ESPECIFICACIONES TÉCNICAS

Funciones de seguridad de ONTAP

Aseguramos el recurso más importante del mundo: los datos

El software para la gestión de datos ONTAP® de NetApp® continúa evolucionando, con la seguridad como parte integral de la solución. Los últimos lanzamientos de ONTAP incluyen numerosas funciones de seguridad que son de gran valor para que tu organización proteja sus datos en el cloud híbrido, evite ataques de ransomware y cumpla las prácticas recomendadas del sector. Estas nuevas funciones también favorecen el avance de tu organización hacia un modelo de Confianza Cero.

Para obtener más información sobre cómo reforzar la solución ONTAP, consulta TR-4569: Guía de seguridad reforzada de ONTAP de NetApp.

El reto

Las empresas de hoy en día sufren la presión de la transformación digital. Tienen que gestionar datos de manera eficiente en su cloud híbrido, que está cada vez más distribuido y es más dinámico y diverso. Las amenazas son cada vez más sofisticadas y peligrosas para los entornos tecnológicos. Los equipos tecnológicos, como administradores y operadores de datos e información, deben gestionar y mantener la seguridad de los datos a lo largo de su ciclo de vida.

La solución

El software ONTAP de NetApp es fundamental para proteger los datos y cumplir con los requisitos de cumplimiento de normativas. Estas especificaciones técnicas y el documento «TR-4569: Guía de seguridad reforzada de ONTAP de NetApp» son esenciales para crear un sistema de seguridad demostrado en el sector para tu recurso más importante: los datos.

Ventajas clave

Mejorar la confidencialidad, la integridad y la disponibilidad de los datos
Protege los datos, el recurso más importante de tu organización, gracias a las tecnologías de seguridad del cloud híbrido de ONTAP.

Reforzar la política de seguridad de tu organización
Aprovecha las funciones de visibilidad y seguridad que permiten crear una infraestructura protegida para establecer una base segura en el cloud híbrido de tu organización.

Aplicar las prácticas recomendadas de NetApp y del sector para conseguir seguridad y protección contra el ransomware
Establece una huella de seguridad probada con el respaldo de la experiencia y el conocimiento del sector de NetApp.

Satisfacer los requisitos de gobernanza y cumplimiento de normativas
Sigue las prácticas recomendadas de seguridad para cumplir la legislación del sector y las normativas pertinentes.

Funciones de seguridad de ONTAP

Software o funciones	Función	Impacto
Protección autónoma contra ransomware	La protección autónoma contra ransomware es una funcionalidad integrada que cuenta con una detección preventiva de machine learning frente a ataques.	Si se detecta una anomalía, ONTAP crea una copia de SnapVault automáticamente y avisa al administrador.
Copias Snapshot™ de NetApp	Una copia de Snapshot de ONTAP es una copia de un momento específico y de solo lectura de tus datos. Una copia de Snapshot muestra cómo estaban exactamente los datos en el momento de realizarla, independientemente de si han pasado horas, días, semanas, meses o incluso años.	Debido a que las copias de Snapshot son de solo lectura, no se pueden infectar mediante ransomware. Para recuperarte de un ataque de ransomware, solo tienes que restaurar los datos de una copia de Snapshot que se haya hecho antes de sufrir el ataque.
