Use a resiliência do ransomware

NetApp Ransomware Resilience

NetApp
February 20, 2026

Índice

Use a resiliência do ransomware

Monitore a integridade da carga de trabalho em NetApp Ransomware Resilience

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.

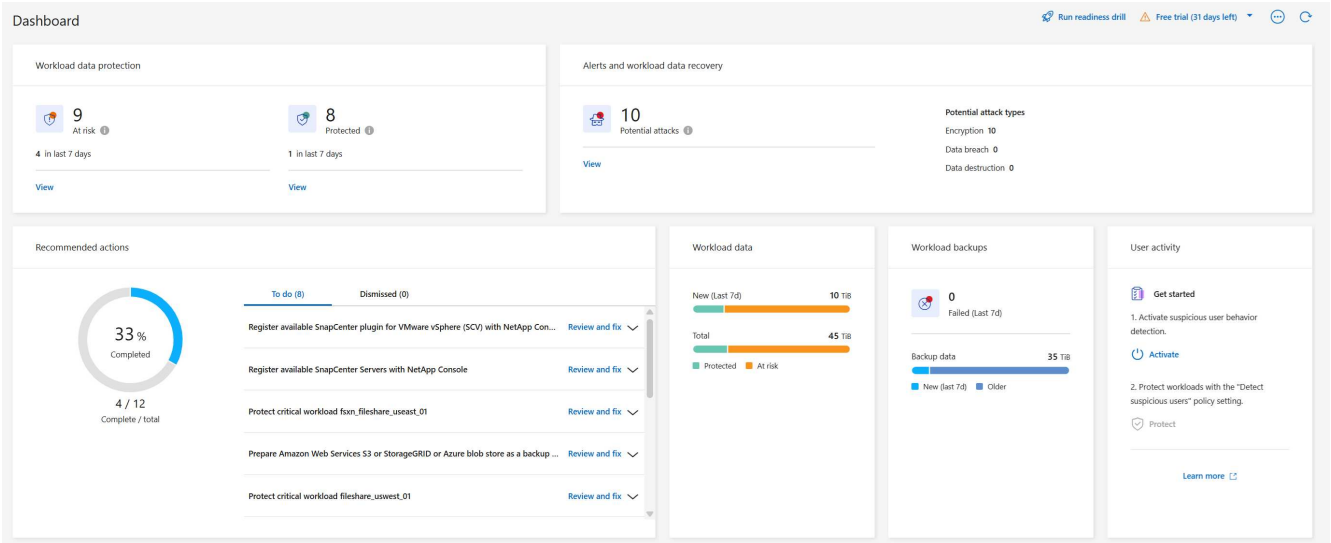
Utilize o Painel de Controle para revisar sugestões de proteção, alterar configurações e baixar relatórios.

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-lo. 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" .
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". Consulte "Proteja cargas de trabalho contra ataques de ransomware". 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

Analise o status de proteção em NetApp Ransomware Resilience

NetApp Ransomware Resilience's painel de proteção oferece uma visão geral do status de proteção e da prontidão das suas cargas de trabalho. Use o painel de proteção para obter informações sobre o que está protegido, o que precisa de proteção e qual o escopo da proteção.

Assim que você entender o alcance da sua proteção atual, "você pode criar e aplicar estratégias de proteção contra ransomware às suas cargas de trabalho".

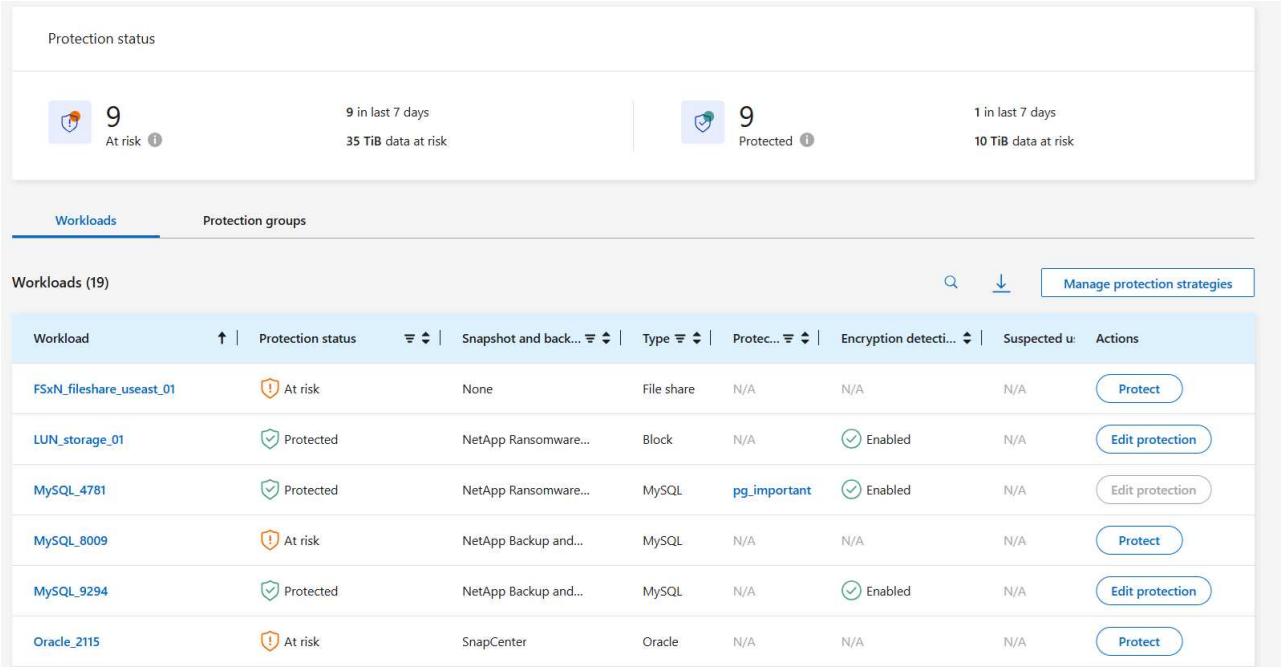
Visualizar proteção em uma carga de trabalho

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**.



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

Veja "Adicione uma estratégia de proteção contra ransomware" para saber como usar a Resiliência a Ransomware quando já existe uma política de proteção com Backup e Recovery.

Entenda o painel de proteção

O painel de proteção do Ransomware Resilience exibe informações detalhadas sobre as cargas de trabalho (por exemplo, nome e tipo da carga de trabalho, Console agent, sistema e storage VM), além de insights sobre o status da proteção. Use o painel de proteção para revisar e gerenciar a preparação para ransomware em cargas de trabalho. As seguintes colunas são especialmente úteis para entender sua postura de proteção:

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:

+ Ransomware Resilience fornece informações sobre o escopo das políticas de detecção de ransomware que você configurou em suas cargas de trabalho. Analise o escopo da detecção com os seguintes campos.

- **Status de detecção de criptografia**
- **Status de detecção de comportamento suspeito do usuário**
- **Bloquear extensões de arquivo suspeitas**

Políticas de Snapshot, replicação e backup: Esta coluna mostra o produto ou serviço que está gerenciando a política. Se não houver política, o campo exibirá N/A.

Importância

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.

Exposição de privacidade: selecione esta opção para "Busca por informações de identificação pessoal com NetApp Data Classification".

Replication destination: Se você configurou a replicação de snapshot, os nomes das storage VMs e sistemas de destino serão listados. Se não houver replicação, este campo exibirá "N/A".

Destino de backup: Se você configurou uma estratégia de proteção contra ransomware com backups, o nome do sistema de destino do backup será listado aqui.

Próximos passos

- "Proteja cargas de trabalho com estratégias de proteção contra ransomware"
- "Gerenciar grupos de proteção"
- "Escaneie dados de identificação pessoal"

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

As estratégias de proteção contra ransomware são um recurso fundamental do NetApp Ransomware Resilience: elas dão suporte à detecção, proteção e replicação. As estratégias de proteção são uma parte essencial da sua postura de cibersegurança.

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 *detecção*, *proteção* e *replicação* policies.

- **Políticas de detecção** identificam ameaças de ransomware
- **Políticas de proteção** incluem políticas de snapshot e backup. Políticas de detecção 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 uma gestão e proteção aprimoradas do seu conjunto de dados, você pode criar "cargas de trabalho em grupo" para proteger coletivamente volumes sob uma única estratégia.

Políticas de proteção com outros serviços gerenciados pela NetApp

Além da Ransomware Resilience, você pode usar NetApp Backup and Recovery para gerenciar a proteção de compartilhamentos de arquivos e compartilhamentos de arquivos de VM.

As informações de proteção dos serviços de Backup & Recovery aparecem no Ransomware Resilience. 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.

O Ransomware Resilience também descobre políticas de proteção do SnapCenter para datastores de VM da VMware e do SnapCenter para Oracle. Você não pode usar esses serviços para restaurar com o Ransomware Resilience.

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 NetApp Backup and Recovery ou pelo NetApp Ransomware Resilience, ela pode ter snapshots criados como parte do ONTAP ou de outros produtos. Se a proteção FPolicy do ONTAP estiver em vigor, você pode alterá-la usando o ONTAP.

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	Freqüência	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

Nível de política	Instantâneo	Freqüência	Retenção (dias)	Número de cópias instantâneas	Número máximo de cópias instantâneas
Política importante 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
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

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 snapshot ou backup existentes da proteção de Backup and Recovery por estratégias de proteção gerenciadas pela 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" .

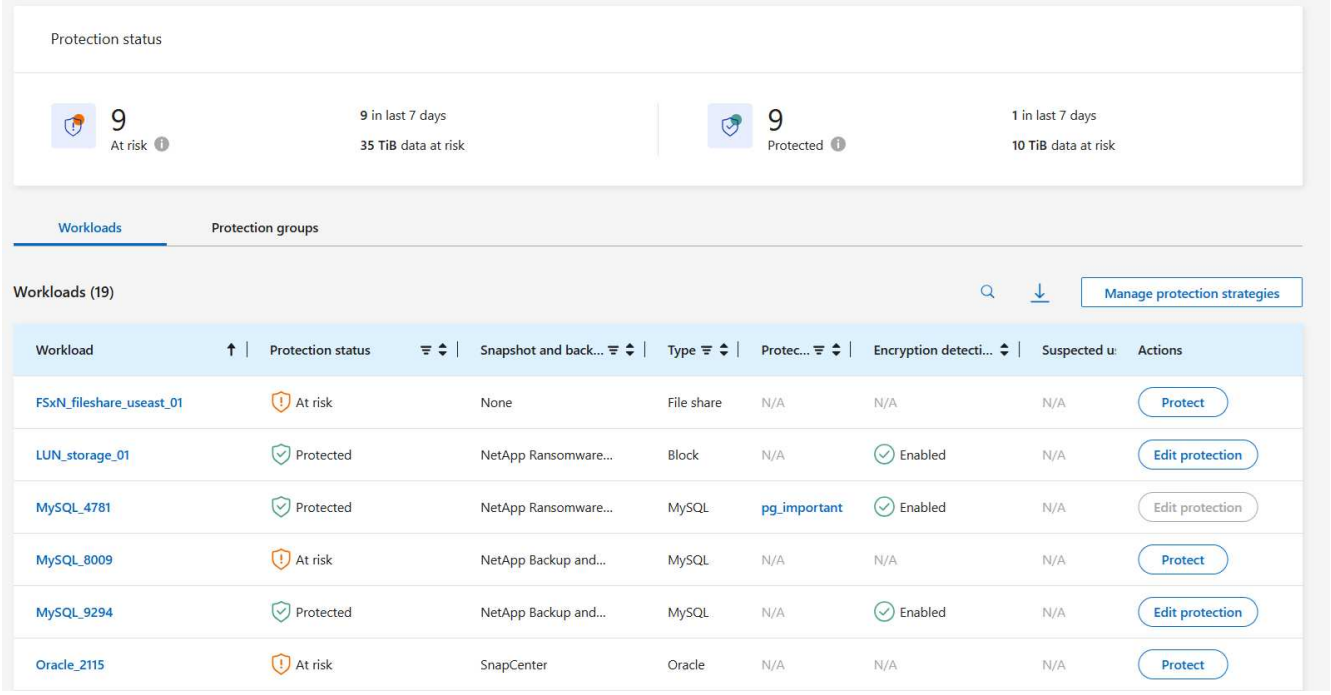
Crie uma estratégia de proteção contra ransomware (se você não tiver políticas de snapshot ou backup)

