Habilite el modelo de confianza cero

ONTAP 9

NetApp
July 12, 2024

Tabla de contenidos

Habilite el modelo de confianza cero

NetApp y Zero Trust

Zero Trust tradicionalmente ha sido un enfoque centrado en la red del diseño del micronúcleo y el perímetro (MCAP) para proteger los datos, los servicios, las aplicaciones o los activos con controles conocidos como puerta de enlace de segmentación. NetApp ONTAP está adoptando un enfoque centrado en los datos de Zero Trust en el que el sistema de gestión del almacenamiento se convierte en la puerta de enlace de segmentación para proteger y supervisar el acceso a los datos de nuestros clientes. En concreto, el motor de confianza cero de FPolicy y el ecosistema de partners de FPolicy se convierten en un centro de control que permite comprender en detalle los patrones de acceso a los datos normales y aberrantes e identificar las amenazas internas.

A partir de julio de 2024, el contenido del informe técnico *TR-4015: NetApp y Confianza Cero: Habilitar un modelo de Confianza Cero* centrado en los datos, que se publicó anteriormente como PDF, se ha integrado con el resto de la documentación de producto de ONTAP.

Los datos son los activos más importantes con los que cuenta la organización. Las amenazas internas son la causa del 18% de las violaciones de datos, según el 2022 "Informe de investigación de infracciones de datos de Verizon". Las organizaciones pueden aumentar su vigilancia mediante la puesta en marcha de controles de confianza cero (Zero Trust) líderes en el sector en torno a los datos con el software de gestión de datos de NetApp ONTAP.

¿Qué es Zero Trust?

El modelo de confianza cero fue desarrollado "A cargo de John Kindervag" por Forrester Research. Prevé la seguridad de la red desde dentro hacia fuera en lugar de desde fuera hacia dentro. El enfoque de confianza cero de dentro hacia fuera identifica el micronúcleo y el perímetro (MCAP). El MCAP es una definición interior de datos, servicios, aplicaciones y activos que debe protegerse mediante un completo conjunto de controles. El concepto de perímetro exterior seguro es obsoleto. Las entidades de confianza que se pueden autenticar correctamente a través del perímetro pueden hacer que la organización sea vulnerable a los ataques. Por definición, las personas con información privilegiada ya se encuentran dentro del perímetro seguro. Los empleados, contratistas y partners son personas con información privilegiada y deben estar habilitados para operar con los controles adecuados para desempeñar sus funciones dentro de la infraestructura de su organización.

Zero Trust fue mencionado como una tecnología que ofrece promesa al DoD en septiembre de 2019 "FY19-23 DoD Estrategia de Modernización Digital". Define Zero Trust como «Una estrategia de ciberseguridad que incorpora la seguridad en toda la arquitectura con el fin de detener las violaciones de datos. Este modelo de seguridad centrado en datos elimina la idea de redes, dispositivos, personas o procesos de confianza o no confiables y cambia a niveles de confianza basados en múltiples atributos que permiten políticas de autenticación y autorización bajo el concepto de acceso con menos privilegios. Implementar la confianza cero requiere repensar cómo utilizamos la infraestructura existente para implementar la seguridad mediante el diseño de una manera más sencilla y eficiente a la vez que permitimos operaciones sin obstáculos».

En agosto de 2020, el NIST publicó "Special Pub 800-207 Zero Trust Arquitectura" (ZTA). ZTA se centra en proteger los recursos, no los segmentos de la red, porque la ubicación de la red ya no se ve como el componente principal de la postura de seguridad del recurso. Los recursos son datos e informática. Las

estrategias ZTA son para arquitectos de redes empresariales. ZTA introduce una nueva terminología de los conceptos originales de Forrester. Los mecanismos de protección denominados punto de decisión de política (PDP) y punto de aplicación de políticas (PEP) son análogos a una puerta de enlace de segmentación de Forrester. ZTA presenta cuatro modelos de implementación:

- Implementación basada en gateway o agente de dispositivo
- Instalación basada en enclave (algo similar al Forrester MCAP)
- Despliegue basado en portal de recursos
- Sandboxing de aplicaciones de dispositivos

Para los fines de esta documentación, utilizamos los conceptos y la terminología de Forrester Research en lugar de la ZTA de NIST.