Tecnología SnapLock® de NetApp	SnapLock de NetApp protege las copias de Snapshot mediante NetApp SnapVault® permitiendo crear un backup lógico, con air gap y totalmente imborrable.	SnapLock elimina el riesgo de que se supriman las copias de Snapshot por parte de un administrador que comete un error, un empleado disgustado o un malhechor que dispone de credenciales robadas.
Bloqueo de copia de SnapVault	El bloqueo de copia de SnapVault usa la tecnología SnapLock para hacer, de forma manual o automática, que las copias de SnapVault sean indelebles durante un período de tiempo determinado.	Las copias de SnapVault pueden ser eliminadas por un administrador debido a un error humano, por un empleado descontento o por un agente malintencionado que aproveche credenciales robadas.
Tecnología FPolicy de NetApp	FPolicy es un componente de infraestructura de ONTAP que permite a las aplicaciones de partners supervisar y establecer permisos de acceso a archivos. Las políticas de archivo pueden basarse en el tipo de archivo. FPolicy determina la forma en que el sistema de almacenamiento maneja las solicitudes de sistemas cliente individuales en operaciones como crear, abrir, cambiar nombre y eliminar. Nota: En ONTAP, el marco de notificaciones de acceso a archivos de FPolicy se ha mejorado con controles de filtrado y resiliencia ante breves interrupciones de red.	El control de acceso es un elemento clave de la seguridad. Por lo tanto, la visibilidad y la capacidad de responder al acceso a archivos y a las operaciones con archivos son cruciales para mantener tu política de seguridad. Para proporcionar visibilidad y control de acceso a los archivos, la solución ONTAP usa la función FPolicy. Los servidores externos de FPolicy, como NetApp Cloud Insights y Cloud Secure, emplean análisis conductuales de usuarios para identificar malware y ransomware a fin de mitigar los efectos de una mayor exposición de los datos al peligro.
Cifrado de volúmenes de NetApp (NVE)	NVE es un mecanismo de cifrado basado en software que te permite cifrar datos en cualquier tipo de disco con una clave única por volumen.	El cifrado de los datos en reposo es un objetivo prioritario del sector. NVE responde a este objetivo a la vez que mantiene un fuerte compromiso con la seguridad en todo el cloud híbrido.
Limpieza segura del NVE	Esta función permite que un comando destruya de forma criptográfica los archivos eliminados de volúmenes NVE al mover los archivos válidos y eliminar la clave que se utilizó para cifrar los archivos infectados.	Puedes subsanar las fugas de datos en línea sin dejar de usar el sistema. Esta función también proporciona la moderna función «derecho a borrar» conforme al Reglamento general de protección de datos (RGPD).
Cifrado de agregados de NetApp (NAE)	NAE es un mecanismo de cifrado basado en software que te permite cifrar datos en cualquier tipo de disco con claves únicas por cada agregado compartido a través de volúmenes cifrados.	Al igual que NVE, NAE permite el cifrado de datos en reposo. Con NAE se habilita la deduplicación de agregados porque los volúmenes comparten claves entre los agregados, lo que proporciona una mayor eficiencia del almacenamiento.