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:

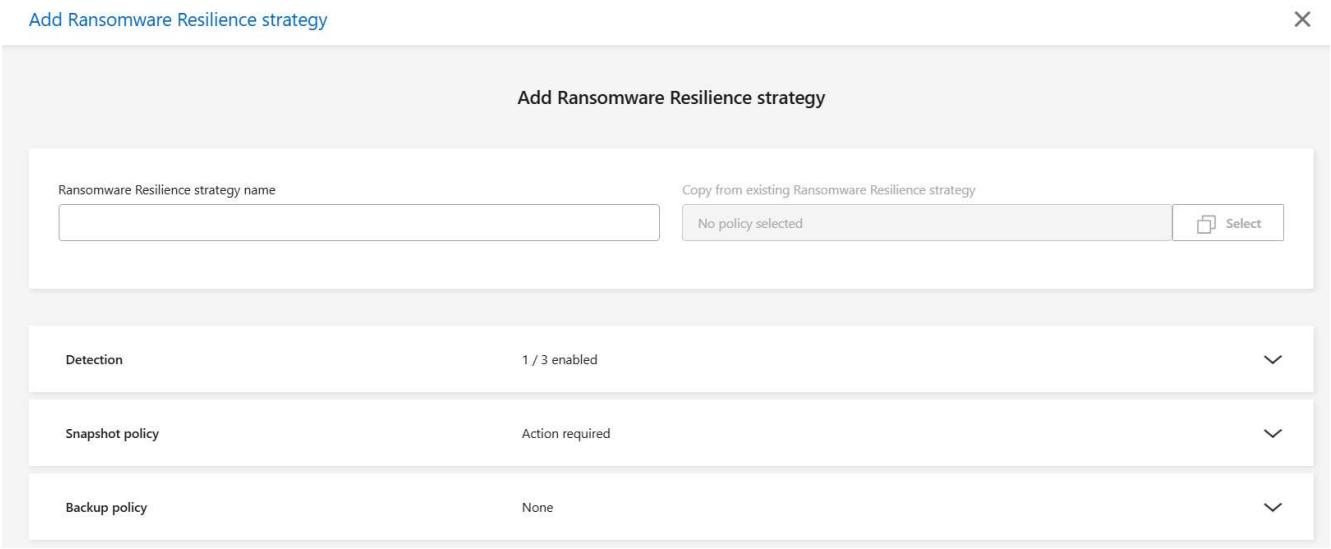
- Política de instantâneo
- Política de backup
- Política de detecção de ransomware
- Replicação secundária para ONTAP

Etapas para criar uma estratégia de proteção contra ransomware

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



2. Na página Proteção, selecione uma carga de trabalho e depois **Proteger**.
3. Na página Estratégias de proteção contra ransomware, selecione **Adicionar**.



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**.

Adicione uma política de detecção às cargas de trabalho com políticas de snapshot e backup existentes gerenciadas pelo Backup and Recovery

Ransomware Resilience permite atribuir uma política de detecção ou uma política de proteção a cargas de trabalho com proteção de snapshot e backup já gerenciada em outros NetApp produtos ou serviços. Backup

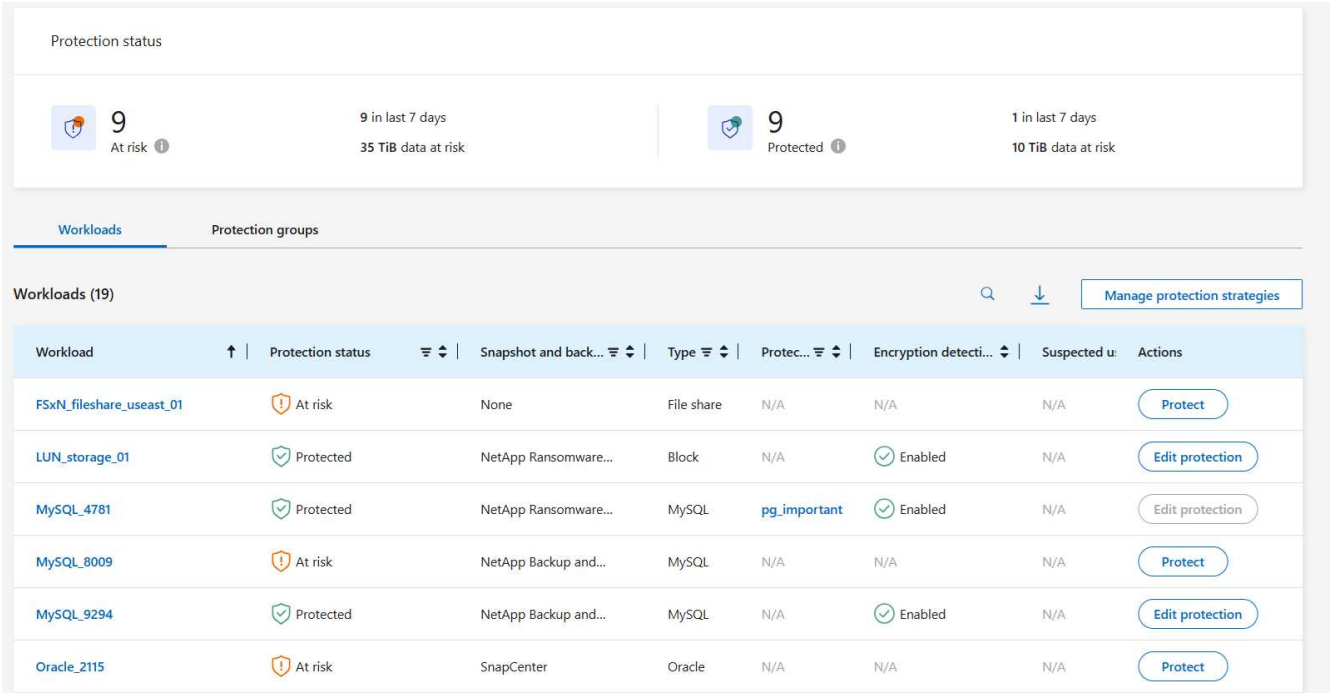
and Recovery utiliza políticas que regem snapshots, replicação para storage secundário ou backups para storage de objetos.

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

Se você já possui políticas de snapshot ou backup com o Backup and Recovery, pode 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**.



2. Na página Proteção, selecione uma carga de trabalho e selecione **Proteger**.
3. Ransomware Resilience detecta se existem políticas de Backup and Recovery ativas.
4. Para manter seu Backup and Recovery existente e aplicar apenas uma política de *detection*, deixe a caixa **Replace existing policies** desmarcada.
5. Selecione as configurações de detecção que você deseja:
   - **Detecção de criptografia**
   - **Detecção de comportamento suspeito do usuário**
   - **Bloquear extensões de arquivo suspeitas**
6. Selecione **Avançar**.
7. Se você selecionou **Detecção 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.

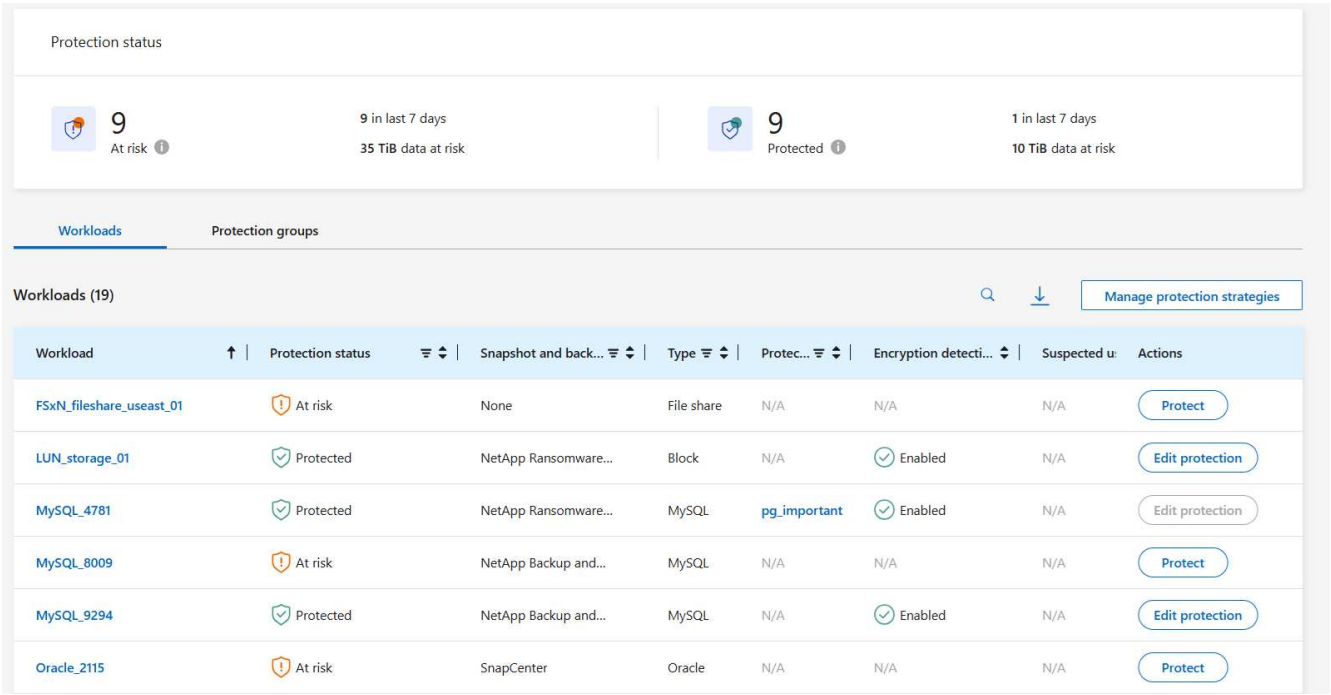
8. Selecione **Avançar**.
9. Reveja suas escolhas. Selecione **Criar** para ativar a detecção.
10. Na página Proteção, revise o **Status de detecção** para confirmar se a detecção está Ativa.

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

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



2. Na página Proteção, selecione uma carga de trabalho e selecione **Proteger**.
3. Ransomware Resilience detecta se existem políticas de Backup and Recovery ativas. Para substituir as políticas existentes, selecione a caixa **Replace existing policies**. Ao selecionar a caixa, o Ransomware Resilience substitui a lista de políticas de detecção por políticas de detecção.
4. 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, consulteCrie uma política de proteção . Selecione **Avançar**.
5. 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 and Recovery existente que você deseja manter, desmarque **Replace existing policies**. Para substituir as políticas existentes, marque **Replace existing policies**.
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.

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

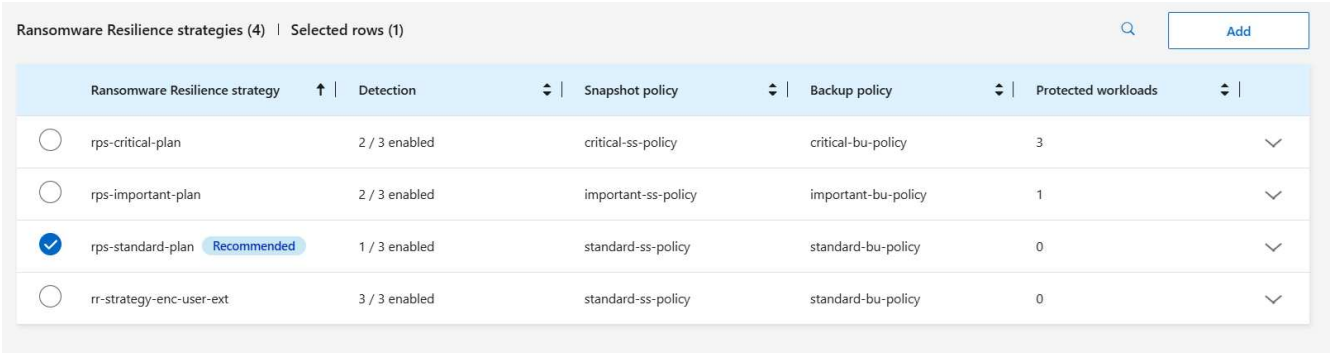
Antes de excluir uma estratégia de proteção contra ransomware, talvez você queira ver quais cargas de trabalho são protegidas por essa estratégia.

