Notas de lançamento

NetApp Ransomware Resilience

NetApp
February 19, 2026

Índice

Notas de lançamento . . . 1
Novidades na NetApp Ransomware Resilience . . . 1
16 de fevereiro de 2026 . . . 1
19 de janeiro de 2026 . . . 1
12 de janeiro de 2026 . . . 1
08 de dezembro de 2025 . . . 2
10 de novembro de 2025 . . . 2
06 de outubro de 2025 . . . 2
12 de agosto de 2025 . . . 4
15 de julho de 2025 . . . 4
9 de junho de 2025 . . . 4
13 de maio de 2025 . . . 5
29 de abril de 2025 . . . 5
14 de abril de 2025 . . . 6
10 de março de 2025 . . . 7
16 de dezembro de 2024 . . . 7
7 de novembro de 2024 . . . 8
30 de setembro de 2024 . . . 9
2 de setembro de 2024 . . . 9
5 de agosto de 2024 . . . 10
1 de julho de 2024 . . . 10
10 de junho de 2024 . . . 10
14 de maio de 2024 . . . 11
5 de março de 2024 . . . 13
6 de outubro de 2023 . . . 13
Limitações conhecidas do NetApp Ransomware Resilience . . . 14
Problema com a opção de reinicialização do exercício de prontidão . . . 14
Limitações do Amazon FSx for NetApp ONTAP . . . 14
Limitações do Azure NetApp Files . . . 14

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 Ransomware Resilience agora capturam informações sobre volumes suportados e não suportados no relatório **Summary**. Use essas informações para diagnosticar por que volumes em um sistema podem não ser elegíveis para ransomware protection.

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 obter detalhes, consulte "Implantar a BlueXP classification na nuvem" e para usar o serviço dentro de 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.

Para iniciar a verificação, na página Proteção, selecione **Identificar exposição** na coluna Exposição à privacidade do painel de proteção. Para obter mais informações, consulte "Verifique dados confidenciais identificáveis pessoalmente com 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

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, BlueXP ransomware protection fornece uma recomendação no painel **Ações recomendadas**: "Corrija uma vulnerabilidade de segurança conhecida no cluster <name>." A partir da recomendação no painel, selecionar **Revisar e corrigir** sugere revisar o Digital Advisor e um artigo de Common Vulnerability & Exposure (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.

Informações sobre direitos autorais

Informações sobre marcas comerciais