Ative o modelo Zero Trust

ONTAP 9

NetApp
January 17, 2025

Índice

Ative o modelo Zero Trust

NetApp e confiança zero

O Zero Trust tradicionalmente tem sido uma abordagem centrada na rede de arquitetura de micro núcleo e perímetro (MCAP) para proteger dados, serviços, aplicativos ou ativos com controles conhecidos como gateway de segmentação. A NetApp ONTAP está adotando uma abordagem centrada em dados para a confiança zero, na qual o sistema de gerenciamento de storage se torna o gateway de segmentação para proteger e monitorar o acesso aos dados de nossos clientes. Em particular, o mecanismo FPolicy Zero Trust e o ecossistema parceiro da FPolicy se tornam um centro de controle para obter uma compreensão detalhada dos padrões de acesso a dados normais e aberrantes e identificar ameaças internas.

A partir de julho de 2024, o conteúdo do relatório técnico *TR-4829: NetApp e confiança zero: Habilitando um modelo de confiança zero centrado em dados*, que foi publicado anteriormente como PDF, foi integrado com o restante da documentação do produto ONTAP.

Os dados são o ativo mais importante que sua organização tem. As ameaças internas são a causa de 18% das violações de dados, de acordo com o 2022 "Relatório de investigações de violação de dados da Verizon". As organizações podem aumentar a vigilância com a implantação de controles de confiança zero líderes do setor relacionados aos dados com o software de gerenciamento de dados NetApp ONTAP.

O que é Zero Trust?

O modelo Zero Trust foi desenvolvido pela primeira vez por John Kindervag na Forrester Research. A abordagem Zero Trust de dentro para fora identifica um micronúcleo e um perímetro (MCAP). O MCAP é uma definição interior de dados, serviços, aplicativos e ativos a serem protegidos com um conjunto abrangente de controles. O conceito de um perímetro externo seguro é obsoleto. As entidades que são confiáveis e têm permissão para se autenticar com êxito através do perímetro podem então tornar a organização vulnerável a ataques. Insiders, por definição, já estão dentro do perímetro seguro. Funcionários, contratados e parceiros são membros da equipe e precisam estar habilitados a operar com controles apropriados para desempenhar suas funções na infraestrutura da organização.

Zero Trust foi mencionado como uma tecnologia que oferece promessa ao DoD em setembro de 2019 "FY19-23 Estratégia de modernização Digital DoD". Ele define Zero Trust como "Uma estratégia de segurança cibernética que incorpora segurança em toda a arquitetura com o objetivo de impedir violações de dados. Esse modelo de segurança centrado em dados elimina a ideia de redes, dispositivos, personas ou processos confiáveis ou não confiáveis e muda para níveis de confiança baseados em múltiplos atributos que permitem políticas de autenticação e autorização sob o conceito de acesso menos privilegiado. A implementação de confiança zero requer repensar a forma como utilizamos a infraestrutura existente para implementar a segurança através do design de uma forma mais simples e eficiente, ao mesmo tempo que permite operações desimpedidas."

Em agosto de 2020, o NIST publicou "Especial Pub 800-207 arquitetura Zero Trust" (ZTA). O ZTA se concentra em proteger recursos, não segmentos de rede, porque a localização da rede não é mais vista como o principal componente da postura de segurança do recurso. Os recursos são dados e computação. As estratégias ZTA são para arquitetos de rede empresarial. O ZTA introduz uma nova terminologia dos conceitos originais da Forrester. Os mecanismos de proteção chamados de ponto de decisão de política (PDP) e ponto de aplicação de políticas (PEP) são análogos a um gateway de segmentação da Forrester. A ZTA apresenta

quatro modelos de implantação:

- Implantação baseada em agente de dispositivo ou gateway
- Implantação baseada em enclave (um pouco análoga ao Forrester MCAP)
- Implantação baseada em portal de recursos
- Aplicação do dispositivo sandboxing

Para os fins desta documentação, usamos os conceitos e a terminologia da Forrester Research em vez do ZTA NIST.