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.



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**.

Gerenciar grupos de proteção em NetApp Ransomware Resilience

NetApp Ransomware Resilience oferece grupos de proteção para facilitar o gerenciamento do seu conjunto de dados. Grupos de proteção são agrupamentos lógicos de cargas de trabalho. Ransomware Resilience pode proteger todos os volumes em um grupo de proteção ao mesmo tempo com uma única estratégia de proteção, poupando você de aplicar uma estratégia a cada carga de trabalho.

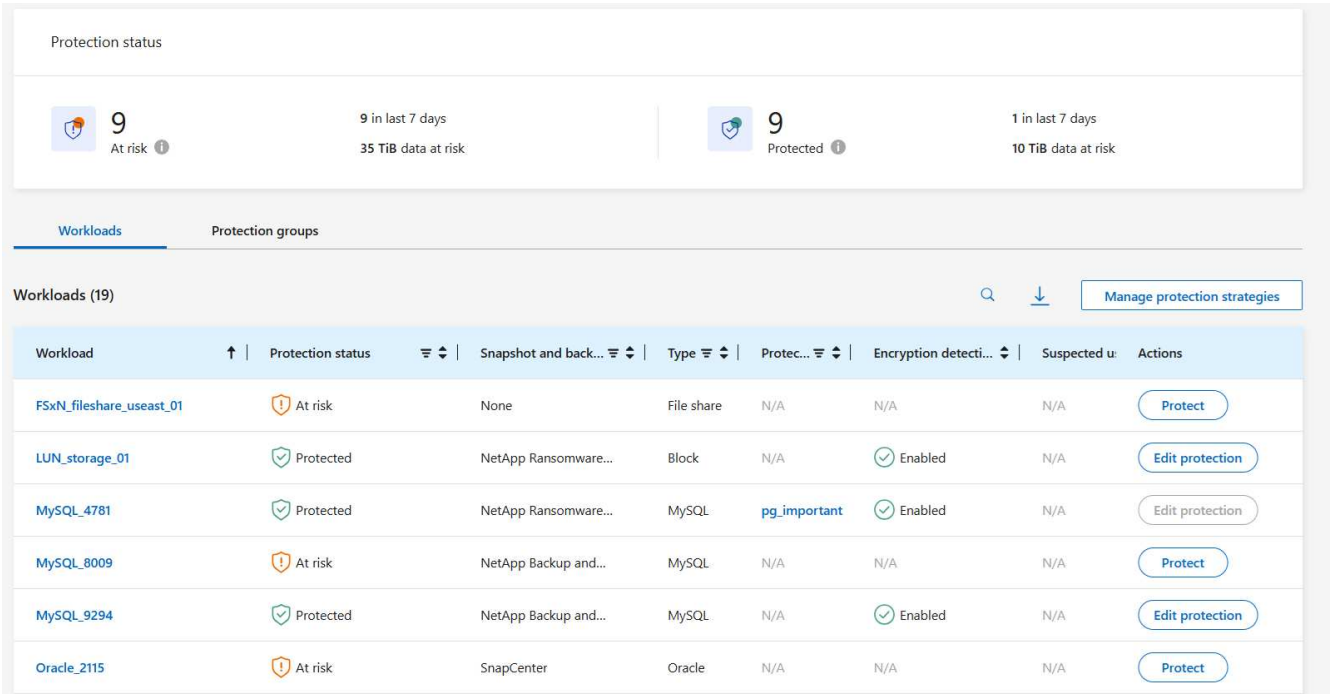
Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console" .

Crie um grupo de proteção

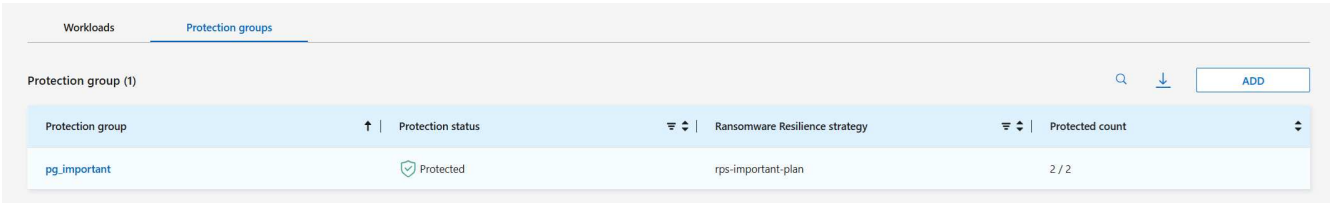
Você pode criar grupos independentemente do status de proteção (ou seja, grupos não protegidos e grupos protegidos). Ao adicionar uma política de proteção a um grupo de proteção, a nova política substitui qualquer política existente, incluindo políticas gerenciadas NetApp Backup and Recovery.

Passos

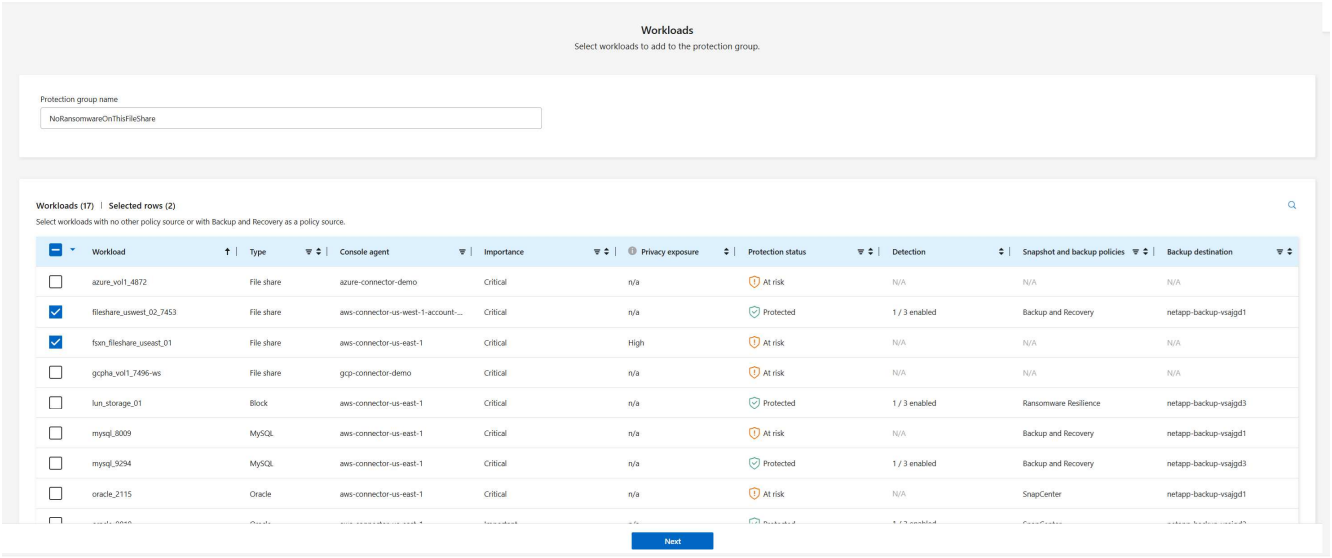
1. No menu Resiliência contra Ransomware, selecione **Proteção**.



2. No painel de proteção, selecione a guia **Protection groups**.



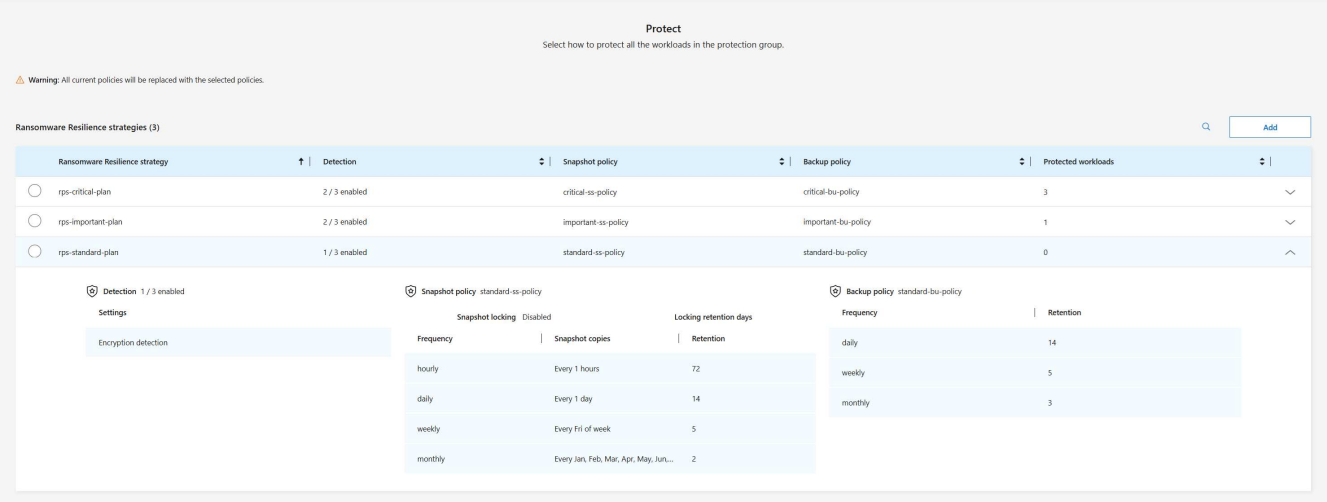
3. Selecione **Adicionar**.



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**.



7. Selecione uma estratégia de proteção para o grupo.
8. Se a estratégia de proteção incluir replicação, revise as configurações de replicação.
   a. 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 o grupo de proteção, selecione **Add**.

Ao revisar o painel de proteção no Ransomware Resilience, você pode classificar as cargas de trabalho por grupo de proteção.

Editar proteção de grupo

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

Passos

1. No menu Resiliência contra Ransomware, selecione **Proteção**.
2. Na página Proteção, selecione a aba **Grupos de proteção** e selecione o grupo cuja política você deseja modificar.
3. Na página de visão geral do grupo de proteção, selecione **Editar proteção**.
4. 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**.
5. Na visão geral do destino de backup, selecione um destino de backup existente ou **Adicione um novo destino de backup**.

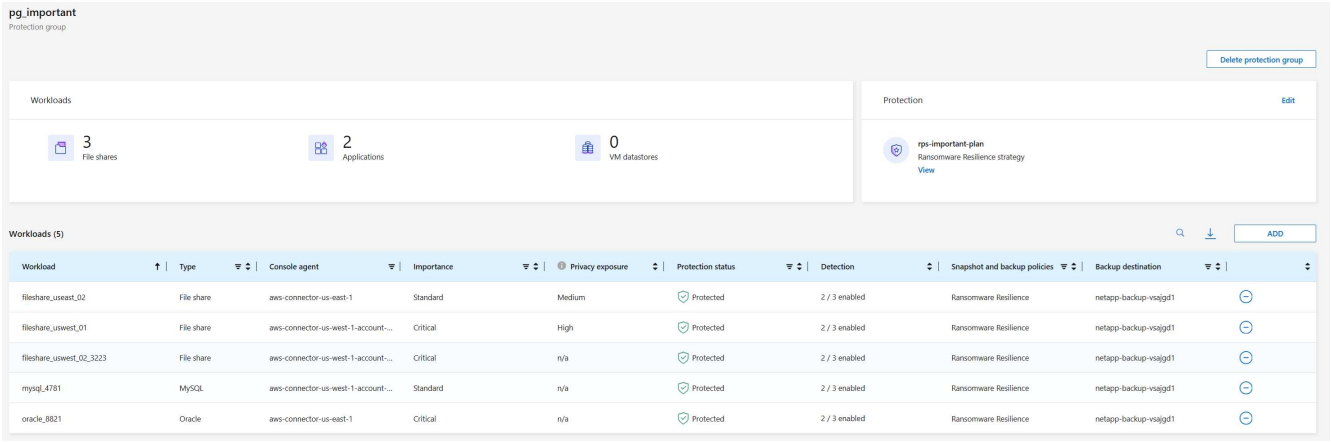
6. Selecione **Avançar** para revisar suas alterações.

Remover cargas de trabalho de um grupo de proteção

Posteriormente, pode ser necessário remover cargas de trabalho de um grupo de proteção 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.



