled	N/A	Edit protection
MySQL_8009	At risk	NetApp Backup and...	MySQL	N/A	N/A	N/A	Protect
MySQL_9294	Protected	NetApp Backup and...	MySQL	N/A	Enabled	N/A	Edit protection
Oracle_2115	At risk	SnapCenter	Oracle	N/A	N/A	N/A	Protect

2. Na página Proteção, selecione a aba **Grupos de proteção**.

Workloads Protection groups

Protection group (1)

Protection group	Protection status	Ransomware Resilience strategy	Protected count
pg_important	Protected	rps-important-plan	2 / 2

3. Seleccione **Adicionar**.

Workloads

Select workloads to add to the protection group.

Protection group name

NoRansomwareOnThisFileShare

Workloads (17) | Selected rows (2)

Select workloads with no other policy source or with Backup and Recovery as a policy source.

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
<input type="checkbox"/> azure_v01_4872	File share	azure-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
<input checked="" type="checkbox"/> fileshare_uswest_02_7453	File share	aws-connector-us-west-1-account...	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsiagd1
<input checked="" type="checkbox"/> fsxn_fileshare_useast_01	File share	aws-connector-us-east-1	Critical	High	At risk	N/A	N/A	N/A
<input type="checkbox"/> gcpsha_v01_7496-ws	File share	gcp-connector-demo	Critical	n/a	At risk	N/A	N/A	N/A
<input type="checkbox"/> lun_storage_01	Block	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Ransomware Resilience	netapp-backup-vsiagd3
<input type="checkbox"/> mysql_8009	MySQL	aws-connector-us-east-1	Critical	n/a	At risk	N/A	Backup and Recovery	netapp-backup-vsiagd1
<input type="checkbox"/> mysql_9294	MySQL	aws-connector-us-east-1	Critical	n/a	Protected	1 / 3 enabled	Backup and Recovery	netapp-backup-vsiagd3
<input type="checkbox"/> oracle_2115	Oracle	aws-connector-us-east-1	Critical	n/a	At risk	N/A	SnapCenter	netapp-backup-vsiagd1

Next

4. Digite um nome para o grupo de proteção.

5. Selecione as cargas de trabalho a serem adicionadas ao grupo.



Para ver mais detalhes sobre as cargas de trabalho, role para a direita.

6. Selecione **Avançar**.

Protect
Select how to protect all the workloads in the protection group.

Warning: All current policies will be replaced with the selected policies.

Ransomware Resilience strategies (3)

Ransomware Resilience strategy	Detection	Snapshot policy	Backup policy	Protected workloads
<input type="radio"/> rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3
<input type="radio"/> rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1
<input type="radio"/> rps-standard-plan	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0

Detection 1 / 3 enabled
Settings:
Encryption detection

Snapshot policy standard-ss-policy
Snapshot locking Disabled
Frequency | Snapshot copies | Locking retention days | Retention

hourly	Every 1 hours	72
daily	Every 1 day	14
weekly	Every Fri of week	5
monthly	Every Jan, Feb, Mar, Apr, May, Jun,...	2

Backup policy standard-bu-policy
Frequency | Retention

daily	14
weekly	5
monthly	3

7. Selecione a política para reger a proteção deste grupo.

8. Se a estratégia de proteção incluir replicação, revise as configurações de replicação.

- Para replicar todos os snapshots para o mesmo destino, marque a opção **Usar o mesmo destino para cada carga de trabalho**. Selecione um **Sistema de destino** e uma **VM de armazenamento de destino** para as cargas de trabalho na seção Agente do console. Para usar destinos diferentes, desmarque essa caixa. Analise cada carga de trabalho em cada agente do Console e atribua um **Sistema de destino** e uma **VM de armazenamento de destino** para cada carga de trabalho. Selecione **Próximo**.

9. Para configurar uma política de backup, escolha uma e selecione **Avançar**.

10. Se sua política de detecção incluir detecção de comportamento do usuário, selecione o coletor de dados que deseja usar e depois **Avançar**.

11. Revise as seleções para o grupo de proteção.

12. Para finalizar a criação do grupo de proteção, selecione **Adicionar**.

Editar proteção de grupo

Você pode alterar a política de detecção em um grupo existente.

Passos

- No menu Resiliência contra Ransomware, selecione **Proteção**.
- Na página Proteção, selecione a aba **Grupos de proteção** e selecione o grupo cuja política você deseja modificar.
- Na página de visão geral do grupo de proteção, selecione **Editar proteção**.
- Selecione uma política de proteção existente para aplicar ou selecione **Adicionar** para criar uma nova política de proteção. Para obter mais informações sobre como adicionar uma política de proteção, consulte [Crie uma política de proteção](#). Em seguida, selecione **Salvar**.
- Na visão geral do destino de backup, selecione um destino de backup existente ou **Adicione um novo destino de backup**.
- Selecione **Avançar** para revisar suas alterações.

Remover cargas de trabalho de um grupo

Mais tarde, pode ser necessário remover cargas de trabalho de um grupo existente.

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, selecione a aba **Grupos de proteção**.
3. Selecione o grupo do qual você deseja remover uma ou mais cargas de trabalho.

pg_important
Protection group

Workloads

3 File shares 2 Applications 0 VM datastores

Protection

pg_important-plan
Ransomware Resilience strategy
View

Workloads (5)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_us-east_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
fileshare_us-west_01	File share	aws-connector-us-west-1-account-...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
fileshare_us-west_02_3223	File share	aws-connector-us-west-1-account-...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
mysql_4781	MySQL	aws-connector-us-west-1-account-...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1

4. Na página do grupo de proteção selecionado, selecione a carga de trabalho que deseja remover do grupo e selecione **Ações**...
5. No menu Ações, selecione **Remover carga de trabalho**.
6. Confirme que deseja remover a carga de trabalho e selecione **Remover**.

Excluir o grupo de proteção

A exclusão do grupo de proteção remove o grupo e sua proteção, mas não remove as cargas de trabalho individuais.

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, selecione a aba **Grupos de proteção**.
3. Selecione o grupo do qual você deseja remover uma ou mais cargas de trabalho.

pg_important
Protection group

Workloads

3 File shares 2 Applications 0 VM datastores

Protection

pg_important-plan
Ransomware Resilience strategy
View

Workloads (5)

Workload	Type	Console agent	Importance	Privacy exposure	Protection status	Detection	Snapshot and backup policies	Backup destination
fileshare_us-east_02	File share	aws-connector-us-east-1	Standard	Medium	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
fileshare_us-west_01	File share	aws-connector-us-west-1-account-...	Critical	High	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
fileshare_us-west_02_3223	File share	aws-connector-us-west-1-account-...	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
mysql_4781	MySQL	aws-connector-us-west-1-account-...	Standard	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1
oracle_8821	Oracle	aws-connector-us-east-1	Critical	n/a	Protected	2 / 3 enabled	Ransomware Resilience	netapp-backup-vsaigd1

4. Na página do grupo de proteção selecionado, no canto superior direito, selecione **Excluir grupo de proteção**.
5. Confirme que deseja excluir o grupo e selecione **Excluir**.

Gerenciar estratégias de proteção contra ransomware

Você pode excluir uma estratégia de ransomware.

Veja cargas de trabalho protegidas por uma estratégia de proteção contra ransomware

Antes de excluir uma estratégia de proteção contra ransomware, talvez você queira ver quais cargas de trabalho são protegidas por essa estratégia.

Você pode visualizar as cargas de trabalho na lista de estratégias ou quando estiver editando uma estratégia específica.

Etapas para visualizar estratégias

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, selecione **Gerenciar estratégias de proteção**.

A página de estratégias de proteção contra ransomware exibe uma lista de estratégias.

Ransomware Resilience strategies (4) | Selected rows (1)

Add

	Ransomware Resilience strategy	↑ Detection	↕ Snapshot policy	↕ Backup policy	↕ Protected workloads	↕
<input type="radio"/>	rps-critical-plan	2 / 3 enabled	critical-ss-policy	critical-bu-policy	3	▼
<input type="radio"/>	rps-important-plan	2 / 3 enabled	important-ss-policy	important-bu-policy	1	▼
<input checked="" type="radio"/>	rps-standard-plan Recommended	1 / 3 enabled	standard-ss-policy	standard-bu-policy	0	▼
<input type="radio"/>	rr-strategy-enc-user-ext	3 / 3 enabled	standard-ss-policy	standard-bu-policy	0	▼

3. Na página Estratégias de proteção contra ransomware, na coluna Cargas de trabalho protegidas, selecione a seta para baixo no final da linha.

Excluir uma estratégia de proteção contra ransomware

Você pode excluir uma estratégia de proteção que não esteja atualmente associada a nenhuma carga de trabalho.

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, selecione **Gerenciar estratégias de proteção**.
3. Na página Gerenciar estratégias, selecione ***Ações***... opção para a estratégia que você deseja excluir.
4. No menu Ações, selecione **Excluir política**.

Procure informações de identificação pessoal com a NetApp Data Classification no Ransomware Resilience

No NetApp Ransomware Resilience, você pode usar o NetApp Data Classification para

verificar e classificar os dados em uma carga de trabalho de compartilhamento de arquivos. Classificar dados ajuda a determinar se o conjunto de dados inclui informações de identificação pessoal (PII), o que pode aumentar os riscos de segurança. A classificação de dados é um componente central do NetApp Console e está disponível sem custo adicional.

"[Classificação de Dados](#)" utiliza processamento de linguagem natural orientado por IA para análise e categorização de dados contextuais, fornecendo insights acionáveis sobre seus dados para atender aos requisitos de conformidade, detectar vulnerabilidades de segurança, otimizar custos e acelerar a migração.



Esse processo pode impactar a importância da carga de trabalho para ajudar a garantir que você tenha a proteção adequada.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Identifique a exposição à privacidade com a Classificação de Dados

Antes de usar a Classificação de Dados na Resiliência do Ransomware, você precisa "[para permitir que a Classificação de Dados escaneie seus dados](#)".

Você pode implantar a Classificação de Dados na página Proteção do Ransomware Resilience. Siga o procedimento para identificar a exposição de privacidade. Ao selecionar **Identificar exposição**, caso você ainda não tenha implantado a Classificação de Dados, uma caixa de diálogo permitirá que você habilite a Classificação de Dados.

Para mais informações sobre Classificação de Dados, consulte:

- "[Aprenda sobre Classificação de Dados](#)"
- "[Categorias de dados privados](#)"
- "[Investigue os dados armazenados em sua organização](#)"

Antes de começar

A varredura de dados PII no Ransomware Resilience está disponível se você tiver "[Classificação de Dados implantada](#)". A Classificação de Dados está disponível como parte do Console sem custo adicional e pode ser implantada no local ou na nuvem do cliente.

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, localize uma carga de trabalho de compartilhamento de arquivos na coluna Carga de trabalho.

Protection

Run readiness drill Free trial (31 days left)

Protection status

7 At risk 7 in last 7 days 35 TiB data at risk

11 Protected 1 in last 7 days 10 TiB data at risk

Workloads Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detection...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_vault_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_us-east_02	File share	Protected	pg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsaigd1	Edit protection
fileshare_us-west_01	File share	Protected	pg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsaigd1	Edit protection
fileshare_us-west_02_3223	File share	Protected	pg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsaigd1	Edit protection
fileshare_us-west_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsaigd1	Edit protection
fsxn_fileshare_us-east_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcp_ha_vault_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsaigd3	Edit protection
mysql_4781	MySQL	Protected	pg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsaigd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsaigd1	Protect

3. Para permitir que a Classificação de Dados verifique seus dados em busca de PII, na coluna **Exposição de privacidade**, selecione **Identificar exposição**.



