Sobre a proteção contra ransomware da NetApp

ONTAP 9

NetApp
January 17, 2025

Índice

Sobre a proteção contra ransomware da NetApp . . . 1
- Portfólio de proteção de ransomware e NetApp . . . 1
- Cópias snapshot à prova de SnapLock e invioláveis para proteção de ransomware . . . 3
- Bloqueio de arquivos FPolicy . . . 4
- Segurança de carga de trabalho de armazenamento Cloud Insights (CISWS) . . . 5
- Detecção e resposta incorporadas baseada em IA on-box da NetApp ONTAP . . . 6
- Proteção WORM com uso de cofres cibernéticos . . . 7
- Proteção contra ransomware do Digital Advisor . . . 8
- Resiliência abrangente com proteção contra ransomware da BlueXP . . . 8

Sobre a proteção contra ransomware da NetApp

Portfólio de proteção de ransomware e NetApp

O ransomware continua sendo uma das ameaças mais significativas que causam interrupções nos negócios na organização em 2024. De acordo com o "Sophos State of ransomware 2024", os ataques de ransomware afetaram 72% do público pesquisado. Os ataques de ransomware evoluíram para serem mais sofisticados e direcionados, com os agentes de ameaças empregando técnicas avançadas como inteligência artificial para maximizar seu impactos e lucros.

As organizações devem examinar toda a postura de segurança de perímetro, rede, identidade, aplicativo e onde os dados estão no nível de storage e proteger essas camadas. A adoção de uma abordagem centrada em dados à proteção cibernética na camada de storage é crucial no cenário de ameaças atual. Embora nenhuma solução única possa impedir todos os ataques, o uso de um portfólio de soluções, incluindo parcerias e terceiros, oferece uma defesa em camadas.

O Portfólio de produtos NetApp oferece várias ferramentas eficazes de visibilidade, detecção e correção, ajudando você a identificar ransomware com antecedência, prevenir propagação e se recuperar rapidamente, se necessário, para evitar tempo de inatividade caro. As soluções tradicionais de defesa em camadas continuam prevalecendo, assim como as soluções de terceiros e parceiros para visibilidade e detecção. A correção eficaz continua sendo uma parte crucial da resposta a qualquer ameaça. A abordagem exclusiva do setor que utiliza a tecnologia imutável Snapshot da NetApp e a solução SnapLock Logical AIR GAP é um diferencial do setor e a prática recomendada do setor para recursos de correção de ransomware.

> A partir de julho de 2024, o conteúdo do relatório técnico *TR-4572: NetApp ransomware Protection*, que foi publicado anteriormente como PDF, foi integrado ao restante da documentação do produto ONTAP.

Os dados são o alvo principal

Os cibercriminosos segmentam cada vez mais os dados diretamente, reconhecendo seu valor. Embora a segurança de perímetro, rede e aplicativos sejam importantes, eles podem ser ignorados. Com o foco na proteção de dados em sua origem, a camada de storage, fornece uma última linha de defesa crítica. Obter acesso aos dados de produção e criptografá-los ou torná-los inacessíveis é o objetivo dos ataques de ransomware. Para chegar lá, os invasores já devem ter perfurado as defesas existentes implantadas pelas organizações hoje, do perímetro à segurança do aplicativo.

[Camadas de segurança do perímetro à segurança dos dados]

Infelizmente, muitas organizações não aproveitam os recursos de segurança na camada de dados. É aqui que entra o portfólio de proteção contra ransomware da NetApp, protegendo você na última linha de defesa.

O custo real do ransomware

O pagamento de resgate em si não é o maior efeito monetário em um negócio. Embora o pagamento não seja insignificante, ele fica pálido em comparação com o custo do tempo de inatividade de sofrer um incidente de ransomware.

Os pagamentos de resgate são apenas um elemento dos custos de recuperação ao lidar com eventos de ransomware. Excluindo quaisquer resgates pagos, em 2024 as organizações relataram um custo médio para

se recuperar de um ataque de ransomware de 2,73M dólares, um aumento de quase 1M dólares em relação aos 1,82M dólares relatados em 2023, de acordo com o "2024 Sophos State of ransomware" relatório. Para organizações que dependem muito da DISPONIBILIDADE DE TI, como e-commerce, negociação de ações e cuidados de saúde, os custos podem ser 10 vezes maiores ou mais.

Os custos do seguro cibernético também continuam a aumentar, dada a probabilidade muito real de um ataque de ransomware a empresas seguradas.