Funciones de seguridad de ONTAP

Software o funciones	Función	Impacto
Cifrado de datos en reposo (DAR) predeterminado	El cifrado de DAR predeterminado se habilita si se define un gestor de claves externo o incorporado. Se utilizará el cifrado basado en software de NVE o de NAE. Si las unidades de cifrado de almacenamiento de NetApp (NSE) forman parte de la configuración del clúster, el cifrado de DAR ya está habilitado y no se utilizará el cifrado basado en software de forma predeterminada.	El cifrado de DAR predeterminado simplifica el mantenimiento de un sistema de seguridad sólido en todo el cloud híbrido.
Cifrado en almacenamiento de NetApp (NSE)	NSE es la implementación de NetApp del cifrado completo de disco (FDE) mediante el uso de unidades de autocifrado FIPS-140-2 de nivel 2. Además, NSE ofrece una implementación de cifrado no disruptivo que respalda toda la gama de tecnologías de eficiencia del almacenamiento de NetApp.	El cifrado de los datos en reposo es un objetivo prioritario del sector. NSE proporciona FDE, que cumple con este objetivo. Data Fabric de NetApp mantiene un sistema de seguridad sólido de forma integral.
Cifrado SMB que utiliza la aceleración de las Nuevas instrucciones de Intel AES (AES-NI)	AES-NI mejora el algoritmo de AES y acelera el cifrado de datos en los productos de procesadores compatibles.	La aceleración de las funciones de seguridad aumenta la eficiencia. El uso eficiente de recursos es fundamental para ofrecer soluciones de seguridad fiables.
Módulo de seguridad criptográfica de NetApp (NCSM)	Este módulo ofrece operaciones criptográficas validadas por FIPS 140-2 para determinados servicios de gestión basados en Secure Sockets Layer (SSL). Empezando con el soporte de ONTAP 9.11.1 y TLS 1.3, se puede validar FIPS 140-2.	La eficiencia de los recursos se mejora con módulos de seguridad dedicados. Además, FIPS 140 es el estándar reconocido del sector para productos y soluciones criptográficas.
CryptoMod de NetApp	Este módulo proporciona operaciones criptográficas validadas por FIPS 140-2 para NVE, NAE y el gestor de claves incorporado (OKM).	FIPS 140-2 es el estándar reconocido del sector para productos y soluciones criptográficas.
Soporte para SHA-2 (SHA-512)	Para mejorar la seguridad de las contraseñas, ONTAP ofrece soporte para la función hash de contraseña SHA-2 y usa de forma predeterminada SHA-512 para los hash de contraseñas nuevas o modificadas.	Gracias a las grandes mejoras en la política de seguridad con respecto al debilitado estándar SHA-1, SHA-2 se ha convertido en el estándar del sector para las funciones hash.
Reenvío de registros seguro (syslog mediante seguridad de la capa de transporte [TLS])	La función de reenvío de registros permite a los administradores aprovisionar objetivos o destinos que puedan recibir información de syslog y auditoría. Dado el carácter seguro de la información de syslog y auditoría, ONTAP puede usar el parámetro de cifrado TCP para enviar esta información con seguridad mediante TLS.	La información de registro y auditoría es muy valiosa para tu organización desde el punto de vista del soporte y la disponibilidad. Además, la información que contienen los registros (syslog) y los informes y resultados de auditoría suele ser confidencial. Para mantener los controles y el sistema de seguridad, debes gestionar los datos de los registros y las auditorías de forma segura.
TLS 1.1 y TLS 1.2	ONTAP utiliza TLS 1.1 y TLS 1.2 para garantizar la seguridad de las funciones de comunicación y administración.	NetApp no recomienda usar TLS 1.0, ya que presenta importantes vulnerabilidades que lo hacen incompatible con estándares de cumplimiento de normativas como PCI-DSS. NetApp recomienda el uso de TLS 1.1 y TLS 1.2 debido a su solidez e integridad.
Protocolo de estado de certificados en línea (OCSP)	Cuando OCSP está habilitado, las aplicaciones de ONTAP que utilizan comunicaciones TLS, como LDAP o TLS, pueden obtener el estado de certificado digital. La aplicación recibe una respuesta firmada que indica si el certificado solicitado es válido, revocado o desconocido.	OCSP ayuda a determinar el estado actual de un certificado digital sin que sea necesario disponer de listas de revocación de certificados (CRL).
Gestión de claves incorporada (OKM)	En ONTAP, OKM proporciona una solución de cifrado independiente para datos en reposo. OKM funciona con NVE, que ofrece un mecanismo de cifrado basado en software con el que puede cifrar datos en cualquier tipo de disco. OKM también funciona con NSE, que ejecuta FDE mediante unidades de autocifrado.	OKM proporciona gestión de claves a NSE y NVE. Además, el uso de esta tecnología de cifrado en ONTAP te permite proteger los datos en reposo, lo que proporciona una solución de seguridad de datos fundamental.
Arranque seguro de OKM	Esta opción puede requerir una frase secreta de acceso para desbloquear unidades y descifrar volúmenes después de reiniciar un nodo.	Cuando NSE y NVE utilizan OKM, el reinicio seguro proporciona protección contra el robo de toda la cabina de almacenamiento, no solo de las unidades. También permite el traslado físico seguro de clústeres enteros y el retorno seguro del equipo.