Se você não tiver implantado a Classificação de Dados, selecionar **Identificar exposição** abrirá uma caixa de diálogo para implantar a Classificação de Dados. Selecione **Implantar**. Depois de implantar a Classificação de Dados, você pode retornar à página Proteção e selecionar **Identificar exposição**.

Resultado

A digitalização pode levar vários minutos, dependendo do tamanho e do número de arquivos. Durante a verificação, a página Proteção indica que está identificando arquivos e fornece uma contagem de arquivos. Quando a digitalização estiver concluída, a coluna Exposição de privacidade classificará o nível de exposição como Baixo, Médio ou Alto.

Revise a exposição da privacidade

Após a verificação da Classificação de Dados em busca de PII, avalie o risco.

Os dados PII são classificados em uma das três designações:

- **Alto:** Mais de 70% dos arquivos contêm PII
- **Médio:** Mais de 30% e menos de 70% dos arquivos contêm PII
- **Baixo:** Mais de 0% e menos de 30% dos arquivos contêm PII

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, localize a carga de trabalho do compartilhamento de arquivos na coluna Carga de trabalho que mostra um status na coluna Exposição de privacidade.

Protection

Protection status

7

At risk

7 in last 7 days

35 TiB data at risk

11

Protected

1 in last 7 days

10 TiB data at risk

Workloads

Protection groups

Workloads (23)

Workload	Type	Protection status	Protect...	Encryption detectio...	Suspected user beh...	Block suspicious fil...	Snapshot and back...	Console agent	Importance	Privacy ex...	Backup destination	Actions
azure_voif_4872	File share	At risk	N/A	N/A	N/A	N/A	N/A	azure-connector-demo	Critical	Identify exposure	N/A	Protect
fileshare_useast_02	File share	Protected	pgg.important	Enabled	N/A	Enabled	Ransomware Resilience	aws-connector-us-east-1	Standard	Medium	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_01	File share	Protected	pgg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Critical	High	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_3223	File share	Protected	pgg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fileshare_uwest_02_7453	File share	Protected	N/A	Enabled	N/A	N/A	Backup and Recovery	aws-connector-us-west...	Critical	Identify exposure	netapp-backup-vsajgd1	Edit protection
fsxn_fileshare_useast_01	File share	At risk	N/A	N/A	N/A	N/A	N/A	aws-connector-us-east-1	Critical	High	N/A	Protect
gcp_ha_voif_7496-ws	File share	At risk	N/A	N/A	N/A	N/A	N/A	gcp-connector-demo	Critical	Identify exposure	N/A	Protect
lun_storage_01	Block	Protected	N/A	Enabled	N/A	N/A	Ransomware Resilience	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd3	Edit protection
mysql_4781	MySQL	Protected	pgg.important	Enabled	N/A	enabled	Ransomware Resilience	aws-connector-us-west...	Standard	N/A	netapp-backup-vsajgd1	Edit protection
mysql_8009	MySQL	At risk	N/A	N/A	N/A	N/A	Backup and Recovery	aws-connector-us-east-1	Critical	N/A	netapp-backup-vsajgd1	Protect

3. Selecione o link da carga de trabalho na coluna Carga de trabalho para ver detalhes da carga de trabalho.

Protection > FSxN_fileshare_useast_01

FSxN_fileshare_useast_01

Critical Importance

Protected

Protection health

Edit protection

0 Alerts

Not marked for recovery

Recovery

High Privacy exposure

Files with PII 181 hits in 150 files

Types of PII

Credit cards 20 hits in 150 files

Contacts 95 hits in 150 files

Passwords 28 hits in 150 files

Data subjects 38 hits in 150 files

Protection

2 / 3 enabled Detection

rps-critical-plan Policy View policy

n/a Backup destination View backup destination

File share

Location svm-fsxEnvironment

Console agent console-agent-us-east

Amazon FSx for NetApp ONTAP

Volume: FSxN_fileshare_useas...

Cluster id aaa111a1a-1a11-11aa-1...

System name fsxEnvironment...

Storage VM name svm-fsxEnvironment...

4. Na página Detalhes da carga de trabalho, observe os detalhes no bloco Exposição de privacidade.

Impacto da exposição à privacidade na importância da carga de trabalho

Alterações na exposição da privacidade podem impactar a importância da carga de trabalho.

Quando a exposição da privacidade:	A partir desta exposição de privacidade:	Para esta exposição de privacidade:	Então, a importância da carga de trabalho faz isso:
Diminui	Alto, Médio ou Baixo	Médio, Baixo ou Nenhum	Permanece o mesmo

98

Quando a exposição da privacidade:	A partir desta exposição de privacidade:	Para esta exposição de privacidade:	Então, a importância da carga de trabalho faz isso:
Aumenta	Nenhum	Baixo	Permanece no padrão
	Baixo	Médio	Mudanças de Padrão para Importante
	Baixo ou Médio	Alto	Mudanças de Padrão ou Importante para Crítico

Para maiores informações

Para obter detalhes sobre a Classificação de Dados, consulte a documentação da Classificação de Dados:

- ["Aprenda sobre Classificação de Dados"](#)
- ["Categorias de dados privados"](#)
- ["Investigue os dados armazenados em sua organização"](#)

Gerencie alertas no NetApp Ransomware Resilience.

Quando o NetApp Ransomware Resilience detecta um possível ataque, ele exibe um alerta no Painel de Controle e na área de Notificações. O Ransomware Resilience tira um instantâneo imediatamente. Revise o risco potencial na aba **Alertas** de resiliência contra ransomware.

Se o Ransomware Resilience detectar um possível ataque, uma notificação será exibida nas configurações de Notificação do Console e um e-mail será enviado para os endereços configurados. O e-mail inclui informações sobre a gravidade, a carga de trabalho impactada e um link para o alerta na guia **Alerts** do Ransomware Resilience.

Você pode descartar falsos positivos ou decidir recuperar seus dados imediatamente.



Se você ignorar o alerta, o Ransomware Resilience aprende esse comportamento, associa-o às operações normais e não inicia um alerta sobre ele novamente.

Para começar a recuperar seus dados, marque o alerta como pronto para recuperação para que seu administrador de armazenamento possa iniciar o processo de recuperação.

Cada alerta pode incluir vários incidentes em diferentes volumes e status. Revise todos os incidentes.

O Ransomware Resilience fornece informações chamadas *evidências* sobre o que causou a emissão do alerta, como as seguintes:

- Extensões de arquivo foram criadas ou alteradas
- Criação de arquivo com comparação de taxas detectadas e esperadas
- Exclusão de arquivos com comparação de taxas detectadas e esperadas
- Quando a criptografia é alta, sem alterações na extensão do arquivo

Um alerta é classificado como um dos seguintes:

- **Ataque potencial:** Um alerta ocorre quando o Autonomous Ransomware Protection detecta uma nova extensão e a ocorrência se repete mais de 20 vezes nas últimas 24 horas (comportamento padrão).
- **Aviso:** Um aviso ocorre com base nos seguintes comportamentos:
 - A detecção de uma nova extensão não foi identificada antes e o mesmo comportamento não se repete vezes suficientes para declará-lo como um ataque.
 - Alta entropia é observada.
 - A atividade de leitura, gravação, renomeação ou exclusão de arquivos dobrou em comparação aos níveis normais.



Para ambientes SAN, os avisos são baseados apenas em alta entropia.

As evidências são baseadas em informações da Proteção Autônoma contra Ransomware no ONTAP. Para mais detalhes, consulte "[Visão geral da proteção autônoma contra ransomware](#)".

Um alerta pode ter um dos seguintes status:

- **Novo**
- **Inativo**

Um incidente de alerta pode ter os seguintes estados:

- **Novo:** Todos os incidentes são marcados como "novos" quando são identificados pela primeira vez.
- **Em análise:** Você pode marcar um incidente como em análise enquanto o avalia.
- **Rejeitado:** Se você suspeitar que a atividade não é um ataque de ransomware, você pode alterar o status para "Rejeitado".



Depois de rejeitar um ataque, você não poderá reverter seu status. Se você descartar uma carga de trabalho, todas as cópias instantâneas feitas automaticamente em resposta ao possível ataque de ransomware serão excluídas permanentemente.

- **Descartando:** O incidente está em processo de ser descartado.
- **Resolvido:** O incidente foi corrigido.
- **Resolvido automaticamente:** Para alertas de baixa prioridade, o incidente é resolvido automaticamente se nenhuma ação for tomada dentro de cinco dias.



Se você configurou um sistema de gerenciamento de segurança e eventos (SIEM) no Ransomware Resilience na página Configurações, o Ransomware Resilience envia detalhes de alerta para seu sistema SIEM.

Ver alertas

Você pode acessar alertas no Painel de Resiliência de Ransomware ou na aba **Alertas**.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. "[Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console](#)".

Passos

1. No Painel de Resiliência de Ransomware, revise o painel Alertas.
2. Selecione **Ver tudo** em um dos status.
3. Selecione um alerta para revisar todos os incidentes em cada volume para cada alerta.
4. Para revisar alertas adicionais, selecione **Alerta** nas trilhas de navegação no canto superior esquerdo.
5. Revise os alertas na página Alertas.

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	filesystem_uswest_02_3223, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8621	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9823	Encryption	Potential attack	Unable to detect	oracle_9819	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_datastore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1...	Active	1	2 GiB	1 month ago
lun_alert_6285	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_vol1	Data breach	Potential attack	Raj Patel	uba_rps_test_vol1, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vol2	Data breach	Potential attack	Raj Patel	uba_rps_test_vol2, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vol3	Data breach	Potential attack	Raj Patel	uba_rps_test_vol3, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago

6. Continue com um dos seguintes:

- [Detecte atividades maliciosas e comportamento anômalo do usuário](#) .
- [Marcar incidentes de ransomware como prontos para recuperação \(após os incidentes serem neutralizados\)](#) .
- [Descartar incidentes que não sejam ataques potenciais](#) .

Responder a um e-mail de alerta

Quando o Ransomware Resilience detecta um possível ataque, ele envia uma notificação por e-mail aos usuários inscritos, de acordo com as preferências de notificação de inscrição configuradas nas definições do NetApp Console. O e-mail contém informações sobre o alerta, incluindo a gravidade e os recursos afetados.



Para configurar notificações por e-mail no Console, consulte ["Definir configurações de notificação por e-mail"](#).

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#) .

Passos

1. Veja o e-mail.
2. No e-mail, selecione **Exibir alerta** e faça login no Ransomware Resilience.

A página Alertas é exibida.

3. Revise todos os incidentes em cada volume para cada alerta.
4. Para revisar alertas adicionais, clique em **Alerta** no menu de navegação no canto superior esquerdo.
5. Continue com um dos seguintes:
 - [Detecte atividades maliciosas e comportamento anômalo do usuário](#) .
 - [Marcar incidentes de ransomware como prontos para recuperação \(após os incidentes serem neutralizados\)](#) .
 - [Descartar incidentes que não sejam ataques potenciais](#) .

Detecte atividades maliciosas e comportamento anômalo do usuário

Observando a aba Alertas, você pode identificar se há atividade maliciosa ou comportamento anômalo do usuário.