Proteção contra ransomware na camada de dados

A NetApp entende que sua postura de segurança é ampla e profunda em toda a organização, desde o perímetro até o local onde os dados estão na camada de storage. Sua pilha de segurança é complexa e deve fornecer segurança em todos os níveis de sua pilha de tecnologia.

A proteção em tempo real na camada de dados é ainda mais importante e tem requisitos exclusivos. Para serem eficazes, as soluções nessa camada devem oferecer esses atributos críticos:

- **Segurança por design** para minimizar a chance de ataque bem-sucedido
- **Detecção e resposta em tempo real** para minimizar o impactos de um ataque bem-sucedido
- **Proteção WORM com ar-gapped** para isolar backups de dados críticos
- * Um único plano de controle* para uma defesa abrangente contra ransomware

A NetApp pode oferecer tudo isso e muito mais.

[Portfólio de proteção contra ransomware do NetApp que inclui os atributos essenciais descritos]

Portfólio de proteção contra ransomware da NetApp

A NetApp "proteção incorporada contra ransomware"oferece defesa em tempo real, robusta e multifacetada para seus dados críticos. Na sua essência, os algoritmos avançados de detecção habilitados por IA monitoram continuamente os padrões de dados, identificando rapidamente possíveis ameaças de ransomware com precisão de 99%. Reagir rapidamente a ataques permite que nosso storage snapshots rapidamente os dados e proteja as cópias, garantindo uma recuperação rápida.

Para fortalecer ainda mais os dados, a capacidade do NetApp "vaulting cibernético"isola os dados com uma lacuna de ar lógica. Ao proteger os dados essenciais, garantimos a rápida continuidade dos negócios.

O NetApp "Proteção contra ransomware da BlueXP"reduz o sobrecarga operacional com um único plano de controle para coordenar e executar de forma inteligente uma defesa contra ransomware centrada no workload de ponta a ponta. Assim, você identifica e protege os dados críticos dos workloads em risco com um único clique. Com apenas um clique, a detecção e resposta precisas e automáticas para limitar o impacto de um possível ataque e recuperar workloads em minutos e não dias, protegendo os dados valiosos dos workloads e minimizando interrupções dispendiosos.

Como uma solução ONTAP nativa e integrada para proteger o acesso não autorizado aos seus dados, "Verificação multi-admin (MAV)" tem um conjunto robusto de recursos que garante que operações como excluir volumes, criar usuários administrativos adicionais ou excluir cópias snapshot possam ser executadas somente após aprovações de pelo menos um segundo administrador designado. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados. Você pode configurar quantos aprovadores de administrador designados desejar antes que uma cópia de snapshot possa ser excluída.

O NetApp ONTAP atende ao requisito para a autenticação de CLI SSH baseada na Web "Autenticação multifator (MFA)" no Gerenciador de sistema.

A proteção contra ransomware da NetApp oferece tranquilidade em um cenário de ameaças em constante evolução. Sua abordagem abrangente não só defende as variantes atuais de ransomware, mas também se adapta a ameaças emergentes, fornecendo segurança em longo prazo para sua infraestrutura de dados.

Saiba mais sobre outras opções de proteção

- "Proteção contra ransomware do Digital Advisor"
- "Segurança de carga de trabalho de armazenamento Cloud Insights (CISWS)"
- "FPolicy"
- "Cópias snapshot à prova de SnapLock e invioláveis"

Garantia de recuperação de ransomware

A NetApp oferece a garantia de restaurar os dados do Snapshot se ocorrer um ataque de ransomware. Nossa garantia: Se não pudermos ajudá-lo a restaurar seus dados de snapshot, faremos isso certo. A garantia está disponível em novas aquisições de sistemas AFF A-Series, AFF C-Series, ASA e FAS.

Saiba mais

- "Descrição do serviço de garantia de recuperação"
- "Blog de garantia de recuperação de ransomware".

Informações relacionadas

- "Página de recursos do site de suporte da NetApp"
- "Segurança do produto NetApp"

Cópias snapshot à prova de SnapLock e invioláveis para proteção de ransomware

Uma arma vital no arsenal de NetApp Snap é o SnapLock, que provou ser altamente eficaz na proteção contra ameaças de ransomware. Ao impedir a exclusão não autorizada de dados, o SnapLock fornece uma camada adicional de segurança, garantindo que os dados críticos permaneçam intactos e acessíveis, mesmo em caso de ataques mal-intencionados.