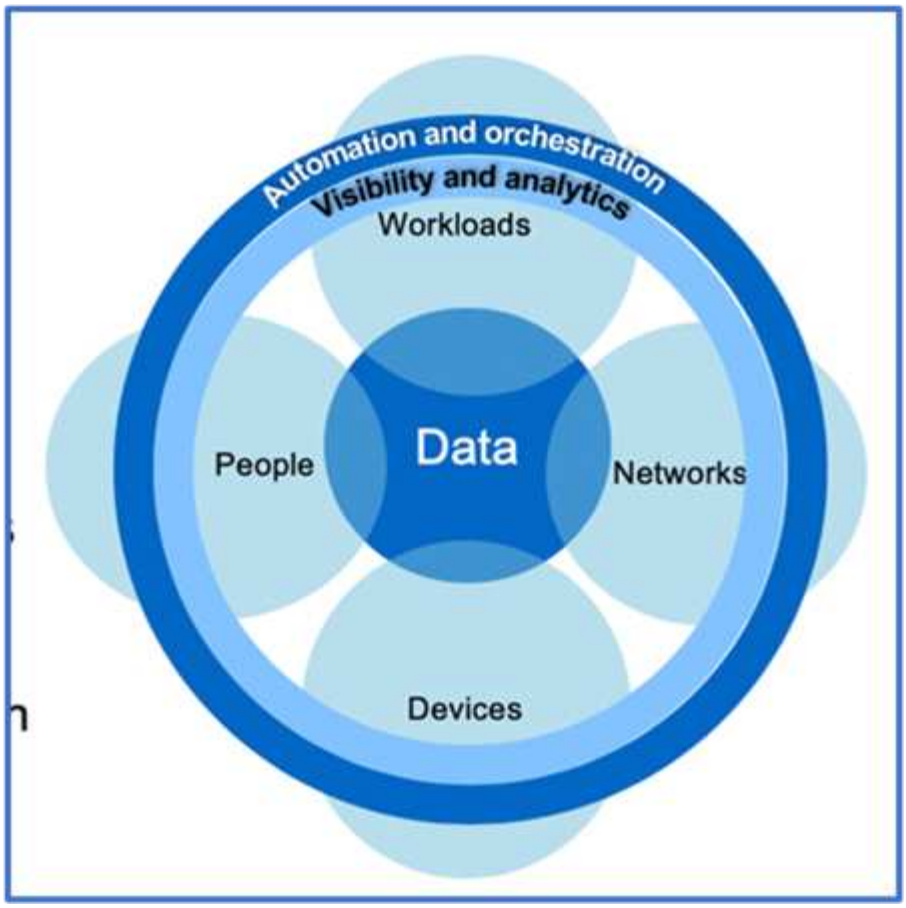
Recursos de seguridad

Para obtener información sobre la creación de informes sobre vulnerabilidades e incidentes, las respuestas de seguridad de NetApp y la confidencialidad del cliente, consulte la "Portal de seguridad de NetApp".

Diseñe un enfoque de Zero Trust centrado en los datos con ONTAP

Una red de confianza cero se define por un enfoque centrado en los datos en el que los controles de seguridad deben estar lo más cerca posible de los datos. Las funcionalidades de ONTAP y el ecosistema de partners de FPolicy de NetApp pueden ofrecer los controles necesarios para el modelo de confianza cero centrado en datos.

ONTAP es un software de gestión de datos de alta seguridad de NetApp, y el motor de confianza cero de FPolicy es una funcionalidad de ONTAP líder del sector que proporciona una interfaz de notificaciones de eventos granular basada en archivos. Los partners de FPolicy de NetApp pueden usar esta interfaz para facilitar el acceso a los datos en ONTAP.



Cree un MCAP centrado en los datos de confianza cero

Para diseñar un MCAP de confianza cero centrado en los datos, siga estos pasos:

1. Identifique la ubicación de todos los datos de la organización.
2. Clasifique los datos.
3. Elimine de forma segura los datos que ya no necesite.
4. Comprender qué roles deben tener acceso a las clasificaciones de datos.
5. Aplique el principio de privilegio mínimo para aplicar los controles de acceso.
6. Use la autenticación multifactor para el acceso administrativo y el acceso a los datos.
7. Utilice el cifrado para los datos en reposo y los datos en tránsito.
8. Supervisar y registrar todo el acceso.
9. Alerte de accesos o comportamientos sospechosos.