Você deve ter configurado um agente de atividade do usuário e habilitado uma política de proteção com detecção de comportamento do usuário para visualizar alertas em nível de usuário. A coluna **Usuário suspeito** aparece no painel de alertas somente quando a detecção de comportamento do usuário está habilitada. Para habilitar a detecção de usuários suspeitos, consulte ["Atividade suspeita do usuário"](#).

Ver atividade maliciosa

Quando o Autonomous Ransomware Protection aciona um alerta no Ransomware Resilience, você pode visualizar os seguintes detalhes:

- Entropia de dados recebidos
- Taxa de criação esperada de novos arquivos em comparação com a taxa detectada
- Taxa de exclusão esperada de arquivos comparada à taxa detectada
- Taxa de renomeação esperada de arquivos em comparação com a taxa detectada
- Arquivos e diretórios impactados



Esses detalhes podem ser visualizados para cargas de trabalho NAS. Para ambientes SAN, somente os dados de entropia estão disponíveis.

Passos

1. No menu Resiliência contra Ransomware, selecione **Alertas**.
2. Selecione um alerta.
3. Revise os incidentes no alerta.

Alerts > ee_alert8727

ee_alert8727

Impacted workloads: oracle_8821

Mark restore needed

2 Potential attacks

286 Impacted files

2 GiB Impacted data

September 25, 2025, 6:51 AM
First detected

Incidents (2)

Incident ID	Volume	Storage VM	System	Severity	Status	First detec...	Most rece...	Evidence	Automated res...
inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

4. Selecione um incidente para revisar seus detalhes.

Visualizar comportamento anômalo do usuário

Se você configurou a detecção de usuários suspeitos para visualizar comportamentos anômalos do usuário, poderá visualizar dados em nível de usuário e bloquear usuários específicos. Para habilitar configurações de usuários suspeitos, consulte ["Configurar as definições de resiliência contra ransomware"](#).

Passos

1. No menu Resiliência contra Ransomware, selecione **Alertas**.
2. Selecione um alerta.
3. Revise os incidentes no alerta.
 - a. Para bloquear um usuário suspeito em seu ambiente, selecione **Block** ao lado do nome do usuário.
 - b. Para desativar os alertas de um determinado usuário que é alvo de um alerta que você sabe ser falso, selecione os três pontos (...) e, em seguida, **Excluir este usuário do monitoramento**. Revise a caixa de diálogo e selecione **Excluir** para confirmar.



Para reativar os alertas para um usuário, retorne o alerta. Selecione os três pontos e então **Incluir este usuário no monitoramento**. Você também pode ["Excluir usuários"](#) do monitoramento.

Marcar incidentes de ransomware como prontos para recuperação (após os incidentes serem neutralizados)

Após interromper o ataque, notifique o administrador de storage que os dados estão prontos para que ele possa iniciar o processo de recuperação.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Passos

1. No menu Resiliência contra Ransomware, selecione **Alertas**.

Alerts

Overview

10 Alerts

20 GiB Impacted data

Automated responses

9 Snapshots

Alerts (10)

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	fileshare_uswest_02_3023, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8621	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9623	Encryption	Potential attack	Unable to detect	oracle_9619	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_datastore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1...	Active	1	2 GiB	1 month ago
lun_alert_6285	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_vol1	Data breach	Potential attack	Raj Patel	uba_rps_test_vol1, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vol2	Data breach	Potential attack	Raj Patel	uba_rps_test_vol2, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_vol3	Data breach	Potential attack	Raj Patel	uba_rps_test_vol3, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago

2. Na página Alertas, selecione o alerta.

3. Revise os incidentes no alerta.

Alerts > ee_alert8727

ee_alert8727

Impacted workloads: oracle_8821

Mark restore needed

2 Potential attacks

286 Impacted files

2 GiB Impacted data

September 25, 2025, 6:51 AM
First detected

Incidents (2)

Incident ID	Volume	Storage VM	System	Severity	Status	First detec...	Most rece...	Evidence	Automated res...
inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

4. Se você determinar que os incidentes estão prontos para recuperação, selecione **Marcar restauração necessária**.

5. Confirme a ação e selecione **Marcar restauração necessária**.

6. Para iniciar a recuperação da carga de trabalho, selecione **Recuperar** carga de trabalho na mensagem ou selecione a guia **Recuperação**.

Resultado

Depois que o alerta é marcado para restauração, ele é movido da guia Alertas para a guia Recuperação.

Descartar incidentes que não sejam ataques potenciais

Depois de analisar os incidentes, você precisa determinar se eles são ataques em potencial. Se não forem ameaças reais, podem ser descartadas.

Você pode descartar falsos positivos ou decidir recuperar seus dados imediatamente. Se você descartar o alerta, o Ransomware Resilience aprenderá esse comportamento e o associará às operações normais, não iniciando um alerta novamente para esse comportamento.

Se você descartar uma carga de trabalho, todas as cópias de instantâneos feitas automaticamente em resposta a um possível ataque de ransomware serão excluídas permanentemente.



Se você descartar um alerta, não poderá alterar seu status nem desfazer essa alteração.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Passos

- 1. No menu Resiliência contra Ransomware, selecione **Alertas**.

Alerts

Overview

10 Alerts

20 GiB impacted data

Automated responses

9 Snapshots

Alerts (10)

Alert ID	Alert type	Severity	Suspicious user	Workload	Console agent	Status	Incidents	Impacted data	Detected
ub_alert3223	Suspicious user behavior	Potential attack	Aiden Smith	fileshare_uswest_02_3223, +3	aws-connector-us-east-1	Active	1	2 GiB	8 days ago
ee_alert8727	Encryption	Potential attack	Unable to detect	oracle_8821	aws-connector-us-east-1	Active	2	2 GiB	14 days ago
ee_alert9823	Encryption	Potential attack	Unable to detect	oracle_9819	aws-connector-us-east-1	Active	1	2 GiB	17 days ago
db_alert3932	Suspicious user behavior	Warning	Liam O'Reilly	mysql_9294, +3	aws-connector-us-east-1	Active	4	2 GiB	26 days ago
dd_alert7918	Data destruction	Potential attack	Amina Khan	vm_datastore_4719, +3	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_other_alert5319	Encryption	Potential attack	Raj Patel	vm_fileshare_6699	aws-connector-us-west-1...	Active	1	2 GiB	1 month ago
lun_alert_6285	Encryption	Potential attack	Unable to detect	lun_storage_01	aws-connector-us-east-1	Active	1	2 GiB	1 month ago
uba_alert_voi1	Data breach	Potential attack	Raj Patel	uba_rps_test_voi1, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_voi2	Data breach	Potential attack	Raj Patel	uba_rps_test_voi2, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago
uba_alert_voi3	Data breach	Potential attack	Raj Patel	uba_rps_test_voi3, +2	aws-connector-us-east-1...	Active	3	2 GiB	1 month ago

- 2. Na página Alertas, selecione o alerta.

Alerts > ee_alert8727

ee_alert8727

Impacted workloads: oracle_8821

Mark restore needed

2 Potential attacks

286 Impacted files

2 GiB Impacted data

September 25, 2025, 6:51 AM First detected

Incidents (2)

Edit status

Incident ID	Volume	Storage VM	System	Severity	Status	First detec...	Most rece...	Evidence	Automated res...
inc4922	oracle_useast_data2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	4 new extensions...	1 snapshot
inc3163	oracle_useast_log2	svm_VsaWorkingEnviro...	VsaWorkingEnvironme...	Potential attack	New	22 days ago	21 days ago	6 new extensions...	1 snapshot

- 3. Selecione um ou mais incidentes. Alternativamente, selecione todos os incidentes marcando a caixa ID do incidente no canto superior esquerdo da tabela.
- 4. Se você determinar que o incidente não é uma ameaça, descarte-o como um falso positivo:
 - Selecione o incidente.
 - Selecione o botão **Editar status** acima da tabela.

Edit status

Change the status to keep track of incidents that are not a threat.

Status

Select status ▲

Resolved

Dismissed

Save

Cancel

5. Na caixa Editar status, escolha o status **Dispensado**.

Aparecem informações adicionais sobre a carga de trabalho e as cópias de instantâneo excluídas.

6. Selecione **Salvar**.

O status do incidente ou incidentes muda para "Arquivado".

Ver uma lista de arquivos afetados

Antes de restaurar uma carga de trabalho de aplicativo no nível de arquivo, você pode visualizar uma lista de arquivos afetados. Você pode acessar a página Alertas para baixar uma lista de arquivos afetados. Em seguida, use a página Recuperação para carregar a lista e escolher quais arquivos restaurar.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Passos

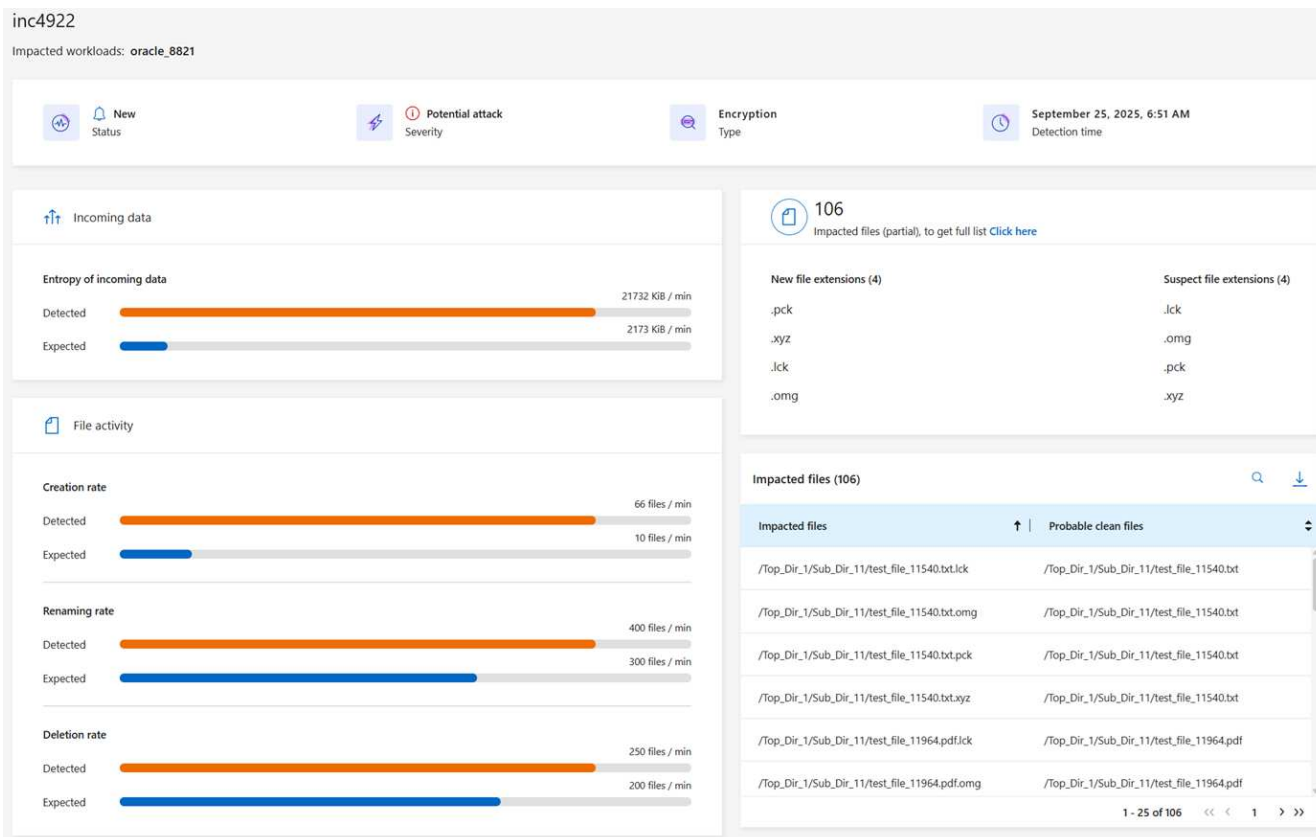
Use a página Alertas para recuperar a lista de arquivos afetados.



