DATASHEET

Security features in ONTAP

Securing the world's most vital resource: data

NetApp® ONTAP® data management software continues to evolve, with security as an integral part of the solution. The latest releases of ONTAP contain many new security features that are invaluable for your organization to protect its data across your hybrid cloud, prevent ransomware attacks, and adhere to industry best practices. These new features also support your organization's move toward a Zero Trust model.

To learn more about hardening the ONTAP solution, see TR-4569: Security Hardening Guide for NetApp ONTAP.

The challenge

Businesses today are under pressure from their digital transformation. They need to effectively manage data across their hybrid cloud that is becoming distributed, dynamic, and diverse. Each day, the threat landscape becomes more sophisticated and increasingly dangerous for IT environments. As administrators and operators of data and information, IT teams are expected to manage and to maintain data in a secure manner throughout its lifecycle.

The solution

NetApp ONTAP software is central to protecting your data and meeting compliance requirements. This datasheet and TR-4569: Security Hardening Guide for NetApp ONTAP are essential elements for creating an industry-proven security posture for your most important resource: data.

Key benefits

Enhance data confidentiality, integrity, and availability
Protect your organization's most important resource – data – with ONTAP hybrid cloud security technologies.

Strengthen Your organization's security posture
Establish a secure foundation across your organization's hybrid cloud by leveraging the visibility and security functions that create a secure infrastructure.

Apply NetApp and industry best practices for security and ransomware protection
Establish a vetted security footprint with help from NetApp expertise and industry knowledge.

Meet governance and compliance requirements
Use established security best practices to adhere to and support industry regulation and security compliance.

Security features in ONTAP

Software or features	Function	Impact
Autonomous ransomware protection	Autonomous ransomware protection is an on box capability with machine learning preemptive detection against attacks.	If an anomaly is detected, ONTAP automatically takes a Snapshot copy and alerts the administrator.
NetApp Snapshot™ copies	An ONTAP Snapshot is an efficient, point-in-time, read-only copy of your data. A Snapshot represents exactly what your data looked like at the moment that the Snapshot was taken, whether it was hours, days, weeks, months, or even years ago.	Because Snapshot copies are read only, they can't be infected by ransomware. To recover from a ransomware attack, you can simply restore from a Snapshot that was taken before the attack occurred.
NetApp SnapLock® technology	NetApp SnapLock protects Snapshot copies using NetApp SnapVault® by enabling a truly indelible logical air-gapped backup.	SnapLock eliminates the risk of Snapshot copies being deleted by an administrator through human error, a disgruntled employee, or a bad actor leveraging stolen credentials.
NetApp FPolicy technology	FPolicy is an infrastructure component of ONTAP that enables partner applications to monitor and to set file access permissions. File policies can be based on file type. FPolicy determines how the storage system handles requests from individual client systems for operations such as create, open, rename, and delete. Note: In ONTAP, the FPolicy file access notification framework is enhanced with filtering controls and resiliency against short network outages.	Access control is a key security construct. Therefore, visibility and the ability to respond to file access and file operations are critical for maintaining your security posture. To provide visibility and access control to files, the ONTAP solution uses the FPolicy feature. External FPolicy servers, including NetApp Cloud Insights/ Cloud Secure, make use of user behavioral analytics to identify malware and ransomware to mitigate the effects of broader compromise to data.
NetApp Volume Encryption (NVE)	NVE is a software-based encryption mechanism that enables you to encrypt data on any type of disk with a unique key per volume.	Data encryption at rest remains an industry focus. NVE satisfies this focus while also maintaining a strong security posture across the full breadth of your hybrid cloud.
NVE secure purge	This feature enables a command to cryptographically shred deleted files on NVE volumes by moving good files and deleting the key used to encrypt infected files.	You can remediate data spillage online while the system is still in use. This feature also provides state-of-the-art "right-to-erasure" capability for General Data Protection Regulation (GDPR).
NetApp Aggregate Encryption (NAE)	NAE is a software-based encryption mechanism that enables you to encrypt data on any type of disk with unique keys per aggregate shared across encrypted volumes.	Like NVE, NAE enables data encryption at rest. Aggregate deduplication is enabled with NAE because volumes share keys across the aggregate, thus providing greater storage efficiency.

