Technical Report

NetApp and Zero Trust

Enabling a Data-Centric Zero Trust Model

Dan Tulledge, NetApp
April 2020 | TR-4829

Abstract

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.

NetApp®

TABLE OF CONTENTS

1 Introduction

The old model: Trust but verify. The new model: Verify and never trust.

Data is the most important asset your organization has. Insider threats are the cause of 34% of data breaches, which is up 18% from the previous year according to the 2019 Verizon Data Breach Investigations Report. For example, the insiders Chelsea (formerly Bradley) Manning and Edward Snowden leaked classified data, but they didn't need to have access to that data to perform their jobs. So, who should be trusted? Nobody. Organizations need to ramp up their vigilance to DEFCON 1—but how? By deploying industry-leading Zero Trust controls around data with NetApp ONTAP data management software.

2 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 The concept of a secure outer perimeter is obsolete.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.

Although Zero Trust is over 10 years old, it has recently received a lot attention. Zero Trust was a central topic at the recent Black Hat and RSA security conferences.

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 utilize existing infrastructure to implement security by design in a simpler and more efficient way while enabling unimpeded operations."

In September of 2019, the NIST published Special Pub 800-207 Zero Trust Architecture (ZTA). Then, in February of 2020, NIST published a second draft that is open for comments until March of 2020. 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:

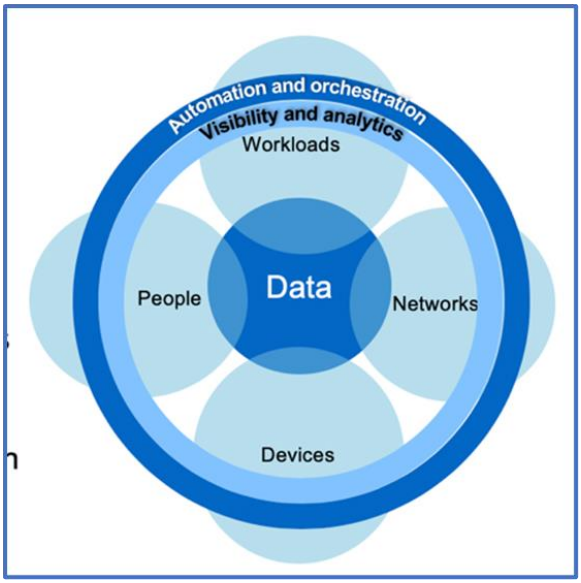
- Device-agent or gateway-based deployment
- Enclave-based deployment (somewhat analogous to the Forrester MCAP)
- Resource portal-based deployment
- Device application sandboxing

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

3 Achieving a Data-Centric Approach to Zero Trust with ONTAP

To build a Zero Trust network, you can apply a data-centric approach. 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.

Figure 1) Zero Trust architecture.



4 Steps to 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.

4.1 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 section 4.7. 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.

4.2 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 quickly see the value of a data-centric Zero Trust architecture as a framework for meeting an organization's compliance requirements.

4.3 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 section 4.6.

4.4 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.

4.5 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 NetApp 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.

4.6 Use Encryption for Data at Rest and Data in Flight

Data at Rest Encryption

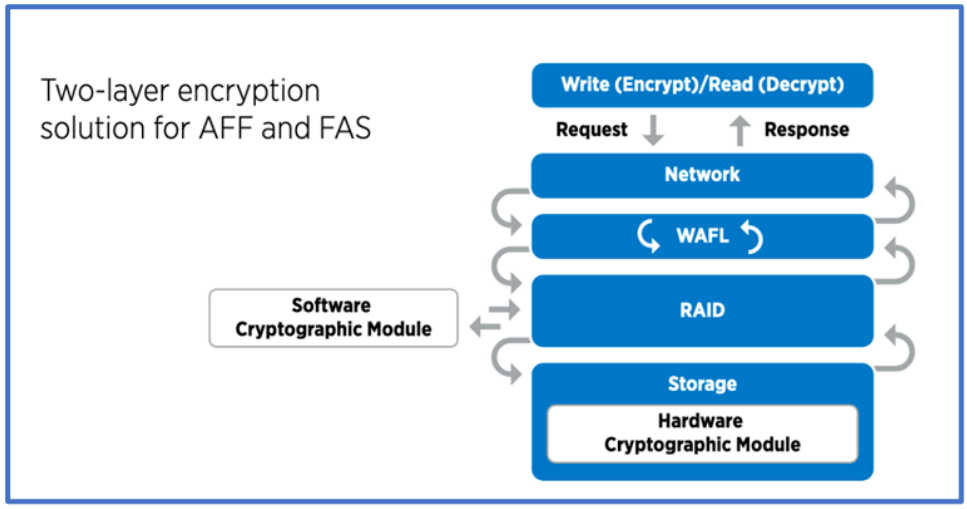
Each day, there are new requirements for mitigating storage-system risks and infrastructure gaps when an organization repurposes drives, returns defective drives, or upgrades to larger drives by selling or trading them in. As administrators and operators of data, storage engineers are expected to manage 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 in to ONTAP, or approved third-party external key managers can be used with NSE and NVE to securely store keying material.