Se um volume tiver vários alertas, talvez seja necessário baixar a lista CSV dos arquivos afetados para cada alerta.

1. No menu Resiliência contra Ransomware, selecione **Alertas**.

2. Na página Alertas, classifique os resultados por carga de trabalho para mostrar os alertas para a carga de trabalho do aplicativo que você deseja restaurar.
3. Na lista de alertas para essa carga de trabalho, selecione um alerta.
4. Para esse alerta, selecione um único incidente.



5. Para esse incidente, selecione o ícone de download para baixar a lista de arquivos afetados no formato CSV.

Recupere-se de um ataque de ransomware (após a neutralização dos incidentes) com a NetApp Ransomware Resilience

Depois que as cargas de trabalho são marcadas como "Restauração necessária", o NetApp Ransomware Resilience recomenda um ponto de recuperação real (RPA) e orquestra o fluxo de trabalho para uma recuperação resistente a falhas.

- Se o aplicativo ou a VM for gerenciado pelo SnapCenter, o Ransomware Resilience restaurará o aplicativo ou a VM ao seu estado anterior e à última transação usando o processo consistente com o aplicativo ou com a VM. A restauração consistente com o aplicativo ou com a VM adiciona quaisquer dados que não foram armazenados, por exemplo, dados no cache ou em uma operação de E/S, aos dados no volume.
- Se o aplicativo ou a VM *não* for gerenciado pelo SnapCenter e for gerenciado pelo NetApp Backup and Recovery ou pelo Ransomware Resilience, o Ransomware Resilience executará uma restauração consistente em caso de falha, em que todos os dados que estavam no volume no mesmo ponto no tempo serão restaurados, por exemplo, se o sistema travar.

Você pode restaurar a carga de trabalho selecionando todos os volumes, volumes específicos ou arquivos específicos.



A recuperação da carga de trabalho pode afetar as cargas de trabalho em execução. Você deve coordenar os processos de recuperação com as partes interessadas apropriadas.

Uma carga de trabalho pode ter um dos seguintes status de restauração:

- **Restauração necessária:** A carga de trabalho precisa ser restaurada.
- **Em andamento:** A operação de restauração está em andamento.
- **Restaurado:** A carga de trabalho foi restaurada.
- **Falha:** O processo de restauração da carga de trabalho não pôde ser concluído.

Exibir cargas de trabalho que estão prontas para serem restauradas

Revise as cargas de trabalho que estão no status de recuperação "Restauração necessária".

Passos

1. Faça um dos seguintes:
 - No Painel, revise os totais de "Restauração necessária" no painel Alertas e selecione **Exibir tudo**.
 - No menu, selecione **Recuperação**.
2. Revise as informações da carga de trabalho na página **Recuperação**.

Recovery

Run readiness drill

Free trial (31 days left)

Recovery status

8

Restore needed

8 GiB data at risk

0

In progress

0 MiB data at risk

0

Restored

2 GiB data at risk

Workloads (8)

Workload	↑	Type	↕	Location	↕	Console agent	↕	Snapshot and backup poli...	↕	Recovery status	↕	Progress	↕	Importance	↕	Total data	↕	Action	↕
lun_storage_01		Block		10.0.1.10		aws-connector-us-east-1		Ransomware Resilience		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
mysql_9294		MySQL		10.0.1.10		aws-connector-us-east-1		Backup and Recovery		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
oracle_9819		Oracle		10.0.1.10		aws-connector-us-east-1		SnapCenter		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
uba_rps_test_vo1		File share		svm_cvoawsesd01rpsdemosand...		aws-connector-us-east-1-account-14092025		Ransomware Resilience		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
uba_rps_test_vo12		File share		svm_cvoawsesd01rpsdemosand...		aws-connector-us-east-1-account-14092025		Ransomware Resilience		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
uba_rps_test_vo13		File share		svm_cvoawsesd01rpsdemosand...		aws-connector-us-east-1-account-14092025		Ransomware Resilience		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	
vm_datastore_4719		VM datastore		10.0.1.57		aws-connector-us-east-1		SnapCenter for VMware		<div>Restore needed</div>		N/A		Standard		2 GiB		<div>Restore</div>	
vm_fileshare_6699		VM file share		10.0.1.215		aws-connector-us-west-1-account-LX05600...		Ransomware Resilience		<div>Restore needed</div>		N/A		Critical		2 GiB		<div>Restore</div>	

Restaurar uma carga de trabalho gerenciada pelo SnapCenter

Usando o Ransomware Resilience, o administrador de armazenamento pode determinar a melhor forma de restaurar cargas de trabalho a partir do ponto de restauração recomendado ou do ponto de restauração preferencial.

O estado do aplicativo será alterado se necessário para a restauração. O aplicativo será restaurado ao seu estado anterior a partir dos arquivos de controle, se eles estiverem incluídos no backup. Após a conclusão da restauração, o aplicativo é aberto no modo LEITURA-GRAVAÇÃO.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba](#)

Passos

1. Em Ransomware Resilience, selecione **Recuperação**.
2. Revise as informações da carga de trabalho na página **Recuperação**.
3. Selecione uma carga de trabalho que esteja no estado "Restauração necessária".
4. Para restaurar, selecione **Restaurar**.
5. **Escopo de restauração**: consistente com o aplicativo (ou para SnapCenter para VMs, o escopo de restauração é "Por VM")
6. **Fonte**: Selecione a seta para baixo ao lado de Fonte para ver detalhes. Selecione o ponto de restauração que você deseja usar para restaurar os dados.



O Ransomware Resilience identifica o melhor ponto de restauração como o backup mais recente imediatamente anterior ao incidente e mostra uma indicação "Recomendado".

7. **Destino**: Selecione a seta para baixo ao lado de Destino para ver detalhes.
 - a. Selecione o local original ou alternativo.
 - b. Selecione o sistema.
 - c. Selecione a VM de armazenamento.
8. Se o destino original não tiver espaço suficiente para restaurar a carga de trabalho, uma linha "Armazenamento temporário" será exibida. Você pode selecionar o armazenamento temporário para restaurar os dados da carga de trabalho. Os dados restaurados serão copiados do armazenamento temporário para o local original. Clique na **Seta para baixo** na linha Armazenamento temporário e defina o cluster de destino, a VM de armazenamento e a camada local.
9. Selecione **Salvar**.
10. Selecione **Avançar**.
11. Revise suas seleções.
12. Selecione **Restaurar**.
13. No menu superior, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Restaurar uma carga de trabalho não gerenciada pelo SnapCenter

Usando o Ransomware Resilience, o administrador de armazenamento pode determinar a melhor forma de restaurar cargas de trabalho a partir do ponto de restauração recomendado ou do ponto de restauração preferencial.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#) .

O administrador de armazenamento de segurança pode recuperar dados em diferentes níveis:

- Recuperação de todos os volumes
- Recuperar um aplicativo no nível de volume ou de arquivo e pasta.
- Recupere um compartilhamento de arquivos no nível de volume, diretório ou arquivo/pasta.

- Recuperar de um armazenamento de dados no nível de VM.

O processo difere dependendo do tipo de carga de trabalho.

Passos

1. No menu Resiliência contra Ransomware, selecione **Recuperação**.
2. Revise as informações da carga de trabalho na página **Recuperação**.
3. Selecione uma carga de trabalho que esteja no estado "Restauração necessária".
4. Para restaurar, selecione **Restaurar**.
5. **Escopo de restauração**: Selecione o tipo de restauração que deseja concluir:
 - Todos os volumes
 - Por volume
 - Por arquivo: você pode especificar uma pasta ou arquivos individuais para restaurar.



Para cargas de trabalho SAN, você só pode restaurar por carga de trabalho.



Você pode selecionar até 100 arquivos ou uma única pasta.

6. Continue com um dos procedimentos a seguir, dependendo se você escolheu aplicativo, volume ou arquivo.

Restaurar todos os volumes

1. No menu Resiliência contra Ransomware, selecione **Recuperação**.
2. Selecione uma carga de trabalho que esteja no estado "Restauração necessária".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no escopo Restaurar, selecione **Todos os volumes**.

Restore

Workload: mysql_9294 Host: 10.0.1.10 Type: MySQL Console agent: aws-connector-us-east-1

Restore scope: ☒ All volumes ☐ By volume ☐ By file

Source

First attack reported: October 2, 2025, 6:51 AM Restore points: ☒ Safest for all volumes ⓘ

Volumes (2)

Volume	Restore point	Type	Date	Size
mysql_useast_21	cts-snapshot-adhoc-16975531705	Backup	October 2, 2025, 6:21 AM	2 GiB
mysql_useast_22	cts-snapshot-adhoc-169755327497	Backup	September 29, 2025, 3:51 AM	2 GiB

Destination ☒ Action required

5. **Fonte**: Selecione a seta para baixo ao lado de Fonte para ver detalhes.
 - a. Selecione o ponto de restauração que você deseja usar para restaurar os dados.



O Ransomware Resilience identifica o melhor ponto de restauração como o backup mais recente imediatamente anterior ao incidente e mostra uma indicação "Mais seguro para todos os volumes". Isso significa que todos os volumes serão restaurados para uma cópia anterior ao primeiro ataque ao primeiro volume detectado.

6. **Destino:** Selecione a seta para baixo ao lado de Destino para ver detalhes.
 - a. Selecione o sistema.
 - b. Selecione a VM de armazenamento.
 - c. Selecione o agregado.
 - d. Altere o prefixo de volume que será adicionado a todos os novos volumes.



O novo nome do volume aparece como prefixo + nome do volume original + nome do backup + data do backup.

7. Selecione **Salvar**.
8. Selecione **Avançar**.
9. Revise suas seleções.
10. Selecione **Restaurar**.
11. No menu superior, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Restaurar uma carga de trabalho do aplicativo no nível do volume

1. No menu Resiliência contra Ransomware, selecione **Recuperação**.
2. Selecione uma carga de trabalho do aplicativo que esteja no estado "Restauração necessária".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no escopo Restaurar, selecione **Por volume**.

Restore

Workload: MySQL_9294 | Host: 10.0.1.10 | Type: MySQL | Connector: aws-connector-us-eas...

Restore scope: ☐ All volumes ☒ By volume ☐ By file

Select volume you want to restore and edit its settings.

Volumes (2) | 1 selected

Volume
<input checked="" type="checkbox"/> mysql_useast_21
<input type="checkbox"/> mysql_useast_22

mysql_useast_21 settings:

Attack reported October 17, 2023, 11:11 AM

Source	Select restore point

Destination	Action required

5. Na lista de volumes, selecione o volume que você deseja restaurar.
6. **Fonte:** Selecione a seta para baixo ao lado de Fonte para ver detalhes.
 - a. Selecione o ponto de restauração que você deseja usar para restaurar os dados.



O Ransomware Resilience identifica o melhor ponto de restauração como o backup mais recente imediatamente anterior ao incidente e mostra uma indicação "Recomendado".