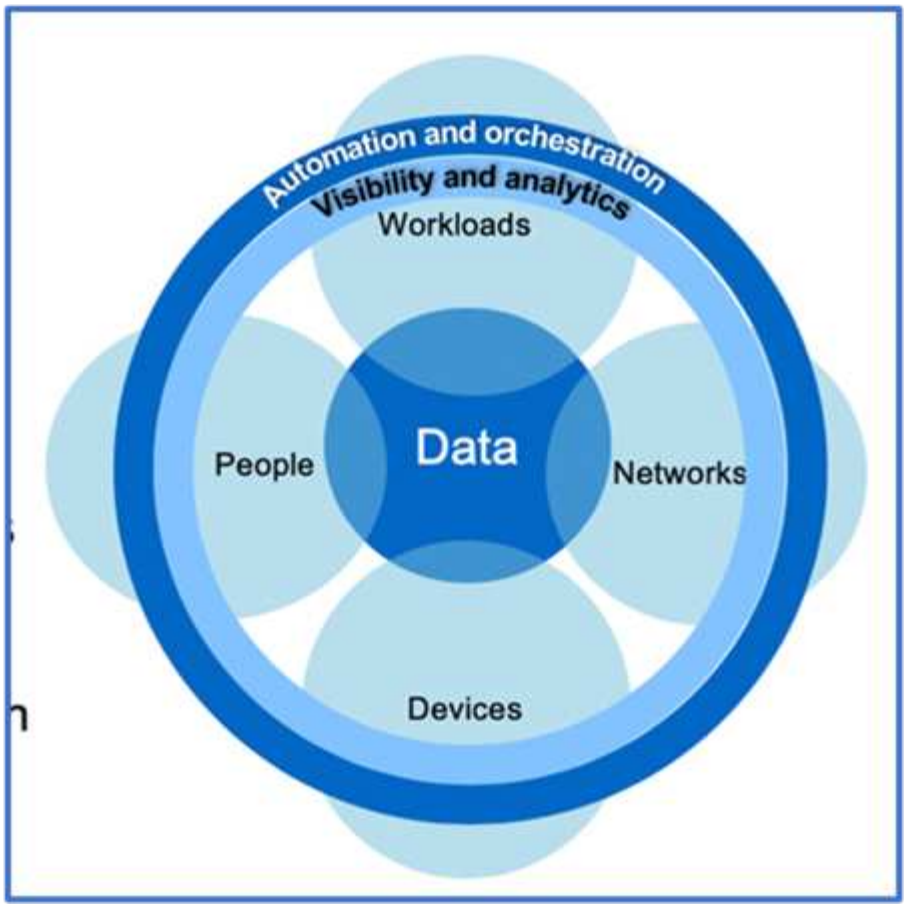
Recursos de segurança

Para obter informações sobre como reportar vulnerabilidades e incidentes, respostas de segurança do NetApp e confidencialidade do cliente, consulte o "Portal de segurança da NetApp".

Projete uma abordagem centrada em dados para zero confiança com o ONTAP

Uma rede Zero Trust é definida por uma abordagem centrada em dados, na qual os controles de segurança devem estar o mais próximos possível dos dados. As funcionalidades do ONTAP, somadas ao ecossistema parceiro do NetApp FPolicy, podem fornecer os controles necessários para o modelo de confiança zero centrado em dados.

O ONTAP é um software de gerenciamento de dados seguro da NetApp, e o mecanismo de confiança zero da FPolicy é um recurso ONTAP líder do setor que oferece uma interface de notificação granular com eventos baseados em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP.



Crie um MCAP centrado em dados Zero Trust

Para arquitetar um MCAP Zero Trust centrado em dados, siga estas etapas:

1. Identificar a localização de todos os dados organizacionais.
2. Classificar os dados.
3. Elimine com segurança os dados que já não necessita.
4. Entenda quais funções devem ter acesso às classificações de dados.
5. Aplique o princípio de privilégio mínimo para aplicar controles de acesso.
6. Use a autenticação multifator para acesso administrativo e acesso aos dados.
7. Uso de criptografia para dados em repouso e dados em trânsito.
8. Monitore e Registre todo o acesso.
9. Alertar acessos ou comportamentos suspeitos.

Identificar a localização de todos os dados organizacionais

O recurso FPolicy do ONTAP, juntamente com o ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. Mais detalhes sobre a análise comportamental do usuário são discutidos no Monitor e log todo o acesso. Se você não entender onde seus dados estão e quem tem acesso a eles, a análise comportamental do usuário pode fornecer uma linha de base para criar classificação e política a partir de observações empíricas.