SnapLock Compliance

O SnapLock Compliance (SLC) fornece proteção indelével para seus dados. O SLC proíbe que os dados sejam excluídos mesmo quando um administrador tenta reinicializar a matriz. Ao contrário de outros produtos competitivos, o SnapLock Compliance não é vulnerável a ataques de engenharia social por meio das equipes de suporte desses produtos. Os dados protegidos por volumes do SnapLock Compliance são recuperáveis até que esses dados atinjam a data de expiração.

Para ativar o SnapLock, é necessária uma "ONTAP One" licença.

Saiba mais

- "Documentação do SnapLock"

Cópias Snapshot à prova de violações

As cópias Snapshot (TPS) à prova de violações fornecem uma maneira conveniente e rápida de proteger os dados de atos maliciosos. Ao contrário do SnapLock Compliance, o TPS é normalmente usado em sistemas primários onde o usuário pode proteger os dados por um determinado tempo e deixado localmente para recuperações rápidas ou onde os dados não precisam ser replicados fora do sistema primário. O TPS usa tecnologias SnapLock para impedir que a cópia snapshot principal seja excluída, mesmo por um administrador do ONTAP que use o mesmo período de expiração de retenção do SnapLock. A exclusão de cópias snapshot é impedida mesmo que o volume não esteja habilitado para SnapLock, embora os snapshots não tenham a mesma natureza indelével dos volumes SnapLock Compliance.

Para fazer cópias snapshot à prova de violações, é necessária uma "ONTAP One" licença.

Saiba mais

- "Bloqueie uma cópia snapshot para proteção contra ataques de ransomware".

Bloqueio de arquivos FPolicy

O FPolicy impede que arquivos indesejados sejam armazenados em seu dispositivo de armazenamento de nível empresarial. O FPolicy também oferece uma maneira de bloquear extensões de arquivo ransomware conhecidas. Um usuário ainda tem permissões de acesso total à pasta inicial, mas o FPolicy não permite que um usuário armazene arquivos que suas marcas de administrador como bloqueados. Não importa se esses arquivos são arquivos MP3 ou extensões de arquivo ransomware conhecidas.

Bloqueie arquivos maliciosos com o modo nativo FPolicy

O modo nativo do NetApp FPolicy (uma evolução do nome, Política de arquivos) é uma estrutura de bloqueio de extensão de arquivo que permite bloquear extensões de arquivo indesejadas de entrar em seu ambiente. Faz parte do ONTAP há mais de uma década e é incrivelmente útil para ajudar você a proteger contra ransomware. Esse mecanismo de confiança zero é valioso porque você obtém medidas de segurança extras além das permissões da lista de controle de acesso (ACL).

No ONTAP System Manager e no BlueXP , uma lista de mais de 3000 extensões de arquivo está disponível para referência.

> Algumas extensões podem ser legítimas em seu ambiente e bloqueá-las pode levar a problemas inesperados. Crie sua própria lista apropriada para o seu ambiente antes de configurar o FPolicy nativo.

O modo nativo FPolicy está incluído em todas as licenças do ONTAP.

Saiba mais

- "Blog: Fighting ransomware: Parte três - ONTAP FPolicy, outra ferramenta nativa poderosa (também conhecida como gratuita)"

Ative a análise de comportamento do usuário e da entidade (UEBA) com o modo externo FPolicy

O modo externo FPolicy é uma estrutura de notificação e controle de atividade de arquivo que fornece visibilidade da atividade de arquivo e do usuário. Essas notificações podem ser usadas por uma solução

externa para executar análises baseadas em IA para detetar comportamentos maliciosos.

O modo externo FPolicy também pode ser configurado para aguardar a aprovação do servidor FPolicy antes de permitir que atividades específicas passem. Várias políticas como essa podem ser configuradas em um cluster, o que proporciona grande flexibilidade.

> Os servidores FPolicy devem ser responsivos às solicitações FPolicy se configurados para fornecer aprovação; caso contrário, o desempenho do sistema de storage pode ser afetado negativamente.

O modo externo FPolicy está incluído no "Todas as licenças ONTAP".

Saiba mais

- "Blog: Fighting ransomware: Parte quatro - UBA e ONTAP com o modo externo FPolicy."

Segurança de carga de trabalho de armazenamento Cloud Insights (CISWS)

A segurança de workload de storage (SWS) é um recurso do NetApp Cloud Insights que aprimora a postura de segurança, a capacidade de recuperação e a responsabilidade de um ambiente ONTAP. O SWS adota uma abordagem centrada no usuário, rastreando todas as atividades de arquivos de todos os usuários autenticados no ambiente. Ele usa análises avançadas para estabelecer padrões de acesso normais e sazonais para cada usuário. Esses padrões são usados para identificar rapidamente comportamentos suspeitos sem a necessidade de assinaturas de ransomware.