7. **Destino:** Selecione a seta para baixo ao lado de Destino para ver detalhes.

- a. Selecione o sistema.
- b. Selecione a VM de armazenamento.
- c. Selecione o agregado.
- d. Revise o novo nome do volume.



O novo nome do volume aparece como o nome do volume original + nome do backup + data do backup.

8. Selecione **Salvar**.
9. Selecione **Avançar**.
10. Revise suas seleções.
11. Selecione **Restaurar**.
12. No menu superior, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Restaurar uma carga de trabalho do aplicativo no nível do arquivo

Antes de restaurar uma carga de trabalho de aplicativo no nível de arquivo, você pode visualizar uma lista de arquivos afetados. Você pode acessar a página Alertas para baixar uma lista de arquivos afetados. Em seguida, use a página Recuperação para carregar a lista e escolher quais arquivos restaurar.

Você pode restaurar uma carga de trabalho de aplicativo no nível de arquivo para o mesmo sistema ou para um sistema diferente.

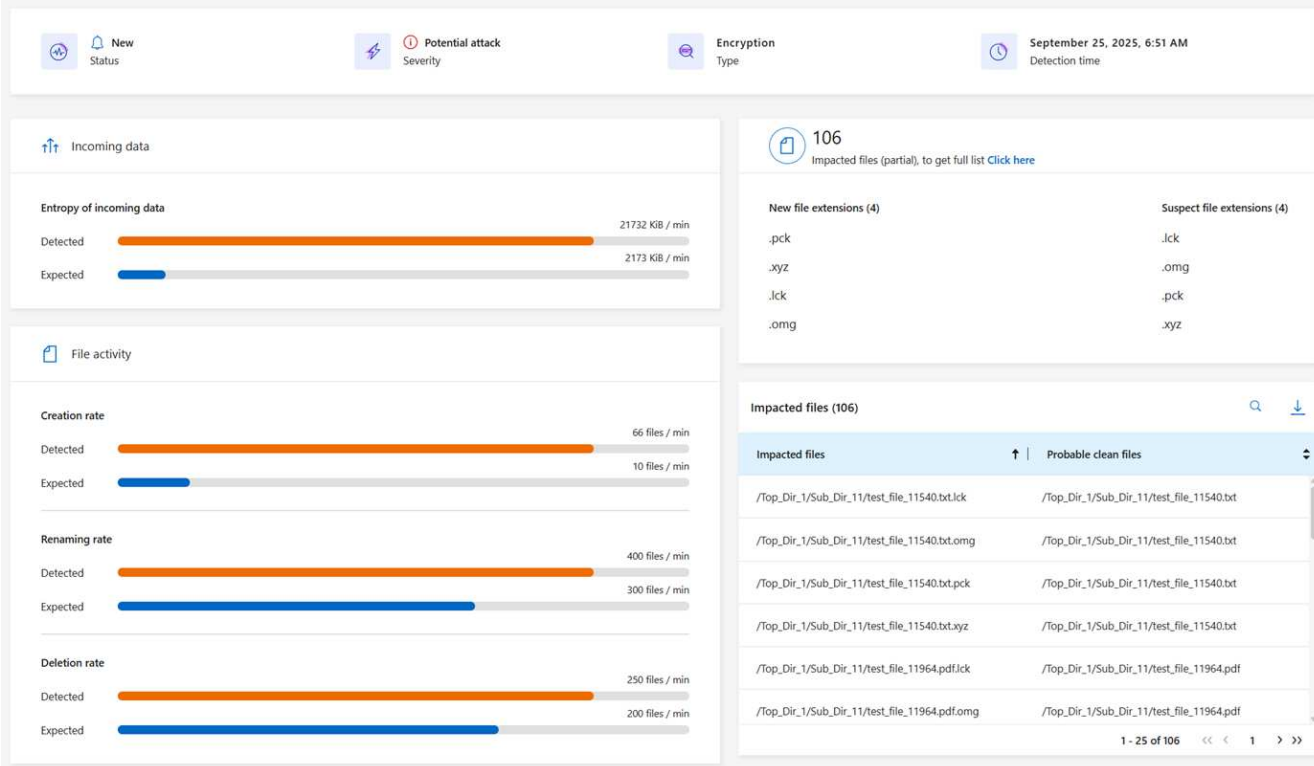
Etapas para obter a lista de arquivos afetados

Use a página Alertas para recuperar a lista de arquivos afetados.



Se um volume tiver vários alertas, você precisará baixar a lista CSV dos arquivos afetados para cada alerta.

1. No menu Resiliência contra Ransomware, selecione **Alertas**.
2. Na página Alertas, classifique os resultados por carga de trabalho para mostrar os alertas para a carga de trabalho do aplicativo que você deseja restaurar.
3. Na lista de alertas para essa carga de trabalho, selecione um alerta.
4. Para esse alerta, selecione um único incidente.



- Para ver a lista completa de arquivos, selecione **Clique aqui** na parte superior do painel Arquivos afetados.
- Para esse incidente, selecione o ícone de download e baixe a lista de arquivos afetados no formato CSV.

Etapas para restaurar esses arquivos

- No menu Resiliência contra Ransomware, selecione **Recuperação**.
- Selecione uma carga de trabalho do aplicativo que esteja no estado "Restauração necessária".
- Para restaurar, selecione **Restaurar**.
- Na página Restaurar, no escopo Restaurar, selecione **Por arquivo**.
- Na lista de volumes, selecione o volume que contém os arquivos que você deseja restaurar.
- Ponto de restauração:** Selecione a seta para baixo ao lado de **Ponto de restauração** para ver detalhes. Selecione o ponto de restauração que você deseja usar para restaurar os dados.



A coluna Motivo no painel Pontos de restauração mostra o motivo do snapshot ou backup como "Agendado" ou "Resposta automatizada ao incidente de ransomware".

7. Arquivos:

- **Selecionar arquivos automaticamente:** Deixe o Ransomware Resilience selecionar os arquivos a serem restaurados.
- **Carregar lista de arquivos:** Carregue um arquivo CSV que contenha a lista de arquivos afetados que você obteve na página Alertas ou que você possui. Você pode restaurar até 10.000 arquivos por vez.

Restore scope: ☐ All volumes ☐ By volume ☒ By file

Select volume you want to restore and edit its settings.

Volumes (2) | Selected rows (1)

Volume	
<input type="radio"/> mysql_useast_21	
<input checked="" type="radio"/> mysql_useast_22	

mysql_useast_22settings:

First attack reported September 9, 2025, 1:57 PM

Source: Restore point: cbs-snapshot-adho... | Type: Backup | Date: September 6, 2025, 10:57 AM

Files

File selection: ☐ Automatically select files ☒ Upload list of files ☐ Manually select files

Upload a list of files impacted by the ransomware attack that you want to restore from the selected restore point.

Warning: Download the list of 3 impacted files that must be restored from a different restore point and then restore them later.

Upload list of impacted files (CSV) ⓘ

Uploaded impacted file list (2) ☒ Download impacted file list (3)

Destination ⓘ Action required

- **Selecionar arquivos manualmente:** Selecione até 10.000 arquivos ou uma única pasta para restaurar.

Restore "mysql_9294"

Restore scope: ☐ All volumes ☐ By volume ☒ By file

Select volume you want to restore and edit its settings.

Volumes (2) | Selected rows (1)

Volume	
<input checked="" type="radio"/> mysql_useast_21	
<input type="radio"/> mysql_useast_22	

mysql_useast_21settings:

First attack reported October 2, 2025, 6:51 AM

Source: Restore point: Ant ransomware_b... | Type: Snapshot | Date: October 1, 2025, 6:21 AM

Files

File selection: ☐ Automatically select files ☐ Upload list of files ☒ Manually select files

Selected files

file_to_verify_first_snapshot.txt
mysql.ibd
file_to_verify_third_snapshot.txt
src_file
ibdata1
file_to_verify_second_snapshot.txt

Selected Files or directory (6)

Type	Name	Last modified	Size
<input type="checkbox"/>	ant_ransomware_analytic_log	October 1, 2025, 6:21 AM	4 KB
<input checked="" type="checkbox"/>	file_to_verify_first_snapshot.txt	October 1, 2025, 6:21 AM	12.00 B
<input checked="" type="checkbox"/>	mysql.ibd	October 1, 2025, 6:21 AM	24 MB
<input checked="" type="checkbox"/>	file_to_verify_second_snapshot.txt	October 1, 2025, 6:21 AM	12.00 B
<input type="checkbox"/>	simulate_ransomware_attack.sh	October 1, 2025, 6:21 AM	2 KB
<input checked="" type="checkbox"/>	ibdata1	October 1, 2025, 6:21 AM	12 MB
<input checked="" type="checkbox"/>	src_file	October 1, 2025, 6:21 AM	1 MB
<input checked="" type="checkbox"/>	file_to_verify_third_snapshot.txt	October 1, 2025, 6:21 AM	12.00 B

Destination ⓘ Action required

Next



Se algum arquivo não puder ser restaurado usando o ponto de restauração selecionado, uma mensagem será exibida indicando o número de arquivos que não podem ser restaurados e permitirá que você baixe a lista desses arquivos selecionando **Baixar lista de arquivos afetados**.

- Destino:** Selecione a seta para baixo ao lado de Destino para ver detalhes.
 - Escolha onde restaurar os dados: local de origem ou um local alternativo que você pode especificar.



Embora os arquivos ou diretórios originais sejam substituídos pelos dados restaurados, os nomes dos arquivos e pastas originais permanecerão os mesmos, a menos que você especifique novos nomes.

- b. Selecione o sistema.
- c. Selecione a VM de armazenamento.
- d. Opcionalmente, insira o caminho.



Se você não especificar um caminho para a restauração, os arquivos serão restaurados em um novo volume no diretório de nível superior.

- e. Selecione se você deseja que os nomes dos arquivos ou diretórios restaurados sejam os mesmos nomes do local atual ou nomes diferentes.
9. Selecione **Avançar**.
 10. Revise suas seleções.
 11. Selecione **Restaurar**.
 12. No menu superior, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Restaurar um compartilhamento de arquivos ou armazenamento de dados

1. Depois de selecionar um compartilhamento de arquivos ou armazenamento de dados para restaurar, na página Restaurar, no escopo Restaurar, selecione **Por volume**.

The screenshot displays the 'Restore' interface. At the top, it shows the workload 'uba_rps_test_vol3' and the host 'svm_cvawest01rpsdemoandbox-14092025'. The 'Restore scope' is set to 'By volume'. A table lists the volume 'uba_rps_test_vol3' as selected. The 'Destination' section is expanded, showing the 'System' as 'system_uba_rps_test_vol3', the 'Storage VM' as 'svm_cvawest01rpsdemoandbox-14092025', and the 'Aggregate' as 'agr1'. The 'New volume name' is 'uba_rps_test_vol3_daily_2023_11_23_0010'. A 'Save' button is at the bottom of the destination section.

2. Na lista de volumes, selecione o volume que você deseja restaurar.
3. **Fonte:** Selecione a seta para baixo ao lado de Fonte para ver detalhes.
 - a. Selecione o ponto de restauração que você deseja usar para restaurar os dados.



O Ransomware Resilience identifica o melhor ponto de restauração como o backup mais recente imediatamente anterior ao incidente e mostra uma indicação "Recomendado".

4. **Destino:** Selecione a seta para baixo ao lado de Destino para ver detalhes.
 - a. Escolha onde restaurar os dados: local de origem ou um local alternativo que você pode especificar.