Classificar os dados

Na terminologia do modelo Zero Trust, a classificação dos dados envolve a identificação de dados tóxicos. Dados tóxicos são dados confidenciais que não se destinam a ser expostos fora de uma organização. A divulgação de dados tóxicos pode violar a conformidade regulamentar e prejudicar a reputação de uma organização. Em termos de conformidade regulamentar, os dados tóxicos incluem dados do titular do cartão para a, dados pessoais para a "Padrão de segurança de dados do setor de cartões de pagamento (PCI-DSS)" UE "Regulamento Geral de proteção de dados (GDPR)" ou dados de cuidados de saúde para a "Lei de portabilidade e responsabilidade de seguros de saúde (HIPAA)". Você pode usar o NetApp "Classificação BlueXP " (anteriormente conhecido como Cloud Data Sense), um kit de ferramentas orientado por IA, para verificar, analisar e categorizar automaticamente seus dados.

Elimine com segurança os dados que já não necessita

Depois de classificar os dados da sua organização, você pode descobrir que alguns dos seus dados não são mais necessários ou relevantes para a função da sua organização. A retenção de dados desnecessários é uma responsabilidade, e esses dados devem ser excluídos. Para obter um mecanismo avançado para apagar dados criptograficamente, consulte a descrição da limpeza segura na criptografia dados em repouso.

Entenda quais funções devem ter acesso às classificações de dados e aplique o princípio de menor privilégio para impor controles de acesso

Mapear o acesso a dados confidenciais e aplicar o princípio do menor privilégio significa dar às pessoas em sua organização acesso apenas aos dados necessários para executar seus trabalhos. Esse processo envolve controle de acesso baseado em função ("RBAC"), que se aplica ao acesso a dados e acesso administrativo.

Com o ONTAP, uma máquina virtual de storage (SVM) pode ser usada para segmentar o acesso a dados organizacionais por locatários em um cluster do ONTAP. O RBAC pode ser aplicado ao acesso aos dados, bem como ao acesso administrativo ao SVM. O RBAC também pode ser aplicado no nível administrativo do cluster.

Além do RBAC, você pode usar o ONTAP "verificação multi-admin"(MAV) para exigir que um ou mais administradores aprovem comandos como `volume delete` ou `volume snapshot delete`. Uma vez que o MAV está ativado, modificar ou desativar o MAV requer a aprovação do administrador do MAV.

Outra maneira de proteger as cópias Snapshot é com o ONTAP "Bloqueio de cópias snapshot". O bloqueio de cópias snapshot é uma funcionalidade do SnapLock em que as cópias Snapshot são tornadas indeléveis manual ou automaticamente, com um período de retenção na política de cópia Snapshot de volume. O bloqueio de cópias snapshot também é conhecido como bloqueio de cópias Snapshot à prova de violação. O objetivo do bloqueio de cópias Snapshot é impedir que administradores desonestos ou não confiáveis excluam cópias Snapshot nos sistemas ONTAP primário e secundário. A recuperação rápida de cópias Snapshot bloqueadas em sistemas primários pode ser obtida para restaurar volumes corrompidos por ransomware.

Use a autenticação multifator para acesso administrativo e acesso aos dados

Além do RBAC administrativo de cluster, "Autenticação de vários fatores (MFA)" pode ser implantado para acesso à linha de comando ONTAP web administrative Access e Secure Shell (SSH). O MFA para acesso administrativo é um requisito para organizações do setor público dos EUA ou aquelas que precisam seguir o PCI-DSS. O MFA torna impossível para um invasor comprometer uma conta usando apenas um nome de usuário e senha. O MFA requer dois ou mais fatores independentes para autenticar. Um exemplo de autenticação de dois fatores é algo que um usuário possui, como uma chave privada, e algo que um usuário conhece, como uma senha. O acesso administrativo à Web ao ONTAP System Manager ou ao ActiveIQ Unified Manager é habilitado pela Security Assertion Markup Language (SAML) 2,0. O acesso à linha de comando SSH usa autenticação de dois fatores encadeada com uma chave pública e uma senha.

Você pode controlar o acesso de usuário e máquina por meio de APIs com os recursos de gerenciamento de identidade e acesso no ONTAP:

- Utilizador:
  - **Autenticação e autorização.** Por meio de funcionalidades de protocolo nas para SMB e NFS.
  - **Auditoria.** Syslog de acessos e eventos. Registo de auditoria detalhado do protocolo CIFS para testar políticas de autenticação e autorização. Auditoria granular fina de FPolicy de acesso detalhado nas no nível do arquivo.
- Dispositivo:
  - **Autenticação.** Autenticação baseada em certificado para acesso à API.
  - **Autorização.** Controle de acesso padrão ou personalizado baseado em função (RBAC).
  - **Auditoria.** Syslog de todas as ações tomadas.

