Notas de lançamento

BlueXP ransomware protection

NetApp
December 20, 2024

Índice

Notas de lançamento 1
Novidades na proteção contra ransomware do BlueXP 1

Notas de lançamento

Novidades na proteção contra ransomware do BlueXP

Saiba o que há de novo na proteção contra ransomware do BlueXP .

16 de dezembro de 2024

Detecte um comportamento anômalo do usuário usando a segurança de workloads de storage do Data Infrastructure Insights

Com esta versão, você pode usar a segurança de workload de storage do Data Infrastructure Insights para detectar um comportamento incomum dos usuários em seus workloads de storage. Esse recurso ajuda você a identificar possíveis ameaças à segurança e bloquear usuários potencialmente maliciosos para proteger seus dados.

Para obter detalhes, "Responda a um alerta de ransomware detetado" consulte .

Antes de usar a segurança de workload de storage para detectar comportamento anômalo do usuário, você precisa configurar a opção usando a opção **Configurações** de proteção contra ransomware da BlueXP .

Consulte a "Configurar as configurações de proteção contra ransomware do BlueXP ".

Selecione workloads para descobrir e proteger

Com esta versão, agora você pode fazer o seguinte:

- Em cada conetor, 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 em outros.
- Durante a descoberta do workload, é possível habilitar a detecção automática de workloads por conector. Esse recurso permite selecionar as cargas de trabalho que você deseja proteger.
- Descubra cargas de trabalho recém-criadas para ambientes de trabalho selecionados anteriormente.

Consulte a "Localizar workloads".

7 de novembro de 2024

Ativar a classificação de dados e procurar informações de identificação pessoal (PII)

Com essa versão, você pode habilitar a classificação do BlueXP , um componente essencial da família BlueXP , para verificar e classificar dados em seus workloads de compartilhamento de arquivos. A classificação de dados ajuda a identificar se os 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 proteção contra ransomware do BlueXP geralmente está disponível para clientes que implantaram a classificação BlueXP . A classificação do BlueXP está disponível como parte da plataforma BlueXP sem custo adicional e pode ser implantada no local ou na nuvem do cliente.

Consulte a "Configurar as configurações de proteção contra ransomware do BlueXP ".

Para iniciar a digitalização, na página proteção, clique em **Identify exposure** (identificar exposição à privacidade) na coluna Privacy exposure (exposição à privacidade).

"Procure dados confidenciais pessoalmente identificáveis com a classificação BlueXP ".

Integração SIEM com o Microsoft Sentinel

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

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

Teste gratuito agora 30 dias

Com esse lançamento, novas implantações de proteção contra ransomware do BlueXP agora têm 30 dias para uma avaliação gratuita. Anteriormente, a proteção contra ransomware da BlueXP forneceu 90 dias como uma avaliação gratuita. Se você já está no teste gratuito de 90 dias, essa oferta continua por 90 dias.

Restaure a carga de trabalho do aplicativo no nível do arquivo para o Podman

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode ver uma lista de ficheiros que podem ter sido afetados por um ataque e identificar os que pretende restaurar. Anteriormente, se os conetores BlueXP em uma organização (anteriormente uma conta) estavam usando o Podman, esse recurso foi desativado. Agora está habilitado para Podman. Você pode permitir que a proteção contra ransomware do BlueXP escolha os arquivos a serem restaurados, você pode carregar um arquivo CSV que lista todos os arquivos afetados por um alerta ou você pode identificar manualmente quais arquivos deseja restaurar.

"Saiba mais sobre como recuperar de um ataque de ransomware".

30 de setembro de 2024

Agrupamento personalizado de workloads de compartilhamento de arquivos

Com essa versão, agora você pode agrupar compartilhamentos de arquivos em grupos para facilitar a proteção do data Estate. O serviço pode proteger todos os volumes de um grupo ao mesmo tempo. Anteriormente, você precisava proteger cada volume separadamente.

"Saiba mais sobre como agrupar cargas de trabalho de compartilhamento de arquivos em estratégias de proteção contra ransomware".

2 de setembro de 2024

Avaliação de riscos de segurança do Digital Advisor

A proteção contra ransomware da BlueXP agora reúne informações sobre riscos de segurança altos e críticos relacionados a um cluster do consultor digital da NetApp. Se algum risco for encontrado, a proteção contra ransomware do BlueXP fornece uma recomendação no painel **ações recomendadas** do Painel: "Corrigir uma vulnerabilidade de segurança conhecida no cluster <name>." A partir da recomendação no Dashboard, clicar em **Review and FIX** sugere rever o Digital Advisor e um artigo CVE (Common Vulnerability & Exposure) para resolver o risco de segurança. Se houver vários riscos de segurança, revise as informações no Digital Advisor.

