Security

ONTAP Technical Reports

NetApp
January 23, 2026

Table of Contents

Security

ONTAP security technical reports

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

These technical reports expand on the ONTAP security and data encryption product documentation.

ONTAP cyber vault

ONTAP cyber vault
NetApp's ONTAP based cyber vault provides organizations with a comprehensive and flexible solution for protecting their most critical data assets. By leveraging logical air-gapping with robust hardening methodologies, ONTAP enables you to create secure, isolated storage environments that are resilient against evolving cyber threats. With ONTAP, you can ensure the confidentiality, integrity, and availability of your data while maintaining the agility and efficiency of your storage infrastructure.

Ransomware

TR-4572: The NetApp solution for ransomware
Learn how ransomware has evolved; and how to identify attacks, prevent the spread, and recover as quickly as possible using the NetApp solution for ransomware. The guidance and solutions provided in this document are designed to help organizations have cyber-resilient solutions while meeting their prescribed security objectives for information system confidentiality, integrity, and availability.

TR-4526: Compliant WORM storage using NetApp SnapLock
Many businesses rely on some use of write once, read many (WORM) data storage to meet regulatory compliance requirements or simply to add another layer to their data protection strategy. Learn how to integrate SnapLock, the WORM solution in ONTAP, into environments that require WORM data storage.

Zero Trust

NetApp and Zero Trust
Zero Trust traditionally has been a network-centric approach of architecting micro core and perimeter (MCAP) to protect data, services, applications, or assets with controls known as a segmentation gateway. ONTAP takes a 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.

Multifactor authentication

TR-4647: Multifactor authentication in ONTAP best practices and implementation guide
Learn about ONTAP's multifactor authentication capability for administrative access using System Manager, Active IQ Unified Manager and ONTAP secure shell (SSH) CLI authentication.

TR-4717: ONTAP SSH authentication with a common access card
Learn how to configure and test third-party SSH clients, in conjunction with ActivClient software, to authenticate an ONTAP storage administrator via the public key stored on a common access card (CAC) when it is configured in ONTAP.

Multitenancy

TR-4160: Secure multitenancy in ONTAP
Learn how to implement secure multitenancy using storage VMs in ONTAP, including design considerations and recommended practices.

Standards

TR-4401: PCI-DSS 4.0 and ONTAP
Learn how to validate a system against the PCI DSS 4.0 standard and meet the requirements of the controls that you apply to a NetApp ONTAP system.

Attribute-based access control

Attribute-based access control with ONTAP
Learn how to configure NFSv4.2 security labels and extended attributes (xattrs) to support role-based access control (RBAC) and attribute-based access control (ABAC), an authorization strategy that defines permissions based on user, resource, and environmental attributes.

NetApp solution for ransomware

Ransomware and NetApp's protection portfolio

Ransomware remains one of the most significant threats causing business interruption for organization in 2024. According to the Sophos State of Ransomware 2024, ransomware attacks affected 72% of their surveyed audience. Ransomware attacks have evolved to be more sophisticated and targeted, with threat actors employing advanced techniques like artificial intelligence to maximize their impact and profits.

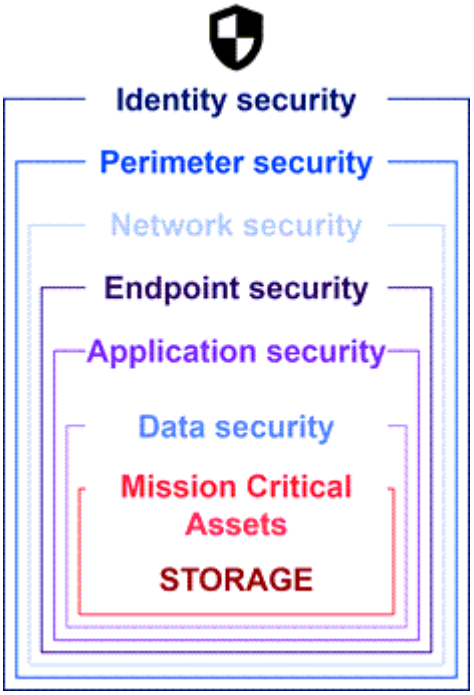
Organizations must look across their entire security posture from perimeter, network, identity, application, and where the data lives at the storage level and secure these layers. Adopting a data-centric approach to cyber protection at the storage layer is crucial in today's threat landscape. Although no single solution can thwart all attacks, using a portfolio of solutions, including partnerships and third parties, provides a layered defense.

The NetApp product portfolio provides various effective tools for visibility, detection, and remediation, helping you to spot ransomware early, prevent spread, and recover quickly, if necessary, to avoid costly downtime. Traditional layered defense solutions remain prevalent, as do third parties and partner solutions for visibility and detection. Effective remediation remains a crucial part of the response to any threat. The unique industry approach leveraging immutable NetApp Snapshot technology and SnapLock logical air gap solution is an industry differentiator and the industry best practice for ransomware remediation capabilities.

Beginning in July 2024, content from the technical report *TR-4572: NetApp Ransomware Protection*, which was previously published as a PDF, is available on docs.netapp.com.

Data is the primary target

Cybercriminals increasingly target data directly, recognizing its value. While perimeter, network, and application security are important, they can be bypassed. Focusing on protecting data at its source, the storage layer, provides a critical last line of defense. Gaining access to production data and encrypting or rendering it inaccessible is the objective of ransomware attacks. To get there, attackers must have already pierced existing defenses deployed by organizations today, from perimeter to application security.



Unfortunately, many organizations don't take advantage of security capabilities at the data layer. This is where NetApp ransomware protection portfolio comes in, protecting you at the last line of defense.

The real cost of ransomware

The ransom payment itself is not the largest monetary effect on a business. Although the payment is not insignificant, it pales in comparison to the downtime cost of suffering a ransomware incident.

Ransom payments are just one element of recovery costs when dealing with ransomware events. Excluding any ransoms paid, in 2024 organizations reported a mean cost to recover from a ransomware attack of $2.73M, an increase of almost $1M from the $1.82M reported in 2023 according to the 2024 Sophos State of Ransomware report. For organizations that rely heavily on IT availability, such as e-commerce, equities trading, and health care, costs can be 10 times higher or more.

Cyber insurance costs also continue to rise given the very real likelihood of a ransomware attack on insured companies.