Identifique la ubicación de todos los datos de la organización

La funcionalidad FPolicy de ONTAP junto con el ecosistema de partners de alianza de NetApp formado por partners de FPolicy le permite identificar dónde existen los datos de su organización y quién tiene acceso a ellos. Esto se hace con el análisis del comportamiento del usuario, que identifica si los patrones de acceso a los datos son válidos. Más detalles sobre el análisis del comportamiento del usuario se discuten en Supervisar y registrar todo el acceso. Si no entiende dónde están sus datos y quién tiene acceso a ellos, el análisis de comportamiento del usuario puede proporcionar una línea base para construir la clasificación y la política a partir de observaciones empíricas.

Clasifique los datos

En la terminología del modelo de confianza cero (Zero Trust), la clasificación de los datos implica la identificación de datos tóxicos. Los datos tóxicos son datos confidenciales que no están destinados a ser expuestos fuera de una organización. La revelación de datos tóxicos puede infringir el cumplimiento de normativas y dañar la reputación de una organización. En términos de cumplimiento normativo, los datos tóxicos incluyen los datos del titular de la tarjeta para los "Estándar de seguridad de datos del sector de tarjetas de pago (PCI-DSS)"datos personales de la UE "Reglamento general sobre la protección de datos (GDPR)"o los datos sanitarios de la "Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)". Puedes utilizar NetApp "Clasificación de BlueXP" (antes conocido como Cloud Data Sense), un kit de herramientas impulsado por IA, para analizar, categorizar y analizar automáticamente los datos.

Deseche de forma segura los datos que ya no necesite

Después de clasificar los datos de su organización, puede descubrir que algunos de sus datos ya no son necesarios o relevantes para la función de su organización. La retención de datos innecesarios es una responsabilidad, y dichos datos deben ser eliminados. Para ver un mecanismo avanzado para borrar datos de forma criptográfica, consulte la descripción de la purga segura en el cifrado de datos en reposo.

Comprender qué roles deben tener acceso a las clasificaciones de datos y aplicar el principio de privilegio mínimo para aplicar los controles de acceso

La asignación de acceso a datos confidenciales y la aplicación del principio de privilegio mínimo significa dar a las personas de su organización acceso a solo los datos necesarios para realizar sus trabajos. Este proceso implica el control de acceso basado en roles ("RBAC"), que se aplica al acceso a los datos y al acceso administrativo.

Con ONTAP, puede utilizarse una máquina virtual de almacenamiento (SVM) para segmentar el acceso a los datos de la organización por parte de los inquilinos dentro de un clúster de ONTAP. Es posible aplicar el control de acceso basado en roles al acceso a los datos, así como al acceso administrativo a la SVM. RBAC también se puede aplicar en el nivel administrativo del clúster.

Además de RBAC, puede utilizar ONTAP "verificación multiadministrativa" (MAV) para requerir que uno o más administradores aprueben comandos `volume delete` como o `volume snapshot delete`. Una vez que MAV está activado, la modificación o desactivación de MAV requiere la aprobación del administrador de MAV.

Otra forma de proteger las copias snapshot es con ONTAP "Bloqueo de copia de snapshot". El bloqueo de copia de Snapshot es una función de SnapLock en la que las copias de Snapshot se vuelven indelebles manual o automáticamente con un período de retención en la política de copias de Snapshot para volúmenes. El bloqueo de copia de SnapVault también se conoce como bloqueo de copias de Snapshot a prueba de manipulaciones. El propósito del bloqueo de copias de Snapshot es evitar que los administradores malintencionados o que no sean de confianza eliminen copias de Snapshot en los sistemas ONTAP principales y secundarios. Es posible llevar a cabo una rápida recuperación de copias Snapshot bloqueadas en sistemas principales para restaurar volúmenes dañados por el ransomware.

Use la autenticación multifactor para el acceso administrativo y el acceso a los datos

Además del control de acceso basado en roles administrativo del clúster, "Autenticación multifactor (MFA)" es posible poner en funcionamiento para el acceso administrativo web de ONTAP y para el acceso por línea de comandos de Secure Shell (SSH). La MFA para el acceso administrativo es un requisito para las organizaciones del sector público de EE. UU. O las que deben seguir la PCI-DSS. MFA hace que sea imposible para un atacante comprometer una cuenta usando solo un nombre de usuario y contraseña. La MFA requiere dos o más factores independientes para autenticarse. Un ejemplo de autenticación de dos factores es algo que posee un usuario, como una clave privada, y algo que un usuario conoce, como una contraseña. El acceso web administrativo a ONTAP System Manager o ActiveIQ Unified Manager está habilitado con Security

Assertion Markup Language (SAML) 2,0. El acceso a la línea de comandos SSH utiliza autenticación encadenada de dos factores con una clave pública y una contraseña.

