



White Paper

NetApp product security overview

Version 1.7

NetApp USPS, NetApp
July 2021 | WP-7344

Abstract

This white paper outlines the basic tenets of security found within the NetApp® product portfolio.

TABLE OF CONTENTS

Executive summary	4
Product vulnerability, assessment, and reporting	4
NetApp's data-centric posture on Zero Trust	5
NetApp AFF and FAS systems	6
Common Criteria	6
Integrated security features	7
Data Encryption at Rest.....	8
Data in transit	11
SAN and block-based protocols	11
NAS file-based protocols	11
S3-based object protocol	12
File auditing	12
Third-party integrations	12
Ransomware detection and remediation	13
NetApp SolidFire and Element software	14
StorageGRID	19
Data access security features.....	19
Object and metadata security features	20
Administration security features.....	22
Platform security features	23
E-Series and EF-Series	23
Introduction/overview and theory of operation	23
SANtricity security features	24
Built-in roles and local user accounts	25
LDAP user and group account mapping.....	25
Secure SMcli logical architecture.....	26
Audit log	27
Certificate management	27
Public cloud services	28
DoD Impact Level (IL) definition	28
Types of data security layers and Cloud Volumes ONTAP	30

Azure NetApp Files	32
Conclusion	33
Where to find additional information	34

LIST OF TABLES

Table 1) ONTAP certifications (https://security.netapp.com/certs/).	7
Table 2) SolidFire/Element certifications.	18
Table 3) SANtricity E-Series and EF-Series platform certifications.	24
Table 4) DoD Impact Level definitions.	28
Table 5) NetApp Public Cloud Services certifications.	29

LIST OF FIGURES

Figure 1) Zero Trust architecture	5
Figure 2) ONTAP protection workflow.	8
Figure 3) NAE/NVE encryption function.	8
Figure 4) NSE encryption function.	9
Figure 5) Preconfigured FlexPod solution with Virsec and NetApp SnapLock.	14
Figure 6) A typical StorageGrid architecture.	21
Figure 7) LDAP configuration parameters.	26
Figure 8) Supported management features of the different management clients.	28
Figure 9) Cloud Volumes ONTAP enables you to optimize storage costs and protect your data.	30

Executive summary

NetApp is an industry leader in developing and implementing product security standards. We follow strict security guidelines, principles, and policies throughout our product development lifecycle, enabling our customers to maintain confidentiality, integrity, and availability of their data. We expand and improve on our secure development programs on a continuing basis. NetApp's security culture is built on employee specialists who have extensive experience in the fields of data science, engineering, systems administration, and product management in multiprotocol enterprise environments. Many of these employee specialists are honored veterans from our military forces, and all have gone through the vigorous hiring standards and requirements for employment at NetApp. NetApp's philosophy is data is the new currency. Data, however, is the property of our customers. We design solutions in collaboration with our customers to protect it according to their imperatives with many types of storage innovations, including, but not limited to, data encryption, both in-flight and at rest, compliance, and protection.

Product vulnerability, assessment, and reporting

As a part of our standard procedures, we implement secure design principles, developer training, and extensive testing programs. When product vulnerabilities are identified, NetApp follows a standard process to address vulnerabilities and notify our customers.

- **Vulnerability report received.** NetApp encourages customers and researchers to use PGP-encrypted emails to transmit confidential details to our Vulnerability Response Team (PSIRT). NetApp investigates a suspected vulnerability in our products and confirms receipt of the vulnerability report within seven business days.
- **Verification.** NetApp PSIRT engineers verify the vulnerability and provide assessment within the Common Vulnerability Scoring System (CVSS) framework.
- **Resolution development.** NetApp strives to deliver critical fixes and mitigations to the customer base as rapidly as our stringent quality-control standards allow; testing and verification is often a time-intensive process.
- **Notification.** NetApp will disclose the minimum amount of information required for a customer to assess the impact of a vulnerability in their environment, as well as any steps required to mitigate the threat. NetApp does not intend to provide details that could enable a malicious actor to develop an exploit.
- **Attribution.** NetApp credits external vulnerability discoverer or discoverers in the advisory if they have provided explicit consent to be identified, and if they provide NetApp the opportunity to remediate and notify our customer base before making the vulnerability public.

NetApp scores security vulnerabilities and prioritizes responses according to industry standards.

To standardize the description of each public vulnerability, NetApp security advisories reference a CVE-ID. NetApp uses version 3.0 of the CVSS to determine vulnerability priority and notification strategy.

Our security advisories and notices include the NetApp-determined Base vulnerability score. We encourage customers using CVSS for vulnerability classification and management to compute their own temporal and environmental scores to take full advantage of the CVSS metrics.

Standard delivery methods for NetApp security information:

- **Security Advisory.** Provides information regarding security vulnerabilities that might affect NetApp products and require an upgrade, patch, or direct customer action to remediate. Advisories are also used when a third party makes an unconfirmed public statement about a perceived NetApp product vulnerability, or NetApp products are unofficially implicated in security incidents. NetApp security advisories are listed on the <https://security.netapp.com> site.
- **Security Bug Report.** Provides information about low-severity or false positive security vulnerabilities and is available on Bugs Online (requires login).

Read more about CVE-IDs, see [Mitre.org](https://www.mitre.org).

In addition, NetApp's adherence to standards and participation in standards bodies shows our commitment to security best practices. The following industry standards and mandates guide the handling of product vulnerabilities at NetApp and the disclosure of vulnerabilities to our customers and the broader technology community:

- **National Infrastructure Advisory Council (NIAC)**—Disclosing and Managing Vulnerability Guidelines
- **ISO/IEC 29147:2014(E)**—Information technology—Security techniques—Vulnerability disclosure
- **ISO/IEC 30111:2013(E)**—Information technology—Security techniques—Vulnerability handling processes

NetApp is currently participating in the following security communities:

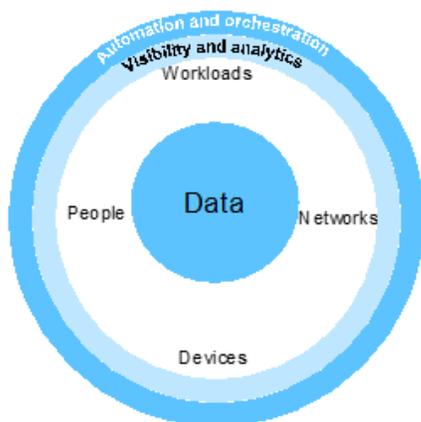
- [FIRST](#)—Forum of Incident Response and Security Teams
- [BSIMM](#)—Building Security In Maturity Model
- [Linux Foundation – Core Infrastructure Initiative](#)

This document provides an executive overview and summary of NetApp's current security posture across our product portfolio. NetApp has been a technology solutions supplier to the DoD/IC community for over 25 years and continues to drive a comprehensive data management posture from the tactical edge to the data center core now to the cloud.

NetApp's data-centric posture on Zero Trust

When it comes to enterprise data security, the old model of “trust but verify” is being replaced by the new Zero Trust model of “Verify and never trust”. The Zero Trust Architecture (ZTA) was first developed by John Kindervag at Forrester Research. It envisions network security from the inside out rather than from the outside in. The inside out Zero Trust approach identifies a microcore and perimeter (MCAP). The MCAP is an interior definition of data, services, applications, and assets to be protected with a comprehensive set of controls. The security controls should be as close to the data as possible (Figure 1).

Figure 1) Zero Trust architecture.



As stated in the National Security Agency published cybersecurity product, “[Embracing a Zero Trust Security Model](#),” dated February 25;

“The Zero Trust model eliminates trust in any one element, node, or service by assuming that a breach is inevitable or has already occurred. The data-centric security model constantly limits access while also looking for anomalous or malicious activity”.

Adopting the Zero Trust mindset and leveraging Zero Trust principles enables systems administrators to control how users, processes, and devices engage with data. These principles can prevent the abuse of compromised user credentials, remote exploitation, or insider threats, and even mitigate effects of supply chain malicious activity.”

As an example, the NetApp ONTAP[®], data management software is capable of a complete data-centric approach to Zero Trust in which the storage management system becomes the segmentation gateway to protect and monitor access of our customer’s data. In particular, the FPolicy[™] Zero Trust engine and the FPolicy partner ecosystem becomes a control center to gain a detailed understanding of normal and aberrant data access patterns and identify insider threats. For a deep-dive on NetApp data-centric Zero Trust methodology, see [TR-4829: NetApp and Zero Trust](#). The following steps represent our path to configuring data-centric Zero Trust on your data fabric.

Follow these steps to architect a Zero Trust data-centric MCAP:

1. Identify the location of all organizational data.
2. Classify your data.
3. Securely dispose of data that you no longer require.
4. Understand what roles should have access to the data classifications.
5. Apply the principle of least privilege to enforce access controls.
6. Use multifactor authentication for administrative access and data access.
7. Use encryption for data at rest and data in flight.
8. Monitor and log all access.
9. Alert suspicious access or behaviors.

NetApp AFF and FAS systems

As the [#1 provider of data storage and management to the U.S. federal government](#), NetApp understands the importance of data security. NetApp’s continued support of the public sector market is underscored by our ongoing commitment to security certification and to the confidentiality, integrity, and availability needs of customers and partners. NetApp was the first storage provider to:

- Achieve [Common Criteria \(ISO/IEC 15408\) certification](#)
- Be certified and listed on the [Unified Capabilities \(UC\) Approved Products List \(APL\)](#)

NetApp follows a security life cycle model to ensure the integrity of our solutions. Our kernel and architecture provide reliability and security in the following areas:

- **Confidentiality.** Preventing unauthorized access to customer data
- **Integrity.** Preventing unauthorized changes to customer data
- **Availability.** Making sure customer data is available (resisting denial of service attacks)

NetApp products are equipped with strict role-based access control (RBAC) measures to control administrative access, as well as secure protocols, audit logging, and industry standard encryption. Together, these features help to ensure secure products and solutions for our customers.