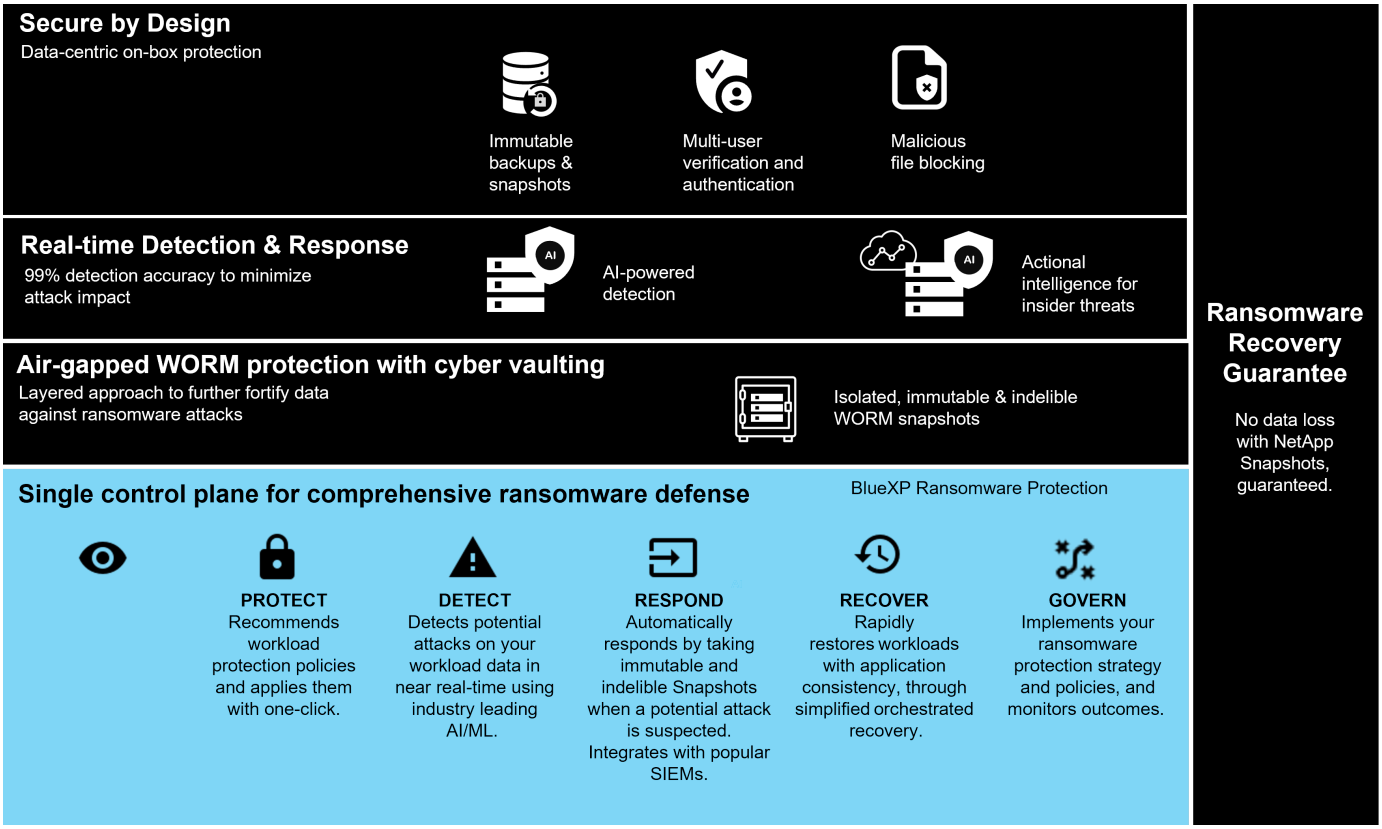
Ransomware protection at the data layer

NetApp understands your security posture is wide and deep across your organization from the perimeter to the where your data lives at the storage layer. Your security stack is complex and should provide security at every level of your technology stack.

Real-time protection at the data layer is even more important and has unique requirements. To be effective, solutions at this layer must offer these critical attributes:

- **Security by design** to minimize chance of successful attack
- **Real-time detection and response** to minimize impact of a successful attack
- **Air-gapped WORM protection** to isolate critical data backups
- **A single control plane** for comprehensive ransomware defense

NetApp can deliver all of this and more.



NetApp's ransomware protection portfolio

NetApp's built-in ransomware protection delivers real-time, robust, multi-faceted defense for your critical data. At its core, advanced AI-powered detection algorithms continuously monitor data patterns, swiftly identifying potential ransomware threats with 99% accuracy. Reacting quickly to attacks allows our storage to quickly snapshot data and secure the copies ensuring rapid recovery.

To further fortify data, NetApp's cyber vaulting capability isolates data with a logical air gap. By safeguarding critical data, we ensure rapid business continuity.

NetApp NetApp ransomware protection reduces operational burdens with a single control plane to intelligently coordinate and execute an end-to-end workload-centric ransomware defense, so you can identify and protect critical workload data at risk with a single click, accurately and automatically detect and respond to limit the impact of a potential attack, and recover workloads within minutes, not days, safeguarding your valuable workload data and minimizing costly disruption.

As a native, built-in ONTAP solution for protecting unauthorized access to your data, multi-admin verification (MAV) has a robust set of capabilities that ensure that operations such as deleting volumes, creating additional administrative users, or deleting snapshots can be executed only after approvals from at least a second designated administrator. This prevents compromised, malicious, or inexperienced administrators from making undesirable changes or deleting data. You can configure as many designated administrator approvers as you

want before a snapshot can be deleted.

NetApp ONTAP addresses the requirement for web-based multi-factor authentication (MFA) in System Manager and for SSH CLI authentication.

NetApp's ransomware protection offers peace of mind in an ever-evolving threat landscape. Its comprehensive approach not only defends against current ransomware variants but also adapts to emerging threats, providing long-term security for your data infrastructure.

Learn about other protection options

- Digital Advisor ransomware protection
- Data Infrastructure Insights Storage Workload Security
- FPolicy
- SnapLock and tamperproof snapshots

Ransomware recovery guarantee

NetApp offers a guarantee to restore snapshot data if a ransomware attack occurs. Our guarantee: If we can't help you restore your snapshot data, we'll make it right. The guarantee is available on new purchases of AFF A-Series, AFF C-Series, ASA, and FAS systems.

Learn more

- Recovery guarantee service description
- Ransomware recovery guarantee blog.

Related information

- NetApp Support site resources page
- NetApp product security

SnapLock and tamperproof snapshots for ransomware protection

A vital weapon in NetApp's Snap arsenal is SnapLock, which has proven highly effective in safeguarding against ransomware threats. By preventing unauthorized data deletion, SnapLock provides an additional layer of security, ensuring that critical data remains intact and accessible even in the event of malicious attacks.

SnapLock Compliance

SnapLock Compliance (SLC) provides indelible protection for your data. SLC prohibits data from being deleted even when an administrator attempts to re-initialize the array. Unlike other competitive products, SnapLock Compliance is not vulnerable to social engineering hacks through those products' support teams. Data protected by SnapLock Compliance volumes is recoverable until that data has reached its expiration date.

To enable SnapLock, an ONTAP One license is required.

Learn more

- Snaplock documentation

Tamperproof snapshots

Tamperproof Snapshot (TPS) copies provide a convenient and fast way to protect data from malicious acts. Unlike SnapLock Compliance, TPS is typically used on primary systems where the user can protect the data for a determined time and left locally for fast recoveries or where data does not need to be replicated off of the primary system. TPS uses SnapLock technologies to prevent the primary snapshot from being deleted even by an ONTAP administrator using the same SnapLock retention expiration period. Snapshot deletion is prevented even if the volume is not SnapLock enabled, although snapshots do not have the same indelible nature of SnapLock Compliance volumes.

To make snapshots tamperproof, an ONTAP One license is required.

Learn more

- Lock a snapshot for protection against ransomware attacks.

FPolicy file blocking

FPolicy blocks unwanted files from being stored on your enterprise-grade storage appliance. FPolicy also gives you a way to block known ransomware file extensions. A user still has full access permissions to the home folder, but FPolicy doesn't allow a user to store files your administrator marks as blocked. It doesn't matter if those files are MP3 files or known ransomware file extensions.

Block malicious files with FPolicy native mode

NetApp FPolicy native mode (an evolution of the name, File Policy) is a file-extension blocking framework that allows you to block unwanted file extensions from ever entering your environment. It has been part of ONTAP for over a decade and is incredibly useful in helping you protect against ransomware. This Zero Trust engine is valuable because you get extra security measures beyond access control list (ACL) permissions.

In ONTAP System Manager and the NetApp Console, a list of over 3000 file extensions is available for reference.

> Some extensions might be legitimate in your environment and blocking them can lead to unexpected issues. Create your own list that is appropriate for your environment before configuring native FPolicy.

FPolicy native mode is included in all ONTAP licenses.

Learn more

- Blog: Fighting Ransomware: Part Three — ONTAP FPolicy, another powerful native (aka free) tool

Enable user and entity behavior analytics (UEBA) with FPolicy external mode

FPolicy external mode is a file activity notification and control framework that provides visibility of file and user activity. These notifications can be used by an external solution to perform AI-based analytics to detect malicious behavior.

FPolicy external mode can also be configured to wait for approval from the FPolicy server before allowing specific activities to go through. Multiple policies like this can be configured on a cluster, giving you great flexibility.

FPolicy servers must be responsive to FPolicy requests if configured to provide approval; otherwise, storage system performance might be negatively impacted.

FPolicy external mode is included in all ONTAP licenses.

Learn more

- Blog: Fighting Ransomware: Part Four — UBA and ONTAP with FPolicy external mode.

Data Infrastructure Insights Storage Workload Security

Storage Workload Security (SWS) is a feature of NetApp Data Infrastructure Insights that greatly enhances the security posture, recoverability, and accountability of an ONTAP environment. SWS takes a user-centric approach, tracking all file activity from every authenticated user in the environment. It uses advanced analytics to establish normal and seasonal access patterns for every user. These patterns are used to quickly identify suspicious behavior without the need for ransomware signatures.

When SWS detects a potential ransomware, or data deletion, it can take automatic actions such as:

- Take a snapshot of the affected volume.
- Block the user account and IP address that is suspected of malicious activity.
- Send an alert to admins.

Because it can take automated action to quickly stop an insider threat as well as track every file activity, SWS makes recovery from a ransomware event much simpler and faster. With advanced auditing and forensics tools built in, users can immediately see what volumes and files were affected by an attack, which user account the attack came from, and what malicious action was performed. Automatic snapshots mitigate the damage and accelerate file restoration.

Alerts from ONTAP's Autonomous Ransomware Protection (ARP) are also visible in SWS, providing a single interface for customers using both ARP and SWS to protect from ransomware attacks.