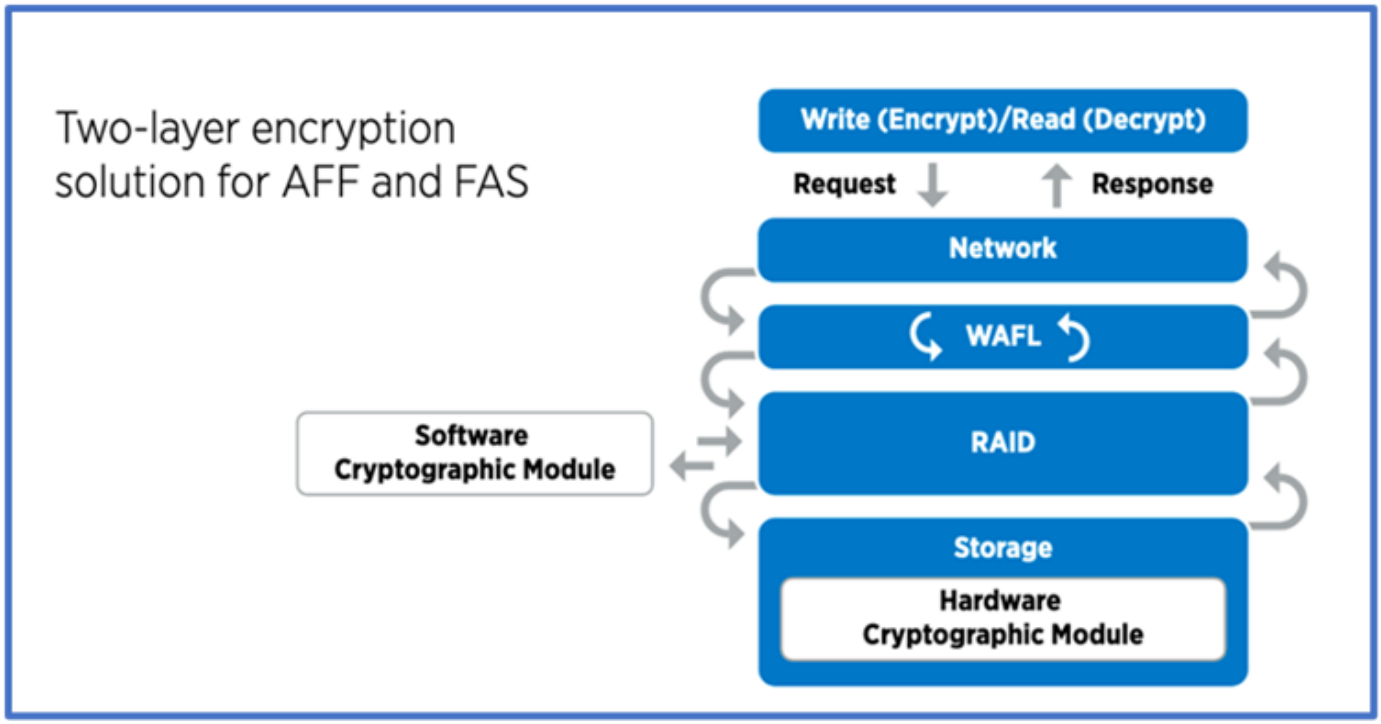
Uso de criptografia para dados em repouso e dados em trânsito

Criptografia de dados em repouso

Todos os dias, há novos requisitos para mitigar os riscos do sistema de storage e as lacunas de infraestrutura quando uma organização reutiliza unidades, retorna unidades com defeito ou atualiza "NetApp Storage Encryption (NSE) n.o 44; NetApp volume Encryption (NVE) n.o 44; e NetApp Aggregate Encryption" ajude você a criptografar todos os seus dados em repouso o tempo todo, seja tóxico ou não, sem afetar as operações diárias. "NSE" É uma solução de hardware ONTAP "dados em repouso"que utiliza unidades com autocriptografia validadas FIPS 140-2 nível 2. "NVE e NAE" São uma solução de software ONTAP "dados em repouso"que utiliza o "Módulo criptográfico NetApp validado FIPS 140-2 nível 1". Com NVE e NAE, os discos rígidos ou unidades de estado sólido podem ser usados para criptografia de dados em repouso. Além disso, as unidades NSE podem ser usadas para fornecer uma solução de criptografia nativa em camadas que fornece redundância de criptografia e segurança adicional. Se uma camada for violada, a segunda camada ainda protege os dados. Esses recursos tornam o ONTAP bem posicionado para "criptografia pronta para quantum"o .