Puede controlar el acceso de usuarios y máquinas a través de API con las capacidades de gestión de acceso e identidad en ONTAP:

- Usuario:
  - **Autenticación y autorización.** Mediante las funcionalidades del protocolo NAS para SMB y NFS.
  - **Auditoría.** Syslog de acceso y eventos. Registro de auditorías detallado del protocolo CIFS para probar las políticas de autenticación y autorización. Auditoría granular de FPolicy precisa de acceso NAS detallado a nivel de archivo.
- Dispositivo:
  - **Autenticación.** Autenticación basada en certificados para el acceso a API.
  - **Autorización.** Control de acceso basado en roles (RBAC) predeterminado o personalizado.
  - **Auditoría.** Syslog de todas las acciones realizadas.

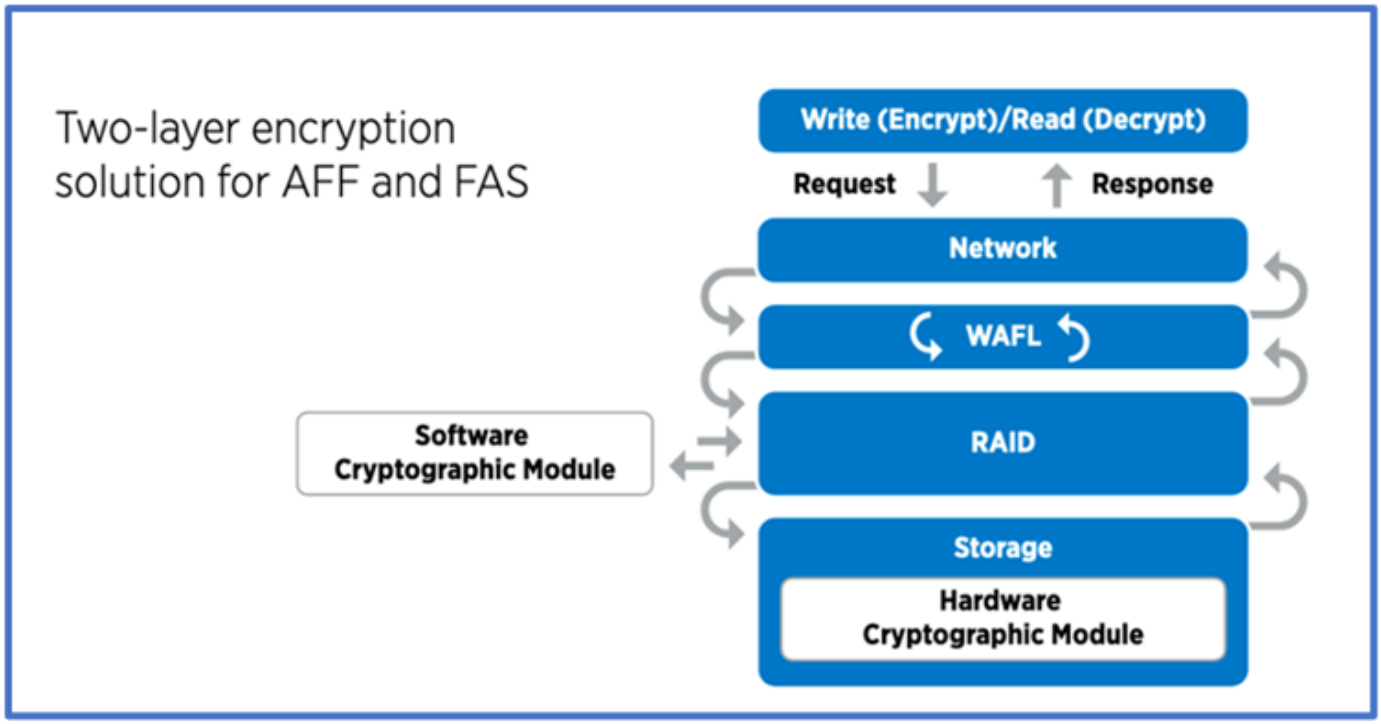
Utilice el cifrado para los datos en reposo y los datos en tránsito