Common Criteria

The Common Criteria certification is an international standard (ISO/IEC 15408) for IT Security Evaluation. The Common Criteria is the driving force for the widest available mutual recognition of secure IT products,

officially recognized by [31](#) countries. NetApp was the first storage provider to achieve Common Criteria certification.

- ONTAP 9.5 [EAL 2+ Assurance Continuity](#)
- ONTAP 9.3 [EAL 2+ Assurance Continuity](#)
- ONTAP 9.1 [EAL 2+](#)
- Data ONTAP 7-Mode 8.2.2 [EAL 2+ Assurance Continuity](#)
- Data ONTAP 7-Mode 8.2.1 [EAL 2+](#)

Table 1 below summarizes our current certification status for ONTAP. As this is a constantly evolving process, the link provided is regularly updated with the most recent info.

Table 1) ONTAP certifications (<https://security.netapp.com/certs/>).

Certification	Level	Comments
Common Criteria (ISO/IEC 15408)		
<ul style="list-style-type: none"> • NetApp ONTAP 9.3 	EAL 2+	See Maintenance Report
<ul style="list-style-type: none"> • ONTAP 9.5* 	EAL 2+	See Certification Report
FIPS 140-2		
NetApp CryptoMod	Level 1	Used in ONTAP for NetApp Volume Encryption (NVE) & Onboard Key Manager (OKM) See FIPS 140-2 Certificate # 3072
NetApp Cryptographic Security Module (NCSM)	Level 1	Used in ONTAP for OpenSSL See FIPS 140-2 Certificate # 2648
NetApp Storage Encryption (NSE) and NetApp SANtricity® full disk encryption, NetApp SolidFire® full disk encryption	Level 2	Used in ONTAP See NetApp Disk Drive and Firmware Matrix
Department of Defense Information Network Approved Products List		
National Information Assurance Partnership (NIAP)	CSfC	In process

Integrated security features

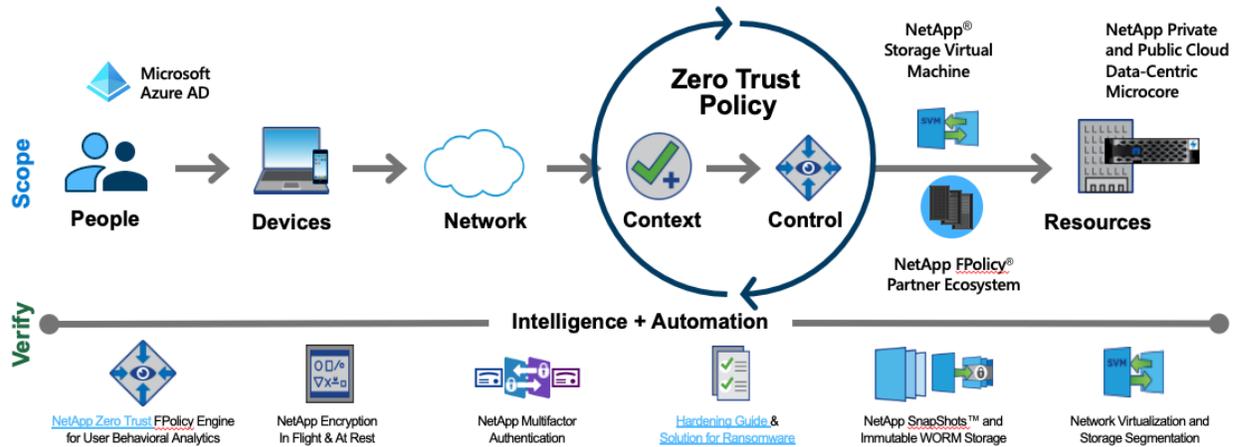
Refer to the [ONTAP 9 Security Data Sheet](#) for the latest updates. In addition, [TR-4569:Security Hardening Guide for ONTAP 9](#) provides guidance and configuration settings for ONTAP 9 to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability.

The NetApp microcore architecture is designed to protect customer data by following the three basic principles of Zero Trust.

The following are the Zero Trust basic principles as shown in Figure 2:

- Verify explicitly
- Use least privilege access
- Assume breach

Figure 2) ONTAP protection workflow.

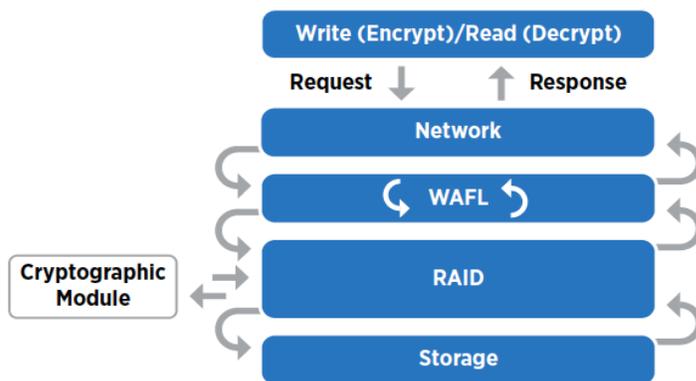


Data Encryption at Rest

NetApp offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. With software-based encryption, data encryption is supported one volume at a time. Whereas, with hardware-based encryption, data is encrypted with full-disk encryption (FDE) as it is written. NetApp uses FIPS 140-2 certified self-encrypting drives, and other non-certified self-encrypting drive (SED) options are available as part of our data encryption-at-rest solutions. Following is a detailed explanation of our software-based encryption offering, as shown in Figure 3.

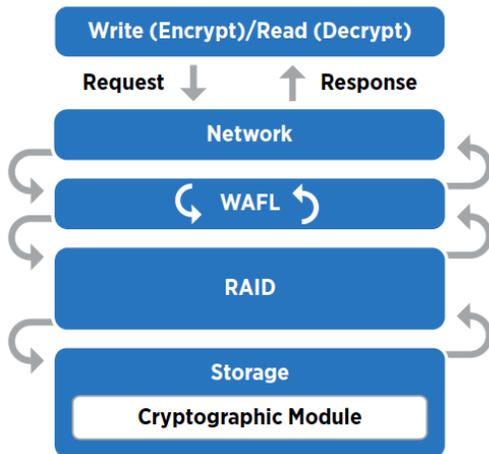
- **NetApp Volume Encryption (NVE).** NVE is a software-based encryption mechanism that enables you to encrypt data on any type of disk with a unique key per volume.
- **NetApp Aggregate Encryption (NAE).** NAE is also a software-based encryption mechanism that enables you to encrypt data on any type of disk with unique keys per aggregate shared across encrypted volumes.

Figure 3) NAE/NVE encryption function.



- **NetApp Storage Encryption (NSE).** NSE is the NetApp implementation of FDE by using FIPS-140-2 level 2 self-encrypting drives. Furthermore, NSE provides a nondestructive encryption implementation that supports the entire suite of NetApp storage efficiency technologies, as shown in Figure 4.

Figure 4) NSE encryption function.



- **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.
- **Dual-layer encryption.** NSA's Commercial Solutions for Classified (CSfC) Program enables certified vendor solutions to be used for secret/top secret information. CSfC dictates that two layers (hardware and software) be used to encrypt AFF/FAS systems with NSE, and NVE provides two layers. You can see the CSfC website [here](#).

Key management

- **Onboard Key Manager (OKM).** The OKM feature 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 enables you to encrypt data and use any type of disk. OKM also works with NSE, which performs FDE by using self-encrypting drives.
- **OKM secure boot.** This option can require a passphrase for unlocking drives and decrypting volumes after a node is rebooted.
- **Key Management Interoperability Protocol (KMIP).** 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 a Secure Sockets Layer (SSL) connection to contact the external key management server to store and retrieve authentication keys or volume data encryption keys through the KMIP.
- **Multitenant key management.** Multitenant external key management provides the ability for individual tenants or storage virtual machines (SVMs) to maintain their own keys through OKM or KMIP for NVE.
- Customers have the flexibility to migrate their existing keys from OKM to KMIP infrastructures as requirements change.

Encryption in transit

- **TLS 1.2 for management.** ONTAP 9 uses TLS 1.2 for secure communication and administration functions.
- **FIPS compliance mode.** With FIPS-compliant mode, the cluster automatically selects only compliant TLS protocols.
- **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®, NetApp SnapVault®, and NetApp FlexCache®).

- **IPsec.** IPsec offers data encryption in flight for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols.

FIPS modules

- **NetApp cryptographic security module.** This module provides FIPS 140-2 validated cryptographic operations for select SSL-based management services.
- **NetApp CryptoMod.** This module provides FIPS 140-2 validated cryptographic operations for NVE, NAE, and the onboard key manager (OKM).

Fpolicy

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.

- With ONTAP 9, the FPolicy file access notification framework is enhanced with filtering controls and resiliency against short network outages. FPolicy is an infrastructure component of ONTAP that enables partner applications to monitor and to set file access permissions.
- Additionally, the FPolicy file access notification framework has been enhanced with filtering controls and resiliency against short network outages.

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 partitions are called SVMs. Each SVM can support multifactor authentication for administrative access.

- **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 publickey as one of the two factors for Secure Shell (SSH) command-line administrative access.

Additional integrated features

- **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.
- **Syslog** 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 9 can send this information securely through TLS by using the TCP-encrypted parameter.
- **SSHv2 support.** ONTAP 9 provides updated SSH ciphers and key exchanges, including AES, 3DES, SHA-256, and SHA-512.
- **NetApp SnapLock®.** ONTAP 9 supports NSE and NVE with the SnapLock feature, which provides administration and storage for write once, read many (WORM) data.
- **Upgrade image validation.** Upgrades for ONTAP verify that an image is genuine ONTAP at upgrade time.
- **UEFI secure boot.** Unified Extensible Firmware Interface (UEFI) secure boot image validation is done each time the system boots.
- **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.