O NVE também fornece uma funcionalidade chamada "purga segura" que remove criptograficamente dados tóxicos de derramamentos de dados quando arquivos confidenciais são gravados em um volume não classificado.

O "Gerenciador de chaves integrado (OKM)", que é o gerenciador de chaves integrado ao ONTAP, ou "aprovado" terceiros "gestores de chaves externos"podem ser usados com NSE e NVE para armazenar com segurança material de codificação.



Como visto na figura acima, a criptografia baseada em hardware e software pode ser combinada. Essa capacidade levou ao "Validação do ONTAP nas soluções comerciais da NSA para o programa classificado" que permite o armazenamento de dados secretos principais.

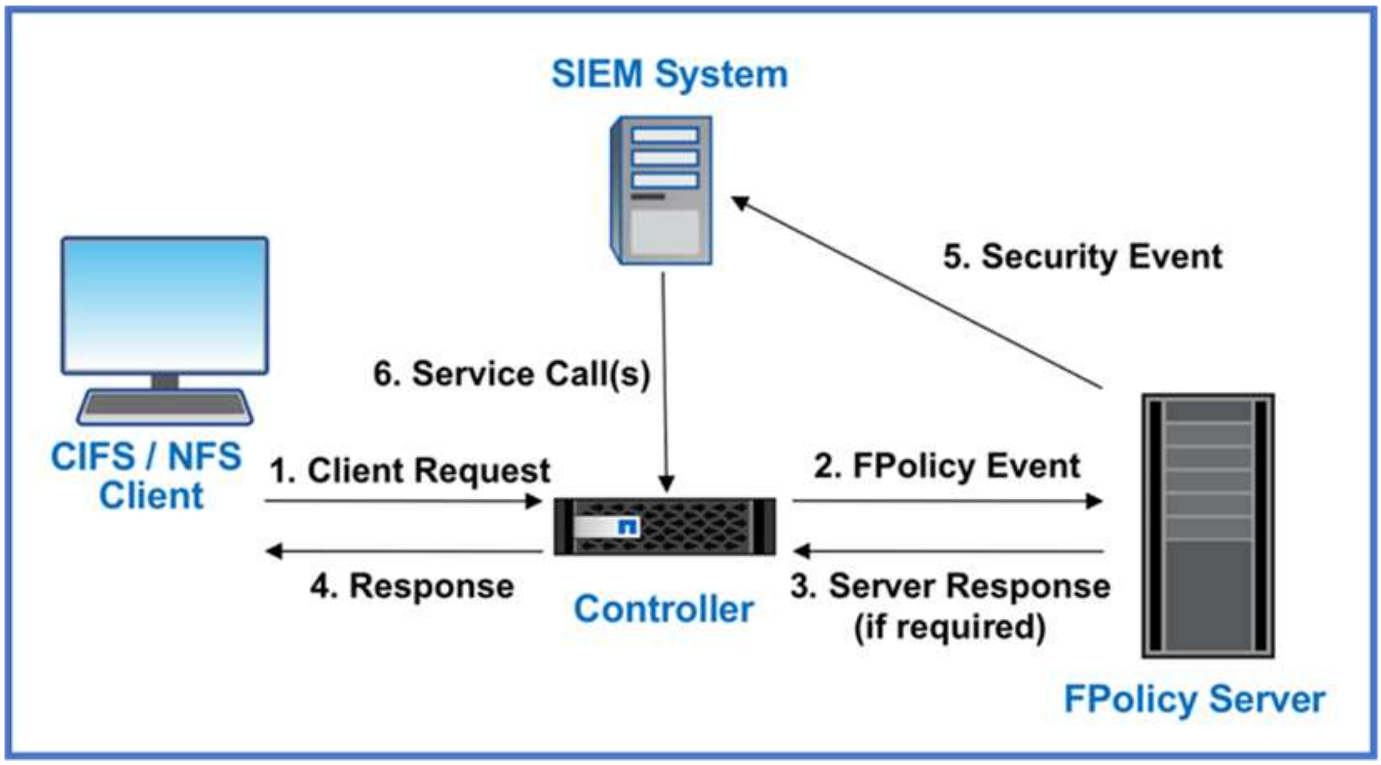
Criptografia de dados em trânsito

A criptografia de dados em trânsito do ONTAP protege o acesso aos dados do usuário e o acesso ao plano de controle. O acesso aos dados do usuário pode ser criptografado pela criptografia SMB 3,0 para o Microsoft CIFS Share Access ou pelo krb5P para NFS Kerberos 5. O acesso aos dados do usuário também pode ser criptografado com "IPsec"CIFS, NFS e iSCSI. O acesso ao plano de controle é criptografado com Transport Layer Security (TLS). O ONTAP fornece "FIPS"modo de conformidade para acesso ao plano de controle, o que habilita algoritmos aprovados pela FIPS e desabilita algoritmos que não são aprovados pela FIPS. A replicação de dados é criptografada com "criptografia por peer de cluster"o . Isso fornece criptografia para as tecnologias ONTAP SnapVault e SnapMirror.

Monitore e Registre todo o acesso

Depois que as políticas RBAC estiverem em vigor, você precisará implantar monitoramento, auditoria e alertas ativos. O mecanismo de confiança zero de FPolicy da NetApp ONTAP, juntamente com o "Ecossistema de parceiros do NetApp FPolicy", fornece os controles necessários para o modelo de confiança zero centrado em dados. O NetApp ONTAP é um software de gerenciamento de dados seguro e "FPolicy"é um recurso ONTAP líder do setor que oferece uma interface granular de notificação de eventos baseada em arquivo. Os parceiros do NetApp FPolicy podem usar essa interface para fornecer mais informações sobre o acesso aos dados no ONTAP. O recurso FPolicy do ONTAP, associado ao ecossistema de parceiros da Aliança NetApp dos parceiros FPolicy, permite identificar onde os dados da sua organização existem e quem tem acesso a eles. Isso é feito com análise comportamental do usuário, que identifica se os padrões de acesso aos dados são válidos. A análise comportamental do usuário pode ser usada para alertar para acesso a dados suspeitos ou aberrantes que estejam fora do padrão normal e, se necessário, tomar medidas para negar acesso.