Security Features in ONTAP

Software or features	Function	Impact
Data at Rest (DAR) Encryption by Default	DAR encryption by default is enabled if either an external key manger or the onboard key manager is defined. Either NVE or NAE software-based encryption will be used. If NSE drives are part of the cluster configuration, DAR encryption is in place and software-based encryption will not be used by default.	DAR encryption by default simplifies the maintenance of a strong security posture across the full breadth of your hybrid cloud.
NetApp Storage Encryption (NSE)	NSE is the NetApp implementation of full disk encryption (FDE) by using FIPS-140-2 level 2 self-encrypting drives. Furthermore, NSE provides a nondisruptive encryption implementation that supports the entire suite of NetApp storage efficiency technologies.	Data encryption at rest remains an industry focus. NSE provides FDE, which satisfies this focus. The NetApp Data Fabric maintains a strong security posture from end to end.
SMB encryption that uses Intel AES New Instructions (AES-NI) acceleration	Intel AES-NI improves on the AES algorithm and accelerates data encryption with supported processor families.	Accelerating security functions increases efficiency. Efficient use of resources is vital to providing successful security solutions.
NetApp cryptographic security module	This module provides FIPS 140-2 validated cryptographic operations for select Secure Sockets Layer (SSL)–based management services. Starting with ONTAP 9.11.1 and TLS 1.3 support, FIPS 140-2 can be validated.	Dedicated security modules improve resource efficiency. In addition, FIPS 140 is the recognized industry standard for cryptography products and solutions.
NetApp CryptoMod	This module provides FIPS 140-2 validated cryptographic operations for NVE, NAE, and the onboard key manager (OKM).	FIPS 140-2 is the recognized industry standard for cryptography products and solutions.
SHA-2 (SHA-512) support	To enhance password security, ONTAP supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords.	SHA-2 has become the industry standard for hash functions because of its much-improved security posture relative to the often-infiltrated SHA-1 standard.
Secure log forwarding (syslog over Transport Layer Security [TLS])	The log-forwarding function enables your administrators to provision targets or destinations so that they can receive syslog and audit information. Because of the secure nature of syslog and audit information, ONTAP can send this information securely through TLS by using the TCP-encrypted parameter.	Log and audit information is invaluable to your organization from a support and availability standpoint. In addition, the information that's contained in logs (syslog) and in audit reports and output is typically sensitive in nature. To maintain your security controls and security posture, you must manage log and audit data securely.
TLS 1.1 and TLS 1.2	ONTAP uses TLS 1.1 and TLS 1.2 for secure communication and administration functions.	NetApp does not recommend the use of TLS 1.0, because its significant vulnerabilities make it incompatible with compliance standards such as PCI-DSS. NetApp does recommend the use of TLS 1.1 and TLS 1.2 because of their strength and integrity.
Online Certificate Status Protocol (OCSP)	When OCSP is enabled, ONTAP applications that use TLS communications, such as LDAP or TLS, can receive the digital certificate status. The application receives a signed response that signifies whether the certificate requested is good, revoked, or unknown.	OCSP helps determine the current status of a digital certificate without requiring certificate revocation lists (CRLs).
Onboard key manager (OKM)	OKM in ONTAP provides a self-contained encryption solution for data at rest. OKM works with NVE, which offers a software-based encryption mechanism that allows you to encrypt data and use any type of disk. OKM also works with NSE, which performs FDE by using self-encrypting drives.	OKM provides key management for NSE and NVE. In addition, the use of this encryption technology in ONTAP allows you to secure data at rest, which provides a pivotal data security solution.
OKM secure boot	This option can require a passphrase for unlocking drives and decrypting volumes after a node is rebooted.	When NSE and NVE use the OKM, secure reboot provides protection against the entire storage array being stolen, not just the drives. It also allows secure physical transport of entire clusters and secure equipment return.

Security Features in ONTAP

Software or features	Function	Impact
External key management	External key management is handled by using a third-party system in the storage environment. This third-party system securely manages the authentication keys and encryption keys that are used by encryption features in the storage system, such as NSE, NVE, or NAE. The storage system uses an SSL connection to contact the external key management server to store and retrieve authentication keys or volume data encryption keys through the Key Management Interoperability Protocol (KMIP).	With external key management, you can centralize your organization's key management functions while inherently confirming that keys are not stored near the assets. This approach decreases the possibility of compromise.
Secure multitenancy	Secure multitenancy is the use of secure virtual partitions within a shared physical storage environment for the purpose of sharing the physical environment among multiple distinct tenants. In ONTAP, these partition are called storage virtual machines (SVMs).	Secure multitenancy enables ONTAP as a shared platform with SVMs securely isolating all tenants within the platform.
Multitenant external key management	Multitenant external key management provides the ability for individual tenants or storage virtual machines (SVMs) to maintain their own keys through KMIP for NVE.	With multitenant external key management, you can centralize your organization's key management functions by department or tenant while inherently confirming that keys are not stored near the assets. This approach decreases the possibility of compromise.
Clustered external key managers	External KMIP server redundancy is supported by clustering capabilities provided by NetApp KMIP key server partners. Prior to ONTAP 9.11.1, up to four external KMIP servers could be defined where ONTAP wrote keys to each server to provide redundancy.	Clustered external key managers are being widely adopted by ONTAP customers. ONTAP support allows these customers to flawlessly use this capability.
Enhanced file system auditing	ONTAP increases the number of auditing events and details that are reported across the solution. The following key details are logged with the creation of events: File Folder Share access Files created, modified, or deleted Successful file read access Failed attempts to read fields or write files Folder permission changes	NAS file systems have increased their footprint in today's threat landscape. Therefore, the visibility that audit functions provide remains critically important, and the increased audit capability in ONTAP provides more CIFS audit details than ever before.
CIFS SMB signing and sealing	SMB signing helps protect the security of your Data Fabric by protecting the traffic between storage systems and clients from replay or man-in-the-middle attacks. It also confirms that SMB messages have valid signatures. In addition, ONTAP supports SMB encryption, also known as sealing.	A common threat vector for file systems and architectures lies within the SMB protocol. Signing and sealing allow unadulterated validation of traffic in addition to secure data transport on a share-by-share basis.
Kerberos 5 and krb5p support	ONTAP supports 128-bit and 256-bit AES encryption for Kerberos. The privacy service includes the verification of received data integrity, user authentication, and data encryption before transmission.	Krb5p authentication protects against data tampering and snooping by using checksums to encrypt all traffic between the client and the server.
Lightweight Directory Access Protocol (LDAP) SMB signing and sealing	ONTAP supports signing and sealing to protect session security on queries to an LDAP server.	Signing confirms the integrity of the LDAP payload data by using secret key technology. Sealing encrypts the LDAP payload data to avoid the transmission of sensitive information in cleartext.
Ed25519 and NIST curves in Secure Shell (SSH) (updated algorithms and hash-based method authentication codes [HMACs])	ONTAP provides updated SSH ciphers and key exchanges, including AES, 3DES, SHA-256, and SHA-512.	As the threat landscape continues to evolve, the strength of the protocol algorithm, cipher, and key exchanges is vital to the integrity of the protocol and the product function.
Ability to configure the maximum number of unsuccessful SSH login attempts	ONTAP adds parameter-max-authentication-retry-count with the security ssh modify command to set the maximum number of login attempts. The default maximum that is allowed per SSH connection is six, but NetApp recommends three as a security best practice.	This feature helps protect against brute-force attacks.