Figure 2) Two-layer encryption solution for AFF and FAS.



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. 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.

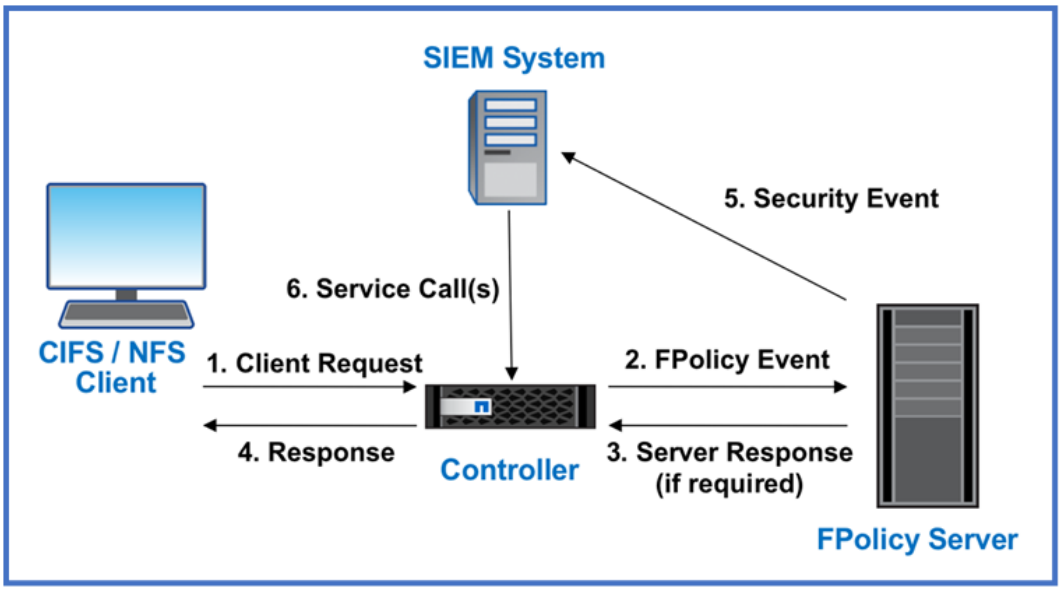
4.7 Monitor and Log All Access

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.

Figure 3) FPolicy architecture.



As an example of one of NetApp's FPolicy partners, Prolion Cryptospike combines the use of FPolicy and user behavioral analytics to defend against malware. Cryptospike is a powerful defense against ransomware that identifies a ransomware attack, quarantines infected users, and recommends an ONTAP Snapshot recovery point. It then restores only the infected files by using ONTAP APIs to prevent data loss from the infected files. It also prevents data loss by not restoring non-infected files written during the attack duration. Watch this Cryptospike video for more information.

5 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.

NetApp solutions allow IT organizations to build a single data management platform that embraces the latest technologies such as cloud, software-defined processes, and flash. NetApp has followed the principles of software-defined storage for over 20 years, providing solutions for automation, integration, scale, optimal application performance, and availability to help you meet business demands and accelerate time-to-market. Large DoD enterprises and DoD service providers with mission-critical storage

environments can simplify, reduce errors in, and improve the efficiency of their storage administration by using NetApp OnCommand® Workflow Automation (WFA). WFA enables you to design highly customized workflows without the need for scripting expertise. These workflows can then be run by operators or distributed IT staff, allowing consistent compliance with best practices across teams and over time. NetApp has also developed a WFA hardening pack for DoD requirements.

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 60 Ansible modules for NetApp Element and 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 (NetApp TR-4754).

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.

NetApp OnCommand Insight (OCI) provides centralized monitoring across hybrid infrastructures through the agentless discovery of multi-vendor, multi-protocol, and multi-cloud (public and private) IT resources on-premises and in geographically dispersed sites. From this discovery process, you can monitor physical and logical device attributes. Whereas a SIEM system might monitor the Zero Trust environment, NetApp OCI monitors data and manages workloads. This is an overlooked capability lacking from most Zero Trust environments. As discussed in the section 4.1, the #1 rule of a data-centric Zero Trust MCAP is know where your organization's data is. OCI makes that possible.

In addition to OCI, NetApp Cloud Insights is an infrastructure monitoring tool that gives you visibility into your complete infrastructure. With Cloud Insights, you can monitor, troubleshoot, and optimize all your resources, including your public cloud instances and your private data centers. Cloud 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 Cloud Secure capability of Cloud Insights enables user behavioral analytics with AI and ML to alert when aberrant user behaviors occur due to an insider threat. For ONTAP in private data centers, Cloud Secure makes use of the Zero Trust FPolicy engine.