Funciones de seguridad de ONTAP

Software o funciones	Función	Impacto
Gestión de claves externa	La gestión de claves externa se lleva a cabo a través de un sistema de terceros en el entorno de almacenamiento. Este sistema de terceros gestiona de forma segura las claves de autenticación y las claves de cifrado que las funciones de cifrado utilizan en el sistema de almacenamiento, como NSE, NVE o NAE. El sistema de almacenamiento utiliza una conexión SSL para contactar con el servidor externo de gestión de claves a fin de almacenar y recuperar claves de autenticación o claves de cifrado de datos de volúmenes a través del protocolo de interoperabilidad de gestión de claves (KMIP).	Con la gestión de claves externa, puedes centralizar las funciones de la gestión de claves de la organización al tiempo que confirmas de forma inherente que las claves no están almacenadas cerca de los activos. Este enfoque reduce la posibilidad de que la seguridad se vulnere.
Multi-tenancy seguro	El multi-tenancy seguro es el uso de particiones virtuales seguras con un entorno de almacenamiento físico compartido con la finalidad de compartir el entorno físico con varios inquilinos. En ONTAP, estas particiones se denominan máquinas virtuales de almacenamiento (SVM).	El multi-tenancy seguro habilita ONTAP como una plataforma compartida que tiene SVM que aíslan de forma segura todos los inquilinos de la plataforma.
Gestión de claves externa multitenant	La gestión de claves externa multitenant ofrece la posibilidad de que los inquilinos particulares o las máquinas virtuales de almacenamiento (SVM) mantengan sus propias claves a través de KMIP para NVE.	Con la gestión de claves externa multitenant, puedes centralizar las funciones de la gestión de claves de la organización por departamento o inquilino, al tiempo que confirmas de forma inherente que las claves no están almacenadas cerca de los activos. Este enfoque reduce la posibilidad de que la seguridad se vulnere.
Gestor de claves externo en clúster	La redundancia del servidor externo KMIP es compatible con las funcionalidades de clustering que ofrecen los partners de servidores de claves KMIP de NetApp. Antes de ONTAP 9.11.1, se podían definir hasta cuatro servidores externos KMIP, en los que ONTAP escribía claves para cada servidor con el finde de ofrecer redundancia.	Los clientes de ONTAP están adoptando de forma amplia los gestores de claves externo en clúster. El soporte de ONTAP permite que estos clientes puedan usar esta funcionalidad de forma ágil.
Auditoría del sistema de archivos mejorada	ONTAP aumenta el número de eventos y detalles de auditoría de los que informa la solución. A continuación se especifican los detalles clave que se registran al crear un evento: Archivo Carpeta Acceso a ubicaciones compartidas Archivos creados, modificados o eliminados Acceso de lectura a archivo realizado Intentos fallidos de leer campos o escribir archivos Cambios de permisos de carpeta	Los sistemas de archivos NAS están cada vez más presentes en la lista de objetivos de las amenazas actuales. Por lo tanto, la visibilidad que proporcionan las funciones de auditoría sigue siendo de vital importancia, y la funcionalidad de auditoría aumentada de ONTAP ofrece más detalles de auditoría de CIFS que nunca.
Firma y sellado CIFS SMB	La firma SMB mejora la seguridad de tu Data Fabric al proteger el tráfico entre clientes y los sistemas de almacenamiento de ataques de reinyección y de intermediario. También confirma que los mensajes SMB tienen firmas válidas. Además, ONTAP admite el cifrado SMB, también conocido como sellado.	El protocolo SMB constituye un vector de amenazas para las arquitecturas y los sistemas de archivos. La firma y el sellado permiten validar el tráfico sin alteraciones, además de asegurar el transporte de datos de recurso en recurso.
Soporte para Kerberos 5 y krb5p	ONTAP es compatible con el cifrado AES de 128 bits y 256 bits para Kerberos. El servicio de privacidad incluye la verificación de la integridad de los datos recibidos, la autenticación de usuarios y el cifrado de los datos antes de la transmisión.	La autenticación Krb5p utiliza sumas de comprobación para cifrar todo el tráfico entre cliente y servidor, lo que protege contra la manipulación y el espionaje de datos.
Firma y sellado SMB de Lightweight Directory Access Protocol (LDAP)	ONTAP admite la firma y el sellado para proteger la seguridad de la sesión en solicitudes enviadas a un servidor LDAP.	La firma comprueba la integridad de los datos de la carga útil LDAP mediante una tecnología de clave secreta. El sellado cifra los datos de la carga útil LDAP para evitar que información confidencial se transfiera en texto sin cifrar.
Curvas ed25519 y NIST en Secure Shell (SSH) (algoritmos actualizados y códigos de autenticación de métodos basados en hash [HMAC])	ONTAP proporciona cifrados e intercambios de claves SSH actualizados, como AES, 3DES, SHA-256 y SHA-512.	A medida que evoluciona el panorama de las amenazas, la solidez del algoritmo, del cifrado y de los intercambios de claves del protocolo es vital para la integridad del funcionamiento del protocolo y del producto.