Learn more

- NetApp Data Infrastructure Insights

NetApp ONTAP built-in on-box AI-based detection and response

As ransomware threats become more and more sophisticated, so should your defense

mechanisms. NetApp's autonomous ransomware protection (ARP) is powered by AI with intelligent anomaly detection that is built in to ONTAP. Turn it on to add another layer of defense to your cyber resiliency.

ARP and ARP/AI are configurable through the ONTAP built-in management interface, System Manager, and enabled on a per-volume basis.

Autonomous Ransomware Protection (ARP)

Autonomous Ransomware Protection (ARP), another native built-in ONTAP solution since 9.10.1, looks at NAS storage volume workload file activity and data entropy to automatically detect potential ransomware. ARP provides administrators with real-time detection, insights, and a data recovery point for unprecedented on-box potential ransomware detection.

For ONTAP 9.15.1 and earlier versions that support ARP, ARP starts in learning mode to learn typical workload data activity. This can take seven days for most environments. After learning mode is complete, ARP will automatically switch to active mode and start looking for abnormal workload activity that might potentially be ransomware.

If abnormal activity is detected, an automatic snapshot is immediately taken, which provides a restoration point as close as possible to the time of attack with minimal infected data. Simultaneously, an automatic alert (configurable) is generated that allows administrators to see the abnormal file activity so that they can determine whether the activity is indeed malicious and take appropriate action.

If the activity is an expected workload, administrators can easily mark it as a false positive. ARP learns this change as normal workload activity and no longer flags it as a potential attack going forward.

To enable ARP, an ONTAP One license is required.

Learn more

- Autonomous Ransomware Protection

Autonomous Ransomware Protection/AI (ARP/AI)

Introduced as a tech preview in ONTAP 9.15.1, ARP/AI takes NAS storage systems on-box real-time detection to the next level. The new AI-powered detection technology is trained on over a million files and various known ransomware attacks. In addition to the signals used in ARP, ARP/AI also detects header encryption. The AI power and additional signals allow ARP/AI to deliver better than 99% detection accuracy. This has been validated by SE Labs, an independent test lab that gave ARP/AI its highest AAA rating.

Because training the models continuously happens in the cloud, ARP/AI does not require a learning mode. It is active the moment it is turned on. Continuous training also means that ARP/AI is always validated against new ransomware attack types as they arise. ARP/AI also comes with auto-update capabilities that deliver new parameters to all customers to keep ransomware detection up to date. All other detection, insight, and data recovery point capabilities of ARP are maintained for ARP/AI.

To enable ARP/AI, an ONTAP One license is required.

Learn more

- Blog: NetApp's AI-based real-time ransomware detection solution achieves AAA rating

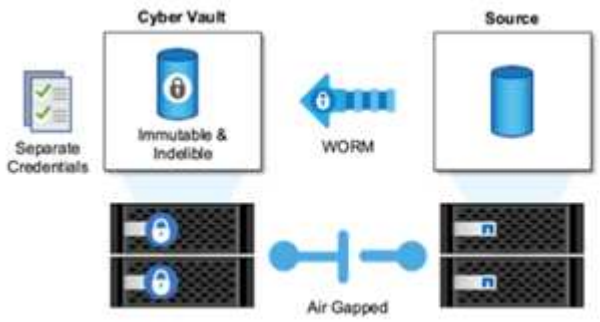
Air-gapped WORM protection with cyber vaulting in ONTAP

NetApp's approach to a cyber vault is a purpose-built reference architecture for a logically air-gapped cyber vault. This approach takes advantage of security hardening and compliance technologies, such as SnapLock, to allow for immutable and indelible snapshots.

Cyber vaulting with SnapLock Compliance and a logical air gap

A growing trend is for attackers to destroy the backup copies and, in some cases, even encrypt them. That is why many in the cybersecurity industry recommend using air gap backups as part of an overall cyber resiliency strategy.

The problem is that traditional air gaps (tape and offline media) can significantly increase restoration time, thus increasing downtime and the overall associated costs. Even a more modern approach to an air-gap solution can prove problematic. For example, if the backup vault is temporarily opened to receive new backup copies and then disconnects and closes its network connection to primary data to once again be "air gapped", an attacker could take advantage of the temporary opening. During the time the connection is online, an attacker could strike to compromise or destroy the data. This type of configuration also generally adds unwanted complexity. A logical air gap is an excellent substitute for a traditional or modern air gap because it has the same security protection principles while keeping the backup online. With NetApp, you can solve the complexity of tape or disk air gapping with logical air gapping, which can be achieved with immutable snapshots and NetApp SnapLock Compliance.



NetApp released the SnapLock feature more than 10 years ago to address the requirements of data compliance, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and other regulatory data rules. You can also vault primary snapshots to SnapLock volumes so that the copies can be committed to WORM, preventing deletion. There are two SnapLock license versions: SnapLock Compliance and SnapLock Enterprise. For ransomware protection, NetApp recommends SnapLock Compliance because you can set a specific retention period during which snapshots are locked and cannot be deleted, even by ONTAP administrators or NetApp Support.

Learn more

- Blog: ONTAP cyber vault overview

Tamperproof snapshots

While leveraging SnapLock Compliance as a logical air gap provides the ultimate protection in preventing attackers from deleting your backup copies, it does require you to move the snapshots using SnapVault to a secondary SnapLock-enabled volume. As a result, many customers deploy this configuration on secondary storage across the network. This can lead to longer restoration times versus restoring a primary volume Snapshot on primary storage.

Beginning in ONTAP 9.12.1, tamperproof snapshots provide near SnapLock Compliance level protection for your snapshots on primary storage and in primary volumes. There is no need to vault the snapshot using SnapVault to a secondary SnapLocked volume. Tamperproof snapshots use SnapLock technology to prevent the primary snapshot from being deleted, even by a full ONTAP administrator using the same SnapLock retention expiration period. This allows for quicker restore times and the ability for a FlexClone volume to be backed up by a tamperproof, protected snapshot, something you cannot do with a traditional SnapLock Compliance vaulted snapshot.

The major difference between SnapLock Compliance and tamperproof snapshots is that SnapLock Compliance does not allow the ONTAP array to be initialized and wiped if SnapLock Compliance volumes exist with vaulted snapshots that have not yet reached their expiration date. To make snapshots tamperproof, a SnapLock Compliance license is required.

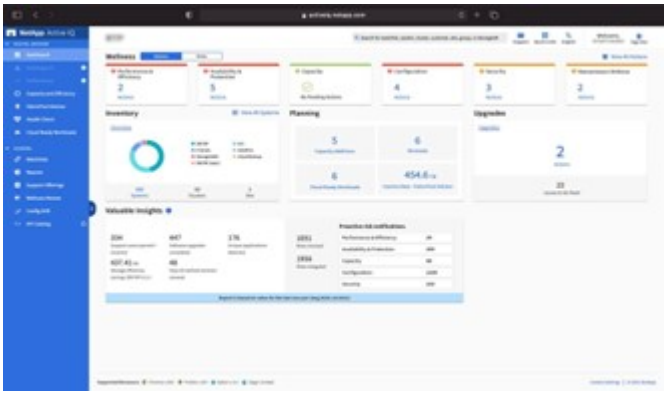
Learn more

- Lock a snapshot for protection against ransomware attacks

Digital Advisor ransomware protection

Digital Advisor powered by Active IQ simplifies the proactive care and optimization of NetApp storage with actionable intelligence for optimal data management. Fueled by telemetry data from our highly diverse installed base, it uses advanced AI and ML techniques to uncover opportunities to reduce risk and improve the performance and efficiency of your storage environment.

Not only can NetApp Digital Advisor help eliminate security vulnerabilities, but it also provides insights and guidance specific to protecting against ransomware. A dedicated wellness card shows the actions needed and the risks addressed, so you can be sure that your systems are meeting those best practices recommendations.



Risks and actions tracked on the Ransomware Defense Wellness page include the following (and much more):

- Volume snapshot count is low, decreasing potential ransomware protection.
- FPolicy is not enabled for all storage virtual machines (SVMs) configured for NAS protocols.

To see ransomware protection in action, see Digital Advisor.