Embora os arquivos ou diretórios originais sejam substituídos pelos dados restaurados, os nomes dos arquivos e pastas originais permanecerão os mesmos, a menos que você especifique novos nomes.

- b. Selecione o sistema.
- c. Selecione a VM de armazenamento.
- d. Opcionalmente, insira o caminho.



Se você não especificar um caminho para a restauração, os arquivos serão restaurados em um novo volume no diretório de nível superior.

5. Selecione **Salvar**.
6. Revise suas seleções.
7. Selecione **Restaurar**.
8. No menu, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Restaurar um compartilhamento de arquivos de VM no nível da VM

Na página Recuperação, depois de selecionar uma VM para restaurar, continue com estas etapas.

1. **Fonte:** Selecione a seta para baixo ao lado de Fonte para ver detalhes.

Restore

Workload: vm_datastore_4719 | Location: 10.0.1.57 | VCenter: 10.195.52.128 | Type: VM datastore | Console agent: aws-connector-us-east-1

Restore scope

VM-consistent
Restore a VM back to its previous state and last transaction using SnapCenter for VMware

Source

First attack reported October 2, 2025, 6:51 AM

Restore points (8)

Restore point	Type	Date
<input type="radio"/> RG-vm_datastore_202_11.30.01.0238	backup	October 2, 2025, 6:21 AM
<input type="radio"/> vsim56_rg1_05.26.00.0742	snapshot	October 2, 2025, 1:21 AM
<input type="radio"/> vsim56_rg1_05.46.18.0046	snapshot	October 2, 2025, 12:51 AM
<input type="radio"/> vsim56_rg1_04.54.00.0716	snapshot	October 2, 2025, 12:21 AM
<input type="radio"/> vsim56_rg1_04.42.40.0486	snapshot	October 1, 2025, 11:51 PM
<input type="radio"/> RG-vm_datastore_202_11.30.01.0260	backup	October 1, 2025, 6:21 AM
<input type="radio"/> RG-vm_datastore_202_11.30.01.0250	backup	September 30, 2025, 6:21 AM
<input type="radio"/> RG-vm_datastore_202_11.30.01.0871	backup	September 28, 2025, 6:21 AM

Destination

Original location

2. Selecione o ponto de restauração que você deseja usar para restaurar os dados.
3. **Destino:** Para o local original.
4. Selecione **Avançar**.
5. Revise suas seleções.
6. Selecione **Restaurar**.
7. No menu, selecione **Recuperação** para revisar a carga de trabalho na página Recuperação, onde o status da operação passa pelos estados.

Baixe relatórios no NetApp Ransomware Resilience

Você pode exportar dados de proteção e baixar os arquivos CSV ou JSON que mostram detalhes de exercícios de prontidão para ataques, proteção, alertas e recuperação.



Antes de baixar os arquivos, atualize o painel para obter os dados mais recentes em seus relatórios.

Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto, administrador do Ransomware Resilience ou visualizador do Ransomware Resilience. ["Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console"](#).

Quais dados você pode baixar? Você pode baixar arquivos de qualquer uma das opções do menu principal:

- **Resumo:** Inclui listas de cargas de trabalho suportadas e não suportadas, ações recomendadas para melhorar sua postura de resiliência cibernética e informações coletadas no painel de Resiliência a Ransomware.
- **Proteção:** Inclui o status e os detalhes de todas as cargas de trabalho, incluindo o número total de cargas protegidas e em risco.
- **Alertas:** Inclui o status e os detalhes de todos os alertas, incluindo o número total de alertas e instantâneos automatizados.
- **Recuperação:** Inclui o status e os detalhes de todas as cargas de trabalho que precisam ser restauradas, incluindo o número total de cargas de trabalho marcadas como "Restauração necessária", "Em andamento", "Falha na restauração" e "Restauradas com sucesso".
- **Relatórios:** Você pode exportar dados de qualquer uma das páginas e baixar os arquivos.



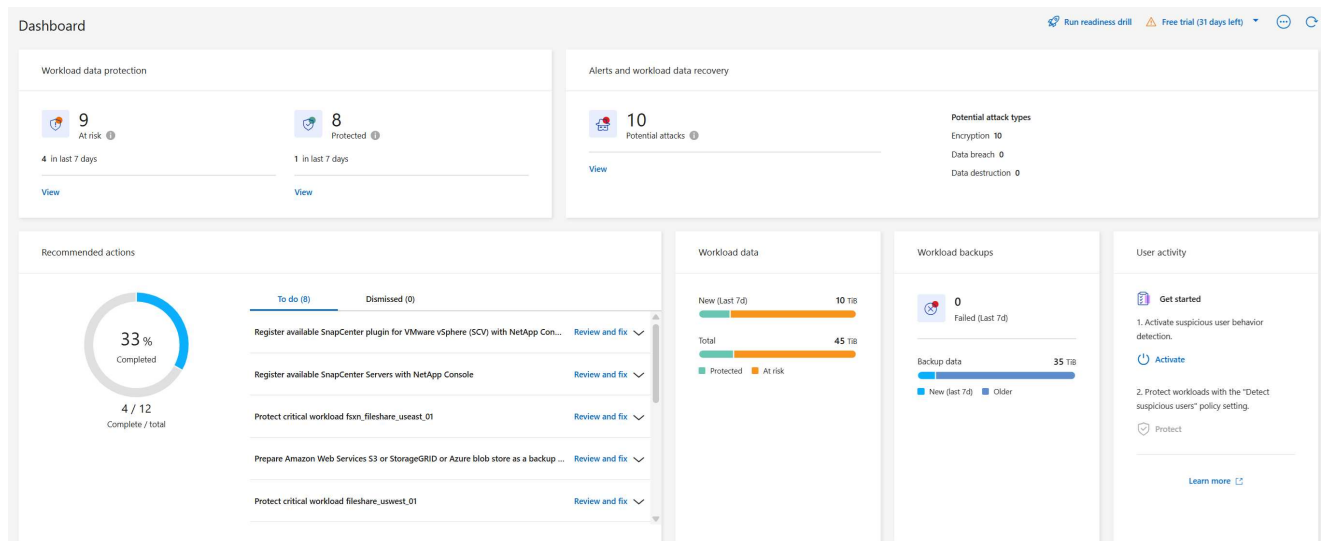
Você pode baixar relatórios de exercícios de prontidão somente na página **Relatórios**.



Se você baixar arquivos CSV ou JSON da página Proteção, Alertas ou Recuperação, os dados mostrarão apenas os dados dessa página.

Os arquivos CSV ou JSON incluem dados para todas as cargas de trabalho em todos os sistemas do Console.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção > Resiliência a Ransomware**.








- No Painel ou em outra página, selecione *Atualizar*  opção no canto superior direito para atualizar os dados que aparecerão nos relatórios.
- Faça um dos seguintes:
 - Na página, selecione *Download*  opção.
 - No menu NetApp Ransomware Resilience, selecione **Relatórios**.
- Se você selecionou a opção **Relatórios**, selecione um dos nomes de arquivo pré-configurados e selecione **Baixar**.

Reports

Review protection status, alerts, and recovery details to monitor and maintain system health.

Run readiness drill | Free trial (30 days left)

	Summary Summary of workload metrics	Download (JSON)
	Protection Tabular details for all workloads that are at risk and protected	Download (CSV)
	Alerts Tabular details for all alerts	Download (CSV)
	Recovery Tabular details for workloads marked restore needed, in progress, restore failed, and successfully restored	Download (CSV)
	Readiness drills Details for simulated ransomware attacks and recovery	Download (JSON)

Conhecimento e suporte

Registre-se para obter suporte

O registro de suporte é necessário para receber suporte técnico específico para o NetApp Console e suas soluções de armazenamento e serviços de dados. O registro de suporte também é necessário para habilitar fluxos de trabalho importantes para sistemas Cloud Volumes ONTAP .

O registro para suporte não habilita o suporte da NetApp para um serviço de arquivo do provedor de nuvem. Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte "Obter ajuda" na documentação do produto.

- ["Amazon FSx para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Visão geral do registro de suporte

Existem duas formas de registro para ativar o direito ao suporte:

- Registrando o número de série da sua conta do NetApp Console (seu número de série 960xxxxxxxxx de 20 dígitos localizado na página Recursos de suporte no Console).

Isso serve como seu único ID de assinatura de suporte para qualquer serviço no Console. Cada conta do Console deve ser registrada.

- Registrando os números de série do Cloud Volumes ONTAP associados a uma assinatura no marketplace do seu provedor de nuvem (são números de série 909201xxxxxxxx de 20 dígitos).

Esses números de série são comumente chamados de *números de série PAYGO* e são gerados pelo NetApp Console no momento da implantação do Cloud Volumes ONTAP .

Registrar ambos os tipos de números de série habilita recursos como abertura de tickets de suporte e geração automática de casos. O registro é concluído adicionando contas do NetApp Support Site (NSS) ao Console, conforme descrito abaixo.

Registre o NetApp Console para suporte ao NetApp

Para se registrar para obter suporte e ativar o direito ao suporte, um usuário na sua conta do NetApp Console deve associar uma conta do NetApp Support Site ao seu login no Console. A maneira como você se registra para o suporte da NetApp depende se você já tem uma conta no NetApp Support Site (NSS).

Cliente existente com uma conta NSS

Se você for um cliente NetApp com uma conta NSS, basta se registrar para receber suporte pelo Console.

Passos

1. Selecione **Administração > Credenciais**.
2. Selecione **Credenciais do usuário**.

3. Selecione **Adicionar credenciais NSS** e siga o prompt de autenticação do NetApp Support Site (NSS).
4. Para confirmar que o processo de registro foi bem-sucedido, selecione o ícone Ajuda e selecione **Suporte**.

A página **Recursos** deve mostrar que sua conta do Console está registrada para suporte.

Observe que outros usuários do Console não verão o mesmo status de registro de suporte se não tiverem associado uma conta do Site de Suporte da NetApp ao seu login. No entanto, isso não significa que sua conta não esteja registrada para suporte. Desde que um usuário na organização tenha seguido essas etapas, sua conta foi registrada.

Cliente existente, mas sem conta NSS

Se você já for um cliente da NetApp com licenças e números de série existentes, mas *nenhuma* conta NSS, será necessário criar uma conta NSS e associá-la ao seu login do Console.

Passos

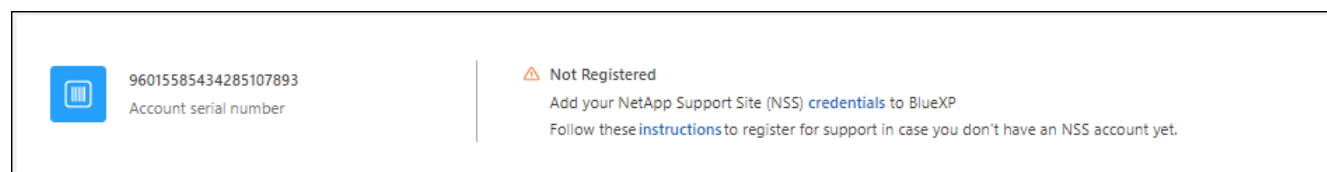
1. Crie uma conta no site de suporte da NetApp preenchendo o ["Formulário de registro de usuário do site de suporte da NetApp"](#)
 - a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
 - b. Certifique-se de copiar o número de série da conta do Console (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento da conta.
2. Associe sua nova conta NSS ao seu login do Console concluindo as etapas em [Cliente existente com uma conta NSS](#).