Cifrado de los datos en reposo

Cada día se cumplen nuevos requisitos para mitigar los riesgos del sistema de almacenamiento y las deficiencias en la infraestructura cuando una organización reasigna unidades, devuelve unidades defectuosas o actualiza unidades de mayor tamaño vendiéndolas o canjeándolas. Los ingenieros de almacenamiento, como administradores y operadores de datos, deben gestionar y mantener los datos de forma segura a lo largo de su ciclo de vida. "NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), y NetApp Aggregate Encryption" le ayudamos a cifrar todos sus datos en reposo todo el tiempo, sean tóxicos o no, y sin afectar a las operaciones diarias. "NSE" Es una solución de datos en reposo de hardware de ONTAP que utiliza unidades de autocifrado validadas FIPS 140-2 de nivel 2. "NVE y NAE" Son una solución de datos en reposo del software ONTAP que utiliza el "Módulo criptográfico NetApp validado FIPS 140-2 nivel 1". Con NVE y NAE, pueden utilizarse unidades de disco duro o unidades de estado sólido para el cifrado de datos en reposo. Además, pueden utilizarse unidades NSE para proporcionar una solución de cifrado nativa por capas que ofrezca redundancia de cifrado y seguridad adicional. Si se rompe una capa, la segunda capa aún protege los datos. Estas funcionalidades hacen que ONTAP esté bien posicionado para "cifrado preparado para quantum".

NVE también proporciona una funcionalidad denominada "limpieza segura" que elimina criptográficamente los datos tóxicos de las fugas de datos cuando los archivos confidenciales se escriben en un volumen no clasificado.

```
https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-nve/GUID-
466E3BFC-F7FA-4B79-A8C9-2540C3BF1408.html["Gestión de claves incorporada
(OKM)"^]El , que es el gestor de claves integrado en ONTAP, o bien
https://mysupport.netapp.com/matrix/imt.jsp?components=69551;&solution=115
6&isHWU&src=IMT["aprobada"^] https://docs.netapp.com/ontap-
9/topic/com.netapp.doc.pow-nve/GUID-DD718B42-038D-4009-84FF-
20BBD6530BC2.html["gestores de claves externos"^] se puede usar con NSE y
NVE para almacenar material de claves de forma segura.
```



Como se ve en la figura anterior, se puede combinar el cifrado basado en hardware y software. Esta función permitió "Validación de ONTAP en las soluciones comerciales para el programa clasificado de la NSA" el almacenamiento de datos confidenciales.

