Datasheet

Security Features in ONTAP 9

Securing the world's most vital resource: data

Key Benefits

Enhance Data Confidentiality, Integrity, and Availability
Leverage NetApp ONTAP 9 Data Fabric security constructs to solidify the confidentiality, integrity, and availability of your organization's most important resource: data.

Create a Security Posture for Your Environment
Establish a secure foundation in your organization's Data Fabric and understand the visibility and security functions that create a secure infrastructure.

Leverage NetApp and Industry Best Practices for Security
Establish a vetted security footprint with help from NetApp expertise, industry knowledge, and common practices.

Satisfy Governance and Compliance Requirements
Leverage established security best practices to adhere to and support industry regulation and security compliance.

NetApp® ONTAP® storage management software continues to evolve, with security as an integral part of the solution. The latest release, ONTAP 9, contains many new security features and functions that are invaluable for your organization to protect its security posture and to adhere to industry best practices. These new features make data confidentiality, integrity, and availability top priorities.

To learn more about hardening the ONTAP 9 solution, see TR-4569: Security Hardening Guide for NetApp ONTAP 9.

The Challenge

Each day, the threat landscape becomes larger, more sophisticated, and increasingly dangerous for environments. As administrators and operators of data and information, storage engineers are expected to manage and to maintain data in a secure manner throughout its lifecycle.

The Solution

NetApp ONTAP 9 software is the solution for your organization to protect your data and meet compliance requirements. This datasheet provides an overview of the new and existing security features and functions in the ONTAP 9 solution. This datasheet and TR-4569: Security Hardening Guide for NetApp ONTAP 9 are essential elements for creating an industry-proven security posture for your most important resource: data.

NetApp®

New Security Features in ONTAP 9

TABLE 1) NEW SECURITY FEATURES

Software or Feature	Function	Impact
NetApp Volume Encryption (NVE)	NetApp Volume Encryption is a software-based encryption mechanism that enables you to encrypt data on any type of disk.	Data encryption at rest continues to be an industry focus. NetApp Volume Encryption satisfies this focus while also maintaining a strong security posture across the full breadth of the NetApp Data Fabric.
NVE secure purge	Enables a command to cryptographically shred deleted files on NVE volumes by moving good files and deleting the key used to encrypt infected files.	Data spillage remediation that can be done online while the system is still in use. State-of-the-art "right-to-erasure" capability for General Data Protection Regulation (GDPR).
SMB encryption that uses Intel Advanced Encryption Standard 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 pivotal 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.	Dedicated security modules improve resource efficiency. In addition, FIPS 140-2 is the recognized industry standard for cryptography products and solutions.
NetApp CryptoMod	This module provides FIPS 140-2 validated cryptographic operations for NVE 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 9 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 s ecure nature of syslog and audit information, ONTAP 9 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 v1.1 and TLS v1.2	ONTAP 9 leverages TLS v1.1 and TLS v1.2 for secure communication and administration functions.	NetApp does not recommend the use of TLS v1.0 because its significant vulnerabilities make it incompatible with compliance standards such as PCI-DSS. NetApp does recommend the use of TLS v1.1 and TLS v1.2 because of their strength and integrity.
Online Certificate Status Protocol (OCSP)	When OCSP is enabled, ONTAP 9 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).
OKM	OKM in ONTAP 9 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 NetApp Storage Encryption (NSE), which performs full-disk encryption by using self-encrypting drives.	OKM provides key management for NSE and NVE. In addition, the use of this encryption technology in ONTAP 9 allows you to secure data at rest, which provides a pivotal data security solution.
OKM secure boot	An option is allowed to require a passphrase for unlocking drives and decrypting volumes after a node is rebooted.	For NSE and NVE, protected reboot provides protection against the entire storage array being stolen, not just the drives when using the OKM. Also allows for secure physical transport of entire clusters and secure equipment return.
Enhanced file system auditing	OONTAP 9 increases the number of auditing events nd 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 9 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 9 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.

New Security Features in ONTAP 9 (cont'd)

Software or Feature	Function	Impact
Kerberos 5 and krb5p support	ONTAP 9 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 9 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 9 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 9 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.
Multifactor authentication (MFA)	MFA is enabled for NetApp OnCommand® System Manager and OnCommand Unified Manager for administrative web access through Security Assertion Markup Language (SAML) and through the use of external identity providers. Administrative command-line access to ONTAP is enabled through local two-factor authentication methods that make use of user ID/password and a public key as the two factors. Nsswitch can be used with publickey 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 9 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. This state can be preserved 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 will 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 will be done each time the system boots.	Signed ONTAP images are verified by the boot loader, thus preventing counterfeit images at every boot.

Existing ONTAP Security Features

TABLE 2) EXISTING SECURITY FEATURE

Software or Feature	Function	Impact
NSE	NSE is the NetApp implementation of full-disk encryption by using self-encrypting drives. Furthermore, NSE provides a nondisruptive encryption implementation that supports the entire suite of NetApp storage efficiency technologies.	Data encryption at rest continues to be an industry focus. NSE provides full-disk encryption, which satisfies this focus. It also confirms that the full breadth of the NetApp Data Fabric maintains a strong security posture from end to end.
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 exploits, including data exfiltration and escalation of privileges.
Aggregate encryption for ONTAP Cloud	ONTAP Cloud creates an encryption key for each aggregate on the system and sends it to the key managers. Administrators can view the ID for these keys from NetApp OnCommand Cloud Manager. It is important to note that because keys are not automatically deleted, they must be deleted by the administrator.	The individual encryption keys for each aggregate improve secure key management, which is critical for a secure solution.

Existing ONTAP Security Features (cont'd)

Software or Feature	Function	Impact
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.
Logging	Log and audit information is invaluable to your organization for support and availability. In addition, the information and the details that are contained in logs (syslog) and in audit reports or output are generally of a sensitive nature. Therefore, to maintain your security controls and security posture, your organization must manage log and audit data securely.	The offloading of syslog information is necessary to limit to a single system or single solution the scope or the footprint of a breach.
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 or NVE. The storage system uses an SSL connection to contact the external key management server to store and retrieve authentication keys through the use of 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, decreasing the possibility of compromise.
krbp5	The krbp5 authentication mode is secure and protects against data tampering and snooping by using checksums to encrypt all traffic between the client and the server. ONTAP supports 128-bit and 256-bit AES encryption for Kerberos. This privacy service verifies the integrity of received data, authenticates users, and encrypts data before transmission.	Krbp5 integrity checksums are an evolution in Kerberos authentication that verify that the authentication communications have not been edited or altered.
SMB v3 signing and sealing	ONTAP supports signing and sealing to enable session security on traffic between the storage system and the client.	Signing confirms the integrity of the SMB payload data by using secret key technology. Sealing encrypts the SMB payload data to avoid the transmission of sensitive information in cleartext.
Sanitize a disk function	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 sanitize disk function provides this capability.
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 set 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 9, 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.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation.

Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit www.netapp.com. #DataDriven