- **Disk sanitization.** Disk sanitization enables you to remove data from a disk or a set of disks so that the data can never be recovered.
- **Certificate-based authentication.** When using the NetApp Manageability SDK API or REST API access to ONTAP, you must use certificate-based authentication instead of the user ID and password authentication.

Data in transit

In addition to data-at-rest encryption, ONTAP offers a robust set of standard and optional features for securing and encrypting data in transit. These features are broken down by host protocol.

For additional information, see [TR-4569: Security Hardening Guide for NetApp ONTAP 9](#).

SAN and block-based protocols

For SAN and block-based protocols, the following security elements are supported.

- **Fibre Channel Protocol (FCP) encryption over the wire with Brocade/Cisco FC-SP-2.** Fibre Channel Security Protocol (FC-SP) capabilities provide switch to switch and hosts to switch authentication to overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DHCHAP) is an FC-SP protocol that provides authentication between switches and other devices. DHCHAP consists of the CHAP protocol combined with the Diffie-Hellman exchange.
- **Over the wire encryption with internet protocol security (IPsec).** IPsec offers data encryption in flight for all IP traffic including the NFS, iSCSI, and SMB and its corresponding implementation known as CIFS protocols.
- **CHAP authentication.** The Challenge Handshake Authentication Protocol (CHAP) enables authenticated communication between iSCSI initiators and targets. When you use CHAP authentication, you define CHAP usernames and passwords on both the initiator and the storage system.

NAS file-based protocols

For NAS file based protocols, the following specific security elements are supported.

- **NFS: Kerberos 5 and krb5p encryption.** 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. For additional information, see [TR-4067: Network File Systems \(NFS\) in NetApp ONTAP](#).
- **IPsec.** IPsec offers data encryption in flight for all IP traffic including the NFS, iSCSI, and SMB/CIFS protocols.
- **LDAP signing and sealing.** ONTAP 9 supports signing and sealing to protect session security on queries to an LDAP server.
- **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.
- **SMB encryption.** SMB encryption leverages the Intel AES New Instructions (AES-NI) acceleration. Intel AES-NI improves on the AES algorithm and accelerates data encryption with supported processor families.

S3-based object protocol

For the S3-based object protocol, the following specific security elements are supported.

- **Local storage tier.** NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), and NetApp Aggregate Encryption (NAE) work equally well for objects written to buckets in ONTAP. Neither NSE, NVE, nor NAE are required for S3 in ONTAP.
- **Over the wire.** TLS/SSL encryption is enabled by default using a system-generated certificate. Using signed certificates from a third-party certificate authority is a recommended best practice.

Client-object store communication without TLS encryption (HTTP, Port 80) is supported but is not a recommended best practice.

Signature Version 4: S3 in ONTAP requires the use of Signature Version 4 (v4 signatures).

In addition, the following features are available:

- **Custom object metadata and tags.** Client applications can create user-defined object metadata and tags by using ONTAP to drive custom operations and automated workflows using metadata and tags attached to objects. Compatible with applications that need the ability to create metadata and tags, requested by multiple accounts for custom-built and commercial applications
- Modernizing supported password hash algorithms.
- Authenticate to the ONTAP management plane by using external accounts instead of using local accounts for administrating ONTAP.
- RedHat IdM and other IPA-based LDAP servers can be leveraged to manage ONTAP administrator access with the addition of SHA512 and SSHA512 hash algorithm support.
- Keep security teams happy while enhancing administrator secure access to ONTAP, frequent request from accounts that do not use Active Directory and would like to maintain default hash settings for identity providers.

For more detailed information, see [TR-4814: S3 in ONTAP best practices](#).

File auditing

ONTAP 9 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

Third-party integrations

NetApp has several data security technology partners that provide FPolicy solutions for ONTAP.

Refer to the [NetApp IMT](#) for the latest updates. You can find additional details [here](#).

- Fpolicy partners and solutions
 - [Varonis DatAdvantage](#)
 - [PeerLink](#)
 - [Cloud Insights with Cloud Secure](#)

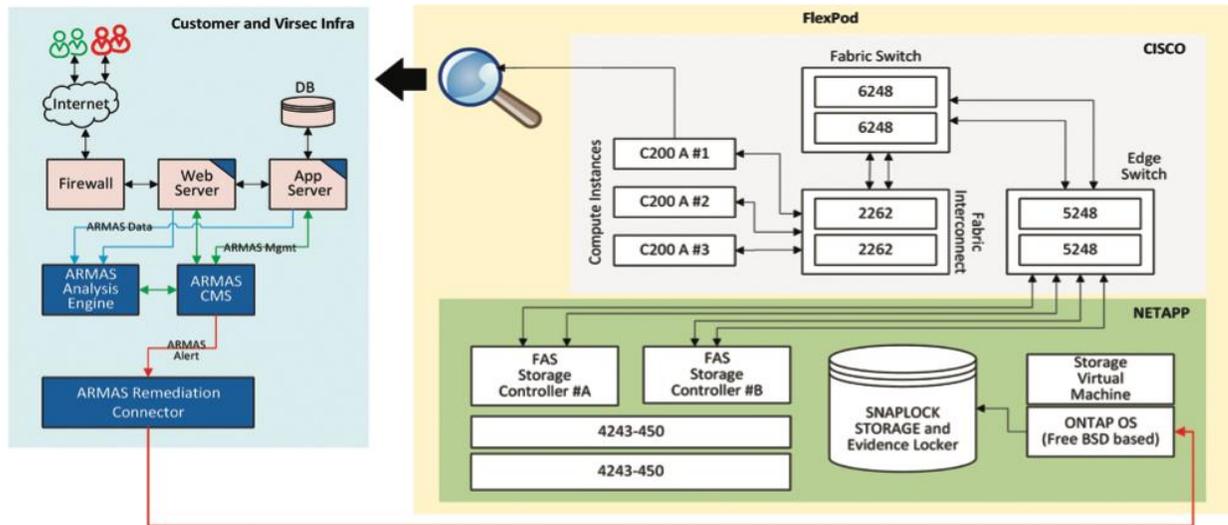
- [Cleondris](#)
- [ProLion](#)
- [Stealth Bits](#)
- [Symantec](#)
- Key management partners (KMIP)
 - [Thales \(CipherTrust/Gemalto/Vormetric\)](#)
 - [Thales TCT](#)
 - [HashiCorp](#)
 - [Foretix](#)
 - [IBM SLCK](#)
 - [HyTrust](#)
- Antivirus software partners
 - McAfee
 - Trend
 - Symantec
 - Sophos
- MFA technology partners (IDP)
 - Shibboleth
 - ADFS

Ransomware detection and remediation

When used in conjunction with Virsec ARMASTM, NetApp ONTAP and SnapLock solutions form a powerful and innovative new offering against ransomware. The solution counts on Virsec's ability to detect sophisticated cyberattacks at high rates of precision (near 100% accuracy), and NetApp brings its SnapLock immutable disk capability on ONTAP-based storage systems. The joint solution uses SnapLock WORM technology to ensure corrupted or tampered with files are rapidly replaced when ransomware affects any portion of data, application code, or system log. Organizations can thus ensure business continuity and avoid system disruption from ransomware on critical servers.

The solution provides high-cost savings for incident response teams that would traditionally need to piece together negative impacts from various systems and replace damaged files from backups. Virsec ARMASTM's protection capabilities include configurable file system monitoring on critical servers that complement its full stack protection of both memory and web layers of application processes. For ease and speed of deployment, a FlexPod® preconfigured and integrated rack solution is available as shown in Figure 5.

Figure 5) Preconfigured FlexPod solution with Virsec and NetApp SnapLock.



NetApp SolidFire and Element software

The advanced and dynamic threats and vulnerabilities that organizations face is ever-increasing in sophistication. Coupled with an increase in the effectiveness of obfuscation and surveillance techniques on the part of potential intruders, system managers must address the security of their data proactively. The NetApp Element software found in the NetApp SolidFire® scale-out storage system is designed to help organizations meet prescribed security objectives for information system confidentiality, integrity, and availability. For more information, see [TR-4806:VMware vSphere for Element Software Configuration Guide](#).

NetApp has partnered with trusted partners such as Coalfire and HyTrust to provide fully validated multitenant solutions that are fully integrated to meet the key security measures for FISMA as defined in NIST SP 800-53 Revision 4 and Payment Card Industry Data Security Standard (PCI DSS) V3.2.1.

Security based HCI solutions

- NetApp HCI Reference Architecture for [FISMA](#) with [Coalfire](#)
- [NetApp Verified Reference Architecture for PCI DSS V3.2.1 with Coalfire](#)

System management

NetApp provides multiple options to manage all components in the storage solution stack. This section describes each method and best practice for your SolidFire environment.

Out-of-band management

All SolidFire nodes provide out-of-band management capabilities through a dedicated management port. NetApp H410S and H610S nodes also enable baseboard management controller (BMC) access through a dedicated port.

Command-line management

By default, SSH is disabled. SSH is enabled and disabled with the Support Access option in the Element UI. Support access is enabled to allow temporary access to the Element storage cluster by NetApp.

Support access can only be enabled for a minimum of 1 hour and a maximum of 24 hours. If access is required for a duration longer than 24 hours, you can use the Element API to set the desired time.

VMware

By default, SSH is disabled in vCenter and vSphere. It is best practice to leave the SSH protocol disabled if not in use.