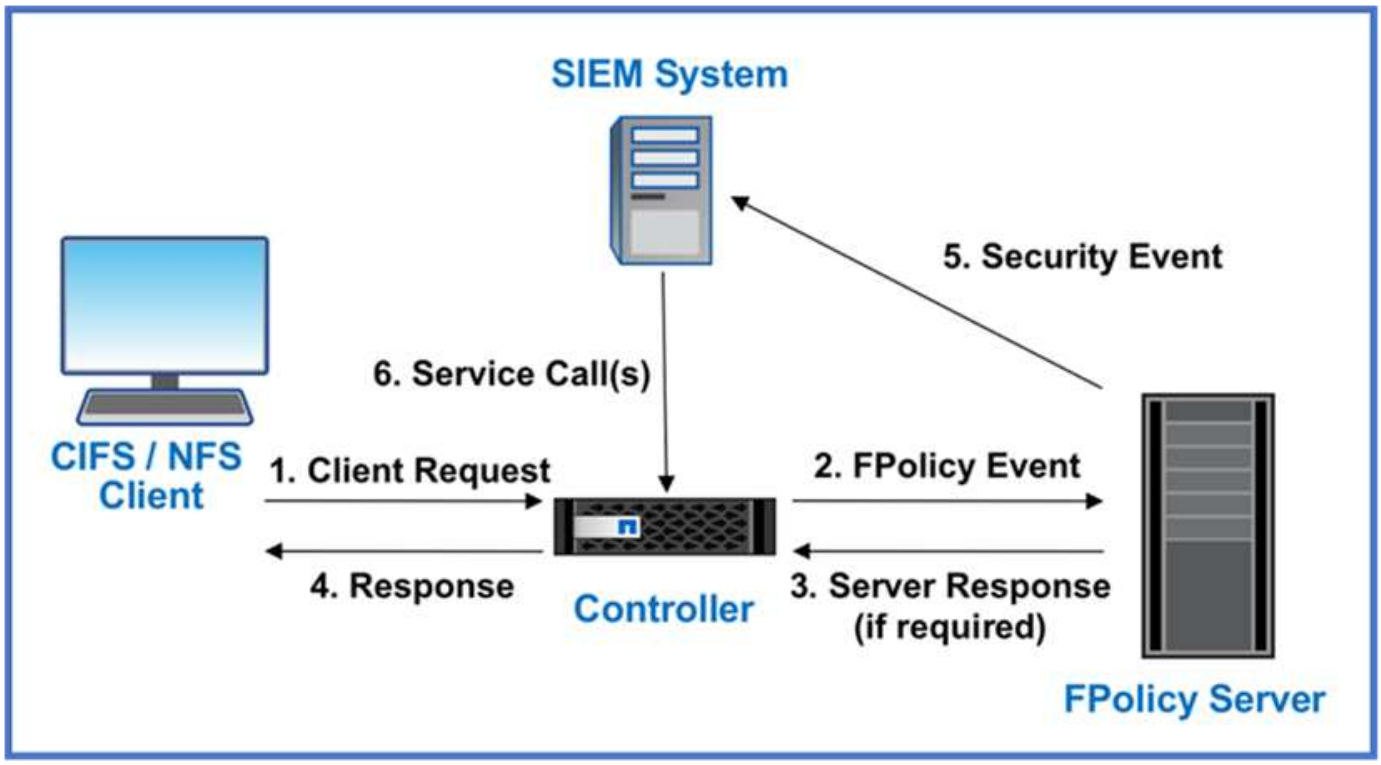
Cifrado de datos en tránsito

El cifrado de datos en tiempo real de ONTAP protege el acceso a los datos de usuario y el acceso al plano de control. El acceso a los datos del usuario puede cifrarse mediante el cifrado SMB 3,0 para el acceso a recursos compartidos de Microsoft CIFS o por krb5P para Kerberos 5 NFS. El acceso a los datos del usuario también puede cifrarse con "IPSec" para CIFS, NFS e iSCSI. El acceso al plano de control está cifrado con Transport Layer Security (TLS). ONTAP proporciona "FIPS" el modo de cumplimiento para el acceso al plano de control, que habilita algoritmos aprobados por FIPS y deshabilita los algoritmos que no están aprobados por FIPS. La replicación de datos está cifrada con "cifrado de pares de clústeres". Esto proporciona cifrado para las tecnologías ONTAP SnapVault y SnapMirror.

Supervisar y registrar todo el acceso

Una vez implementadas las políticas de RBAC, debe implementar supervisión activa, auditoría y alertas. El motor de confianza cero FPolicy de NetApp ONTAP junto con "Ecosistema de partners FPolicy de NetApp", proporciona los controles necesarios para el modelo de confianza cero centrado en datos. NetApp ONTAP es un software de gestión de datos de alta seguridad y "FPolicy" una funcionalidad ONTAP líder del sector que proporciona una interfaz granular de notificaciones de eventos basada en archivos. Los partners de FPolicy de NetApp pueden usar esta interfaz para facilitar el acceso a los datos en ONTAP. La funcionalidad FPolicy de ONTAP, junto con el ecosistema de partners de alianza de NetApp formado por partners de FPolicy, le permite identificar dónde existen los datos de su organización y quién tiene acceso a ellos. Esto se hace con el análisis del comportamiento del usuario, que identifica si los patrones de acceso a los datos son válidos. El análisis de comportamiento del usuario se puede utilizar para alertar de acceso a datos sospechosos o aberrantes que estén fuera del patrón normal y, si es necesario, tomar medidas para denegar el acceso.

Los partners de FPolicy van más allá del análisis de comportamiento del usuario hacia el aprendizaje automático (ML) y la inteligencia artificial (IA) para ofrecer una mayor fidelidad a los eventos y menos falsos positivos, si los hay. Todos los eventos deben registrarse en un servidor de syslog o en un sistema de gestión de información y eventos de seguridad (SIEM) que también pueda emplear ML e AI.