Quando o SWS deteta um potencial ransomware, exclusão de dados ou ataque de exfiltração, ele pode tomar ações automáticas, como:

- Tire um instantâneo do volume afetado.
- Bloqueie a conta de utilizador e o endereço IP suspeito de atividade maliciosa.
- Envie um alerta para administradores.

Como pode tomar medidas automatizadas para parar rapidamente uma ameaça privilegiada, bem como rastrear todas as atividades de arquivos, o SWS torna a recuperação de um evento de ransomware muito mais simples e rápida. Com ferramentas avançadas de auditoria e forense integradas, os usuários podem ver imediatamente quais volumes e arquivos foram afetados por um ataque, de qual conta de usuário o ataque veio e de que ação maliciosa foi realizada. Instantâneos automáticos mitigam os danos e aceleram a restauração de arquivos.

[Resultados de ataques de segurança para workloads do Cloud Insights]

Alertas da proteção autônoma contra ransomware (ARP) da ONTAP também são visíveis no SWS, fornecendo uma única interface para clientes que usam ARP e SWS para proteger contra ataques de ransomware.

Saiba mais

- "NetApp Cloud Insights"

Detecção e resposta incorporadas baseada em IA on-box da NetApp ONTAP

À medida que as ameaças de ransomware se tornam cada vez mais sofisticadas, os seus mecanismos de defesa também devem ser aplicados. A proteção autônoma contra ransomware (ARP) da NetApp é baseada em AI com detecção inteligente de anomalias incorporada ao ONTAP. Ative-o para adicionar mais uma camada de defesa à sua resiliência cibernética.

ARP e ARP/AI são configuráveis por meio da interface de gerenciamento integrada do ONTAP, do Gerenciador de sistema e habilitados por volume.

Proteção autônoma contra ransomware (ARP)

A proteção autônoma contra ransomware (ARP), outra solução nativa da ONTAP incorporada desde 9.10.1, analisa a atividade do arquivo de workload de volume de storage nas e a entropia de dados para detectar automaticamente possíveis ransomwares. O ARP fornece aos administradores detecção, insights e um ponto de recuperação de dados em tempo real para deteção on-box de ransomware sem precedentes.

Para o ONTAP 9.15,1 e versões anteriores que suportam ARP, o ARP começa no modo de aprendizado para aprender a atividade típica de dados de carga de trabalho. Isso pode levar sete dias para a maioria dos ambientes. Depois que o modo de aprendizado estiver concluído, o ARP mudará automaticamente para o modo ativo e começará a procurar atividade anormal da carga de trabalho que possa potencialmente ser ransomware.

Se for detetada atividade anormal, uma cópia automática de instantâneos é imediatamente obtida, o que fornece um ponto de restauração o mais próximo possível do momento do ataque com dados infetados mínimos. Simultaneamente, é gerado um alerta automático (configurável) que permite que os administradores vejam a atividade anormal do arquivo para que possam determinar se a atividade é realmente maliciosa e tomar as medidas apropriadas.

Se a atividade for uma carga de trabalho esperada, os administradores podem marcá-la facilmente como um falso positivo. O ARP aprende essa mudança como atividade normal de carga de trabalho e não a sinaliza mais como um ataque potencial no futuro.

Para ativar o ARP, é necessária uma "ONTAP One" licença.

Saiba mais

- "Proteção autônoma contra ransomware"

Proteção autônoma contra ransomware/AI (ARP/AI)

Apresentado como uma prévia técnica no ONTAP 9.15,1, o ARP/AI leva a deteção em tempo real dos sistemas de armazenamento nas on-box para o próximo nível. A nova tecnologia de detecção habilitada por AI é treinada em mais de um milhão de arquivos e vários ataques de ransomware conhecidos. Além dos sinais usados no ARP, o ARP/AI também deteta criptografia de cabeçalho. A potência de IA e os sinais adicionais permitem que o ARP/AI forneça uma precisão de deteção superior a 99%. Isso foi validado pelo se Labs, um laboratório de testes independente que deu à ARP/AI a sua maior classificação AAA.