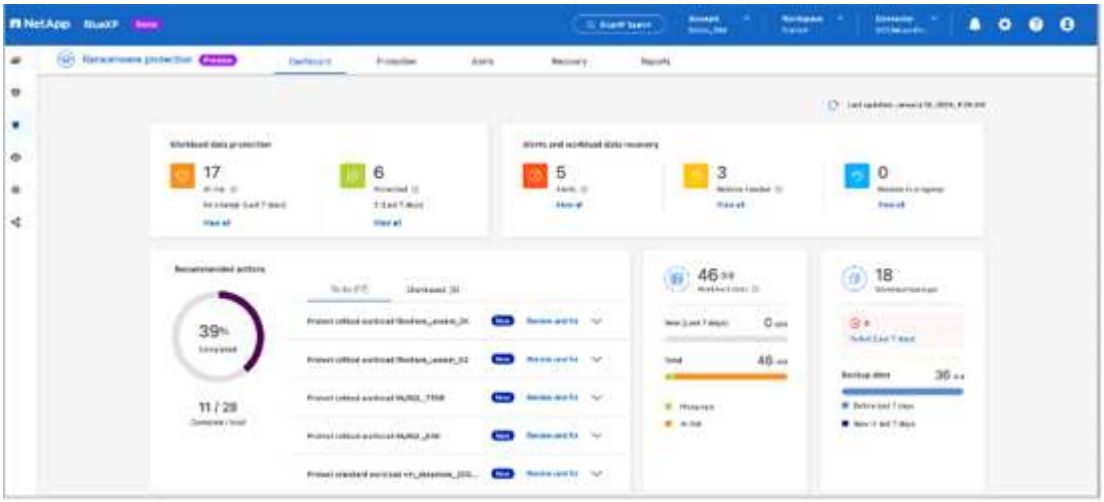
Comprehensive resilience with NetApp ransomware protection

It is important for ransomware detection to occur as early as possible so that you can prevent the spread and avoid costly downtime. An effective ransomware detection

strategy, however, should include more than a single layer of protection. NetApp's ransomware protection takes a comprehensive approach that includes real-time, on-box capabilities extending to data services using the NetApp Console and an isolated, layered solution for cyber vaulting.

NetApp ransomware protection

The NetApp Console is a single control plane to intelligently orchestrate a comprehensive, workload-centric ransomware defense. NetApp ransomware protection brings together the powerful cyber-resilience features of ONTAP, such as ARP, FPolicy, and tamperproof snapshots, and NetApp data services, such as NetApp Backup and Recovery. It also adds recommendations and guidance with automated workflows to provide an end-to-end defense through a single UI. It operates at the workload level to ensure that the applications that run your business are protected and can be recovered as quickly as possible in case of an attack.



Customer benefits:

- Assisted ransomware preparedness reduces operational overhead and improves efficacy
- AI/ML-powered anomaly detection delivers greater accuracy and faster response to contain risk
- Guided application-consistent restoration allows you to recover workloads more easily and within minutes

NetApp ransomware protection makes these NIST functions easier to achieve:

- Automatically **discover** and prioritize data in NetApp storage **with a focus on top application-based workloads**.
- **One-click protection** of top-workload data backup, immutable, secure configuration, malicious file blocking, and different security domain.
- **Accurately detect** ransomware as **quickly** as possible using **next-generation AI-based anomaly detection.**
- Automated response and workflows and integration with top **SIEM and XDR solutions.**
- Rapidly restore data using a simplified **orchestrated recovery** to accelerate application uptime.
- Implement your ransomware protection **strategy** and **policies**, and **monitor outcomes**.

NetApp and Zero Trust

NetApp and Zero Trust

Zero Trust traditionally has been a network-centric approach of architecting micro core and perimeter (MCAP) to protect data, services, applications, or assets with controls known as a segmentation gateway. NetApp ONTAP is taking a 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.

Beginning in July 2024, content from the technical report *TR-4829: NetApp and Zero Trust: Enabling a data-centric Zero Trust model*, which was previously published as a PDF, is available on docs.netapp.com.

Data is the most important asset your organization has. Insider threats are the cause of 18% of data breaches, according to the 2022 Verizon Data Breach Investigations Report. Organizations can ramp up their vigilance by deploying industry-leading Zero Trust controls around data with NetApp ONTAP data management software.

What Is Zero Trust?

The Zero Trust model 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 concept of a secure outer perimeter is obsolete. Entities that are trusted and allowed to successfully authenticate through the perimeter can then make the organization vulnerable to attacks. Insiders, by definition, are already inside the secure perimeter. Employees, contractors, and partners are insiders, and they must be enabled to operate with appropriate controls for performing their roles within your organization's infrastructure.

Zero Trust was mentioned as a technology that offers promise to the DoD in September 2019 FY19-23 DoD Digital Modernization Strategy. It defines Zero Trust as, "A cybersecurity strategy that embeds security throughout the architecture for the purpose of stopping data breaches. This data-centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi-attribute based confidence levels that enable authentication and authorization policies under the concept of least privileged access. Implementing zero trust requires rethinking how we use existing infrastructure to implement security by design in a simpler and more efficient way while enabling unimpeded operations."

In August of 2020, the NIST published Special Pub 800-207 Zero Trust Architecture (ZTA). ZTA focuses on protecting resources, not network segments, because the network location is no longer seen as the prime component of the security posture of the resource. Resources are data and computing. ZTA strategies are for enterprise network architects. ZTA introduces some new terminology from the original Forrester concepts. Protection mechanisms called the policy decision point (PDP) and the policy enforcement point (PEP) are analogous to a Forrester segmentation gateway. ZTA introduces four deployment models:

- Device-agent or gateway-based deployment
- Enclave-based deployment (somewhat analogous to the Forrester MCAP)
- Resource portal-based deployment
- Device application sandboxing

For the purposes of this documentation, we use Forrester Research concepts and terminology rather than the NIST ZTA.

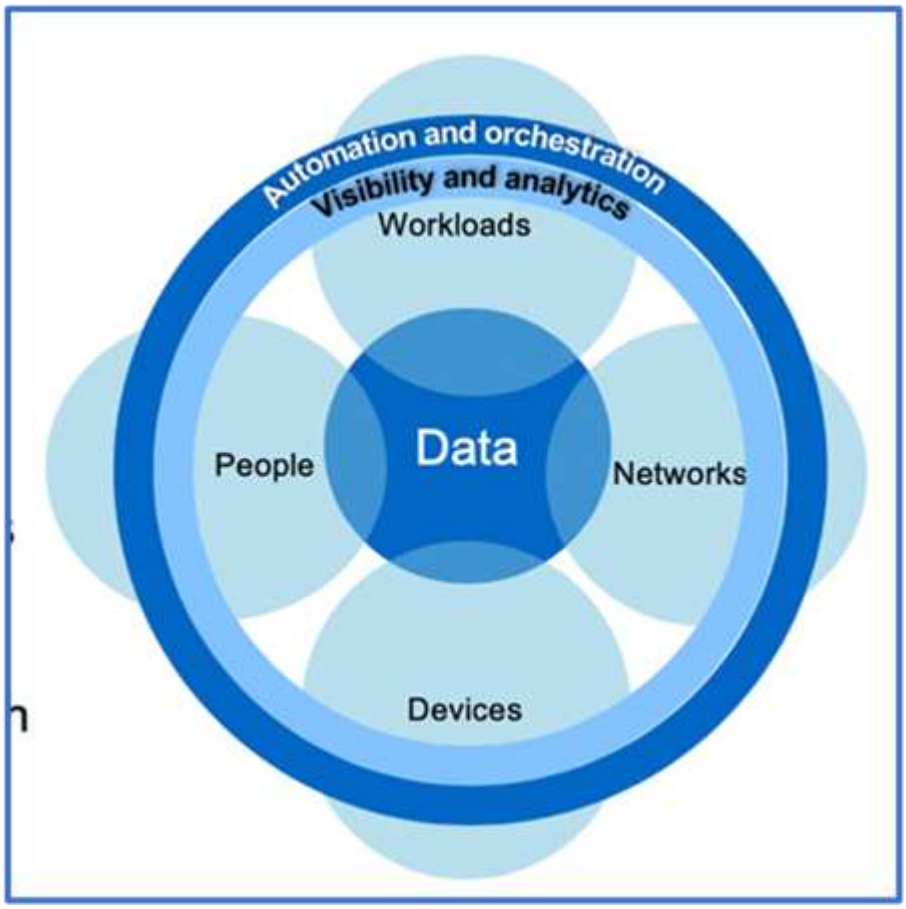
Security resources

For information about reporting vulnerabilities and incidents, NetApp security responses, and customer confidentiality, see the NetApp security portal.

Architect a data-centric approach to Zero Trust with ONTAP

A Zero Trust network is defined by a data-centric approach in which the security controls should be as close to the data as possible. The capabilities of ONTAP, coupled with the NetApp FPolicy partner ecosystem, can provide the necessary controls for the data-centric Zero Trust model.

ONTAP is security-rich data management software from NetApp, and the FPolicy Zero Trust Engine is an industry-leading ONTAP capability that provides a granular, file-based event notification interface. NetApp FPolicy partners can use this interface to provide greater illumination of data access within ONTAP.