Enable or disable SSH for vCenter

Support for the vCenter Server Appliance (VCSA) is found in the vCenter Server Appliance Management Interface (VAMI). For more information, see [Enable or Disable SSH and Bash Shell Access](#).

Enable or disable SSH for vSphere

Support for SSH for an ESXi host, can be enabled by logging into vCenter and select Host → Configure → System → SSH → Start. For more information, see [Using ESXi Shell in ESXi 5.x, 6.x, and 7.x \(2004746\)](#).

NetApp Element Plug-in for VMware vCenter Server

Administrators have the option to use the built-in NetApp Element Plug-in for VMware vCenter Server, which is a web-based tool integrated with the VMware vSphere Web Client UI. The plug-in is an extension and alternative scalable, user-friendly interface for VMware vSphere that can manage and monitor storage clusters running NetApp Element software.

Management node (mNode)

Administrators can leverage the management node (mNode) to upgrade system services, manage cluster assets and settings, run system tests and utilities, configure Active IQ for system monitoring, and enable NetApp Support access for troubleshooting. The management node (mNode) is a virtual machine that runs in tandem with an Element software-based storage cluster.

Login and password parameters

An effective security posture adheres to established organizational policies, guidelines, and any governance or standards that apply to the organization. Examples of these requirements include user-name lifetime, password-length requirements, character requirements, and the storage of such accounts. The NetApp HCI solution provides features and functions to address these security constructs.

SHA-512 support

To enhance password security, Element and VMware supports the SHA-2 password hash function and defaults to using SHA-512 for hashing newly created or changed passwords. Operators and administrators can also expire or lock accounts as needed.

Role-based access control (RBAC)

Organizations can maximize the security and manageability of their NetApp environment by following best practices for roles and permissions.

Local users

In greenfield deployments, the initial local cluster administrator accounts are created for Element and vCenter clusters when using the NetApp Deployment Engine (NDE). This account is used to conduct initial administrative tasks in Element and vCenter environments.

In brownfield deployments, NetApp leverages existing RBAC implementations.

Lightweight Directory Application Protocol (LDAP/LDAPS)

Both Element and VMware supports the Lightweight Directory Application Protocol (LDAP/LDAPS) and Active Directory. With LDAP/Active Directory user accounts, administrators can create, modify, or delete custom access control roles, and they can specify account restrictions for specific users.

With RBAC, local users have access to only the systems and options that are required for their job roles and functions. The RBAC solution within VMware and Element limits users' administrative access to the level granted for their defined role, which allows administrators to manage local users by assigned roles.

MFA

MFA uses a third-party identity provider through the Security Assertion Markup Language (SAML) to manage user sessions. MFA enables administrators to configure additional factors of authentication as required, such as password and text message, and password and email message.

Event notification in Element

Authorized users can review event logs for operations performed on the selected cluster along with cluster faults that might occur. Most errors are resolved automatically by the system. Other faults might require manual intervention. Event notifications are consolidated and found in vCenter server.

Forwarding syslog

Log and audit information is invaluable to an organization from a support and availability standpoint. In addition, the information and details contained in logs (syslog), audit reports, and outputs are generally of a sensitive nature. To maintain security controls and posture, it is imperative that organizations manage log and audit data in a secure manner.

Offloading of syslog information is necessary for limiting the scope or footprint of a breach to a single system or solution. Therefore, NetApp recommends securely offloading syslog information to a secure storage or retention location. The logging server must monitor on TCP. SolidFire sends logs through TCP only, not UDP. Everything that is logged to `/var/log/*` on the storage nodes is sent to the syslog server and collected in each log file name.

NetApp Active IQ

Active IQ is a web-based tool that provides continually updated historical views of cluster-wide data. You can set up alerts for specific events, thresholds, or metrics. Active IQ enables you to monitor system performance and capacity as well as stay informed about cluster health.

SNMP monitoring

Both Element and VMware supports alert notifications to be sent through email, SNMP traps, and syslog. Alerts notify administrators about important events that occur on the storage array. Element supports SNMPv3c and version 3, which supports authentication and encryption.

Capabilities include the following:

- SNMP requestor
- Select which version of SNMP to use
- Identify the SNMP User-based Security Model (USM) user
- Configure traps to monitor

Data security and integrity

Element clusters enable you to encrypt all data stored on the cluster. All drives in storage nodes capable of encryption use AES 256-bit encryption at the drive level. Each drive has its own encryption key, which

is created when the drive is first initialized. When you enable the encryption feature, a cluster-wide password is created, and chunks of the password are then distributed to all nodes in the cluster. No single node stores the entire password. The password is then used to password-protect all access to the drives. The password is needed to unlock the drive, and it is not needed unless power is removed from the drive, or the drive is locked.

Enabling the encryption at rest feature does not affect performance or efficiency on the cluster. Additionally, if an encryption-enabled drive or node is removed from the cluster with the Element API or Element UI, encryption at rest will be disabled on the drives. After the drive is removed, the drive can be securely erased by using the secure erase drives API method. If a drive or node is forcibly removed from the cluster, the data remains protected by the cluster-wide password and the drive's individual encryption keys.

Enabling FIPS drives

Security is becoming increasingly critical for the deployment of solutions in many customer environments. Federal Information Processing Standards (FIPS) are standards for computer security and interoperability. FIPS 140-2 certified encryption for data at rest is a component of the overall security solution.

Enabling FIPS 140-2 for HTTPS

With Element software, you can enable FIPS140-2 operating mode on your cluster. Enabling this mode activates the NetApp Cryptographic Security Module (NCSM) and leverages FIPS 140-2 Level 1 certified encryption for all communication through HTTPS to the NetApp Element UI and API.

SED and key management

External key management (EKM) provides secure authentication key (AK) management in conjunction with an off-cluster external key server (EKS). The EKS provides secure generation and storage of AKs.

The AKs are used to lock and unlock self-encrypting drives (SEDs) when encryption at rest (EAR) is enabled on the cluster. The cluster utilizes the Key Management Interoperability Protocol (KMIP), an OASIS defined standard protocol, to communicate with the EKS.

Installing a CA-signed digital certificate

When an Element software cluster is created, the cluster creates a unique self-signed SSL certificate and private key that is used for all HTTPS communication through the Element UI, per-node UI, or APIs. Element software supports self-signed certificates as well as certificates that are issued and verified by a trusted certificate authority (CA).

You can change the default SSL certificate and private key of the storage node in the cluster by using the NetApp Element API.

You can use the following API methods to get more information about the default SSL certificate and make changes.

- **GetSSLCertificate.** You can use this method to retrieve information about the currently installed SSL certificate including all certificate details.
- **SetSSLCertificate.** You can use this method to set the cluster and per-node SSL certificates to the certificate and private key you supply. The system validates the certificate and private key to prevent an invalid certificate from being applied.
- **RemoveSSLCertificate.** This method removes the currently installed SSL certificate and private key. The cluster then generates a new self-signed certificate and private key.

TLS and SSL

SSL ciphers are encryption algorithms used by hosts to establish a secure communication. There are standard ciphers that Element software supports and non-standard ones when FIPS 140-2 mode is enabled. The following lists provide the standard SSL ciphers supported by Element software and the SSL ciphers supported when FIPS 140-2 mode is enabled:

- **FIPS 140-2 disabled:**

```

TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_IDEA_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_RC4_128_MD5 (rsa 2048) - C
TLS_RSA_WITH_RC4_128_SHA (rsa 2048) - C
TLS_RSA_WITH_SEED_CBC_SHA (rsa 2048) - A
    
```

- **FIPS 140-2 enabled:**

```

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (dh 2048) - A
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp256r1) - A
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp256r1) - A
TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
    
```

Table 2 illustrates some of the certifications awarded to the SolidFire platform.

Table 2) SolidFire/Element certifications.

Certification	Level	Comments
Common Criteria (ISO/IEC 15408)		
NetApp Element software 10.x	EAL 2+	See Certification Report
FIPS 140-2		
NetApp Cryptographic Security Module (NCSM)	Level 1	Used in Element software See FIPS 140-2 Certificate # 2648
NetApp Storage Encryption and NetApp SolidFire full disk encryption	Level 2	Used in Element software See NetApp Disk Drive & Firmware Matrix

StorageGRID

As outlined previously, NetApp StorageGRID® follows the NetApp Product Security Vulnerability Response and Notification Policy as previously described. Reported vulnerabilities are verified and responded to according to the product security incident response process. For object storage in general, security is a particularly important concern because much of the rich content that is well suited for an object store is also sensitive in nature and subject to corresponding regulation and compliance. As the capabilities of NetApp StorageGRID continue to evolve, NetApp continues to introduce new security features that are invaluable for enforcing an organization's security posture and helping customers adhere to industry best practices and data governance.

This section is an overview of the many security features in StorageGRID and is divided into the following five categories:

- Data access security features
- Object and metadata security features
- Administration security features
- Platform security features
- Cloud integration

For additional information, see [TR-4645: Security features in StorageGRID 11.5](#)

Data access security features

TLS 1.3 and signed certificate support

NetApp StorageGRID leverages Transport Layer Security (TLS) 1.3 to enable a client and StorageGRID to identify and authenticate each other and communicate with confidentiality and data integrity. StorageGRID supports the following cipher suites for TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Support is also provided for a configurable server certificate enabling customers to centrally manage all StorageGRID API endpoints to use a server certificate signed by their organization's trusted CA. In addition, customers can configure load balancer endpoints to generate or use a server certificate as well. This flexibility enables customers to use digital certificates signed by their standard trusted CA to authenticate all object and endpoint operations.