Os parceiros do FPolicy estão indo além da análise comportamental do usuário em direção ao aprendizado de máquina (ML) e à inteligência artificial (AI) para maior fidelidade de eventos e menos, se houver, falsos positivos. Todos os eventos devem ser registrados em um servidor syslog ou em um sistema de gerenciamento de informações e eventos de segurança (SIEM) que também pode empregar ML e IA.



A Segurança de carga de trabalho de armazenamento da NetApp (anteriormente conhecida como "Cloud Secure") faz uso da interface FPolicy e da análise comportamental do usuário nos sistemas de storage ONTAP na nuvem e no local para fornecer alertas em tempo real sobre comportamento mal-intencionado do usuário. O Storage Workload Security protege os dados organizacionais contra a utilização indevida por usuários mal-intencionados ou comprometidos por meio do aprendizado de máquina avançado e da detecção de anomalias. O Storage Workload Security pode identificar ataques de ransomware ou outros comportamentos mal-intencionados, invocar cópias Snapshot e colocar em quarentena usuários mal-intencionados. O Storage Workload Security também tem uma capacidade forense para visualizar detalhadamente as atividades do usuário e da entidade. A segurança do workload de storage faz parte do NetApp Cloud Insights.

Além da segurança de workload de storage, o ONTAP tem uma funcionalidade de detecção de ransomware integrada conhecida como ARP (Onboard ransomware"Proteção autônoma contra ransomware"). O ARP usa aprendizado de máquina para determinar se uma atividade anormal de arquivos indica que um ataque de ransomware está em andamento e invoca uma cópia Snapshot e um alerta para os administradores. A segurança do workload de storage se integra ao ONTAP para receber eventos ARP e fornece uma camada adicional de análise e respostas automáticas.

Saiba mais sobre os comandos descritos neste procedimento no "Referência do comando ONTAP".

Controles de orquestração e automação de segurança da NetApp externos ao ONTAP

A automação permite que você execute um processo ou procedimento com o mínimo de assistência humana. A automação permite que as organizações escalem implantações Zero Trust muito além dos procedimentos manuais para se defenderem de atividades maliciosas que também são automatizadas.