La seguridad de cargas de trabajo de almacenamiento de NetApp (antes conocida "Cloud Secure"como) utiliza la interfaz de FPolicy y los análisis de comportamiento del usuario en los sistemas de almacenamiento de ONTAP tanto en el cloud como en las instalaciones para brindarle alertas en tiempo real de comportamiento de usuarios maliciosos. Seguridad de las cargas de trabajo de almacenamiento protege los datos de la organización para que los usuarios malintencionados o en riesgo usen incorrectamente mediante el aprendizaje automático avanzado y la detección de anomalías. Almacenamiento Workload Security puede identificar ataques de ransomware u otros comportamientos malvados, invocar copias snapshot y poner en cuarentena a los usuarios maliciosos. Storage Workload Security también tiene una funcionalidad forense para ver con mayor detalle las actividades de usuarios y entidades. La seguridad de la carga de trabajo de almacenamiento forma parte de NetApp Cloud Insights.

Además de la seguridad de las cargas de trabajo de almacenamiento, ONTAP cuenta con una funcionalidad de detección de ransomware incorporada conocida como "Protección autónoma de ransomware" ARP. ARP utiliza el aprendizaje automático para determinar si una actividad anormal de archivos indica que un ataque de ransomware está en curso y invoca una copia Snapshot y una alerta a los administradores. Seguridad de carga de trabajo de almacenamiento se integra con ONTAP para recibir eventos ARP y ofrece una capa de análisis adicional y respuestas automáticas.

Controles de orquestación y automatización de la seguridad de NetApp externos a ONTAP

La automatización le permite realizar un proceso o procedimiento con una asistencia humana mínima. Gracias a la automatización, las organizaciones pueden escalar sus puestas en marcha de confianza cero más allá de los procedimientos manuales para defenderse frente a actividades engañosas que también están automatizadas.

Ansible es una herramienta de aprovisionamiento de software de código abierto, gestión de configuración y puesta en marcha de aplicaciones. Se ejecuta en muchos sistemas similares a Unix, y puede configurar tanto sistemas similares a Unix como Microsoft Windows. Incluye su propio lenguaje declarativo para describir la

configuración del sistema. Ansible fue escrito por Michael DeHaan y adquirido por Red Hat en 2015. Ansible no tiene agentes, se conecta temporalmente de forma remota a través de SSH o Administración remota de Windows (lo que permite la ejecución remota de PowerShell) para realizar tareas. NetApp ha desarrollado más que "150 Módulos Ansible para software ONTAP", lo que permite una mayor integración con el marco de automatización de Ansible. Los módulos de Ansible para NetApp proporcionan un conjunto de instrucciones para definir el estado deseado y transmitirlo al entorno NetApp de destino. Los módulos se incorporarán para dar soporte a tareas como configurar licencias, crear agregados y máquinas virtuales de almacenamiento, crear volúmenes y restaurar instantáneas, entre otras. Una función de Ansible ha sido "Publicado en GitHub" específica de la guía de implementación de funcionalidades unificadas para departamentos de NetApp (UC).

Al utilizar los módulos disponibles en la biblioteca, los usuarios pueden desarrollar fácilmente playbooks de Ansible y personalizarlos para sus propias aplicaciones y necesidades comerciales para automatizar tareas mundanas. Después de escribir un playbook, puede ejecutarlo para ejecutar la tarea especificada, lo que ahorra tiempo y mejora la productividad. NetApp ha creado y compartido playbooks de muestra que puede utilizar directamente o personalizar según sus necesidades.

Cloud Insights es una herramienta de supervisión de infraestructuras que le ofrece visibilidad sobre su infraestructura completa. Con Cloud Insights, podrá supervisar, solucionar problemas y optimizar todos sus recursos, incluidas sus instancias de cloud público y los centros de datos privados. Cloud Insights puede reducir el tiempo medio de resolución en un 90 % y evitar que el 80 % de los problemas de cloud afecten a los usuarios finales. También puede reducir los costes de la infraestructura de cloud en un 33 % de media y reducir su exposición a amenazas internas al proteger los datos con inteligencia práctica. La funcionalidad de seguridad de cargas de trabajo de almacenamiento de Cloud Insights permite que los análisis de comportamiento del usuario con inteligencia artificial y APRENDIZAJE AUTOMÁTICO alerten cuando se producen comportamientos aberrantes de los usuarios debido a una amenaza interna. Para ONTAP, la seguridad de cargas de trabajo de almacenamiento utiliza el motor FPolicy de confianza cero.