Funciones de seguridad de ONTAP

Software o funciones	Función	Impacto
Capacidad para configurar el número máximo de intentos de inicio de sesión SSH fallidos	ONTAP añade el parámetro -max-authentication-retry-count con el comando security ssh modify para poder establecer el número máximo de intentos de inicio de sesión. El máximo permitido de forma predeterminada por conexión SSH es de seis, pero NetApp recomienda establecer tres como práctica recomendada de seguridad.	Esta función ayuda a proteger contra ataques de fuerza bruta.
Autenticación multifactor (MFA)	La MFA está habilitada para ONTAP System Manager de NetApp y Active IQ® Unified Manager de NetApp con el fin de facilitar el acceso web administrativo a través de Security Assertion Markup Language (SAML) y de proveedores de identidad externos. El acceso administrativo de línea de comandos a ONTAP se habilita a través de métodos locales de autenticación de dos factores que emplean ID/contraseña y una clave pública como los dos factores. Puede utilizar nsswitch con una clave pública como uno de los dos factores para el acceso administrativo de línea de comandos SSH. FIDO2 también se puede usar para la autenticación SSH mediante un dispositivo de autenticación de hardware Yubikey u otros dispositivos compatibles con FIDO2.	La mayoría de los riesgos del sistema se deben a credenciales de acceso administrativo poco fiables. La MFA hace que sea imposible obtener acceso administrativo con simples cuentas basadas en contraseñas.
Tecnología SnapLock de NetApp con NSE y NVE	ONTAP admite NSE y NVE con la función SnapLock, que proporciona administración y almacenamiento para datos WORM (escritura única, lectura múltiple).	La tecnología SnapLock crea volúmenes para finalidades especiales en los que los archivos se pueden almacenar y poner en un estado en el que no se pueden borrar ni sobrescribir. SnapLock puede conservar este estado de forma indefinida o durante un período de retención determinado mientras mantiene un sistema seguro (cifrado) para la solución de NSE y NVE.
Renovación de la validación de imágenes	Las renovaciones de ONTAP verifican que una imagen es original de ONTAP en el momento de la renovación.	Esta validación detecta el uso de imágenes dañadas o falsificadas como parte del proceso de renovación.
Arranque seguro de la interfaz de firmware extensible unificada (UEFI)	La validación de la imagen se lleva a cabo cada vez que el sistema arranca.	En cada arranque, el cargador de arranque verifica las imágenes de ONTAP firmadas para evitar que se utilicen imágenes falsificadas.
Cifrado de pares de clústeres	El cifrado de pares de clústeres utiliza TLS 1.2 para cifrar todos los datos en movimiento a través del cable entre pares de clústeres y las funciones de ONTAP subyacentes que utilizan los pares de clústeres para la replicación de datos (SnapMirror®, SnapVault® y FlexCache® de NetApp).	El cifrado en tiempo real de los datos está disponible para las funciones de ONTAP que replican datos. Además, los clientes que utilizan el cifrado de datos en reposo (NVE/NSE) pueden utilizar el cifrado integral entre clústeres de ONTAP que usan el cifrado de pares de clústeres.
Cifrado IPsec	IPsec ofrece un cifrado de datos en tiempo real para todo el tráfico de IP, como el de los protocolos NFS, iSCSI y SMB/CIFS.	IPsec garantiza que los datos en tránsito están protegidos y cifrados de forma continua. El tráfico de red entre el cliente y ONTAP está protegido con medidas preventivas para evitar ataques de reinyección y de intermediario.
Control de acceso basado en roles (RBAC)	El control de acceso basado en roles de ONTAP permite a tus administradores limitar o restringir el acceso administrativo de los usuarios según el nivel que corresponde a su rol. Esta función permite a los administradores gestionar los usuarios según el rol asignado.	El control de acceso es un elemento fundamental para crear una política de seguridad. Funciones como el control de acceso basado en roles ayudan a tu organización a determinar quién tiene acceso a los datos y en qué medida. Esta función limita las vulnerabilidades y las oportunidades de uso indebido de datos, como su extracción y el escalado de privilegios.
Verificación multi-admin (MAV)	MAV evita que un único administrador del clúster ejecute comandos delicados como «volume snapshot delete» o «volume delete» sin la aprobación de uno o más administradores.	MAV impide que los administradores maliciosos o peligrosos puedan destruir datos valiosos. Esto es esencial para fortalecer el entorno de Confianza Cero centrado en datos de ONTAP.
Conector de antivirus (detección de virus)	La detección de virus se realiza en servidores Vscan que ejecutan el conector antivirus y el software antivirus. Normalmente, el sistema que ejecuta ONTAP se configura para que analice los archivos cuando un cliente los modifica o accede a ellos.	Los vectores de amenazas y ataques no cesan de aumentar. Por lo tanto, la detección de virus inline de los archivos accedidos o modificados ayuda a proteger la integridad de los archivos de tu organización.

Funciones de seguridad de ONTAP

Software o funciones	Función	Impacto
Banners de inicio de sesión y mensaje del día (MOTD)	Los banners de inicio de sesión aparecen en pantalla antes de la autenticación. Estos permiten que tu organización y administradores se comuniquen con los usuarios del sistema.	Los banners de inicio de sesión permiten a tu organización informar a los operadores, administradores e incluso a los intrusos sobre los términos y condiciones de uso aceptable de un sistema. Estos banners también indican a quién se le permite acceder al sistema.
Saneamiento de disco	El saneamiento de disco te permite quitar datos de un disco o conjunto de discos de manera que los datos no se puedan recuperar jamás.	Con frecuencia, los protocolos de seguridad requieren que los datos de un disco sean irrecuperables. El saneamiento de disco ofrece esta funcionalidad.

+1 877 263 8277