O Ansible é uma ferramenta de provisionamento de software de código aberto, gerenciamento de configurações e implantação de aplicações. Ele é executado em muitos sistemas Unix-like, e pode configurar

tanto sistemas Unix-like como Microsoft Windows. Ele inclui sua própria linguagem declarativa para descrever a configuração do sistema. Ansible foi escrito por Michael DeHaan e adquirido pela Red Hat em 2015. O Ansible está sem agente, conetando-se temporariamente remotamente por meio de SSH ou Gerenciamento remoto do Windows (permitindo a execução remota do PowerShell) para executar tarefas. O NetApp desenvolveu mais do que "150 módulos do Ansible para o software ONTAP"o , possibilitando ainda mais integração com a estrutura de automação do Ansible. Os módulos do Ansible para NetApp fornecem um conjunto de instruções para definir o estado desejado e reencaminhá-lo para o ambiente NetApp de destino. Os módulos são criados para dar suporte a tarefas como configuração de licenciamento, criação de agregados e máquinas virtuais de armazenamento, criação de volumes e restauração de instantâneos para citar alguns. Uma função do Ansible foi "Publicado no GitHub" específica do Guia de implantação de recursos unificados (UC) do NetApp DoD.

Usando a biblioteca de módulos disponíveis, os usuários podem facilmente desenvolver playbooks do Ansible e personalizá-los de acordo com suas próprias aplicações e necessidades empresariais para automatizar tarefas mundanas. Depois que um manual é escrito, você pode executá-lo para executar a tarefa especificada, o que economiza tempo e melhora a produtividade. A NetApp criou e compartilhou exemplos de playbooks que podem ser usados diretamente ou personalizados para suas necessidades.

O Cloud Insights é uma ferramenta de monitoramento de infraestrutura que oferece visibilidade de toda a sua infraestrutura. Com o Cloud Insights, você pode monitorar, solucionar problemas e otimizar todos os recursos, incluindo instâncias de nuvem pública e data centers privados. O Cloud Insights pode reduzir o tempo médio de resolução em 90% e impedir que 80% dos problemas de nuvem afetem os usuários finais. Ele também pode reduzir os custos de infraestrutura de nuvem em uma média de 33% e reduzir a exposição a ameaças internas protegendo seus dados com inteligência acionável. O recurso de segurança de carga de trabalho de armazenamento do Cloud Insights permite que análises comportamentais de usuários com IA e ML alertem quando comportamentos aberrantes de usuários ocorrem devido a uma ameaça interna. Para o ONTAP, a segurança da carga de trabalho de storage faz uso do mecanismo de FPolicy Zero Trust.

Implantações de nuvem híbrida e de confiança zero

A NetApp é a autoridade em dados para a nuvem híbrida. O NetApp oferece várias opções para estender os sistemas de gerenciamento de dados locais para a nuvem híbrida com o Amazon Web Services (AWS), o Microsoft Azure, o Google Cloud Platform (GCP) e outros fornecedores de nuvem líderes do setor. As soluções de nuvem híbrida da NetApp são compatíveis com os mesmos controles de segurança Zero Trust que estão disponíveis nos sistemas ONTAP no local e no storage definido por software da ONTAP Select.

Amplie a capacidade em nuvens públicas com facilidade sem restrições de capex típicas usando o NetApp Cloud Volumes Service, o primeiro serviço de arquivos nativo em nuvem de classe empresarial para AWS e GCP e o Azure NetApp Files para Microsoft Azure. Ideal para workloads com uso intenso de dados, como análises e DevOps, esses serviços de dados em nuvem combinam storage elástico sob demanda como serviço da NetApp com o gerenciamento de dados da ONTAP em uma oferta totalmente gerenciada.

Para aqueles que buscam serviços avançados de dados para serviços de storage de objetos ou bloco na nuvem, como AWS EBS e S3 ou Azure Storage, o Cloud Volumes ONTAP oferece gerenciamento de dados entre seu ambiente local e a nuvem pública com uma única visualização comum. Executado na AWS ou no Azure como uma instância sob demanda, o Cloud Volumes ONTAP fornece a eficiência de storage, a disponibilidade e a escalabilidade do software ONTAP. O ONTAP permite a movimentação de dados entre os sistemas ONTAP no local e o ambiente de storage da AWS ou do Azure com o software de replicação de dados NetApp SnapMirror.

Informações sobre direitos autorais

Informações sobre marcas comerciais