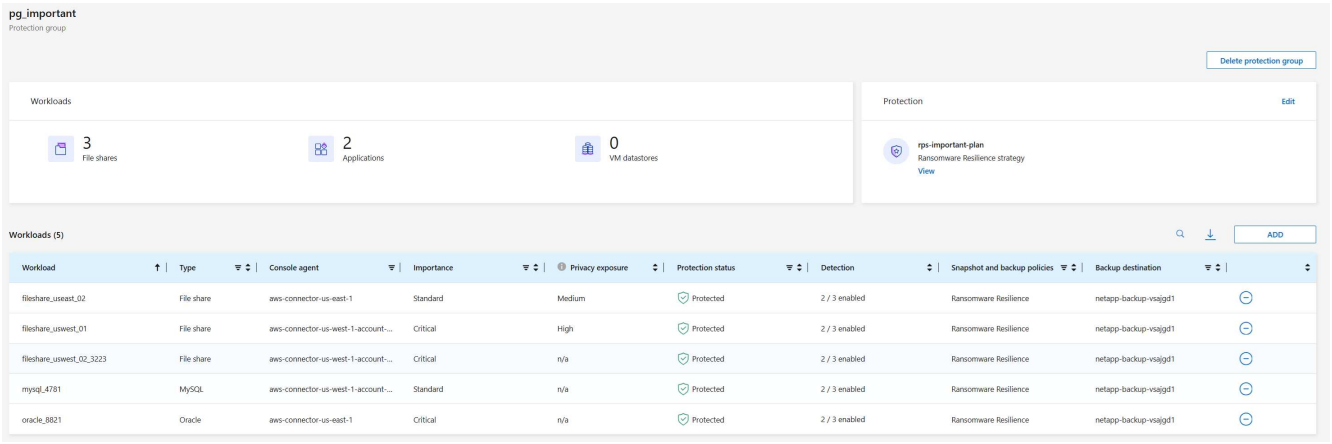
4. Na página do grupo de proteção, selecione a carga de trabalho que deseja remover do grupo e selecione a opção **Ações** ⋯.
5. No menu Ações, selecione **Remover carga de trabalho**.
6. Confirme que deseja remover a carga de trabalho e selecione **Remover**.

Excluir um grupo de proteção

Ao excluir um grupo de proteção, o Ransomware Resilience remove o grupo e a estratégia de proteção das cargas de trabalho. Ele não exclui 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.



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**.

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"

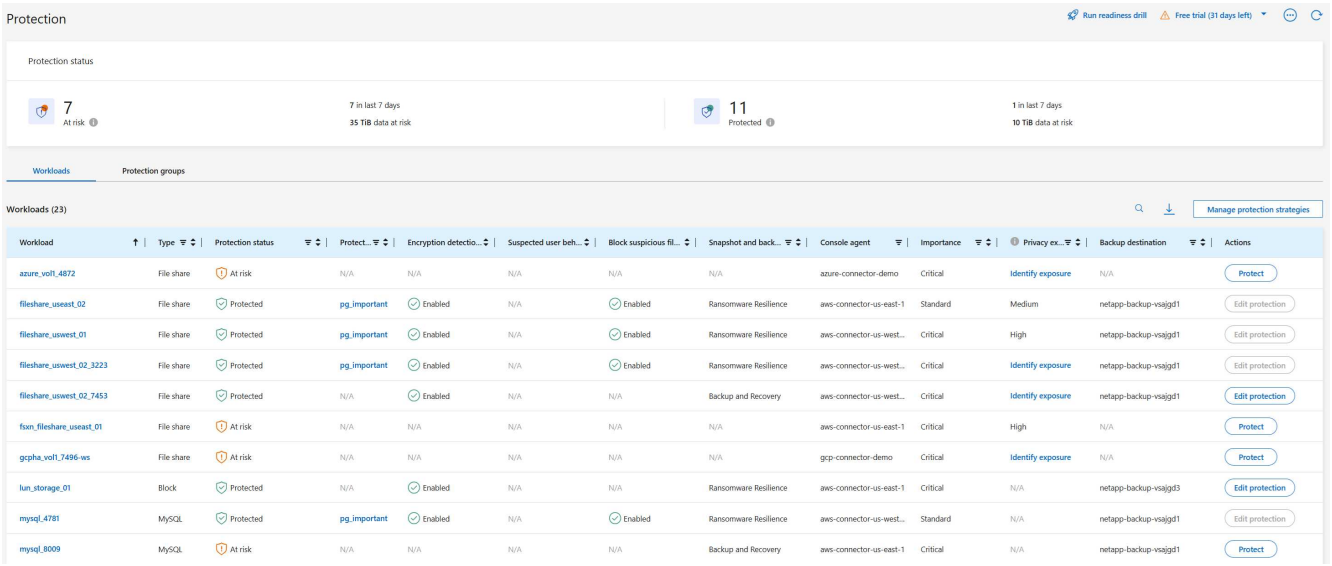
- "Categorias de dados privados"
- "Investigue os dados armazenados em sua organização"

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.



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.

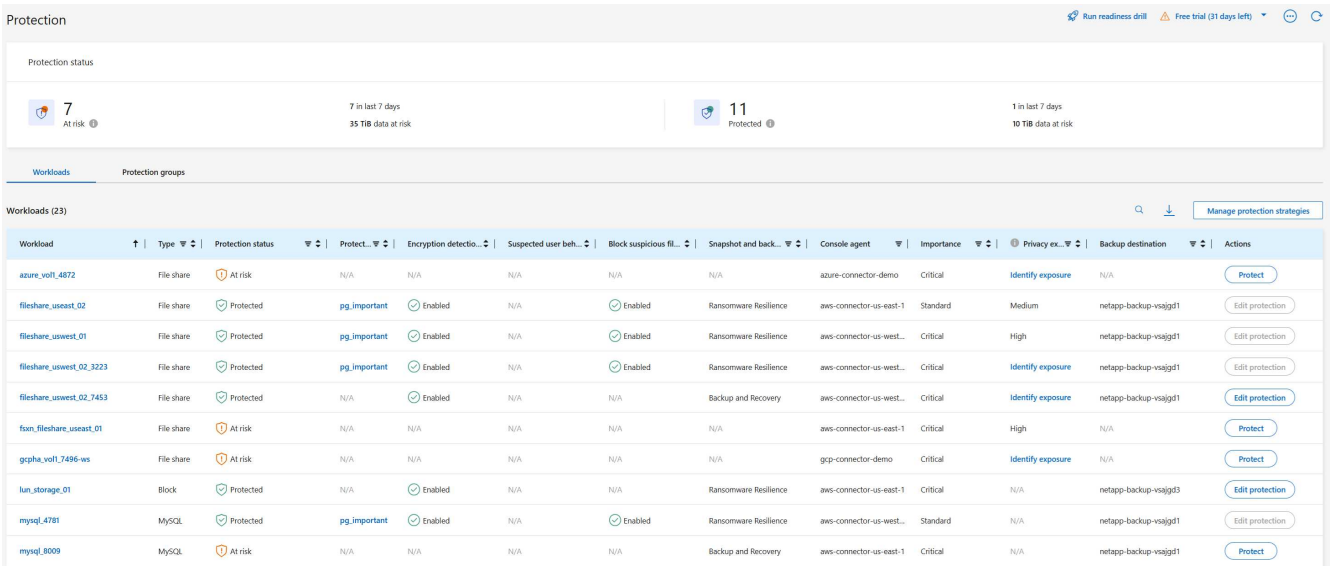
Os dados PII são classificados em uma das três designações:

- **Alto**: Mais de 70% dos arquivos contêm PII

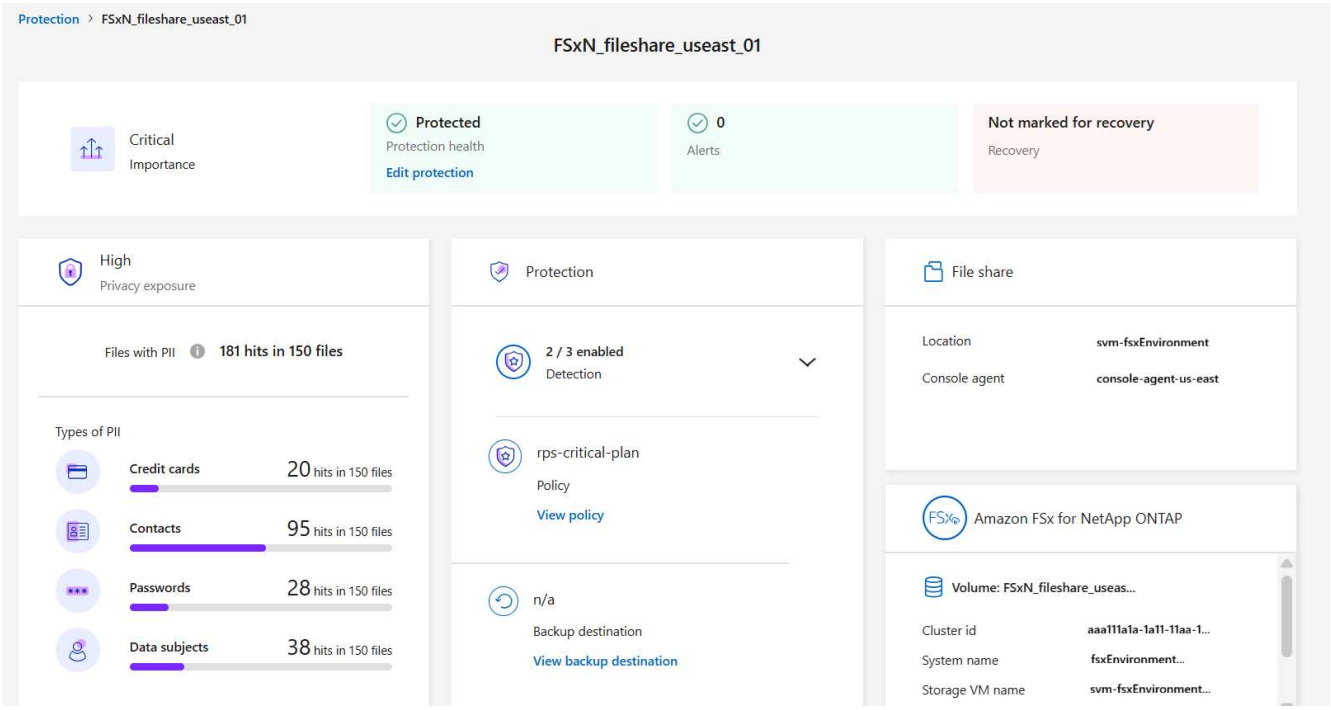
- **Médio**: Mais de 30% e menos de 70% dos arquivos contêm PII
- **Baixo**: Mais de 0% e menos de 30% dos arquivos contêm PII

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.



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



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
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 NetApp Ransomware Resilience detecta um possível ataque, ele exibe um alerta no Dashboard e na área de Notificações. O Ransomware Resilience imediatamente tira um snapshot. Ao receber um alerta, revise o risco potencial na guia **Alerts** do Ransomware Resilience para avaliar o impacto em seus dados e prevenir um possível ataque de 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.

Como os alertas são gerados

Ransomware Resilience se baseia em evidências sobre padrões de entropia de dados, tipos de extensão de arquivo e criptografia para gerar alertas. Os alertas são baseados nos seguintes eventos:

- Violação de dados
- Destruição de dados
- 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
- Comportamento suspeito do usuário
- Quando a criptografia é alta, sem alterações na extensão do arquivo

> Para alertas de violação de dados, destruição de dados e comportamento suspeito do usuário, você deve configurar "detecção de atividade do usuário".

Tipos e status de alerta

Os alertas têm um de dois status: **Novo** ou **Inativo**.

Um alerta é classificado como um dos seguintes tipos:

- **Ataque potencial**: Um alerta é classificado como um ataque potencial quando:
  - Autonomous Ransomware Protection detecta uma nova extensão e a ocorrência se repete mais de 20 vezes nas últimas 24 horas (comportamento padrão).
  - Violações de dados são detectadas.
  - A destruição de dados foi detectada.
- **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" .

Estados de alerta

Um incidente de alerta pode ter os seguintes estados:

Estado	Descrição
Novo	Todos os incidentes são marcados como "novos" quando são identificados pela primeira vez.