Architect a Zero Trust data-centric MCAP

To architect a data-centric Zero Trust MCAP, follow these steps:

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.

Identify the location of all organizational data

The FPolicy capability of ONTAP coupled with the NetApp Alliance Partner ecosystem of FPolicy partners lets you identify where your organization's data exists and who has access to it. This is done with user behavioral analytics, which identifies whether data access patterns are valid. More details about user behavioral analytics are discussed in Monitor and log all access. If you do not understand where your data is and who has access to it, user behavioral analytics can provide a baseline to build classification and policy from empirical observations.

Classify your data

In the terminology of the Zero Trust model, classification of data involves identification of toxic data. Toxic data is sensitive data that is not intended to be exposed outside an organization. Disclosure of toxic data could violate regulatory compliance and damage an organization's reputation. In terms of regulatory compliance, toxic data includes cardholder data for the Payment Card Industry Data Security Standard (PCI-DSS), personal data for the EU General Data Protection Regulation (GDPR), or healthcare data for the Health Insurance Portability and Accountability Act (HIPAA). You can use NetApp NetApp Data Classification (formerly known as Cloud Data Sense), an AI-driven toolkit, to automatically scan, analyze, and categorize your data.

Securely dispose of data you no longer require

After classifying your organization's data, you might discover that some of your data is no longer necessary or relevant to the function of your organization. The retention of unnecessary data is a liability, and such data should be deleted. For an advanced mechanism to cryptographically erase data, see the description of secure purge in Data at rest encryption.

Understand what roles should have access to the data classifications and apply the principle of least privilege to enforce access controls

Mapping access to sensitive data and applying the principle of least privilege means giving people in your organization access to only the data required to perform their jobs. This process involves role-based access control (RBAC), which applies to data access and administrative access.

With ONTAP, a storage virtual machine (SVM) can be used to segment organizational data access by tenants within an ONTAP cluster. RBAC can be applied to data access as well as administrative access to the SVM. RBAC can also be applied at the cluster administrative level.

In addition to RBAC, you can use ONTAP multi-admin verification (MAV) to require one or more administrators to approve commands such as `volume delete` or `volume snapshot delete`. Once MAV is enabled, modifying or disabling MAV requires MAV administrator approval.

Another way of protecting snapshots is with ONTAP snapshot locking. Snapshot locking is a SnapLock capability where snapshots are rendered indelible manually or automatically with a retention period on the volume snapshot policy. Snapshot locking is also referred to as tamper-proof snapshot locking. The purpose of snapshot locking is to prevent rogue or untrusted administrators from deleting snapshots on the primary and secondary ONTAP

systems. Rapid recovery of locked snapshots on primary systems can be achieved in order to restore volumes corrupted by ransomware.

Use multifactor authentication for administrative access and data access

In addition to cluster administrative RBAC, multifactor authentication (MFA) can be deployed for ONTAP web administrative access and Secure Shell (SSH) command-line access. MFA for administrative access is a requirement for U.S. public sector organizations or those that must follow the PCI-DSS. MFA makes it impossible for an attacker to compromise an account using only a username and password. MFA requires two or more independent factors to authenticate. An example of two-factor authentication is something a user possesses, such as a private key, and something a user knows, such as a password. Administrative web access to ONTAP System Manager or ActiveIQ Unified Manager is enabled by Security Assertion Markup Language (SAML) 2.0. SSH command-line access uses chained two-factor authentication with a public key and password.

You can control user and machine access through APIs with the identity and access management capabilities in ONTAP:

- User:
  - **Authentication and authorization.** Through NAS protocol capabilities for SMB and NFS.
  - **Audit.** Syslog of access and events. Detailed audit logging of CIFS protocol to test authentication and authorization policies. Fine granular FPolicy auditing of detailed NAS access at the file level.
- Device:
  - **Authentication.** Certificate-based authentication for API access.
  - **Authorization.** Default or custom role-based access control (RBAC).
  - **Audit.** Syslog of all actions taken.

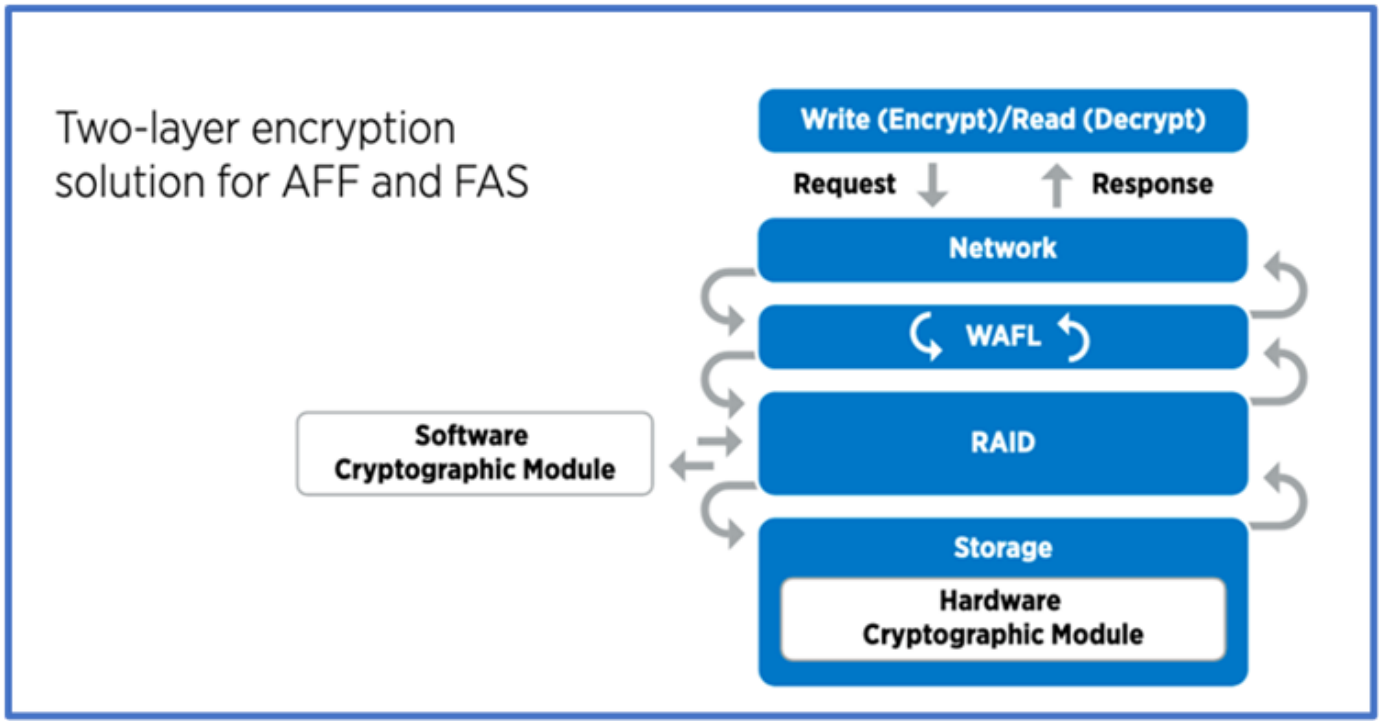
Use encryption for data at rest and data in flight

Data at rest encryption

Each day, there are new requirements for mitigating storage-system risks and infrastructure gaps when an organization repurposes drives, returns defective drives, or upgrades to larger drives by selling or trading them in. As administrators and operators of data, storage engineers are expected to manage and maintain data securely throughout its lifecycle. NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE), and NetApp Aggregate Encryption help you encrypt all your data at rest all the time, whether or not it is toxic, and without affecting daily operations. NSE is an ONTAP hardware data-at-rest solution that makes use of FIPS 140-2 level 2 validated self-encrypting drives. NVE and NAE are an ONTAP software data-at-rest solution that makes use of the FIPS 140-2 level 1 validated NetApp Cryptographic Module. With NVE and NAE, either hard drives or solid-state drives can be used for data-at-rest encryption. Plus, NSE drives can be used to provide a native, layered encryption solution that provides encryption redundancy and additional security. If one layer is breached, then the second layer still secures the data. These capabilities make ONTAP well positioned for quantum-ready encryption.

NVE also provides a capability called secure purge that cryptographically removes toxic data from data spills when sensitive files are written to a non-classified volume.

Either the Onboard Key Manager (OKM), which is the key manager built into ONTAP, or approved third-party external key managers can be used with NSE and NVE to securely store keying material.



As seen in the figure above, hardware and software based encryption can be combined. This capability led to the validation of ONTAP into the NSA's commercial solutions for classified program that allows for storage of top secret data.