Novidade na NetApp

Se você é novo na NetApp e não tem uma conta NSS, siga cada etapa abaixo.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.
2. Localize o número de série do seu ID de conta na página de Registro de Suporte.



3. Navegar para ["Site de registro de suporte da NetApp"](#) e selecione *Não sou um cliente registrado da NetApp*.
4. Preencha os campos obrigatórios (aqueles com asteriscos vermelhos).
5. No campo **Linha de produtos**, selecione **Cloud Manager** e, em seguida, selecione seu provedor de cobrança aplicável.
6. Copie o número de série da sua conta da etapa 2 acima, conclua a verificação de segurança e confirme que você leu a Política Global de Privacidade de Dados da NetApp.

Um e-mail é enviado imediatamente para a caixa de correio fornecida para finalizar esta transação segura. Não deixe de verificar sua caixa de spam caso o e-mail de validação não chegue em alguns minutos.

7. Confirme a ação no e-mail.

A confirmação envia sua solicitação à NetApp e recomenda que você crie uma conta no site de suporte da NetApp .

8. Crie uma conta no site de suporte da NetApp preenchendo o ["Formulário de registro de usuário do site de suporte da NetApp"](#)

- a. Certifique-se de selecionar o Nível de usuário apropriado, que normalmente é * Cliente/Usuário final da NetApp *.
- b. Certifique-se de copiar o número de série da conta (960xxxx) usado acima para o campo de número de série. Isso acelerará o processamento.

Depois que você terminar

A NetApp entrará em contato com você durante esse processo. Este é um exercício de integração único para novos usuários.

Depois de ter sua conta do Site de Suporte NetApp , associe a conta ao seu login do Console concluindo as etapas em [Cliente existente com uma conta NSS](#) .

Credenciais associadas do NSS para suporte do Cloud Volumes ONTAP

É necessário associar as credenciais do NetApp Support Site à sua conta do Console para habilitar os seguintes fluxos de trabalho principais para o Cloud Volumes ONTAP:

- Registrando sistemas Cloud Volumes ONTAP de pagamento conforme o uso para suporte

É necessário fornecer sua conta NSS para ativar o suporte para seu sistema e obter acesso aos recursos de suporte técnico da NetApp .

- Implantando o Cloud Volumes ONTAP quando você traz sua própria licença (BYOL)

É necessário fornecer sua conta NSS para que o Console possa carregar sua chave de licença e habilitar a assinatura para o período que você comprou. Isso inclui atualizações automáticas para renovações de prazo.

- Atualizando o software Cloud Volumes ONTAP para a versão mais recente

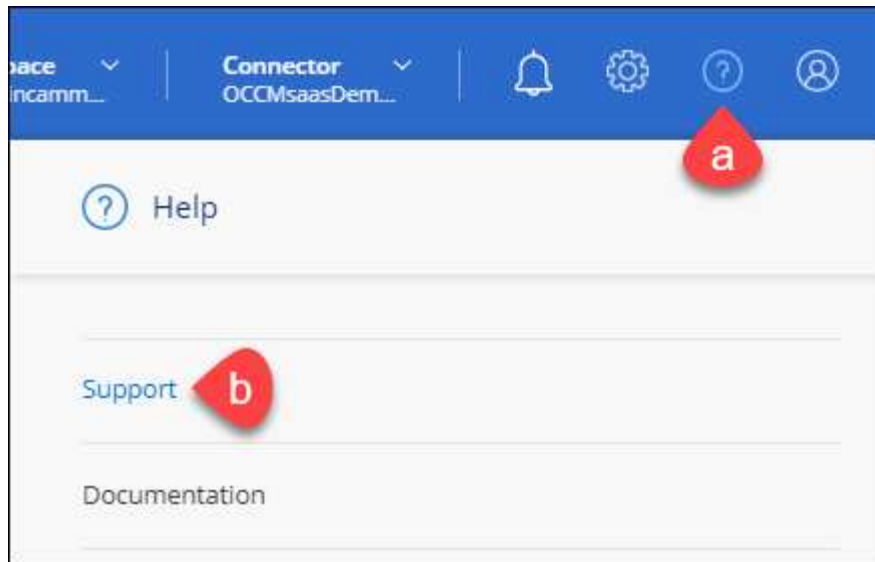
A associação de credenciais do NSS à sua conta do NetApp Console é diferente da associação da conta do NSS a um login de usuário do Console.

Essas credenciais NSS estão associadas ao ID específico da sua conta do Console. Usuários que pertencem à organização Console podem acessar essas credenciais em **Suporte > Gerenciamento NSS**.

- Se você tiver uma conta de nível de cliente, poderá adicionar uma ou mais contas NSS.
- Se você tiver uma conta de parceiro ou revendedor, poderá adicionar uma ou mais contas NSS, mas elas não poderão ser adicionadas junto com contas de nível de cliente.

Passos

1. No canto superior direito do Console, selecione o ícone Ajuda e selecione **Suporte**.



2. Selecione **Gerenciamento NSS > Adicionar conta NSS**.

3. Quando solicitado, selecione **Continuar** para ser redirecionado para uma página de login da Microsoft.

A NetApp usa o Microsoft Entra ID como provedor de identidade para serviços de autenticação específicos para suporte e licenciamento.

4. Na página de login, forneça seu endereço de e-mail e senha registrados no Site de Suporte da NetApp para realizar o processo de autenticação.

Essas ações permitem que o Console use sua conta NSS para coisas como downloads de licenças, verificação de atualização de software e registros de suporte futuros.

Observe o seguinte:

- A conta NSS deve ser uma conta de nível de cliente (não uma conta de convidado ou temporária). Você pode ter várias contas NSS em nível de cliente.
- Só pode haver uma conta NSS se essa conta for uma conta de nível de parceiro. Se você tentar adicionar contas NSS em nível de cliente e existir uma conta em nível de parceiro, você receberá a seguinte mensagem de erro:

"O tipo de cliente NSS não é permitido para esta conta, pois já existem usuários NSS de tipos diferentes."

O mesmo é verdadeiro se você tiver contas NSS pré-existentes em nível de cliente e tentar adicionar uma conta em nível de parceiro.

- Após o login bem-sucedido, o NetApp armazenará o nome de usuário do NSS.

Este é um ID gerado pelo sistema que mapeia para seu e-mail. Na página **NSS Management**, você pode exibir seu e-mail do **...** menu.

- Se você precisar atualizar seus tokens de credenciais de login, também há uma opção **Atualizar credenciais** no **...** menu.

Usar esta opção solicitará que você faça login novamente. Observe que o token para essas contas expira após 90 dias. Uma notificação será publicada para alertá-lo sobre isso.

Obter ajuda

A NetApp fornece suporte para o NetApp Console e seus serviços de nuvem de diversas maneiras. Há diversas opções gratuitas de autoatendimento disponíveis 24 horas por dia, 7 dias por semana, como artigos da base de conhecimento (KB) e um fórum da comunidade. Seu cadastro no suporte inclui suporte técnico remoto por meio de tickets online.

Obtenha suporte para um serviço de arquivo de provedor de nuvem

Para obter suporte técnico relacionado a um serviço de arquivo do provedor de nuvem, sua infraestrutura ou qualquer solução que use o serviço, consulte a documentação desse produto.

- ["Amazon FSx para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Google Cloud NetApp Volumes"](#)

Para receber suporte técnico específico para a NetApp e suas soluções de armazenamento e serviços de dados, use as opções de suporte descritas abaixo.

Use opções de autoapoio

Estas opções estão disponíveis gratuitamente, 24 horas por dia, 7 dias por semana:

- Documentação

A documentação do NetApp Console que você está visualizando no momento.

- ["Base de conhecimento"](#)

Pesquise na base de conhecimento da NetApp para encontrar artigos úteis para solucionar problemas.

- ["Comunidades"](#)

Participe da comunidade do NetApp Console para acompanhar discussões em andamento ou criar novas.

Crie um caso com o suporte da NetApp

Além das opções de autossuporte acima, você pode trabalhar com um especialista em suporte da NetApp para resolver quaisquer problemas após ativar o suporte.

Antes de começar

- Para usar o recurso **Criar um caso**, você deve primeiro associar suas credenciais do site de suporte da NetApp ao seu login do console. ["Aprenda a gerenciar credenciais associadas ao seu login do Console"](#).
- Se você estiver abrindo um caso para um sistema ONTAP que tenha um número de série, sua conta NSS deverá estar associada ao número de série desse sistema.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Na página **Recursos**, escolha uma das opções disponíveis em Suporte Técnico:

- a. Selecione **Ligue para nós** se quiser falar com alguém por telefone. Você será direcionado para uma página no netapp.com que lista os números de telefone para os quais você pode ligar.
- b. Selecione **Criar um caso** para abrir um tíquete com um especialista de suporte da NetApp :
- **Serviço:** Selecione o serviço ao qual o problema está associado. Por exemplo, * NetApp Console* quando específico para um problema de suporte técnico com fluxos de trabalho ou funcionalidade dentro do Console.
 - **Sistema:** Se aplicável ao armazenamento, selecione * Cloud Volumes ONTAP* ou **On-Prem** e, em seguida, o ambiente de trabalho associado.

A lista de sistemas está dentro do escopo da organização do Console e do agente do Console que você selecionou no banner superior.

- **Prioridade do caso:** escolha a prioridade do caso, que pode ser Baixa, Média, Alta ou Crítica.

Para saber mais detalhes sobre essas prioridades, passe o mouse sobre o ícone de informações ao lado do nome do campo.

- **Descrição do problema:** Forneça uma descrição detalhada do seu problema, incluindo quaisquer mensagens de erro aplicáveis ou etapas de solução de problemas que você executou.
- **Endereços de e-mail adicionais:** insira endereços de e-mail adicionais se quiser informar outra pessoa sobre esse problema.
- **Anexo (Opcional):** Carregue até cinco anexos, um de cada vez.

Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

Depois que você terminar

Um pop-up aparecerá com o número do seu caso de suporte. Um especialista em suporte da NetApp analisará seu caso e entrará em contato com você em breve.

Para obter um histórico dos seus casos de suporte, você pode selecionar **Configurações > Linha do tempo** e procurar por ações chamadas "criar caso de suporte". Um botão na extrema direita permite expandir a ação para ver detalhes.

É possível que você encontre a seguinte mensagem de erro ao tentar criar um caso:

"Você não está autorizado a criar um caso contra o serviço selecionado"

Esse erro pode significar que a conta NSS e a empresa registrada à qual ela está associada não são a mesma empresa registrada para o número de série da conta do NetApp Console (por exemplo, 960xxxx) ou o número de série do ambiente de trabalho. Você pode buscar assistência usando uma das seguintes opções:

- Envie um caso não técnico em <https://mysupport.netapp.com/site/help>

Gerencie seus casos de suporte

Você pode visualizar e gerenciar casos de suporte ativos e resolvidos diretamente do Console. Você pode gerenciar os casos associados à sua conta NSS e à sua empresa.

Observe o seguinte:

- O painel de gerenciamento de casos na parte superior da página oferece duas visualizações:
 - A visualização à esquerda mostra o total de casos abertos nos últimos 3 meses pela conta NSS do usuário que você forneceu.
 - A visualização à direita mostra o total de casos abertos nos últimos 3 meses no nível da sua empresa com base na sua conta de usuário NSS.

Os resultados na tabela refletem os casos relacionados à exibição que você selecionou.