Em revisão	Você pode marcar manualmente um incidente de alerta como "em análise" enquanto o avalia.
Dispensado	Se suspeitar que a atividade não é um ataque de ransomware, você pode alterar o status para "dispensado". + CUIDADO: Depois de dispensar um ataque, você não pode reverter o status. Se você dispensar uma carga de trabalho, todas as cópias instantâneas feitas automaticamente em resposta ao possível ataque de ransomware serão excluídas permanentemente.
Resolvido	O incidente foi resolvido.
Resolvido automaticamente	Para alertas de baixa prioridade, o incidente é resolvido automaticamente se nenhuma ação for tomada em relação a ele em cinco dias.

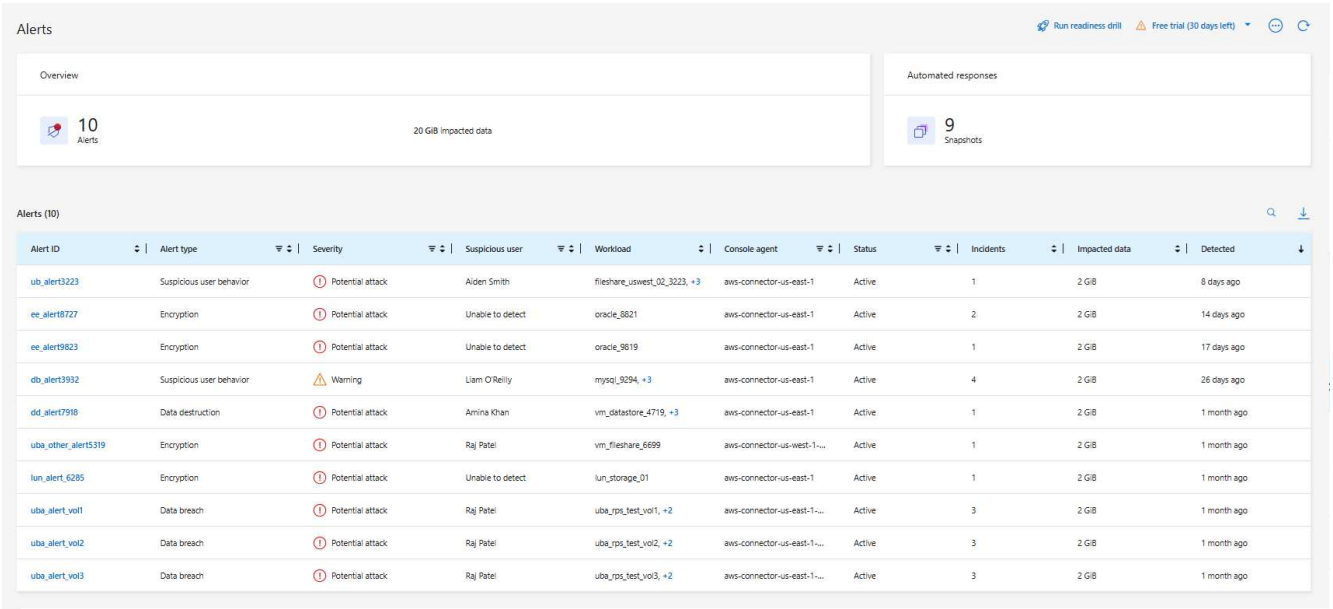
Ver alertas

Você pode acessar alertas no painel de Ransomware Resilience ou na guia **Alerts**.

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.



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 **Ver 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, selecione **Alerta** nas trilhas 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 a Proteção Autônoma contra Ransomware aciona um alerta no NetApp Ransomware Resilience, você pode visualizar os seguintes detalhes:

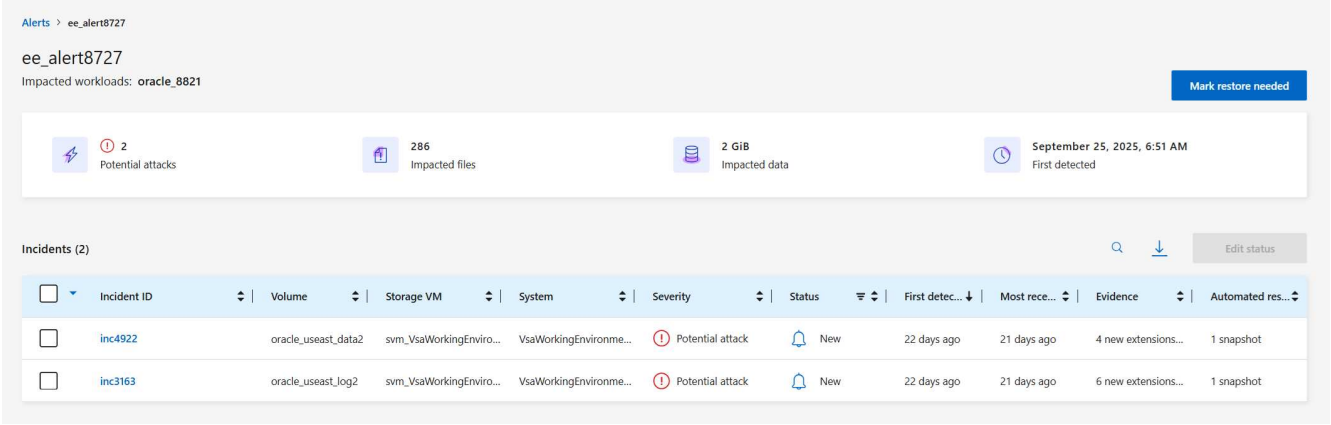
- Quando o alerta foi acionado

- Quando o acesso foi alterado ou negado
- 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
- Cargas de trabalho, volumes, arquivos e diretórios afetados

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.



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.

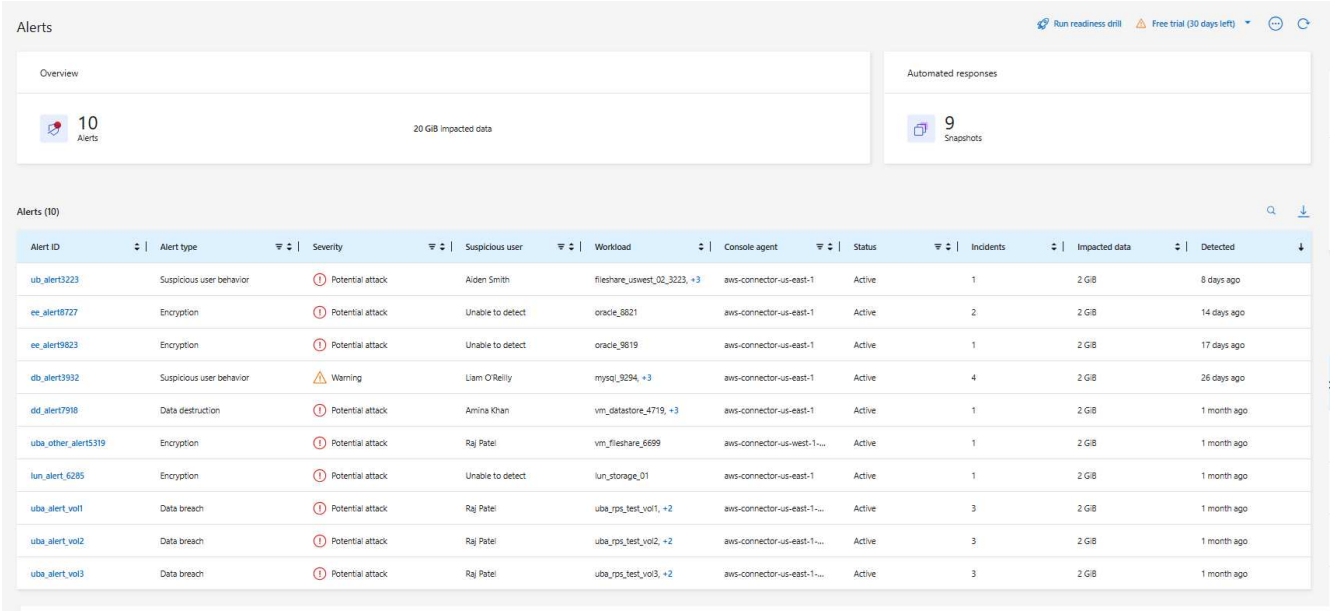
Marcar incidentes de ransomware como prontos para recuperação (após os incidentes serem neutralizados)

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

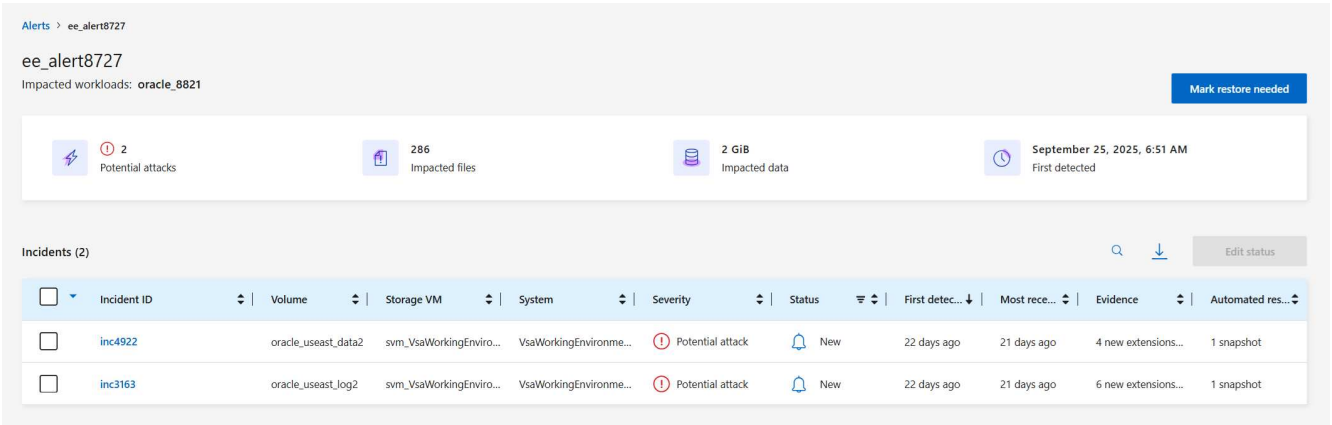
Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console" .

Passos

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



2. Na página Alertas, selecione o alerta.
3. Revise os incidentes no alerta.



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.

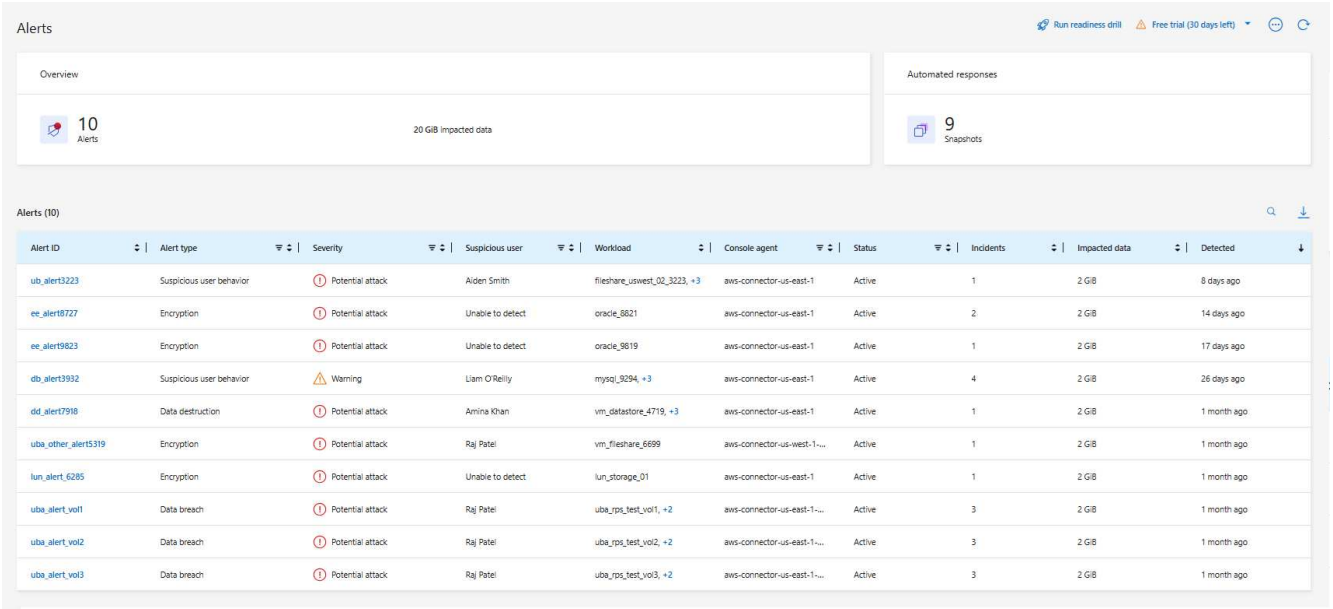
Se você descartar uma carga de trabalho, todas as cópias de instantâneos feitas automaticamente em resposta a um possível ataque de ransomware serão excluídas permanentemente.