Multitenancy

StorageGRID supports multiple tenants per grid, and each tenant has its own namespace. A tenant provides either Simple Storage Service (S3) or Swift protocol; by default, access to buckets/containers and objects is restricted to users within the account. Tenants can have one user (for example, an enterprise deployment, in which each user has their own account) or multiple users (for example, a service provider deployment, in which each account is a company and a customer of the service provider). Users can be local or federated; federated users are defined by Active Directory or LDAP), or by the OpenStack Identity (Keystone) Service, the latter for Swift users only. StorageGRID provides a per-tenant dashboard where users log in using their local or federated account credentials. Users can access visualized reports on tenant usage against the quota assigned by the grid administrator, including usage information in data and objects stored by buckets. Users with administrative permission can perform tenant-level system administration tasks, such as managing users and groups and access keys. This flexibility enables customers to host data from multiple tenants while isolating tenant access, and to

establish user identity by federating users with an external identity provider such as Active Directory, LDAP, or Keystone.

WORM support

Customers can support a grid-wide WORM requirement by enabling the Disable Client Modify option, which prevents clients from overwriting or deleting objects or object metadata in all tenant accounts (S3 and Swift). For S3 accounts, customers can also enable WORM by tenant, bucket, or object prefix by specifying IAM policy, which includes the custom S3: PutOverwriteObject permission for object and metadata overwrite.

The WORM feature might be further enhanced by enabling Compliance WORM which is designed to meet the requirements of the Securities and Exchange Commission (SEC) Rule 17a-4(f) and validated by Cohasset. Customers can enable compliance at the bucket level. Retention can be extended but never reduced. Information lifecycle management (ILM) rules enforce minimum data protection levels.

The following S3 specific data access security features are supported:

- AWS signature version 2 and 4
- Secure storage of S3 credentials with password hashing (SHA-2)
- Time bound S3 access keys: customers can set an expiration date and time per access key.
- Nondisruptive rotation of access keys to discourage key sharing between clients
- S3 IAM Access Policy to allow granular specification of control by user groups per tenant, bucket, or object prefix.

Server-side encryption (SSE-C)

StorageGRID supports server-side encryption with customer-provided encryption keys (SSE-C) enabling multitenant protection of data at rest with encryption keys managed by tenant users. While StorageGRID manages all object encryption and decryption operations, the customer is given the opportunity to self-manage the encryption keys on a per-tenant basis. This enables individual tenants to encrypt objects with keys they control. The encryption keys are required to write and retrieve each tenant's corresponding objects.

Swift-specific data access security features

This feature enables customers to integrate authentication of Swift API users on StorageGRID with an established OpenStack Identity Service framework and gives customers the option to allow Swift access without standing up a Keystone service. Swift uses tokens to authenticate an API request. StorageGRID supports two types of token-based authentication: Swift auth and Keystone auth.

- **Swift auth is enabled.** A client provides its local or federated user account credential and procures a Swift token from the StorageGRID Swift auth URL.
- **Keystone auth is enabled.** The client authenticates its user credential with an external OpenStack Identity (Keystone) service and procures a Keystone token. StorageGRID supports Keystone v3 API and universal unique identifier (UUID) and Fernet format tokens.

In addition, Swift container access control lists (ACLs) provide authorization for API operations that are allowed to act on a specific bucket by authorized users. The Swift container ACLs are supported only with Keystone authentication and provide controlled access to containers by users in the same Swift tenant.

Object and metadata security features

Advanced Encryption Standard (AES) server-side object encryption

StorageGRID provides AES 128- and AES 256-based server-side encryption of objects. Customers can enable encryption as a global default setting. StorageGRID also supports the S3 x-amz-server-side-

encryption header to allow enabling or disabling encryption on a per-object basis. When enabled, objects are encrypted when stored or in transit between grid nodes. This helps customers secure storage and transmission of objects, independent of the underlying storage hardware.

Built-in key management

When encryption is enabled, each object is encrypted with a randomly generated unique symmetric key, which is stored in the grid. This enables encryption of objects without requiring external key management.

FIPS 140-2 media

The StorageGRID appliance supports the use of FIPS 140-2 compliant SEDs. The encryption keys for the drives can optionally be managed by an external key server supporting the KMIP.

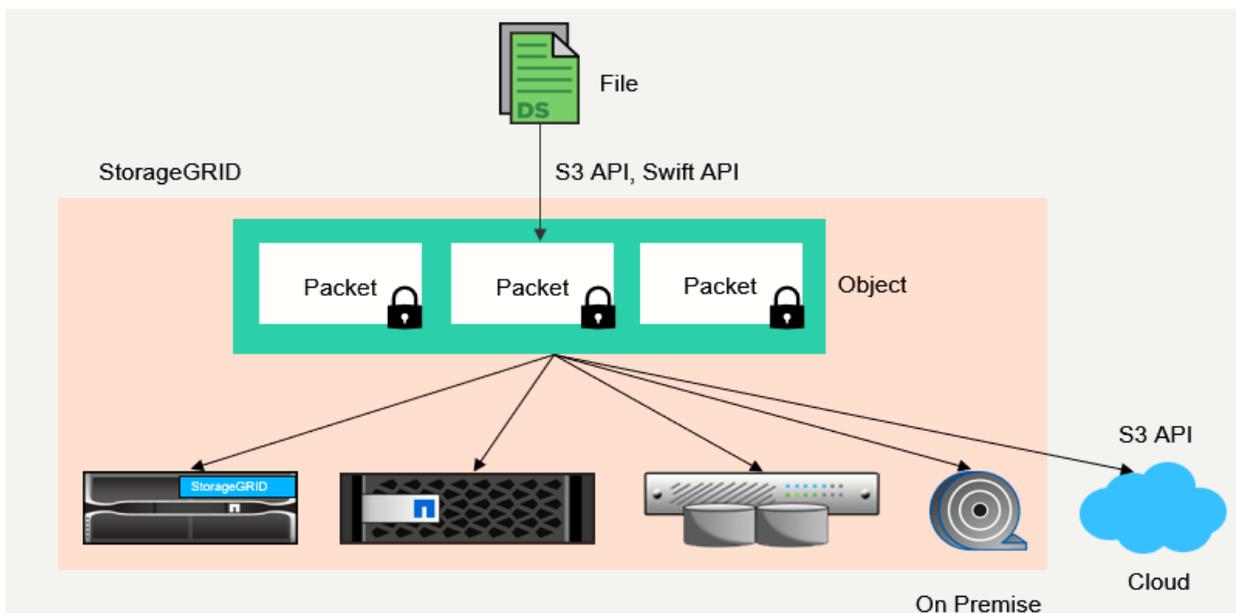
Built-in integrity scan

StorageGRID uses an interlocking mechanism of hashes, checksums, and cyclic redundancy checks (CRCs) at the object and sub-object level to protect against data corruption, tampering, or modification, both when objects are in storage and in transit. StorageGRID automatically detects corrupt and tampered objects and replaces them while quarantining the altered data and alerting the administrator. You can use this advanced capability to help customers detect ransomware or viruses attempting to modify or corrupt their data.

Policy-based object placement and retention

StorageGRID enables customers to configure ILM rules, which specify object retention, placement, protection, transition, and expiration. With this feature, customers can configure StorageGRID to filter objects by their metadata and to apply rules at various levels of granularity, including grid-wide, tenant, bucket, key prefix, and user-defined metadata key-value pairs. StorageGRID ensures that objects are stored according to the ILM rules throughout their lifecycles unless they are explicitly deleted by the client (Figure 6).

Figure 6) A typical StorageGrid architecture.



Administration security features

Server certificate (Grid Management Interface)

Customers can configure the Grid Management Interface to use a server certificate signed by their organization's trusted CA to authenticate management UI and API access between a management client and the grid.

Admin user authentication

Admin users are authenticated using a username and password. Admin users and groups can be local or federated, imported from the customer's Active Directory or LDAP. Local account passwords are stored in a format protected by bcrypt; command-line passwords are stored in a format protected by SHA-2.

SAML support

StorageGRID supports single sign-on (SSO) using the SAML 2.0 standard. When SSO is enabled, all users must be authenticated by an external identity provider before they can access the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API. Local users cannot sign in to StorageGRID.

Granular permission control

Customers can assign permissions to roles and assign roles to admin user groups, which enforces what tasks admin clients are allowed to perform using both the management UI and APIs. This supports the least privileged access control principals found in the Zero Trust methodology.

Distributed audit logging

StorageGRID provides a built-in, distributed audit logging infrastructure, scalable to hundreds of nodes across up to 16 sites. StorageGRID software nodes generate audit messages, which are transmitted through a redundant audit relay system and ultimately captured in one or more audit log repositories. Audit messages capture events at an object-level granularity: from client-initiated S3 and Swift API operations, to object lifecycle events by ILM, to background object health checks, to configuration changes made from the management UI or APIs.

You can export audit logs from admin nodes through CIFS or NFS, allowing audit messages to be mined by tools such as Splunk and ELK. There are four types of audit messages:

- System audit messages
- Object storage audit messages
- HTTP protocol audit messages
- Management audit messages

System audit

System audit messages capture system-related events, such as grid node states, corrupt object detection, objects committed at all specified locations per ILM rule, and progress of system-wide maintenance tasks (grid tasks). This extra attention to detail helps customers troubleshoot system issues and provides proof that objects are stored according to their SLAs, which are implemented by StorageGRID ILM rules and are integrity protected.

Object storage audit

Object storage audit messages capture object API transaction and lifecycle-related events. These events include object storage and retrieval, grid-node to grid-node transfers, and verifications.

HTTP protocol audit

HTTP protocol audit messages capture HTTP protocol interactions related to client applications and StorageGRID nodes. In addition, customers can capture specific HTTP request headers, such as X-Forwarded-For and user metadata (`x-amz-meta-*`), into audit.

Management audit

Management audit messages log admin user requests to the management UI (Grid Management Interface) or APIs. Every request that is not a GET or HEAD request to the API logs a response with the username, IP, and type of request to the API. This helps customers establish a record of system configuration changes made by which user from which source IP and which destination IP at what time.