Consulte a "Documentação do Digital Advisor".

Faça backup do Google Cloud Platform

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

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

Suporte para o Google Cloud Platform

O serviço agora oferece suporte ao Cloud Volumes ONTAP para proteção de storage. Anteriormente, o serviço suportava apenas o Cloud Volumes ONTAP para Amazon Web Services e o Microsoft Azure, juntamente com nas no local.

"Saiba mais sobre a proteção contra ransomware da BlueXP e fontes de dados compatíveis, destinos de backup e ambientes de trabalho".

Controles de acesso baseados em função

Agora é possível limitar o acesso a atividades específicas com o controle de acesso baseado em funções (RBAC). A proteção contra ransomware do BlueXP usa duas funções do BlueXP : Administrador de conta do BlueXP e administrador não-conta (visualizador).

Para obter detalhes sobre as ações que cada função pode executar, "Controles de acesso baseados em função Privileges" consulte .

5 de agosto de 2024

Detecção de ameaças com o Splunk Cloud

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

"Saiba mais sobre como configurar as configurações de proteção contra ransomware do BlueXP".

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 de seu representante de vendas da NetApp

"Saiba mais sobre como configurar o licenciamento".

Restaure o workload do aplicativo no nível do arquivo

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode ver uma lista de ficheiros que podem ter sido afetados por um ataque e identificar os que pretende restaurar. Você pode permitir que a proteção contra ransomware do BlueXP escolha os arquivos a serem restaurados, você pode carregar um arquivo CSV que lista todos os arquivos afetados por um alerta ou você pode identificar

manualmente quais arquivos deseja restaurar.

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

"Saiba mais sobre como recuperar de um ataque de ransomware".

Faça o download de uma lista de arquivos afetados

Antes de restaurar uma carga de trabalho de aplicação no nível do ficheiro, agora pode aceder à página Alertas para transferir uma lista de ficheiros afetados num ficheiro CSV e, em seguida, utilizar a página recuperação para carregar o ficheiro CSV.

"Saiba mais sobre como baixar arquivos afetados antes de restaurar um aplicativo".

Eliminar plano de proteçãoão

Com essa 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 cópias snapshot no storage primário

Isso permite bloquear as cópias Snapshot no storage primário para que elas não possam ser modificadas ou excluídas por um determinado período, mesmo que um ataque de ransomware gerencie seu caminho até o destino do storage de backup.

"Saiba mais sobre como proteger cargas de trabalho e ativar 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 ambiente de trabalho, além do Cloud Volumes ONTAP para AWS e do ONTAP nas local.

"Início rápido para Cloud Volumes ONTAP no Azure"

"Saiba mais sobre a proteção contra ransomware BlueXP ".

Microsoft Azure adicionado como destino de backup

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

"Saiba mais sobre como configurar as configurações de proteção".

14 de maio de 2024

Atualizações de licenciamento

Você pode se inscrever para uma avaliação gratuita de 90 dias. Em breve, você poderá comprar uma assinatura paga conforme o uso com o mercado de Serviços Web da Amazon ou trazer sua própria licença do NetApp.

"Saiba mais sobre como configurar o licenciamento".

Protocolo CIFS

O serviço agora é compatível com ONTAP e Cloud Volumes ONTAP no local em ambientes de trabalho da AWS usando protocolos NFS e CIFS. A versão anterior era compatível apenas com o protocolo NFS.

Detalhes do workload

Esta versão agora fornece mais detalhes nas informações de carga de trabalho das páginas proteção e outras para uma avaliação melhorada da proteção da carga de trabalho. Nos detalhes do workload, você pode revisar a política atribuída no momento e revisar os destinos de backup configurados.

"Saiba mais sobre como visualizar os detalhes da carga de trabalho nas páginas proteção".

Proteção e recuperação consistentes com aplicações e VM

Agora, você pode executar proteção consistente com aplicações com o software NetApp SnapCenter e a proteção consistente com VM com o plug-in SnapCenter para VMware vSphere, obtendo um estado inativo e consistente para evitar a perda de dados em potencial mais tarde se a recuperação for necessária. Se a recuperação for necessária, você poderá restaurar o aplicativo ou a VM de volta para qualquer um dos estados disponíveis anteriormente.