Se você descartar um alerta, não poderá alterar seu status nem desfazer essa alteração.

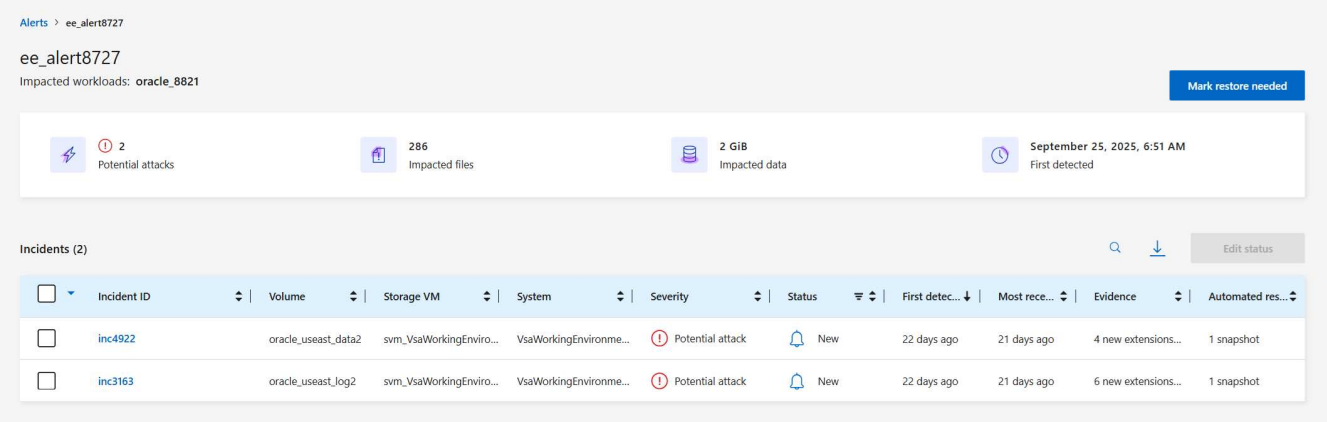
Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console" .

Passos

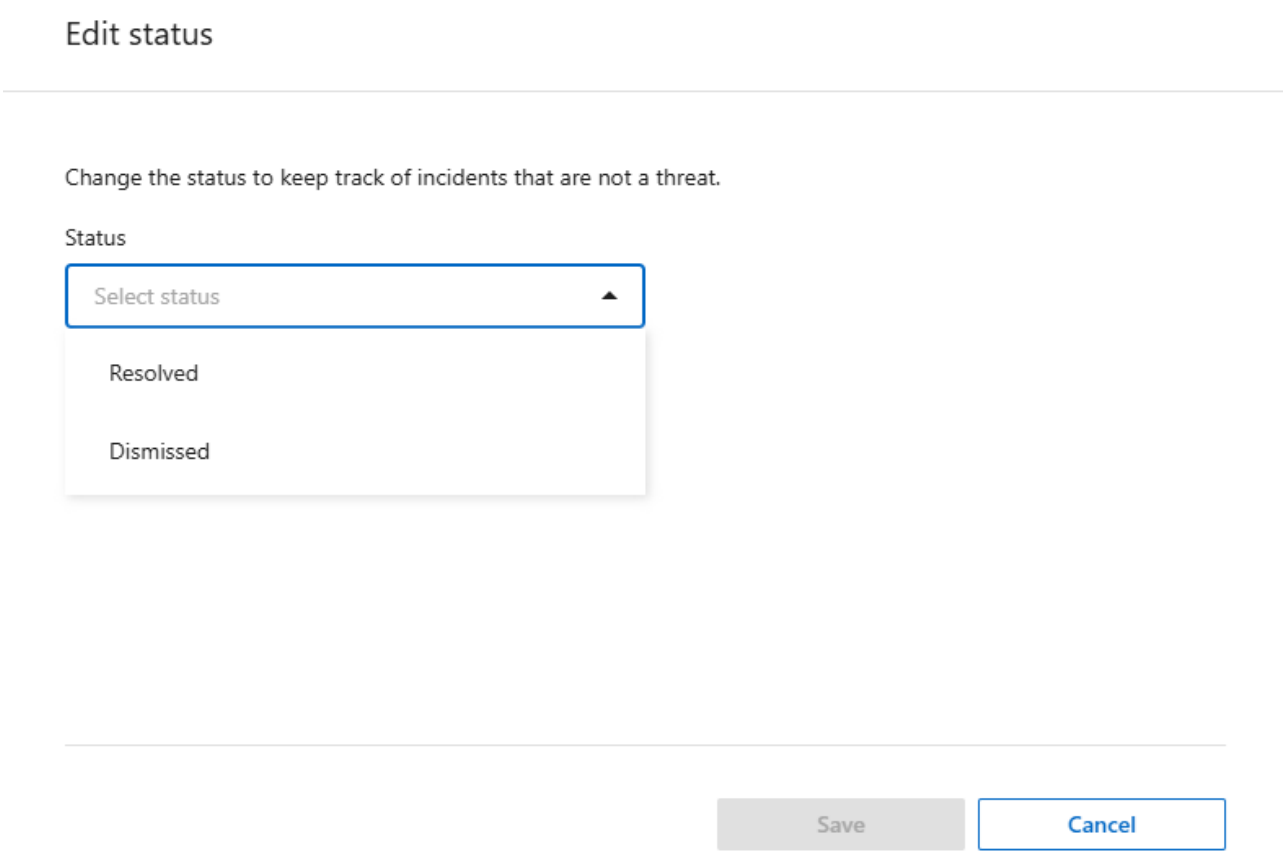
1. No menu Resiliência contra Ransomware, selecione **Alertas**.



2. Na página Alertas, selecione o alerta.



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.



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.

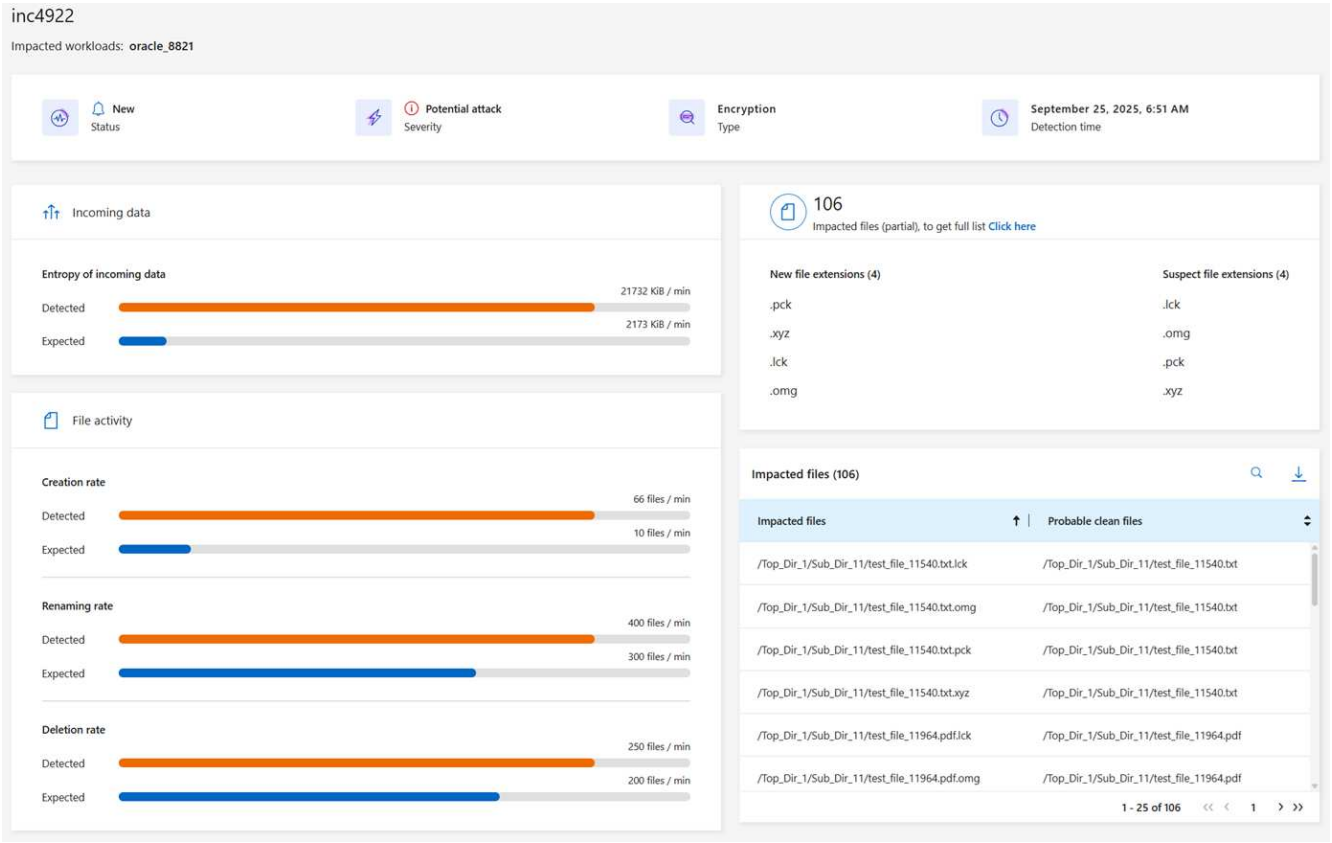
Função de console necessária Para executar esta tarefa, você precisa da função de administrador da organização, administrador de pasta ou projeto ou administrador de resiliência contra ransomware. "Saiba mais sobre as funções de resiliência contra ransomware para o NetApp Console" .

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 máquina virtual for gerenciado pelo NetApp Backup and Recovery ou Ransomware Resilience, o Ransomware Resilience realiza uma restauração consistente com falhas, na qual todos os dados que estavam no volume no mesmo ponto no tempo são 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:

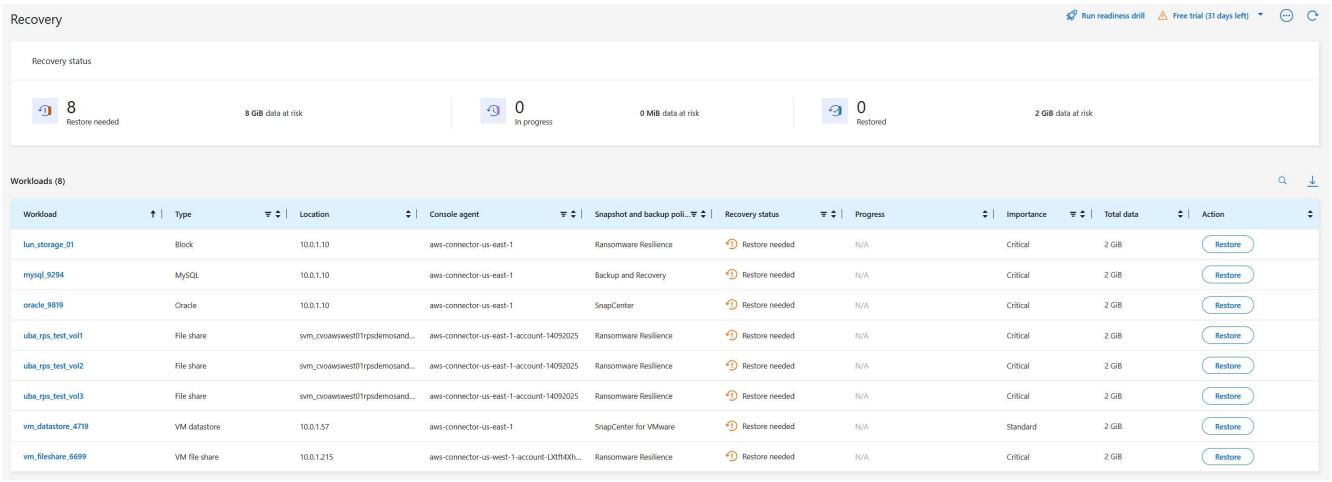
- **Restauração necessária**: A carga de trabalho precisa ser restaurada.
- **Em andamento**: A operação de restauração está em andamento.
- **Restaurado**: A carga de trabalho foi restaurada.
- **Falha**: O processo de restauração da carga de trabalho não pôde ser concluído.