SNMPv3 for StorageGRID monitoring

SNMPv3 provides security by offering both strong authentication and data encryption for privacy. With v3, protocol data units are encrypted using CBC-DES for the encryption protocol.

HMAC-SHA or HMAC-MD5 authentication protocol provides the user authentication of the user who sends the protocol data unit.

Platform security features

Infrastructure (PKI), node certificates, and TLS

StorageGRID uses an internal public-key infrastructure (PKI) and node certificates to authenticate and encrypt internode communication. Internode communication is secured by TLS. This enables customers to secure system traffic over the LAN/WAN particularly in multisite deployments.

Node firewall

StorageGRID automatically configures iptables and firewalling rules to control incoming and outgoing network traffic, as well as closing unused ports.

Separate networks for client, admin, and internal grid traffic

StorageGRID software nodes and hardware appliances support multiple virtual and physical network interfaces, so that customers can separate client, administration, and internal grid traffic over different networks.

Untrusted client network

The untrusted client network interface accepts inbound connections only on ports that have been explicitly configured as load-balancer endpoints.

Cloud integration—Notifications-based virus scanning

StorageGRID platform services support event notifications. Event notifications can be used in conjunction with cloud computing services to trigger virus scanning workflows on the data.

E-Series and EF-Series

Introduction/overview and theory of operation

NetApp E-Series and EF-Series systems provide a secure, role-based access controlled, and auditable management interface for multiple users through a collection of management security features that were introduced in NetApp SANtricity OS 11.40 and enhanced in later SANtricity OS releases. This section

provides detailed information about these NetApp SANtricity System Manager and NetApp SANtricity Storage Manager Security features for NetApp E-Series and EF-Series storage systems. Table 3 illustrates some of the certifications granted for the SANtricity storage OS-based E-Series systems.

Table 3) SANtricity E-Series and EF-Series platform certifications.

Certification	Level	Comments
Common Criteria (ISO/IEC 15408)		
<ul style="list-style-type: none"> NetApp E-Series and EF-Series with NetApp SANtricity OS 11.50 	NDcPP	See Certification Report
FIPS 140-2		
<ul style="list-style-type: none"> NetApp Cryptographic Security Module (NCSM) 	Level 1	Used in SANtricity for OpenSSL See FIPS 140-2 Certificate # 2648
<ul style="list-style-type: none"> NetApp SANtricity Full Disk Encryption 	Level 2	Used in SANtricity See NetApp Disk Drive and Firmware Matrix

SANtricity security features

The SANtricity OS software for the latest E-Series and EF-Series systems supports secure, web-based storage management for individual systems. In addition to this array-level management security, NetApp also supports enterprise-level secure management in NetApp SANtricity Unified Manager and SANtricity Web Services Proxy (WSP), enabling secure, centralized management of hundreds of systems.

By using the embedded Web Services management infrastructure or SANtricity Unified Manager and SANtricity WSP, administrators can manage storage systems from a networked browser client with IP access to E-Series controller management ports, and the WSP web server. Because web-based storage management exposes the managed devices to private and public networks, E-Series and EF-Series systems and SANtricity WSP support appropriate security schemes at various levels, including the transport layer protocol, access methods, and access control, incorporating authentication and authorization aspects.

SANtricity OS supports the concept of multiuser management to securely perform storage setup and management functions on individual systems by using the SANtricity System Manager GUI, the secure CLI (secure SMcli), and API access methods. SANtricity WSP and SANtricity Unified Manager also provide this same level of security.

Users who intend to perform storage or system management functions are authenticated first, either locally or with a directory server using LDAP. After successful authentication, they can perform management tasks according to their assigned role (RBAC). When using LDAP, a user's role is based on the user's group settings in the directory server. For local users, access roles are hardcoded as part of the management access authorization workflow, and passwords are managed by the admin user.

Security is further enhanced by using SANtricity System Manager, SANtricity WSP, and Unified Manager by requiring administrators to set up certificates of trust (web server and CA root or intermediate certificates) between the multiple client-server relationships supported by the systems and WSP:

- SANtricity Storage Manager Enterprise Management Window (EMW)
- SANtricity WSP and SANtricity Unified Manager
- LDAPS servers
- KMIP-compliant external encryption key manager servers

- E-Series and EF-Series systems managed by either method such that user credentials (user ID and password) for active operations are always transferred to a trusted entity using a secure connection, directly to a browser or through another method listed

By streaming the built-in audit log to a log server, you can track events on the array and adjust the level of logging to meet your requirements.

Finally, when using SANtricity OS, customers can choose to use multifactor authentication with SAML 2.0 to secure the management interface for individual systems. SANtricity WSP and SANtricity Unified Manager do not support SAML and cannot discover and manage systems by using SAML. If you use multifactor authentication instead of directory services, you can only use the SANtricity System Manager GUI to manage the storage array. All other management interfaces are disabled, including all API access.

Built-in roles and local user accounts

The current security model enforces the implementation of RBAC. This means that all users are assigned a set of permissions that define what they are authorized to do with respect to the managed array's setup and administration functions. In other words, users are preassigned to one or more of the system-defined roles that give them access to the set of allowed operations mandated by the given roles. The role object is defined to incorporate commonly used LDAP attributes to easily derive this information from LDAP-accessible user and group directories.

The following roles are implemented in this feature:

- **Monitor.** This role gives read-only access to all storage array properties. This user cannot view the security configuration.

Note: All users must have the monitor role to log in to a storage array. Other roles define what users can do after they are authenticated.
- **Root admin.** This is the only role that allows the user to change the passwords of any local users and run any command supported by the array. Combined with the monitor role, the root admin role allows access to all functions on the array.

Note: The root admin username is "admin" rather than "root". The other usernames are security, storage, support, and monitor.
- **Security admin.** This role allows the user to modify the security configuration on the array, including the ability to view audit logs, configure a secure syslog server, set LDAP/LDAPS server connections, and manage certificates. This role does not provide write access to storage array properties such as pool and volume creation/deletion, but it does have read access. It also has privileges to enable/disable SYMbol access to the array.
- **Storage admin.** This role has full read/write access to the storage array properties but with no access to perform any security configuration functions.
- **Support admin.** This role has access to all hardware resources on the array, failure data, MEL/audit log, and CFW upgrades.
- **rw.** This is a legacy WSP account with read/write permissions. It is not supported on new-generation storage systems.
- **ro.** This is a legacy WSP account with read-only permissions. It is not supported on new-generation storage systems.

LDAP user and group account mapping

LDAP is an open, vendor-neutral, industry-standard application protocol for accessing and maintaining distributed directory information services over an IP network. A common use of LDAP is to provide a central place to store usernames and passwords, enabling many different applications and services to connect to the LDAP server to validate users.

For SANtricity OS to validate users through LDAP, it must be configured to authenticate with the Active Directory, Linux 389, or some other directory server. The configuration scheme allows multiple instances of directory server configurations to support multiple LDAP domains. Each LDAP domain has a name that is presumed to match the DNS domain for the LDAP server, but it is not required. See section 5.3, Certificate Management for SANtricity System Manager Controller, to set up certificates for LDAP with SSL.

Domains can be named anything if they are valid DNS names that contain only ASCII letters. In addition to the domain name, Figure 7 shows the attributes that are supported as part of the directory server configuration.

Figure 7) LDAP configuration parameters.

Name	Description
Domain name	Valid DNS names that contain only the ASCII letters a through z (not case sensitive), the digits 0 through 9, and the hyphen (-), but cannot start with a hyphen. Per RFCs 3629 and 4514, conversion of string representation associated with distinguished name from ASN.1 to UTF-8 encoded Unicode representation is allowed.
LDAP URL	The URL to access the LDAP server in the form of <code>ldap[s]://host:port</code> .
User bind attribute (filter base)	The attribute to which the user ID is bound to authenticate the user in the form of <code>attribute=%s</code> , where %s is replaced by the user name. This allows a large amount of flexibility.
Search base	The LDAP context to search for users. Usually in the form of: <code>CN=Users, DC=cpoc, DC=local</code> .
Group attribute	A list of group attributes on the user that is searched for group-to-role mapping.
Group to role mapping	A list of regular expression patterns to match to the user's group attributes to match to roles.
Bind account user ID	Requires a read-only user account for search queries against the LDAP server and/or for searching within the scope of groups.
Bind account password	The password associated with the read-only account for search queries against the LDAP server and/or for searching within the scope of groups.

Secure SMcli logical architecture

The secure SMcli allows an SMcli client to interact with a storage array through a secure HTTPS channel. It provides a thin HTTPS client that allows customers to interoperate with storage systems by using traditional SMcli grammar and command semantics, but with a secure protocol.

Note: SMcli is supported with SANtricity Storage Manager Enterprise Management Window (EMW), but not with WSP or SANtricity Unified Manager.

Instead of the client providing parsing logic and executing commands against an array, the secure SMcli provides a lightweight wrapper that interacts with the storage array where most of the command processing takes place.

Audit log

A feature of the SANtricity OS is the ability to track user activity through an audit trail log. An entry is posted to the log when a user initiates an action or a command through any of the secure access methods that results in a security event. Users attempting login, authentication, and authorization activities also constitute security events. The logs are persisted on the storage system in the non-volatile storage region for access by both controllers. A user who has security administrative privileges can use any of the access methods to view and retrieve the logs or export them into a CSV file format.

Certificate management

In cryptography, a CA is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This certification allows others to rely on signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted by both the owner of the certificate and the party relying on the certificate. The format of these certificates is specified by the International Telecommunications Union's Standardization (ITU-T) X.509 international standard.