Como o treinamento dos modelos acontece continuamente na nuvem, o ARP/AI não requer um modo de aprendizado. Ele está ativo no momento em que é ligado. O treinamento contínuo também significa que o ARP/AI sempre é validado contra novos tipos de ataque de ransomware à medida que eles surgem. O ARP/AI

também vem com recursos de atualização automática que fornecem novos parâmetros a todos os clientes para manter a detecção de ransomware atualizada. Todos os outros recursos de deteção, insight e ponto de recuperação de dados do ARP são mantidos para ARP/AI.

Para ativar o ARP/AI, é necessária uma "ONTAP One" licença.

Saiba mais

- "Blog: A solução de deteção de ransomware em tempo real baseada em IA da NetApp atinge a classificação AAA"

Proteção WORM com uso de cofres cibernéticos

A abordagem da NetApp a um cofre cibernético é uma arquitetura de referência criada especificamente para um cofre cibernético com conexão lógica. Essa abordagem aproveita as tecnologias de fortalecimento da segurança e conformidade, como o SnapLock, para permitir snapshots imutáveis e indeléveis.

Cyber vaulting com SnapLock Compliance e uma lacuna de ar lógica

Uma tendência crescente é que os invasores destruam as cópias de backup e, em alguns casos, até as criptografem. É por isso que muitos no setor de cibersegurança recomendam o uso de backups Air Gap como parte de uma estratégia geral de resiliência cibernética.

O problema é que as lacunas de ar tradicionais (fita e Mídia off-line) podem aumentar significativamente o tempo de restauração, aumentando assim o tempo de inatividade e os custos associados gerais. Mesmo uma abordagem mais moderna de uma solução de abertura de ar pode ser problemática. Por exemplo, se o cofre de backup for temporariamente aberto para receber novas cópias de backup e, em seguida, desconetar e fechar sua conexão de rede com dados primários para que mais uma vez sejam "trocados", um invasor pode aproveitar a abertura temporária. Durante o tempo em que a conexão está online, um invasor pode atacar para comprometer ou destruir os dados. Esse tipo de configuração geralmente também adiciona complexidade indesejada. Uma lacuna de ar lógica é um excelente substituto para uma lacuna de ar tradicional ou moderna, porque tem os mesmos princípios de proteção de segurança, mantendo o backup on-line. Com o NetApp, você pode resolver a complexidade do gapping de ar em fita ou disco com gapping lógico de ar, o que pode ser alcançado com cópias snapshot imutáveis e NetApp SnapLock Compliance.

[Espaço lógico com o NetApp Cyber Vault]

A NetApp lançou o recurso SnapLock há mais de 10 anos para atender aos requisitos de conformidade de dados, como a Lei de portabilidade e responsabilidade de seguros de Saúde (HIPAA), a Sarbanes-Oxley e outras regras de dados regulatórios. Você também pode armazenar cópias snapshot primárias do SnapLock volumes para que as cópias possam ser comprometidas com WORM, impedindo a exclusão. Existem duas versões de licença SnapLock: SnapLock Compliance e SnapLock Enterprise. Para proteção contra ransomware, a NetApp recomenda o SnapLock Compliance porque você pode definir um período de retenção específico durante o qual as cópias snapshot são bloqueadas e não podem ser excluídas, mesmo pelos administradores do ONTAP ou pelo suporte da NetApp.

Saiba mais

- "Blog: Visão geral do ONTAP Cyber Vault"

Cópias snapshot à prova de violações

Embora a utilização do SnapLock Compliance como uma lacuna lógica forneça a melhor proteção para

impedir que atacantes excluam suas cópias de backup, ela exige que você mova as cópias snapshot usando o SnapVault para um volume secundário habilitado para SnapLock. Como resultado, muitos clientes implantam essa configuração em storage secundário na rede. Isso pode levar a tempos de restauração mais longos versus a restauração de uma cópia Snapshot de volume primário no storage primário.

A partir do ONTAP 9.12,1, as cópias snapshot à prova de violações fornecem proteção perto do nível SnapLock Compliance para suas cópias snapshot no storage primário e em volumes primários. Não há necessidade de armazenar a cópia Snapshot usando o SnapVault em um volume secundário SnapLocked. As cópias snapshot à prova de violações usam a tecnologia SnapLock para impedir que a cópia snapshot principal seja excluída, mesmo por um administrador completo da ONTAP usando o mesmo período de expiração de retenção da SnapLock. Isso possibilita tempos de restauração mais rápidos e o backup de um volume FlexClone por uma cópia Snapshot protegida e à prova de violações. Isso é algo que você não pode fazer com uma cópia Snapshot abobadada SnapLock Compliance tradicional.