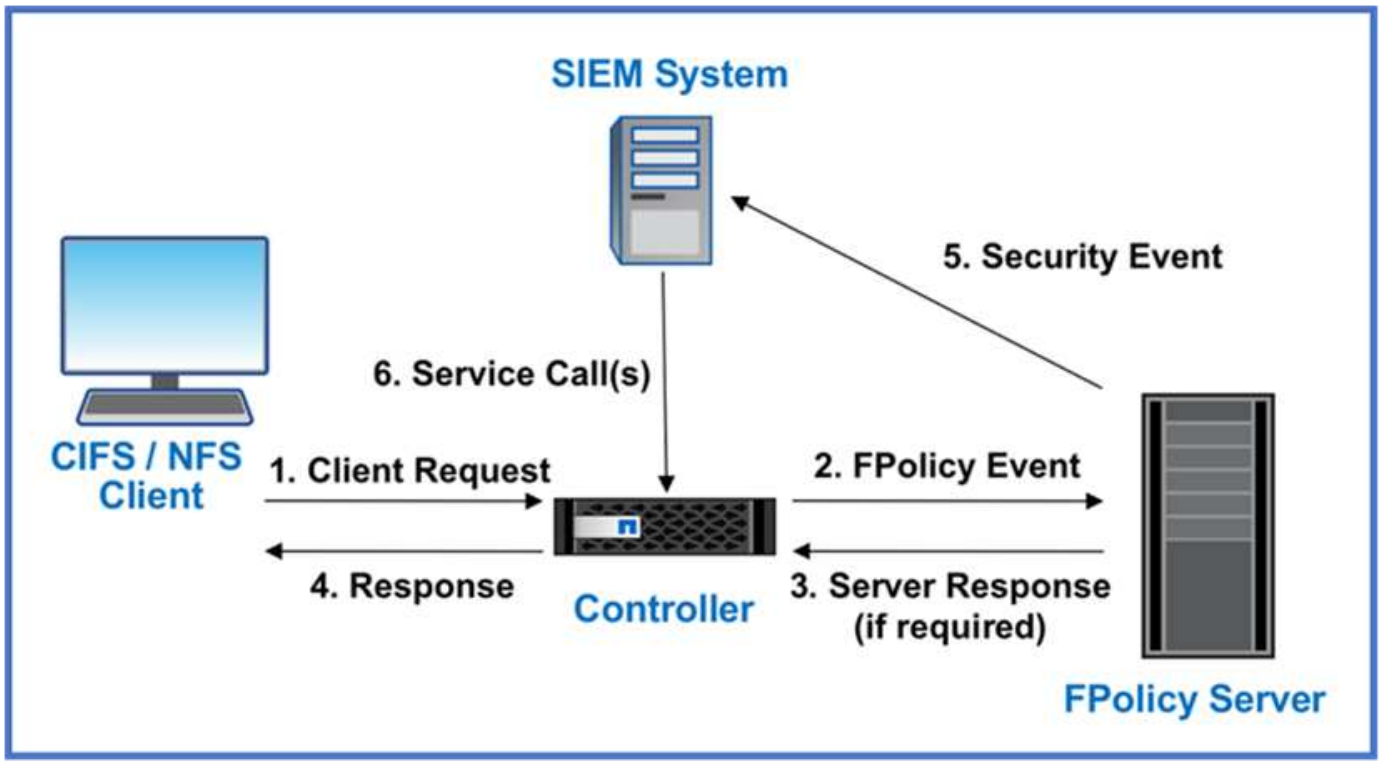
Data-in-flight encryption

ONTAP data-in-flight encryption protects user data access and control-plane access. User data access can be encrypted by SMB 3.0 encryption for Microsoft CIFS share access or by krb5P for NFS Kerberos 5. User data access can also be encrypted with IPsec for CIFS, NFS, and iSCSI. Control plane access is encrypted with Transport Layer Security (TLS). ONTAP provides FIPS compliance mode for control plane access, which enables FIPS-approved algorithms and disables algorithms that are not FIPS approved. Data replication is encrypted with cluster peer encryption. This provides encryption for the ONTAP SnapVault and SnapMirror technologies.

Monitor and log all access

After RBAC policies are in place, you must deploy active monitoring, auditing, and alerting. The FPolicy Zero Trust Engine from NetApp ONTAP, coupled with the NetApp FPolicy partner ecosystem, provides the necessary controls for the data-centric Zero Trust model. NetApp ONTAP is security-rich data management software, and FPolicy is an industry-leading ONTAP capability that provides a granular file-based event notification interface. NetApp FPolicy partners can use this interface to provide greater illumination of data access within ONTAP. The FPolicy capability of ONTAP, coupled with the NetApp Alliance Partner ecosystem of FPolicy partners, lets you identify where your organization's data exists and who has access to it. This is done with user behavioral analytics, which identifies whether data access patterns are valid. User behavioral analytics can be used to alert for suspicious or aberrant data access that is out of the normal pattern and, if necessary, take actions to deny access.

FPolicy partners are moving beyond user behavioral analytics toward machine learning (ML) and artificial intelligence (AI) for greater event fidelity and fewer, if any, false positives. All events should be logged to a syslog server or to a security information and event management
(SIEM) system that can also employ ML and AI.



NetApp's DII Storage Workload Security makes use of the FPolicy interface and user behavioral analytics on both cloud and on-premises ONTAP storage systems to give you real-time alerts of malicious user behavior. Storage Workload Security protects organizational data from being misused by malicious or compromised users through advanced machine learning and anomaly detection. Storage Workload Security can identify ransomware attacks or other miscreant behaviors, invoke snapshots and quarantine malicious users. Storage Workload Security also has a forensics capability to view in great detail user and entity activities. Storage Workload Security is a part of NetApp Data Infrastructure Insights.

In addition to Storage Workload Security, ONTAP has an onboard ransomware detection capability known as Autonomous Ransomware Protection (ARP). ARP uses machine learning to determine if abnormal file activity indicates a ransomware attack is underway and invokes a snapshot and alert to administrators. Storage Workload Security integrates with ONTAP to receive ARP events and provides an additional analytics and automatic responses layer.

Learn more about the commands described in this procedure in the ONTAP command reference.

NetApp security automation and orchestration controls external to ONTAP

Automation allows you to perform a process or procedure with minimal human assistance. Automation enables organizations to scale Zero Trust deployments far beyond manual procedures to defend against miscreant activities that are also automated.

Ansible is an open-source software provisioning, configuration management, and application-deployment tool. It runs on many Unix-like systems, and it can configure both Unix-like systems as well as Microsoft Windows. It includes its own declarative language to describe system configuration. Ansible was written by Michael DeHaan and acquired by Red Hat in 2015. Ansible is agentless, temporarily connecting remotely through SSH or Windows Remote Management (allowing remote PowerShell execution) to perform tasks. NetApp has developed more than 150 Ansible modules for ONTAP software, enabling further integration with the Ansible automation framework. Ansible modules for NetApp deliver a set of instructions for how to define the desired

state and relay it to the target NetApp environment. Modules are built to support tasks like setting up licensing, creating aggregates and storage virtual machines, creating volumes, and restoring snapshots to name a few. An Ansible role has been published on GitHub specific to the NetApp DoD Unified Capabilities (UC) Deployment Guide.

By using the library of available modules, users can easily develop Ansible playbooks and customize them to their own applications and business needs to automate mundane tasks. After a playbook is written, you can run it to execute the specified task, which saves time and improves productivity. NetApp has created and shared sample playbooks that can be used directly or customized for your needs.

Data Infrastructure Insights is an infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Data Infrastructure Insights, you can monitor, troubleshoot, and optimize all your resources, including your public cloud instances and your private data centers. Data Infrastructure Insights can reduce mean time to resolution by 90% and prevent 80% of cloud issues from affecting end users. It can also reduce cloud infrastructure costs by an average of 33% and reduce your exposure to insider threats by protecting your data with actionable intelligence. The Storage Workload Security capability of Data Infrastructure Insights enables user behavioral analytics with AI and ML to alert when aberrant user behaviors occur due to an insider threat. For ONTAP, Storage Workload Security makes use of the Zero Trust FPolicy engine.

Zero Trust and hybrid cloud deployments

NetApp is the data authority for the hybrid cloud. NetApp offers a variety of options for extending on-premises data management systems to the hybrid cloud with Amazon Web Services (AWS), Microsoft Azure, Google Cloud, and other leading cloud providers. NetApp hybrid-cloud solutions support the same Zero Trust security controls that are available with on-premises ONTAP systems and ONTAP Select software-defined storage.