Puesta en marcha de cloud híbrido y confianza cero

NetApp es un referente en materia de datos para el cloud híbrido. NetApp ofrece varias opciones para ampliar los sistemas de gestión de datos en las instalaciones al cloud híbrido con Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP) y otros proveedores líderes de cloud. Las soluciones de cloud híbrido de NetApp admiten los mismos controles de seguridad de confianza cero que están disponibles con los sistemas ONTAP en las instalaciones y el almacenamiento definido por software de ONTAP Select.

Puede ampliar fácilmente la capacidad en clouds públicos sin tener que limitarse a gastos de capital típicas gracias a NetApp Cloud Volumes Service, el primer servicio de archivos nativo en cloud para la gran empresa para AWS y GCP, y Azure NetApp Files para Microsoft Azure. Estos servicios de datos en el cloud son ideales para cargas de trabajo con un gran volumen de datos como las de análisis y DevOps, y combinan el almacenamiento elástico bajo demanda como servicio de NetApp con la gestión de datos de ONTAP en una oferta totalmente gestionada.

Para aquellos que busquen servicios de datos avanzados para servicios de almacenamiento de objetos o basado en bloques de cloud como AWS EBS y S3 o el almacenamiento de Azure, Cloud Volumes ONTAP proporciona la gestión de datos entre su entorno local y el cloud público con una única vista común. Al ejecutarse en AWS o Azure como instancia bajo demanda, Cloud Volumes ONTAP proporciona la eficiencia del almacenamiento, la disponibilidad y la escalabilidad del software ONTAP. ONTAP permite el traslado de datos entre sus sistemas ONTAP locales y los entornos de almacenamiento AWS o Azure con el software de replicación de datos SnapMirror de NetApp.

Más información sobre el contenido de Confianza cero de ONTAP

Si quiere más información sobre la información descrita en el contenido de Confianza cero de ONTAP, consulte los siguientes documentos o sitios web:

- "Informe de investigación de infracciones de datos de Verizon"
- "DoD Estrategia de Modernización Digital"
- "Arquitectura de confianza cero de NIST SP 800-207"
- "Partner Connect de NetApp: Partners de la alianza de seguridad"
- "Mediante FPolicy para la supervisión y la gestión de archivos en las SVM"
- "PCI-DSS 3,2 ONTAP 9"
- "Reglamento general sobre la protección de datos (GDPR)"
- "Resumen de la regla de privacidad de HIPPA"
- "Clasificación de NetApp BlueXP"
- "Verificación de varios administradores"
- "Bloqueo de copias snapshot a prueba de manipulaciones"
- "Autenticación multifactor en ONTAP 9"
- "Cifrado del almacenamiento de NetApp, unidades de autocifrado NVMe, cifrado de volúmenes de NetApp y cifrado agregado de NetApp"
- "Cifrado del almacenamiento de NetApp"
- "Cifrado de volúmenes de NetApp y cifrado de agregados de NetApp"
- "Módulo criptográfico NetApp, certificado FIPS-140-2"
- "Cifrado de datos en reposo preparado para Quantum por NetApp"
- "Innovar con seguridad: NetApp y Ontrack ganan el premio Flash Memory Summit"
- "Habilitación de la gestión de claves incorporada"
- "Herramienta de matriz de interoperabilidad de NetApp"
- "Configuración de la gestión de claves externas"
- "Soluciones comerciales para clasificados"
- "IPsec de ONTAP"
- "Modificación de configuración de seguridad para activar el modo FIPS"
- "Habilitar el cifrado de interconexión de clústeres en una relación de paridad existente"
- "Seguridad de carga de trabajo de almacenamiento (Cloud Secure)"
- "Comienza a trabajar con la automatización de los flujos de trabajo de desarrollo con NetApp y Ansible"
- "Módulo de Ansible específico de la guía de implementación de las capacidades unificadas (UC) de NetApp DoD"
- "Autenticación de administrador y RBAC"
- "Cifrado de datos en reposo de ONTAP"
- "TR-4569 Guía sobre fortalecimiento de la seguridad para NetApp ONTAP 9"

Información de copyright

Información de la marca comercial