- Você pode adicionar ou remover colunas de interesse e filtrar o conteúdo de colunas como Prioridade e Status. Outras colunas fornecem apenas recursos de classificação.



Veja as etapas abaixo para mais detalhes.

- Em cada caso, oferecemos a possibilidade de atualizar notas do caso ou fechar um caso que ainda não esteja no status Fechado ou Pendente Fechado.

Passos

1. No NetApp Console, selecione **Ajuda > Suporte**.
2. Selecione **Gerenciamento de casos** e, se solicitado, adicione sua conta NSS ao Console.

A página **Gerenciamento de casos** mostra casos abertos relacionados à conta NSS associada à sua conta de usuário do Console. Esta é a mesma conta NSS que aparece no topo da página **Gerenciamento NSS**.

3. Modifique opcionalmente as informações exibidas na tabela:
 - Em **Casos da organização**, selecione **Exibir** para visualizar todos os casos associados à sua empresa.
 - Modifique o intervalo de datas escolhendo um intervalo de datas exato ou escolhendo um período de tempo diferente.
 - Filtrar o conteúdo das colunas.
 - Altere as colunas que aparecem na tabela selecionando  e então escolher as colunas que você gostaria de exibir.
4. Gerencie um caso existente selecionando  e selecionando uma das opções disponíveis:
 - **Ver caso**: Veja detalhes completos sobre um caso específico.
 - **Atualizar notas do caso**: Forneça detalhes adicionais sobre seu problema ou selecione **Carregar arquivos** para anexar até no máximo cinco arquivos.

Os anexos são limitados a 25 MB por arquivo. As seguintes extensões de arquivo são suportadas: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx e csv.

- **Fechar caso**: Forneça detalhes sobre o motivo pelo qual você está fechando o caso e selecione **Fechar caso**.

Perguntas frequentes sobre a NetApp Ransomware Resilience

Estas perguntas frequentes podem ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta sobre o NetApp Ransomware Resilience.

Implantação

Você precisa de uma licença para usar o Ransomware Resilience?

Você pode usar os seguintes tipos de licença:

- Inscreva-se para um teste gratuito de 30 dias.
- Adquira uma assinatura pré-paga (PAYGO) do NetApp Intelligent Services e Ransomware Resilience com o Amazon Web Services (AWS) Marketplace, o Google Cloud Marketplace e o Microsoft Azure Marketplace.
- Traga sua própria licença (BYOL), que é um arquivo de licença NetApp (NLF) que você obtém com seu representante de vendas da NetApp . Você pode usar o número de série da licença para ativar o BYOL na seção Licenses and subscriptions do console.

Como habilitar a resiliência a ransomware?

Você pode acessar o Ransomware Resilience no NetApp Console. Certifique-se de que você tem ["funções de acesso"](#) e ["pré-requisitos"](#). Se você configurou com sucesso um agente de console, poderá então... ["descobrir cargas de trabalho"](#).

Para mais informações, consulte ["Resiliência do Access Ransomware"](#) e ["Guia de início rápido para resiliência a ransomware"](#).

A Resiliência a Ransomware está disponível nos modos padrão, restrito e privado?

A Resiliência a Ransomware está disponível atualmente apenas no modo padrão.

Para obter uma explicação sobre esses modos em todos os serviços de dados da NetApp , consulte ["Modos de implantação do NetApp Console"](#).

Acesso

Qual é a URL de Resiliência a Ransomware?

Em um navegador, digite ["https://console.netapp.com/ransomware-resilience"](https://console.netapp.com/ransomware-resilience) Para acessar o Console.

Como são gerenciadas as permissões de acesso?

["Saiba mais sobre as funções de acesso do Console para todos os serviços"](#). A resiliência a ransomware também possui ["funções de acesso dedicadas"](#).

Qual a melhor resolução para o dispositivo?

A resolução de dispositivo recomendada para o Ransomware Resilience é 1920x1080 ou melhor.

Qual navegador devo usar?

Você pode acessar o NetApp Console com qualquer navegador web moderno.

Interoperabilidade

O Ransomware Resilience está ciente das configurações de proteção no ONTAP?

Sim, o Ransomware Resilience descobre agendamentos de snapshots definidos no ONTAP.

Como a Resiliência a Ransomware interage com o NetApp Backup and Recovery e o SnapCenter?

A Resiliência contra Ransomware funciona em conjunto com o Backup e Recuperação para descobrir e definir políticas de snapshot e backup para cargas de trabalho de compartilhamento de arquivos.

O Ransomware Resilience funciona com o SnapCenter ou o SnapCenter para VMware para descobrir e definir políticas de snapshot e backup para cargas de trabalho de aplicativos e máquinas virtuais.

O Ransomware Resilience também funciona com o Backup and Recovery e o SnapCenter (incluindo o SnapCenter para VMware) para realizar a recuperação de arquivos e cargas de trabalho de forma consistente.

Para licenciamento e faturamento, o Ransomware Resilience pode ser integrado ao Backup e Recuperação, mesmo que você não tenha uma licença separada para Backup e Recuperação. Se você tiver o Backup and Recovery e o Ransomware Resilience, quaisquer dados comuns protegidos por ambos os produtos serão cobrados somente pelo Ransomware Resilience.

Cargas de trabalho

O que é uma carga de trabalho no contexto da resiliência a ransomware?

Uma carga de trabalho é um aplicativo, uma VM ou um compartilhamento de arquivos. Uma carga de trabalho inclui todos os volumes usados por uma única instância do aplicativo.

Por exemplo, considere um banco de dados Oracle implantado em ora3.host.com com `vol1` contendo dados e `vol2` contendo registros. Os dois volumes constituem a carga de trabalho para essa instância do Oracle Database.

Como o Ransomware Resilience prioriza os dados de carga de trabalho?

A prioridade da carga de trabalho (crítica, padrão, importante) é determinada pelas frequências de snapshots já aplicadas a cada volume associado à carga de trabalho e pelos backups agendados.

["Aprenda sobre a prioridade ou importância da carga de trabalho"](#) .

Quais cargas de trabalho o Ransomware Resilience suporta?

A ferramenta de Resiliência a Ransomware pode identificar as seguintes cargas de trabalho: Oracle, compartilhamentos de arquivos, armazenamento em blocos, máquinas virtuais e datastores de máquinas virtuais.

Se você usa o SnapCenter ou o SnapCenter para VMware, todas as cargas de trabalho compatíveis com esses produtos também são identificadas no Ransomware Resilience. A Resiliência contra Ransomware pode proteger e recuperar o SnapCenter e as cargas de trabalho do SnapCenter de forma consistente com a carga de trabalho.

Como associar dados a uma carga de trabalho?

A Resiliência a Ransomware descobre os volumes e as extensões de arquivo e os associa à carga de trabalho apropriada.

Se você tiver o SnapCenter ou o SnapCenter para VMware e tiver configurado cargas de trabalho no Backup e Recuperação, o Ransomware Resilience detectará as cargas de trabalho gerenciadas pelo SnapCenter e

SnapCenter para VMware, bem como seus volumes associados.

O que é uma carga de trabalho protegida?

Na Resiliência a Ransomware, uma carga de trabalho exibe o status **protegida** quando possui uma política de *detecção* primária ativada, o que significa que... "[Proteção Autônoma contra Ransomware \(ARP\)](#)" Está habilitado em todos os volumes relacionados à carga de trabalho.

O que é uma carga de trabalho "de risco"?

Se uma carga de trabalho não tiver uma política de *detecção* primária ativada, ela será rotulada como "em risco", mesmo que tenha uma política de backup e snapshot ativada. Para proteção contra ransomware, você deve habilitar um "[política de detecção](#)".

Adicionei um novo volume, mas ele ainda não apareceu. O que devo fazer?

Se você adicionou um novo volume ao seu ambiente, inicie a descoberta da carga de trabalho novamente. Após o volume ter sido descoberto, "[Aplicar políticas de proteção para proteger o novo volume](#)".

Políticas de proteção

As políticas de resiliência a ransomware coexistem com outros tipos de políticas de carga de trabalho?

No momento, o Backup e Recuperação (Cloud Backup) oferece suporte a uma política de backup por volume. Se você configurar a proteção de backup com Backup e Recuperação, ela compartilhará as políticas de backup com a Resiliência a Ransomware.

As cópias de instantâneos não são limitadas e podem ser adicionadas separadamente de cada serviço.

Quais políticas são necessárias em uma estratégia de proteção contra ransomware?

Um "[estratégia de proteção contra ransomware](#)" Requer:

- uma política de *detecção* de ransomware, e
- uma política instantânea

Uma política de backup não é necessária na estratégia de resiliência ao ransomware.

O Ransomware Resilience está ciente das configurações de proteção no ONTAP?

Sim, o Ransomware Resilience descobre agendamentos de snapshots definidos no ONTAP. Ele também descobre se o ARP e o FPolicy estão habilitados em todos os volumes de uma carga de trabalho detectada. As informações exibidas no Painel de Resiliência a Ransomware são agregadas de outras soluções e produtos da NetApp.

A equipe de Resiliência a Ransomware está ciente das políticas já definidas no Backup e Recuperação e no SnapCenter?

Sim, se você tiver cargas de trabalho gerenciadas no Backup and Recovery ou no SnapCenter, as políticas gerenciadas por esses produtos serão trazidas para o Ransomware Resilience.

É possível modificar políticas herdadas do NetApp Backup and Recovery e/ou SnapCenter?

Não, você não pode modificar políticas gerenciadas pelo Backup and Recovery ou SnapCenter do Ransomware Resilience. Você gerencia quaisquer alterações nessas políticas no Backup and Recovery ou no SnapCenter.

Se existirem políticas do ONTAP (como ARP, FPolicy e snapshots), essas políticas são alteradas no Ransomware Resilience?

Não. O Ransomware Resilience não modifica nenhuma política de *detecção* existente (configurações ARP,

FPolicy) do ONTAP.

O que acontece se você adicionar novas políticas no Backup e Recuperação ou no SnapCenter depois de se inscrever no Ransomware Resilience?

A Resiliência contra Ransomware reconhece políticas recém-criadas e alterações de políticas no Backup e Recuperação ou no SnapCenter.

É possível alterar as políticas a partir do ONTAP?

Sim, você pode alterar as políticas do ONTAP no Ransomware Resilience. Você também pode criar novas políticas no Ransomware Resilience e aplicá-las às cargas de trabalho. Esta ação substitui as políticas ONTAP existentes pelas políticas criadas no Ransomware Resilience.

É possível desativar políticas no ONTAP?

É possível desativar o ARP nas políticas de detecção usando a interface do usuário do System Manager, as APIs ou a CLI no ONTAP.

Você pode desabilitar o FPolicy e as políticas de backup aplicando uma política diferente que não as inclua.

Avisos legais

Avisos legais fornecem acesso a declarações de direitos autorais, marcas registradas, patentes e muito mais.

Direitos autorais

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marcas Registradas

NETAPP, o logotipo da NETAPP e as marcas listadas na página de Marcas Registradas da NetApp são marcas registradas da NetApp, Inc. Outros nomes de empresas e produtos podem ser marcas registradas de seus respectivos proprietários.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Patentes

Uma lista atual de patentes de propriedade da NetApp pode ser encontrada em:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Política de Privacidade

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Código aberto

Os arquivos de aviso fornecem informações sobre direitos autorais e licenças de terceiros usados no software NetApp .

- ["Aviso para o NetApp Console"](#)

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTE; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.