You can easily expand capacity in public clouds without typical CAPEX constraints by using enterprise-class, cloud-native file services for AWS (FSxN), Google Cloud (GCNV), and Azure NetApp Files for Microsoft Azure. Ideal for data-intensive workloads such as analytics and DevOps, these cloud data services combine elastic, on-demand storage as a service from NetApp with ONTAP data management in a fully managed offering.

ONTAP enables the movement of data between your on-premises ONTAP systems and AWS, Google Cloud, or Azure storage environment with NetApp SnapMirror data replication software.

Attribute-based access control

Attribute-based access control with ONTAP

Beginning with 9.12.1, you can configure ONTAP with NFSv4.2 security labels and extended attributes (xattrs) to support role-based access control (RBAC) with attributes and attribute-based access control (ABAC).

ABAC is an authorization strategy that defines permissions based on user attributes, resource attributes, and environmental conditions. The integration of ONTAP with NFS v4.2 security labels and xattrs complies with NIST standards for ABAC solutions, as set forth in NIST Special Publication 800-162.

You can use NFS v4.2 security labels and xattrs to assign files user-defined attributes and labels. ONTAP can integrate with ABAC-oriented identity and access management software to enforce granular file and folder access control policies based on these attributes and labels.

Related information

- Approaches to ABAC with ONTAP
- NFS in NetApp ONTAP: Best practice and implementation guide

Approaches to attribute-based access control (ABAC) in ONTAP

ONTAP provides several approaches you can use to achieve file-level attribute-based access control (ABAC), including NFS v4.2 security labels and extended attributes (xattrs) using NFS.

NFS v4.2 security labels

Beginning with ONTAP 9.9.1, the NFS v4.2 feature called Labeled NFS is supported.

NFS v4.2 security labels are a way to manage granular file and folder access by using SELinux labels and Mandatory Access Control (MAC). These MAC labels are stored with files and folders, and they work in conjunction with UNIX permissions and NFS v4.x ACLs.

Support for NFS v4.2 security labels means that ONTAP now recognizes and understands the NFS client's SELinux label settings. NFS v4.2 security labels are covered in RFC-7204.

Use cases for NFS v4.2 security labels include the following:

- MAC labeling of virtual machine (VM) images
- Data security classification for the public sector (secret, top secret, and other classifications)
- Security compliance
- Diskless Linux

Enable NFS v4.2 security labels

You can enable or disable NFS v4.2 security labels with the following command (advanced privilege required):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Learn more about `vserver nfs modify` in the ONTAP command reference.

Enforcement modes for NFS v4.2 security labels

Beginning with ONTAP 9.9.1, ONTAP supports the following enforcement modes:

- **Limited Server Mode**: ONTAP cannot enforce the labels but can store and transmit them.

  The ability to change MAC labels is up to the client to enforce.

- **Guest Mode**: If the client is not labeled NFS-aware (v4.1 or lower), MAC labels are not transmitted.

  ONTAP does not currently support Full Mode (storing and enforcing MAC labels).

NFS v4.2 security labels examples

The following example configuration demonstrates concepts using Red Hat Enterprise Linux release 9.3 (Plow).

The user `jrsmith`, created based on John R. Smith's credentials, has the following account privileges:

- Username = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith) context=user_u:user_r:user_t:s0`

There are two roles: the admin account that is a privileged user and user `jrsmith` as described in the following MLS privileges table:

Users	Role	Type	Levels
`admins`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

In this example environment, user `jrsmith` has access to files at the levels `s0` to `s3`. We can enhance the existing security classifications, as outlined below, to ensure that administrators do not have access to user-specific data.

- s0 = privilege admin user data
- s0 = unclassified data
- s1 = confidential
- s2 = secret data
- s3 = top secret data

NFS v4.2 security labels example with MCS

In addition to Multi-Level Security (MLS), another capability called Multi-Category Security (MCS) allows you to define categories such as projects.

NFS security label	Value
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Extended attributes (xattrs)

Beginning with ONTAP 9.12.1, ONTAP supports xattrs. xattrs allow metadata to be associated with files and directories beyond what is provided by the system, such as access control lists (ACLs) or user-defined attributes.

To implement xattrs, you can use `setfattr` and `getfattr` command-line utilities in Linux. These tools provide a powerful way to manage additional metadata for files and directories. They should be used with care, as improper use can lead to unexpected behavior or security issues. Always refer to the `setfattr` and `getfattr` man pages or other reliable documentation for detailed usage instructions.

When xattrs is enabled on an ONTAP filesystem, users can set, modify, and retrieve arbitrary attributes on files. These attributes can be used to store additional information about the file that is not captured by the standard set of file attributes, such as access control information.

There are several requirements and limits for using xattrs in ONTAP:

- Red Hat Enterprise Linux 8.4 or later
- Ubuntu 22.04 or later
- Each file can have up to 128 xattrs
- Xattr keys are limited to 255 bytes
- The combined key or value size is 1,729 bytes per xattr
- Directories and files can have xattrs
- To set and retrieve xattrs, `w` or write mode bits must be enabled for the user and group

Xattrs are utilized within the user namespace and do not carry any intrinsic significance to ONTAP itself. Instead, their practical applications are determined and managed exclusively by the client-side application that interacts with the file system.

Xattr use case examples:

- Recording the name of the application responsible for creating a file
- Maintaining a reference to the email message from which a file was obtained
- Establishing a categorization framework for organizing file objects
- Labeling files with the URL of their original download source

Commands for managing xattrs

- `setfattr` sets an extended attribute of a file or directory:

  ```
  setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
  ```

  Sample command:

  ```
  setfattr -n user.comment -v test example.txt
  ```

- `getfattr` retrieves the value of a specific extended attribute or lists all extended attributes of a file or directory:

  Specific attribute:
  ```
  getfattr -n <attribute_name> <file or directory name>
  ```

  All attributes:
  ```
  getfattr <file or directory name>
  ```

  Sample command:

```
getfattr -n user.comment example.txt
```

Xattr key value pair examples

The following table shows two xattr key value pair examples:

xattr	Value
`user.digitalIdentifier`	`CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US`
`user.countryOfAffiliations`	`USA`

User permissions with ACE for xattrs

An access control entry (ACE) is a component within an ACL that defines the access rights or permissions granted to an individual user or a group of users for a specific resource, such as a file or directory. Each ACE specifies the type of access allowed or denied and is associated with a particular security principal (user or group identity).

Access Control Entry (ACE) required for xattrs

- Retrieve xattr: The permissions required for a user to read the extended attributes of a file or directory. The "R" signifies that read permission is necessary.
- Set xattrs: The permissions needed to modify or set the extended attributes. "a," "w," and "T" represent different examples of permissions, such append, write, and a specific permission related to xattrs.
- Files: Users need append, write, and potentially a special permission related to xattrs to set extended attributes.
- Directories: A specific permission "T" is required to set extended attributes.

File type	Retrieve xattr	Set xattrs
File	R	a,w,T
Directory	R	T

Integration with ABAC identity and access control software

To fully harness the capabilities of ABAC, ONTAP can integrate with an ABAC-oriented identity and access management software.

In an ABAC system, the Policy Enforcement Point (PEP) and Policy Decision Point (PDP) play crucial roles. The PEP is responsible for enforcing access control policies, while the PDP makes the decision on whether to grant or deny access based on the policies.

In a practical setting, an organization would employ a blend of NFS security labels and xattrs. These are used to represent a variety of metadata, including classification, security, application, and content, which are all instrumental in making ABAC decisions. xattrs, for instance, can be used to store the resource attributes that the PDP uses for its decision-making process. An attribute could be defined to represent the classification level

of a file (for example, "Unclassified", "Confidential", "Secret", or "Top Secret"). The PDP could then utilize this attribute to enforce a policy that restricts users to access only files that have a classification level equal to or lower than their clearance level.

> This content assumes that the customer's identity, authentication, and access services include at minimum a PEP and a PDP that act as intermediaries for access to the file system.

Example process flow for ABAC

1. User presents credentials (for example, PKI, Oauth, SAML) to system access to PEP and gets results from PDP.

   The PEP's role is to intercept the user's access request and forward it to the PDP.