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**.



Restaurar uma carga de trabalho

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.

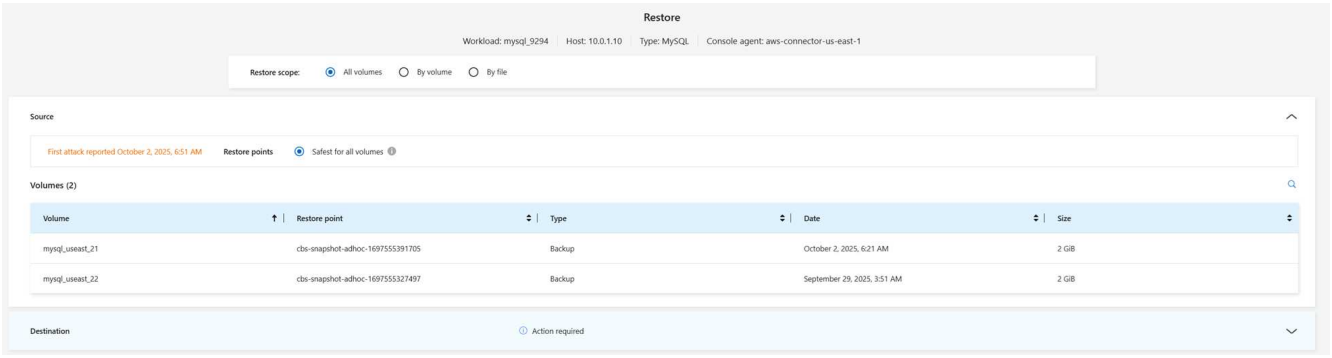
        Para cargas de trabalho SAN, você só pode restaurar por carga de trabalho.

        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**.



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.

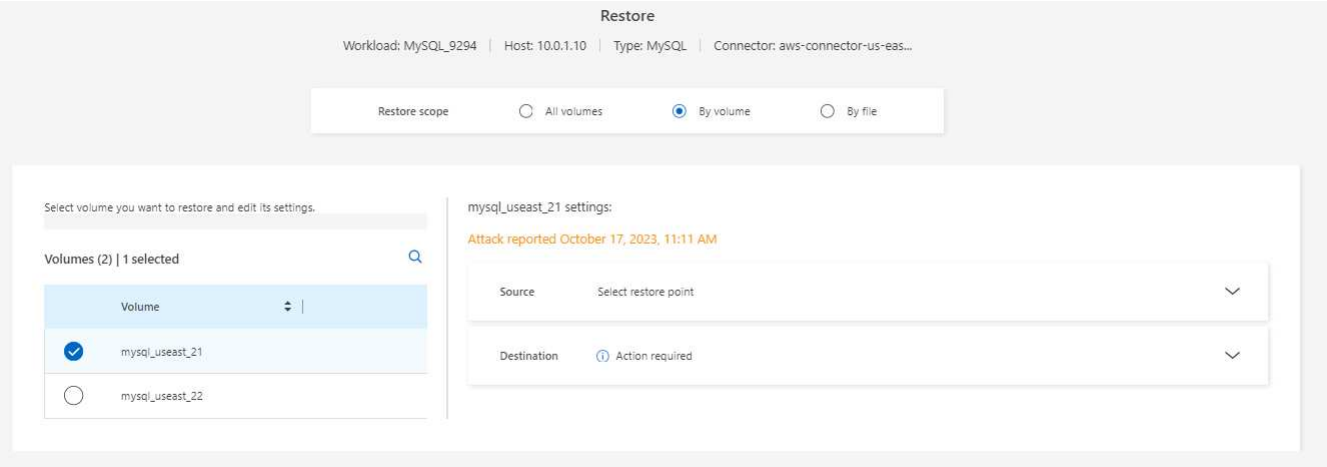
6. **Destino**: Selecione a seta para baixo ao lado de Destino para ver detalhes.
   a. Selecione o sistema.
   b. Selecione a VM de armazenamento.
   c. Selecione o agregado.
   d. Altere o prefixo de volume que será adicionado a todos os novos volumes.

> 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**.



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.

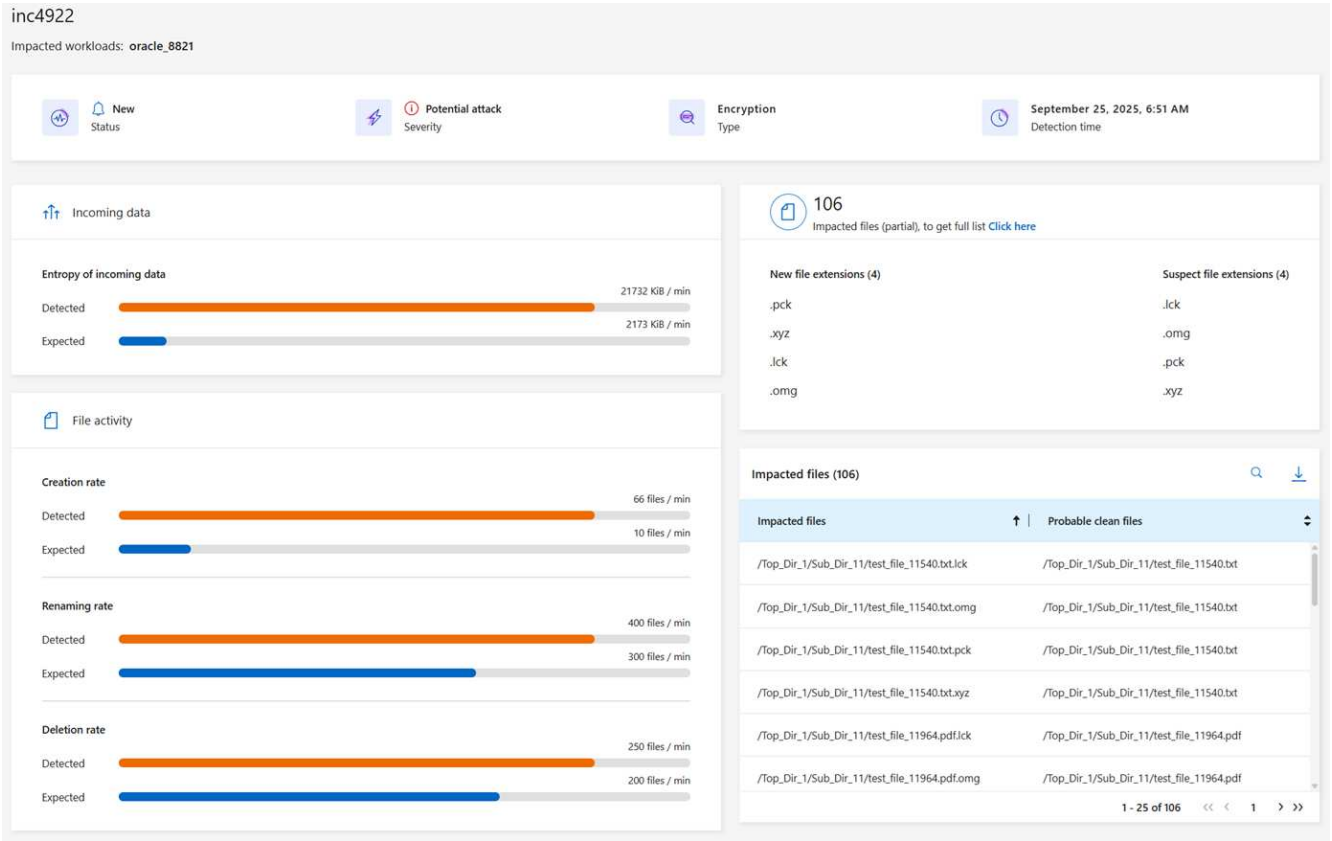
Você pode restaurar uma carga de trabalho de aplicativo no nível de arquivo para o mesmo sistema ou para um sistema diferente.

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.



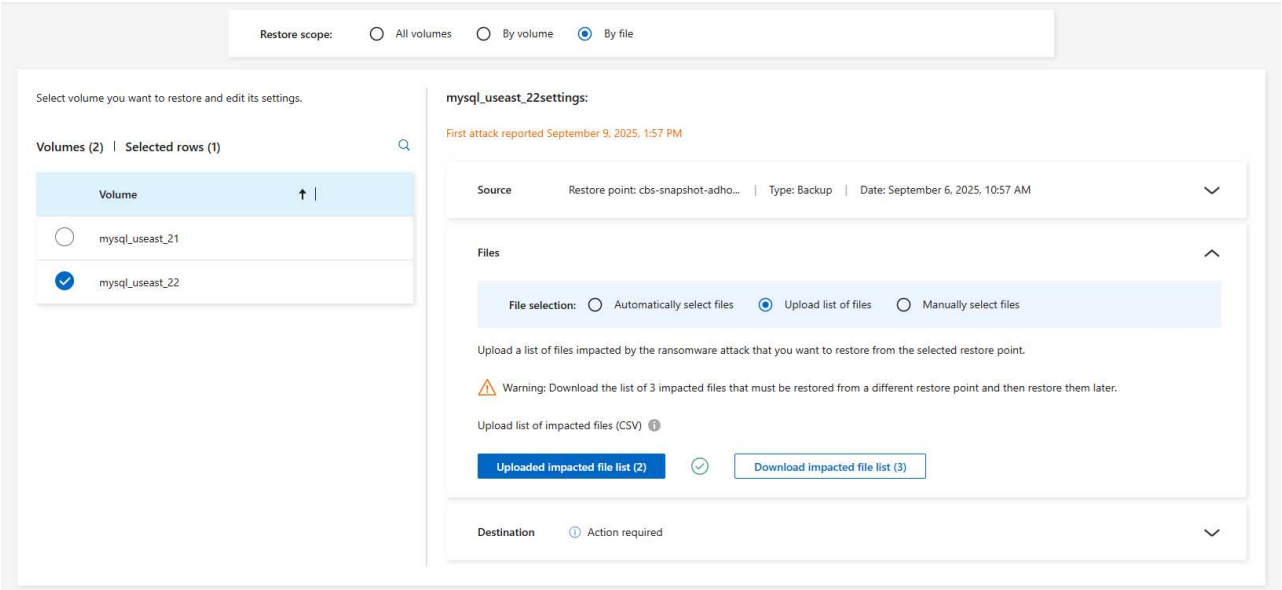
5. Para ver a lista completa de arquivos, selecione **Clique aqui** na parte superior do painel Arquivos afetados.
6. Para esse incidente, selecione o ícone de download e baixe a lista de arquivos afetados no formato CSV.