"Saiba mais sobre como proteger cargas de trabalho".

Estratégias de proteção contra ransomware

Se as políticas Snapshot ou Backup não existirem no workload, você poderá criar uma estratégia de proteção contra ransomware, que pode incluir as seguintes políticas criadas neste serviço:

- Política do Snapshot
- Política de backup
- Política de deteção

"Saiba mais sobre como proteger cargas de trabalho".

Detecção de ameaças

Ativar deteção de ameaças agora está disponível usando um sistema de gerenciamento de eventos e segurança de terceiros (SIEM). O Dashboard agora mostra uma nova recomendação para "habilitar a deteção de ameaças", que pode ser configurada na página Configurações.

"Saiba mais sobre como configurar as opções de Configurações".

Ignorar alertas falsos positivos

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

"Saiba mais sobre como responder a um alerta de ransomware".

Estado de deteção

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".

Faça o download de arquivos CSV

Você pode baixar arquivos CSV* nas páginas proteção, Alertas e recuperação.

"Saiba mais sobre como baixar arquivos CSV do Painel de Controle e outras páginas".

Link de documentação

O link Exibir documentação agora está incluído na interface do usuário. Você pode acessar esta documentação a partir da opção Dashboard vertical **actions***  **. Selecione *Novidades** para visualizar detalhes nas Notas de versão ou **Documentação** para visualizar a página inicial da documentação de proteção contra ransomware do BlueXP .

Backup e recuperação do BlueXP

O serviço de backup e recuperação do BlueXP já não precisa estar habilitado no ambiente de trabalho. "pré-requisitos"Consulte . O serviço de proteção contra ransomware do BlueXP ajuda a configurar um destino de backup por meio da opção Configurações. "Configure as definições"Consulte .

Opção de definições

Agora você pode configurar destinos de backup nas Configurações de proteção contra ransomware do BlueXP .

"Saiba mais sobre como configurar as opções de Configurações".

5 de março de 2024

Gestão da política de proteção

Além de usar políticas predefinidas, agora você pode criar políticas. "Saiba mais sobre como gerenciar políticas".

Imutabilidade no armazenamento secundário (DataLock)

Agora você pode tornar o backup imutável no storage 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 destino de backup. "Saiba mais sobre como configurar destinos de backup".

Recursos adicionais para investigar possíveis ataques

Agora você pode ver mais detalhes forenses para investigar o potencial ataque detetado. "Saiba mais sobre como responder a um alerta de ransomware detetado".

Processo de recuperação

O processo de recuperação foi aprimorado. Agora, você pode recuperar volume por volume ou todos os volumes para um workload. "Saiba mais sobre como recuperar de um ataque de ransomware (após os incidentes terem sido neutralizados)".

"Saiba mais sobre a proteção contra ransomware BlueXP ".

6 de outubro de 2023

O serviço de proteção contra ransomware da BlueXP é uma solução SaaS para proteger dados, detectar possíveis ataques e recuperar dados de um ataque de ransomware.

Para a versão de visualização, o serviço protege workloads baseados em aplicações de Oracle, MySQL, armazenamentos de dados de VM e compartilhamentos de arquivos no storage nas local, bem como o Cloud Volumes ONTAP na AWS (usando o protocolo NFS) em organizações da BlueXP individualmente e faz o backup dos dados no storage de nuvem da Amazon Web Services.

O serviço de proteção contra ransomware da BlueXP fornece uso completo de várias tecnologias NetApp para que seu administrador de segurança ou engenheiro de operações de segurança de dados possam atingir as seguintes metas:

- Visualizar rapidamente a proteção contra ransomware em todos os seus workloads.
- Tenha insights sobre as recomendações de proteção de ransomware
- Melhorar a postura de proteção com base nas recomendações de proteção contra ransomware da BlueXP .
- Atribua políticas de proteção contra ransomware para proteger seus principais workloads e dados de alto risco contra ataques de ransomware.
- Monitore a integridade dos workloads contra ataques de ransomware em busca de anomalias de dados.
- Avalie rapidamente o impactos de incidentes de ransomware em sua carga de trabalho.
- Recupere de incidentes de ransomware de forma inteligente, restaurando os dados e garantindo que a reinfeção dos dados armazenados não ocorra.

"Saiba mais sobre a proteção contra ransomware BlueXP ".

Informações sobre direitos autorais

Informações sobre marcas comerciais