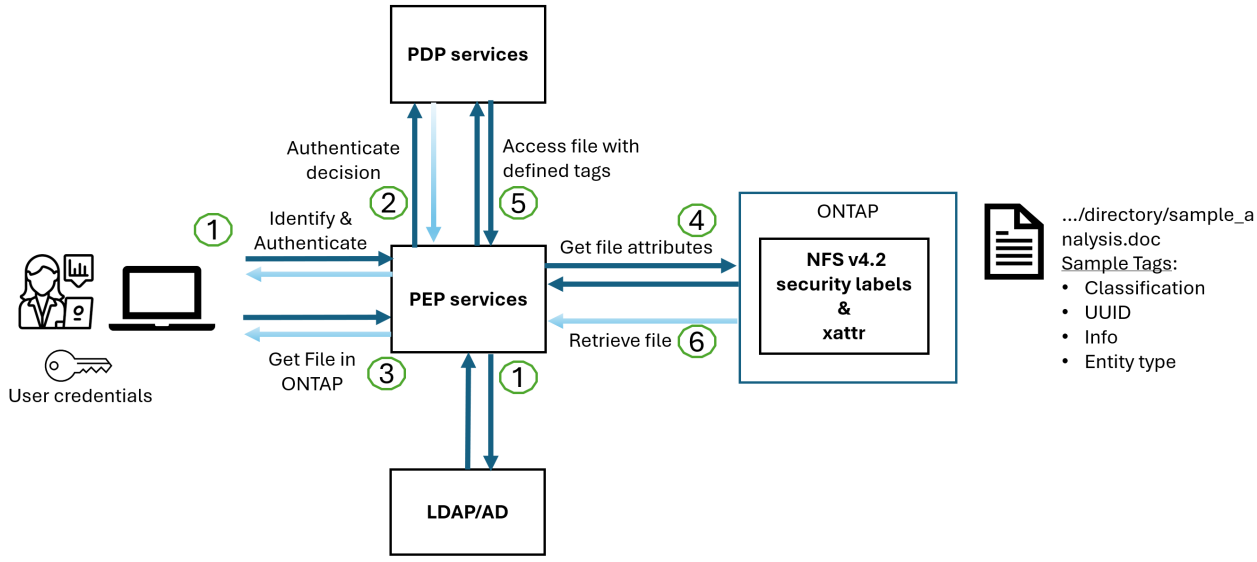
2. The PDP then evaluates this request against the established ABAC policies.

   These policies consider various attributes related to the user, the resource in question, and the surrounding environment. Based on these policies, the PDP makes an access decision to either allow or deny and then communicates this decision back to the PEP.

   PDP provides policy to PEP to enforce. The PEP then enforces this decision, either granting or denying the user's access request as per the PDP's decision.

3. After a successful request, the user requests a file stored in ONTAP (AFF, AFF-C, for example).
4. If the request is successful, PEP gets fine-grain access control tags from document.
5. PEP requests policy for user based on that user's certs.
6. PEP makes a decision based on policy and tags if the user has access to the file and lets the user retrieve the file.

> The actual access might be done using tokens.



ONTAP cloning and SnapMirror

ONTAP's cloning and SnapMirror technologies are designed to provide efficient and reliable data replication

and cloning capabilities, ensuring that all aspects of file data, including xattrs, are preserved and transferred along with the file. xattrs are critical as they store additional metadata associated with a file, such as security labels, access control information, and user-defined data, which are essential for maintaining the file's context and integrity.

When a volume is cloned using ONTAP's FlexClone technology, an exact writable replica of the volume is created. This cloning process is instantaneous and space-efficient, and it includes all file data and metadata, ensuring that xattrs are fully replicated. Similarly, SnapMirror ensures that data is mirrored to a secondary system with full fidelity. This includes xattrs, which are crucial for applications that rely on this metadata to function correctly.

By including xattrs in both cloning and replication operations, NetApp ONTAP ensures that the complete dataset, with all its characteristics, is available and consistent across primary and secondary storage systems. This comprehensive approach to data management is vital for organizations that require consistent data protection, quick recovery, and adherence to compliance and regulatory standards. It also simplifies the management of data across different environments, whether on-premises or in the cloud, providing users with the confidence that their data is complete and unaltered during these processes.

NFS v4.2 security labels have the caveats defined in NFS v4.2 security labels.

Auditing changes to labels

Auditing changes to xattrs or NFS security labels is a critical aspect of file system management and security. Standard file system auditing tools enable the monitoring and logging of all changes to a file system, including modifications to xattrs and security labels.

In Linux environments, the `auditd` daemon is commonly used to establish auditing for file system events. It allows administrators to configure rules to watch for specific system calls related to xattr changes, such as `setxattr`, `lsetxattr`, and `fsetxattr` for setting attributes and `removexattr`, `lremovexattr`, and `fremovexattr` for removing attributes.

ONTAP FPolicy extends these capabilities by providing a robust framework for real-time monitoring and control of file operations. FPolicy can be configured to support various xattr events, offering granular control over file operations and the ability to enforce comprehensive data management policies.

For users utilizing xattrs, especially in NFS v3 and NFS v4 environments, only certain combinations of file operations and filters are supported for monitoring. The list of supported file operation and filter combinations for FPolicy monitoring of NFS v3 and NFS v4 file access events is detailed below:

Supported file operations	Supported filters
`setattr`	`offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory`

Example of an auditd log snippet for a setattr operation:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*"ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

Enabling ONTAP FPolicy for users working with xattrs provides a layer of visibility and control that is essential for maintaining the integrity and security of the file system. By leveraging FPolicy's advanced monitoring capabilities, organizations can ensure that all changes to xattrs are tracked, audited, and aligned with their security and compliance standards. This proactive approach to file system management is why enabling ONTAP FPolicy is highly recommended for any organization looking to enhance its data governance and protection strategies.

Examples of controlling access to data

The following example entry for data stored in John R. Smith's PKI cert shows how NetApp's approach can be applied to a file and provide fine-grained access control.

> These examples are for illustrative purposes, and it is the customer's responsibility to determine the metadata associated with NFS v4.2 security labels and xattrs. Details on updating and label retention are omitted for simplicity.

Example PKI cert values

Key	Value
entitySecurityMark	t:s01 = UNCLASSIFIED

Key	Value

Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"emailAddresses": [
	{
	"value": "jrsmith@dod.mil"
	}
	],
	"employeeId": {
	"value": "00000387835"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"telephoneNumber": {
	"value": "938/260-9537"
	},
	"uid": {
	"value": "jrsmith"
	}
	}

specification	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

adminOrganization	{
	"value": "DoD"
	}

Key	Value
briefings	`[ { "value": "ABC1000" }, { "value": "DEF1001" }, { "value": "EFG2000" } ]`
citizenshipStatus	`{ "value": "US" }`
clearances	`[ { "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" } ]`
countryOfAffiliations	`[ { "value": "USA" } ]`

Key	Value

digitalIdentifier	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s.
	government, c=us"
	}

dissemTos	{
	"value": "DoD"
	}

dutyOrganization	{
	"value": "DoD"
	}

entityType	{
	"value": "GOV"
	}

fineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

These PKI entitlements show John R. Smith’s access details, including access by data type and attribution.

In scenarios where IC-TDF metadata is stored separately from the file, NetApp advocates for an additional layer of fine-grained access control. This involves storing access control information at both the directory level and in association with each file. As an example, consider the following tags linked to a file:

- NFS v4.2 security labels: Utilized for making security decisions

- xattrs: Provide supplementary information pertinent to the file and the organizational program requirements

The following key-value pairs are examples of metadata that could be stored as xattrs and offer detailed information about the file's creator and associated security classifications. This metadata can be leveraged by client applications to make informed access decisions and to organize files according to organizational standards and requirements.

Example of xattr key-value pairs

Key	Value
`user.uuid`	`"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"`
`user.entitySecurityMark`	`"UNCLASSIFIED"`
`user.specification`	`"INFO"`

Key	Value

user.Info	{
	"commonName": {
	"value": "Smith John R jrsmith"
	},
	"currentOrganization": {
	"value": "TUV33"
	},
	"displayName": {
	"value": "John Smith"
	},
	"emailAddresses": [
	"jrsmith@example.org"
	],
	"employeeId": {
	"value": "00000405732"
	},
	"firstName": {
	"value": "John"
	},
	"lastName": {
	"value": "Smith"
	},
	"managers": [
	{
	"value": ""
	}
	],
	"organizations": [
	{
	"value": "TUV33"
	},
	{
	"value": "WXY44"
	}
	],
	"personalTitle": {
	"value": ""
	},
	"secureTelephoneNumber": {
	"value": "506-7718"
	},
	"telephoneNumber": {
	"value": "264/160-7187"
	},
	"title": {
	"value": "Software Engineer"
	},

Key	Value
`user.geo_point`	`[-78.7941, 35.7956]`

```
    }
  }
```

Related information

- NFS in NetApp ONTAP: Best practice and implementation guide
- ONTAP command reference
- Request for comments (RFC)
  - RFC 7204: Requirements for Labeled NFS
  - RFC 2203: RPCSEC_GSS Protocol Specification
  - RFC 3530: Network File System (NFS) Version 4 Protocol

Copyright information

Trademark information