A common use for certificate authorities is to sign certificates used in HTTPS, the secure browsing protocol for the World Wide Web. NetApp introduced the CA certificate management feature in the SANtricity Enterprise Management Window (EMW) to allow a secure browsing protocol between SANtricity System Manager sessions and the EMW to support configuring remote mirroring. The CA Certificate Management feature was later renamed to the Web Services Certificate Management to more accurately describe what the feature does. This functionality on the Web Services Proxy has now been elevated to the SANtricity Unified Manager GUI for ease of use. The certificate management in WSP is still available and is supported directly by using API commands (endpoints) defined in the API Swagger doc.

In addition, NetApp recently introduced the array certificate management feature in the EMW for the supported storage systems to ensure that the communication between the EMW and the storage system is done on a path with a secure connection. To prevent sensitive information from being compromised by a man-in-the-middle attack, EMW makes it possible to establish trust between the two parties with the use of certificates.

To complete the secure framework, support for certificate management was added to the SANtricity WSP to enable secure communications between a server running the Web Services Proxy software and the supported storage systems that are managed and monitored by the proxy. Beginning with SANtricity WSP 3.0 and SANtricity Unified Manager, there are new options for customers who only have new-generation E-Series and EF-Series systems running SANtricity OS 11.40 or later. This extends to customers who want to manage their new systems by using the advanced security features and still manage older generation systems by using SANtricity Storage Manager EMW. The decision about which interface to use depends on your need for security versus the desire to use certain features. Figure 8 describes considerations to help make that decision.

Figure 8) Supported management features of the different management clients.

Management Client	Mirroring Feature	SMcli	Script Editor	Importing Settings from One System to Other Systems
SANtricity Storage Manager	Supports mirroring for legacy and new-generation E-Series and EF-Series systems	Supports standard and secure SMcli	Supported for both legacy and new generation systems with the legacy SYMbol API interface enabled	Not supported
SANtricity WSP 3.0 (and later) and Unified Manager	Supports mirroring only for new-generation E-Series and EF-Series systems	Not supported	Not supported	New feature to automate deploying new systems that use common settings (alerts, ASUP, storage configuration, and more)

Public cloud services

“The Department of Defense is striving to meet the Cloud Smart mandate for IT modernization. With a mission to maximize the full value of federal data to better meet the needs of the agency and its mission, the management of data and moving to the cloud, has become a cornerstone to modernization efforts.”
Editorial Team at GovDataDownload.

For more information, see [GovDataDownload](#). NetApp is working closely with Government Cloud Service Providers to meet these mandates.

DoD Impact Level (IL) definition

Impact Levels are the combination of:

- The sensitivity of the information to be stored and/or processed in the cloud.
- The potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information (Table 4).

Table 4) DoD Impact Level definitions.

DoD Impact Level (IL)	Definition
• IL 2	Accommodates DoD information that has been approved for public release (Low Confidentiality & Moderate Integrity)
• IL 4	Accommodates DoD Controlled Unclassified Information (CUI) (for example, FOUO)
• IL 5	Accommodates DoD CUI and National Security Systems (NSS)
• IL 6	Accommodates DoD Classified Information up to SECRET

Table 5) NetApp Public Cloud Services certifications.

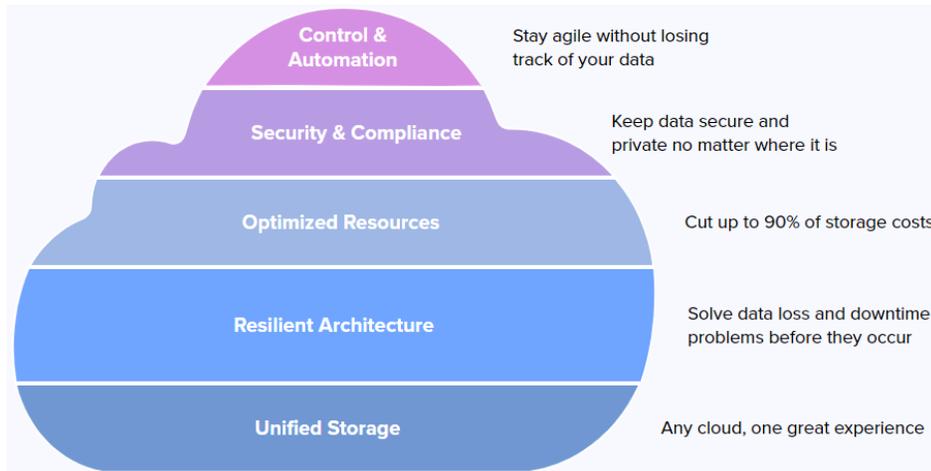
Service	ISO 27001	ISO 27018	SOC 2 Type 1	SOC Type 2	FedRAMP Moderate	FedRAM P High	DoD CC SRG L4	DoD CC SRG L5
 Azure NetApp Files	✓	✓		✓ _{1,2}	✓ ₃	✓ _{3,4}	✓ ₄	✓ ₄
 CVS AWS	✓	✓	✓	✓ ₂				
 CVS GCP	✓	✓						
 Cloud Insights			✓	✓ ₂				
 Cloud Sync		✓	✓					
 Cloud Tiering		✓	✓					
 SaaS Backup	✓	✓	✓	✓ ₂				
 Virtual Desktop Service			In progress					
 Cloud Manager		✓	✓		n/a ⁵	n/a ⁵		
 Cloud Volumes ONTAP					n/a ⁵	n/a ⁵		
 Spot Services				✓ ₂				

1. SOC 1 Type 2
2. SOC 2 Type 2
3. Azure Commercial
4. Azure Government
5. FedRAMP is not applicable to non-service software. Evaluated by cloud service provider.

NetApp Cloud Volumes ONTAP is not a service (SaaS, PaaS, IaaS) as defined by NIST and, thus, is not required or eligible to achieve FedRAMP authorization. Cloud Volumes ONTAP is a software product deployed in a virtual machine (VM) and managed by the consumer, not by NetApp or the Cloud Service Provider (CSP). It is eligible for deployment in FedRAMP authorized Cloud Service Offerings (CSOs) if documented in the agency's authorization package.

Cloud Volumes ONTAP is software that has been specifically designed to operate within a FedRAMP authorized CSO. This software has been evaluated by the FedRAMP authorized CSP to ensure compatibility with their environment and compliance with the security controls documented and tested within their FedRAMP authorized package. Cloud Volumes ONTAP operates in the CSO's FedRAMP authorized boundary and inherits its native security controls. A separate FedRAMP authorization is not required for CVO as by itself it is not a CSO; rather Cloud Volumes ONTAP is included within the authorization boundary of each FedRAMP authorized CSO that is deploying this capability (Figure 9).

Figure 9) Cloud Volumes ONTAP enables you to optimize storage costs and protect your data.



Types of data security layers and Cloud Volumes ONTAP

To establish the end-to-end security of your Cloud Volumes ONTAP deployments, various cloud access control mechanisms should be applied to three layers: at the storage layer, at the network layer, and at the management level, to enable proper data authentication and authorization.

Cloud security at the storage level

The storage level is where the actual data resides. There are multiple configuration options available with Cloud Volumes ONTAP to protect the security of that data.

Data encryption

Encryption of data in flight for SMB3+/NFS4.1+ protocols and of data at rest is supported out of the box in Cloud Volumes ONTAP through multiple encryption technologies. NVE is supported using an external key management server. You can encrypt data, NetApp Snapshot™ copies, and metadata by using a unique XTS-AES-256 key, one per volume. When Cloud Volumes ONTAP is deployed in AWS, customers can enable encryption using AWS Key Management Service (KMS) to ensure encryption and security.

While deploying in Azure, Storage Service Encryption is automatically enabled for data in Cloud Volumes ONTAP. It is a transparent process where all data written to storage is encrypted using a strong 256-bit AES encryption. There are no additional configuration settings to be completed by the customer for security of data at rest while using Cloud Volumes ONTAP in Azure.

Cloud Volumes ONTAP users can also take advantage of NVE to encrypt data at rest at the ONTAP level. This gives users the ability to manage their own keys within their organization rather than with the public cloud provider.

NTFS/share permissions and EXT/export permissions

For secure access of files in Cloud Volume ONTAP over the SMB / CIFS protocol, NTFS permissions should be configured to limit access to the file system so only authorized users can access files. Cloud Volumes ONTAP supports all native NTFS ACLs. Share permissions should be applied to give another layer of protection for protocol level access.

For secure access of files in Cloud Volume ONTAP over NFS, EXT permissions should be configured to limit access to the file system so only authorized users can access the files. Cloud Volumes ONTAP supports all native EXT ACLs. Export permissions should be applied to give another layer of protection for protocol level access.

Ransomware protection

NetApp Cloud Manager highlights the volumes not protected by Snapshot policies so that customers can activate the default Snapshot backup policy, whether for Azure backup or AWS backup. Snapshot copies that are read-only are immune to ransomware attacks. They help recover data from uninfected backups if any data corruption occurs due to ransomware attacks. It also offers granular recovery options in the event of data loss by using the NetApp SnapRestore® feature, which can recover either a single file or multiple data volumes.

Through SnapLock, Cloud Volumes ONTAP makes it possible to get immutable WORM storage in the cloud. These undeletable, unchangeable copies are a surefire way to prevent ransomware attackers from keeping you locked out of your data.

The ONTAP FPolicy component enables you to filter and get alerts about suspicious file extensions to protect against common ransomware extensions. You can also configure FPolicy to operate in file-blocking mode which is enabled through Cloud Manager at no additional charge.