A principal diferença entre as cópias snapshot da SnapLock Compliance e invioláveis é que o SnapLock Compliance não permite que o array ONTAP seja inicializado e apagado se existirem volumes SnapLock Compliance com cópias Snapshot abobadadas que ainda não atingiram sua data de expiração. Para fazer cópias Snapshot à prova de violações, é necessária uma licença SnapLock Compliance.

Saiba mais

- "Bloqueie uma cópia snapshot para proteção contra ataques de ransomware"

Proteção contra ransomware do Digital Advisor

O consultor digital da Active IQ (também conhecido como consultor digital) simplifica o cuidado proativo e a otimização do storage da NetApp com inteligência acionável para o gerenciamento ideal de dados. Alimentado por dados de telemetria de nossa base instalada altamente diversificada, ele usa técnicas avançadas de AI e ML para descobrir oportunidades de reduzir riscos e melhorar a performance e a eficiência do seu ambiente de storage.

Não só "Consultor digital da NetApp" pode ajudar "eliminar vulnerabilidades de segurança", mas também fornece insights e orientações específicos para a proteção contra ransomware. Um cartão de bem-estar dedicado mostra as ações necessárias e os riscos abordados, para que você possa ter certeza de que seus sistemas estão cumprindo essas recomendações de práticas recomendadas.

[Monitores de bem-estar no painel de consultores digitais da NetApp]

Os riscos e ações rastreados na página de bem-estar da Defesa do ransomware incluem o seguinte (e muito mais):

- A contagem de cópias snapshot de volume é baixa, diminuindo a possível proteção contra ransomware.
- O FPolicy não está habilitado para todas as máquinas virtuais de armazenamento (SVMs) configuradas para protocolos nas.

Para ver a proteção contra ransomware do Digital Advisor em ação, "Consultor digital da Active IQ"consulte .

Resiliência abrangente com proteção contra ransomware da BlueXP

É importante que a detecção de ransomware ocorra o mais cedo possível, para que você

possa evitar a propagação e evitar tempo de inatividade caro. No entanto, uma estratégia eficaz de detecção de ransomware deve incluir mais do que uma única camada de proteção. A proteção contra ransomware da NetApp adota uma abordagem abrangente que inclui recursos on-box em tempo real, que se estendem a serviços de dados usando o BlueXP e uma solução isolada em camadas para cofres cibernéticos.

Proteção contra ransomware da BlueXP

O BlueXP é um único plano de controle para orquestrar, de forma inteligente, uma defesa abrangente e centrada em workload. A proteção contra ransomware do BlueXP reúne os recursos avançados de resiliência cibernética do ONTAP, como snapshots ARP, FPolicy e invioláveis, além de serviços de dados da BlueXP , como backup e recuperação do BlueXP . Ele também adiciona recomendações e orientações com fluxos de trabalho automatizados para fornecer uma defesa completa por meio de uma única IU. Ele opera no nível da carga de trabalho para garantir que os aplicativos que executam sua empresa sejam protegidos e possam ser recuperados o mais rápido possível em caso de ataque.

[A proteção contra ransomware do BlueXP é uma inteligência baseada em AI e a assistência necessárias para minimizar a perda de dados de workload e recuperar rapidamente. Esta imagem mostra a IU do BlueXP .]

Benefícios para o cliente:

- A preparação assistida para ransomware reduz a sobrecarga operacional e melhora a eficácia
- A detecção de anomalias alimentada por IA/ML oferece maior precisão e resposta mais rápida para conter riscos
- A restauração orientada consistente com aplicações permite recuperar workloads com mais facilidade e em poucos minutos

"Proteção contra ransomware da BlueXP" Torna estas funções NIST mais fáceis de alcançar:

- **Descubra** e priorize dados automaticamente no armazenamento NetApp **com foco nas principais cargas de trabalho baseadas em aplicativos**.
- * Proteção com um clique* do backup de dados da carga de trabalho superior, configuração imutável e segura, bloqueio de arquivos maliciosos e domínio de segurança diferente.
- * Detecte com precisão* ransomware o mais rápido possível usando **detecção de anomalias baseada em IA de última geração.**
- Resposta automatizada e fluxos de trabalho e integração com as principais soluções **SIEM e XDR.**
- Restaure rapidamente os dados usando uma recuperação simplificada **orquestrada** para acelerar o tempo de atividade da aplicação.
- Implemente sua proteção contra ransomware * estratégia* e **políticas** e **monitore os resultados**.

Informações sobre direitos autorais

Informações sobre marcas comerciais