Etapas para restaurar esses arquivos

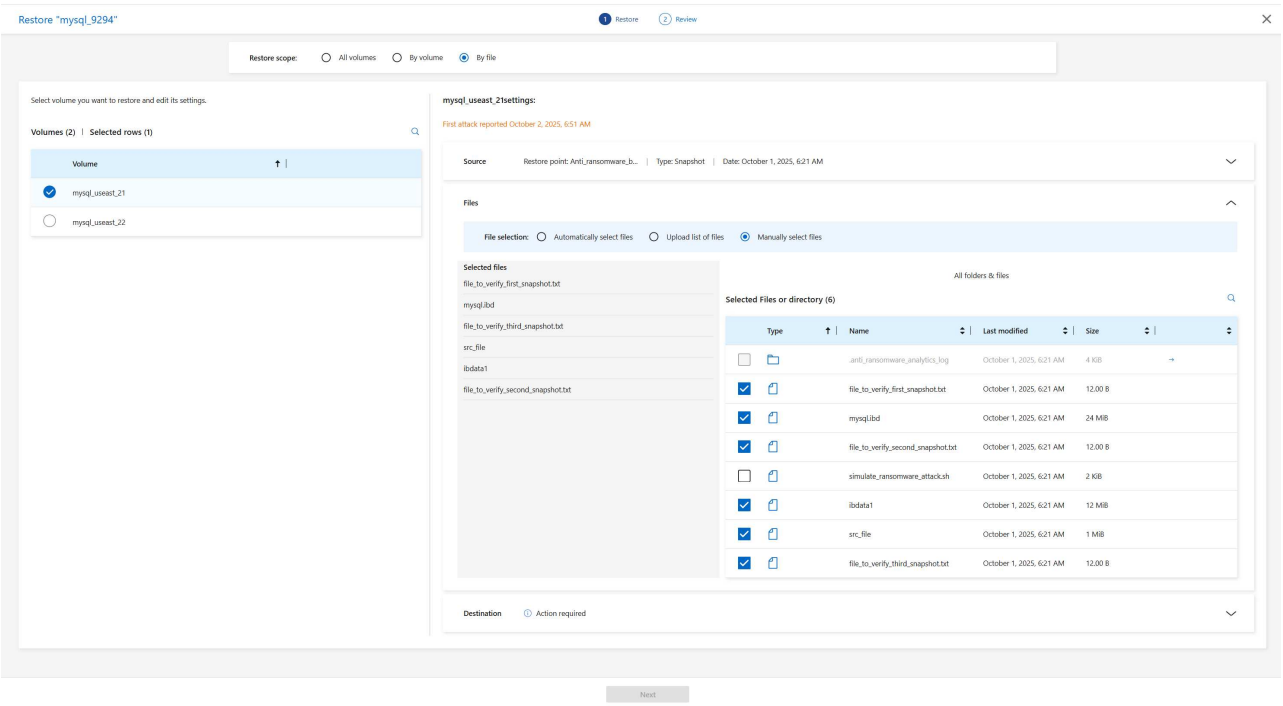
1. No menu Resiliência contra Ransomware, selecione **Recuperação**.
2. Selecione uma carga de trabalho do aplicativo que esteja no estado "Restauração necessária".
3. Para restaurar, selecione **Restaurar**.
4. Na página Restaurar, no escopo Restaurar, selecione **Por arquivo**.
5. Na lista de volumes, selecione o volume que contém os arquivos que você deseja restaurar.
6. **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.



   - **Selecionar arquivos manualmente**: Selecione até 10.000 arquivos ou uma única pasta para restaurar.



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**.

8. **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.

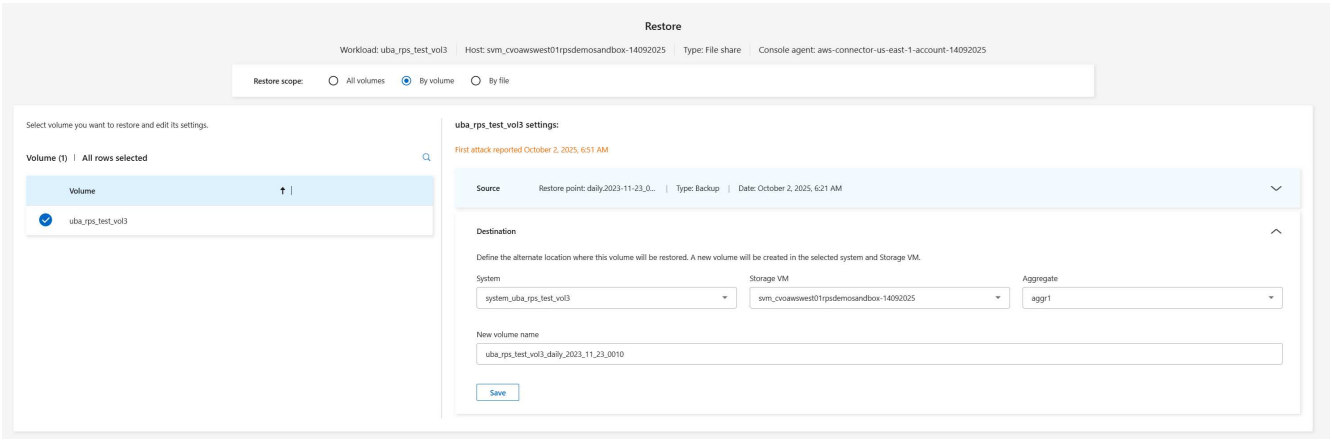
   b. Selecione o sistema.
   c. Selecione a VM de armazenamento.
   d. Opcionalmente, insira o caminho.

      Se você não especificar um caminho para a restauração, os arquivos serão restaurados em um novo volume no diretório de nível superior.

   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**.



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.

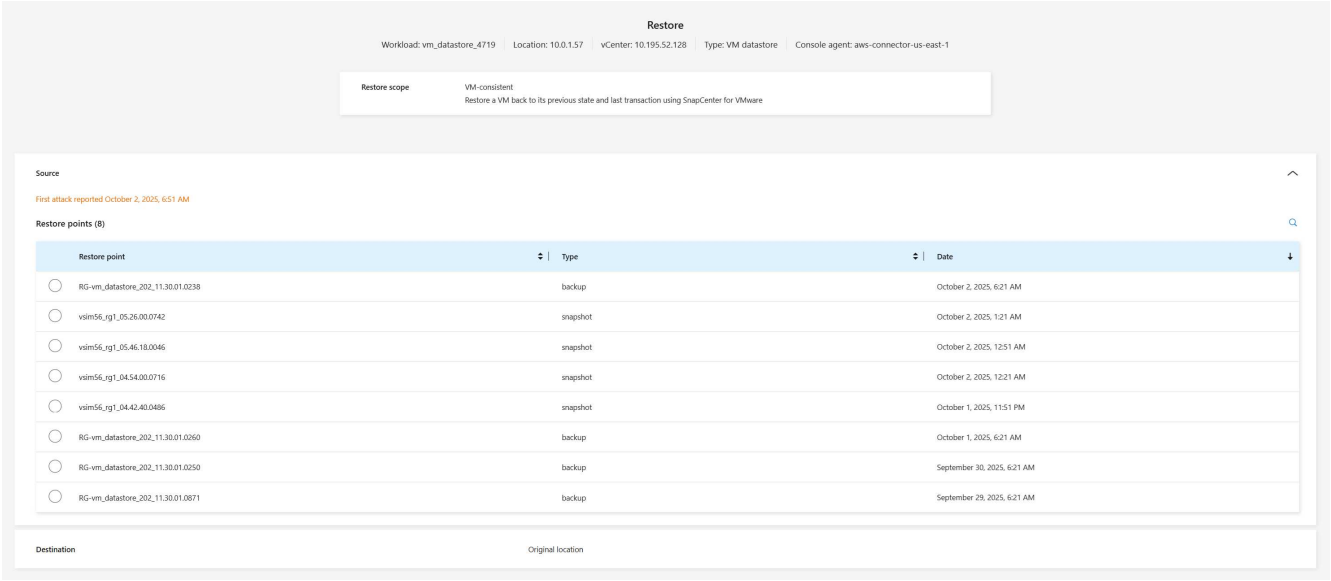
> Se você não especificar um caminho para a restauração, os arquivos serão restaurados em um novo volume no diretório de nível superior.

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.



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

NetApp Ransomware Resilience fornece relatórios em formatos CSV e JSON que mostram detalhes de volumes suportados e não suportados, simulações de prontidão para ataques, proteção, alertas e recuperação. Com relatórios, você pode salvar e revisar relatórios offline sobre simulações, nível de proteção, alertas e eventos de 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.

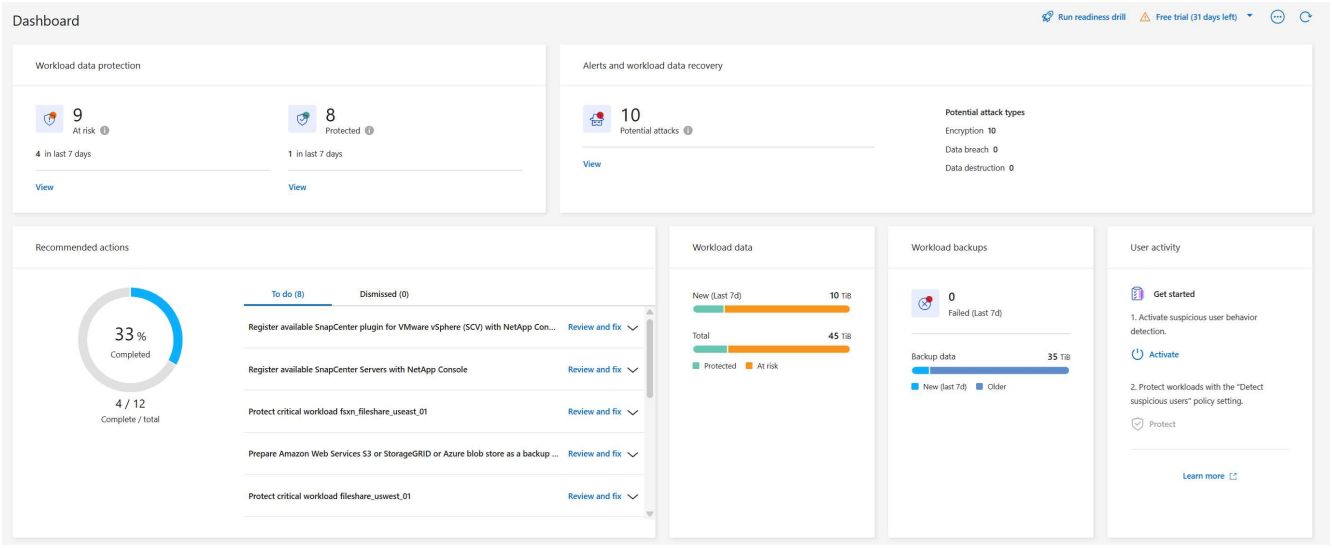
Você pode baixar relatórios de exercícios de prontidão somente na página **Relatórios**.

Se você baixar arquivos CSV ou JSON da página Proteção, Alertas ou Recuperação, os dados mostrarão apenas os dados dessa página.

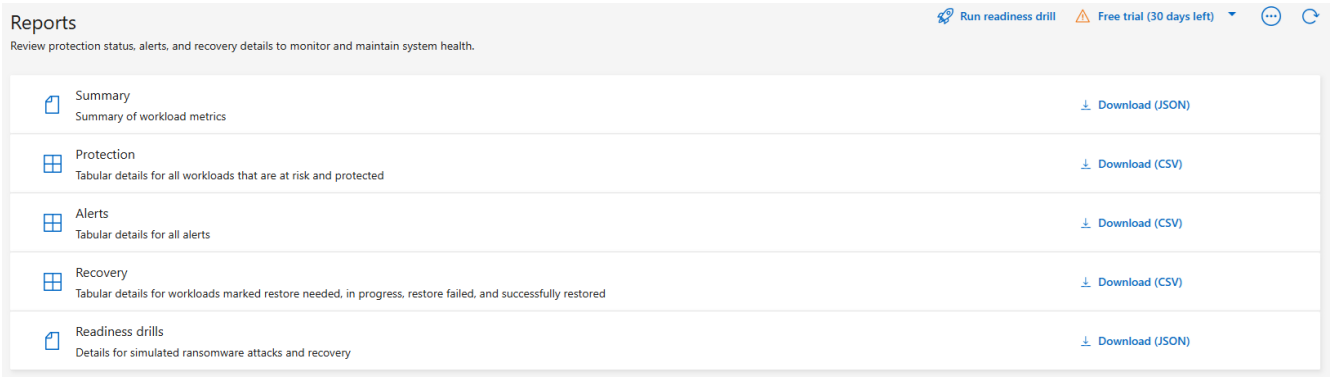
Os arquivos CSV ou JSON incluem dados para todas as cargas de trabalho em todos os sistemas do Console.

Passos

1. Na navegação à esquerda do Console, selecione **Proteção** > **Resiliência a Ransomware**.



2. No Painel ou em outra página, selecione *Atualizar* opção no canto superior direito para atualizar os dados que aparecerão nos relatórios.
3. Faça um dos seguintes:
   - Na página, selecione *Download* opção.
   - No menu NetApp Ransomware Resilience , selecione **Relatórios**.
4. 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)

Informações sobre direitos autorais

Informações sobre marcas comerciais