Vscan antivirus integration

Virus scanning functionality is available in Cloud Volumes ONTAP out of the box through Vscan. Vscan protects the data in your data volumes from virus attacks or malicious codes. It integrates with leading third-party antivirus solutions such as McAfee, Symantec, Sophos, and TrendMicro, all while providing flexibility for the customer to decide which files are getting scanned and when. While on-access scanning is used to protect against possible virus attacks when a file is open, read, closed, and so on., you can use on-demand for virus scanning on a scheduled or ad-hoc basis.

Network layer security

You can implement network security in cloud computing by using first-party cloud service provider tools or using third-party appliances. While deploying in AWS, security groups are created for Cloud Manager and Cloud Volumes ONTAP to restrict the inbound and outbound network traffic. You can configure the rules to allow only the required traffic to reach the data and control plane. Similarly, you should also create network security groups that protect the network layer in Azure deployments.

You should also create these security groups in client subnets to ensure that only clients from authorized networks can access the volumes. Inbound rules should be created for SSH and HTTPS ports so that connections to Cloud Volumes ONTAP happen only over an encrypted channel. This is to protect management-layer traffic that reaches the Cloud Volumes ONTAP system.

If you have selected NFS or multiprotocol for creating a volume in Cloud Volumes ONTAP, you can create an export policy for the volume to secure network level access. You can configure the export policy to allow only clients with specific IP addresses or within an IP range (CIDR) to access the volume. For example, if the VMs using the NFS volume reside in a specific subnet, you should create an export policy in Cloud Volumes ONTAP to allow access to only those subnets. This is to prevent unauthorized mounting of volumes and shares. Such steps, combined with the security groups mentioned previously, provide network layer security to the last mile.

Management layer security: Authentication and authorization

Cloud Manager is the single-pane control panel for Cloud Volumes ONTAP to manage storage resources, alerts, automation, and more.

User roles

Users can be assigned different roles in Cloud Manager that define the Cloud Volumes ONTAP management functions they are authorized to use. The three different user roles are: Cloud Manager Admin, Tenant Admin, and Working Environment Admin. The rule of thumb for managing authentication

and authorization is to provide only the minimum level of permissions to users required to complete activities that they are expected to perform. While Cloud Manager Admin has the highest level of authorization and should be limited to admin users, Tenant Admin and Working Environment Admin can be used to restrict the level of user access to a specific tenancy workspace or a specific Cloud Volumes ONTAP instance working environment.

SSO and identity federation

Cloud Manager integration with NetApp Cloud Central provides a single deployment and management pane for multiple Cloud Manager systems. It uses a centralized user authentication mechanism that enables you to use the same set of credentials for multiple Cloud Manager systems. By using NetApp Cloud Central identity federation, users can use SSO to manage Cloud Volumes ONTAP by using their corporate identity credentials. Identity federation uses open standards including SAML 2.0 and OpenID Connect (OIDC) and currently supports integration with Active Directory Federation Services (ADFS) and Microsoft Azure Active Directory for SSO.

FPolicy auditing

The FPolicy auditing option sends an event to an external system about any file activity. With this advanced auditing enabled, users get visibility into data usage patterns. FPolicy auditing also helps organizations meet compliance, privacy, and security requirements by providing a way to see who is using data in order to implement appropriate data usage policies.

File-level permissions

In addition to the implementation of network layer security using export policies and security groups, as explained in the previous section, setting the right permissions at the file level is important when managing NFS or SMB / CIFS shares. This can prevent unauthorized access even from permitted subnets.

With SMB / CIFS shares, you can integrate individual cloud volumes with Windows Active Directory if you select the SMB dual protocol during volume creation. This allows you to provide file share permissions by using existing Active Directory user accounts, thereby seamlessly integrating with your existing identity and access management solutions.

When it comes to NFS exports, ONTAP restricts permissions to clients based on the export policy defined. The export policy can regulate client access based on criteria such as file access protocol, client identifier (host name/IP), or the authentication method (Kerberos v5/NTLM/AUTH_SYS, and so on). Based on the export policy, users are assigned read only, read/write, or superuser access levels.

Azure NetApp Files

Azure NetApp Files, one of the only Azure-native, high-performance file storage services, offers the TCO, performance, management, and confidence demanded by critical applications for federal, Department of Defense, and state and local agencies that have strict government security and regulatory compliance requirements.

Azure NetApp Files, a leading public cloud file storage solution for the public sector, is securely architected into government virtual networks and fully integrated into Azure, making it the preferred solution to meet cloud-first mandates. And with FedRAMP High Baseline level authorization, the service meets the most stringent security requirements for high-impact unclassified data in the cloud. The result is a flexible cloud service that supports multiprotocol workloads that can be tailored to fit customers' hybrid data environments while scaling storage and service levels based on required speed.

“Combining nearly three decades of NetApp’s extensive experience in data management and storage with Microsoft’s forward-looking capabilities of Microsoft Azure gives government customers the ability to

fulfill the government's cloud-first mandate simply, reliably, and securely," says Anthony Lye, Senior Vice President and General Manager of the NetApp Cloud Data Services business unit. "Azure NetApp Files is a significant Azure differentiator, and a game changer for all organizations that want to fully harness the value of cloud."

"By combining the scale and reach of Microsoft Azure with NetApp's Cloud Volumes technology coupled, customers can achieve new value with Azure NetApp Files," says Lily Kim, General Manager, Azure Global at Microsoft. "With deployment into our government data center regions, government customers can have another great option to migrate and run applications in the cloud with powerful data management capabilities."

Deployment of Azure NetApp Files to government data center regions started in Virginia, followed by Arizona and Texas deployments.

The benefits of Azure NetApp Files include the following:

- **Migrate and run.** Agencies can move and deploy their most demanding enterprise file applications without code changes.
- **No separate contracts or term agreements.** Azure NetApp Files is delivered as an Azure first-party service, which allows customers to provision workloads through their existing Azure agreement. No additional NetApp ONTAP licensing is required. Pay for only what you use. The service has no back-end read or write or other back-end fees.
- **Multiple performance tiers.** Azure NetApp Files offers three levels of performance to enable optimized performance according to needs without sacrificing performance, reliability, or security.
- **FedRAMP certification.** 50% of the \$80 billion per year that the U.S. Government spends on IT is data categorized as High Impact level. With FedRAMP High Impact level certification, agencies with the most rigorous security requirements can take advantage of the smooth migration of their most intensive workloads by using Azure NetApp Files.
- **Simplifies migration to the cloud.** Azure NetApp Files eliminates a common cloud-first barrier by creating the right infrastructure environment for agencies resources, budget, and skillsets.

Conclusion

Data is the lifeblood of an organization and the new currency. From orchestrated environments based on software-defined storage, to traditional application data from email, chat, and conversations over a digital medium, data is everywhere, and unintended sharing of data can greatly influence the success of a mission/project outside of traditional avenues.

When it comes to protecting data at an enterprise scale, methodologies and practices must remain diligent as well as agile to protect against ever evolving threats. By listening to our customers and working with industry partners, NetApp leads the industry in information assurance certifications and industry participation in governing standards bodies. You can find a comprehensive listing at <https://security.netapp.com/certs/>. You can find additional information at our NetApp Trust Center: <https://www.netapp.com/company/trust-center/>

Where to find additional information

NetApp overview

- NetApp Product Security
<https://security.netapp.com>
- Security Resources
<https://security.netapp.com/resources/>

ONTAP

- TR-4829: NetApp and Zero Trust
<https://www.netapp.com/media/19756-tr-4829.pdf>
- Achieve a Data-Centric Approach to Zero Trust with NetApp ONTAP
<https://blog.netapp.com/achieve-a-data-centric-approach-to-zero-trust-with-netapp-ontap/>
- ONTAP security
<https://www.netapp.com/data-protection/ontap-security/>
- TR-4569: Security Hardening Guide for NetApp ONTAP 9
<https://www.netapp.com/pdf.html?item=/media/10674-tr4569.pdf>

SolidFire/ Element OS

- NetApp HCI security
https://docs.netapp.com/us-en/hci/docs/concept_cg_hci_security.html
- NVA-1143: NetApp HCI – NIST Security Controls for FISMA with HyTrust for Multitenant Infrastructure
<https://www.netapp.com/media/17065-nva1143.pdf>
- TR-4641: NetApp HCI Data Protection
<https://www.netapp.com/media/17048-tr4641.pdf>

StorageGRID

- How the StorageGRID system implements security in S3
<https://library.netapp.com/ecmdocs/ECMP12031314/html/GUID-C521E35B-BF96-4446-8616-AB3075AA32B8.html>
- StorageGRID 11.5 System Hardening Guide
<https://docs.netapp.com/sqws-115/index.jsp?topic=%2Fcom.netapp.doc.sg-harden%2Fhome.html>

E-Series

- TR-4855: Security Hardening Guide for NetApp SANtricity 11.60
<https://www.netapp.com/media/19422-tr-4855.pdf>
- Security Feature in E-Series SANtricity OS
<https://www.netapp.com/media/17016-ds-4003.pdf>
- TR-4712: NetApp SANtricity Management Security
<https://www.netapp.com/media/17079-tr4712.pdf>
- TR-4474: SANtricity drive security
<https://www.netapp.com/pdf.html?item=/media/17162-tr4474pdf.pdf>
- TR-4853: Access Management for E-Series Storage Systems
<https://www.netapp.com/media/19404-tr-4853.pdf>

Hyperscaler offerings

- NetApp Cloud Volumes Platform
<https://cloud.netapp.com>

- Cloud Central—Data Protection
<https://cloud.netapp.com/data-protection>
- About Cloud Secure
https://docs.netapp.com/us-en/cloudinsights/cs_intro.html
- Ransomware: Prevention is better than cure
<https://www.netapp.com/blog/ransomware-prevention-is-better-than-cure/>

Refer to the [Interoperability Matrix Tool \(IMT\)](#) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

Copyright © 2021 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

WP-7344-0721