Security Features in ONTAP

Software or features	Function	Impact
Multifactor authentication (MFA)	MFA is enabled for NetApp ONTAP System Manager and NetApp Active IQ® Unified Manager for administrative web access through Security Assertion Markup Language (SAML) and through external identity providers. Administrative command-line access to ONTAP is enabled through local two-factor authentication methods that employ user ID/password and a public key as the two factors. You can use nsswitch with public key as one of the two factors for SSH command-line administrative access.	Weak administrative access credentials account for most system compromises. MFA makes it impossible to gain administrative access with simple password-based accounts.
NetApp SnapLock technology with NSE and NVE	ONTAP supports NSE and NVE with the SnapLock feature, which provides administration and storage for write once, read many (WORM) data.	SnapLock technology creates special-purpose volumes in which files can be stored and committed to a nonerasable, nonrewritable state. SnapLock can preserve this state indefinitely or for a designated retention period while maintaining the secure posture (encryption) of the NSE and NVE solution.
Upgrade image validation	Upgrades for ONTAP verify that an image is genuine ONTAP at upgrade time.	This validation detects corrupt or counterfeit images being used as part of the upgrade process.
Unified Extensible Firmware Interface (UEFI) secure boot	Image validation is done each time the system boots.	Signed ONTAP images are verified by the boot loader, thus preventing counterfeit images at every boot.
Cluster peer encryption	Cluster peer encryption uses TLS 1.2 to encrypt all data in transport over the wire between cluster peers and the underlying ONTAP features that use cluster peering for replication of data (NetApp SnapMirror®, SnapVault®, FlexCache®).	Data-in-flight encryption is available for ONTAP features that replicate data. In addition, customers who use data at rest encryption (NVE/NSE) can use end-to-end encryption between ONTAP clusters that use cluster peer encryption.
IPsec encryption	IPsec offers data encryption in flight for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols.	IPsec ensures data in transit is continuously secure and encrypted. Network traffic between the client and ONTAP is protected with preventive measures to combat replay and man-in-the-middle (MITM) attacks.
Role-based access control (RBAC)	RBAC in ONTAP enables your administrators to limit or to restrict users' administrative access to the level that is granted for their defined role. With this feature, your administrators can manage users by their assigned role.	Access control is a foundational element for creating a security posture. Functions such as RBAC help your organization determine who has data access and to what extent they have such access. This feature limits vulnerabilities and exploitation opportunities, including data exfiltration and escalation of privileges.
Multi-admin verification (MAV)	MAV prevents a single cluster administrator from executing sensitive commands such as “volume snapshot delete” or “volume delete” without approvals from one or more administrators.	MAV stops malicious or compromised administrators from destroying valuable data. This is essential for fortifying the ONTAP data centric Zero Trust environment.
Antivirus connector (virus scanning)	Virus scanning is performed on Vscan servers that run the antivirus connector and antivirus software. Typically, the system that runs ONTAP is configured to scan files when they are modified or accessed by a client.	Threat and attack vectors continue to grow. Therefore, inline virus scanning of accessed or modified files helps protect the integrity of your organization’s files.
Login and message-of-the-day (MOTD) banners	Login banners are printed in the output before authentication. These banners enable your organization and administrators to communicate with system users.	Login banners enable your organization to present operators, administrators, and even miscreants with the terms and conditions of acceptable use for a system. These banners also indicate who is permitted to access the system.
Disk sanitization	Disk sanitization allows you to remove data from a disk or a set of disks so that the data can never be recovered.	Security protocols often require you to make data unrecoverable from a disk. The disk sanitization function provides this capability.

NetApp

+1 877 263 8277