6 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 Platform (GCP), and other leading cloud providers. NetApp hybrid-cloud solutions support the same Zero Trust security controls that are available with on-premise ONTAP systems and ONTAP Select software-defined storage.

You can easily expand capacity in public clouds without typical capex constraints by using the NetApp Cloud Volumes service, the first enterprise-class, cloud-native file service for AWS and GCP, 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.

For those seeking advanced data services for cloud block or object storage services such as AWS EBS and S3 or Azure storage, Cloud Volumes ONTAP provides data management between your on-premises environment and the public cloud with a single common view. Running in AWS or Azure as an on-demand instance, Cloud Volumes ONTAP provides the storage efficiency, availability, and scalability of ONTAP software. ONTAP enables the movement of data between your on-premises ONTAP systems and AWS or Azure storage environment with NetApp SnapMirror® data replication software.

For organizations that need an enterprise-class hybrid cloud with data governance and security, on-premises ONTAP systems can be used in a NetApp Private Storage (NPS) for Cloud solution. With NPS for Cloud, you can directly connect to multiple clouds by using a private, high-bandwidth, low-latency connection. Connect to industry-leading clouds such as AWS, Microsoft Azure, or IBM Cloud and switch between them at any time, all while maintaining complete control of your data on your dedicated, private ONTAP system.

Security Resources

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

Where to Find Additional Information

To learn more about the information described in this document, refer to the following documents and/or websites:

- Verizon Data Breach Investigations Report
  https://enterprise.verizon.com/resources/reports/dbir/
- Bradly Manning sentenced to 35 years in Wikileaks case
  https://www.washingtonpost.com/world/national-security/judge-to-sentence-bradley-manning-today/2013/08/20/85bee184-09d0-11e3-b87c-476db8ac34cd_story.html
- Edward Snowden comes forward as the source of NSA leaks
  https://www.washingtonpost.com/politics/intelligence-leaders-push-back-on-leakers-media/2013/06/09/fff80160-d122-11e2-a73e-826d299ff459_story.html
- DoD Digital Modernization Strategy
  https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF
- NIST SP 800-207 Zero Trust Architecture (2nd Draft)
  https://csrc.nist.gov/publications/detail/sp/800-207/draft
- NetApp Partner Connect: Security Alliance Partners
  https://partner-connect.netapp.com/us/alliance/security
- Using FPolicy for file monitoring and management on SVMs
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cifs-nfs-audit/GUID-F1F54C15-057A-460E-A5E1-21FFBB9773FA.html
- PCI-DSS 3.2 ONTAP 9
  https://www.netapp.com/us/media/tr-4401.pdf
- General Data Protection Regulation (GDPR)
  https://www.netapp.com/us/info/gdpr.aspx
- Summary of HIPPA Privacy Rule
  https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
- Administrator Authentication and RBAC Power Guide
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-adm-auth-rbac/home.html

- Multifactor Authentication in ONTAP 9.3
  https://www.netapp.com/us/media/tr-4647.pdf
- NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption, and NetApp Aggregate Encryption
  https://www.netapp.com/us/media/ds-3898.pdf
- NetApp Storage Encryption
  https://www.netapp.com/us/media/ds-3213-en.pdf
- NetApp Volume Encryption and NetApp Aggregate Encryption
  https://www.netapp.com/us/media/ds-3899.pdf
- NetApp Cryptographic Module FIPS-140-2 Certificate
  https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3072
- Quantum Ready Data-At-Rest Encryption by NetApp
  https://www.netapp.com/us/media/sb-3952.pdf
- Innovating with Security: NetApp and Ontrack win Flash Memory Summit Award
  https://blog.netapp.com/flash-memory-summit-award/
- Enabling onboard key management
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-nve/GUID-466E3BFC-F7FA-4B79-A8C9-2540C3BF1408.html
- NetApp Interoperability Matrix Tool
  https://mysupport.netapp.com/matrix/imt.jsp?components=69551;&solution=1156&isHWU&src=IMT
- Configuring external key management
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-nve/GUID-DD718B42-038D-4009-84FF-20BBD6530BC2.html
- Security config modify to enable FIPS mode
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.dot-cm-cmpr-950/security__config__modify.html
- Enabling cluster peering encryption on an existing peer relationship
  https://docs.netapp.com/ontap-9/topic/com.netapp.doc.pow-csp/GUID-D58CC065-5EB5-4887-9A64-714755CC5B51.html
- Prolion
  https://prolion.com/en/home
- Prolion CryptoSpike
  https://prolion.com/en/cryptospike
- CryptoSpike Video
  https://catalogicsoftware.com/resources/cryptospike-feature-demonstration-video
- WFA Security Hardening Pack for DoD
  https://automationstore.netapp.com/pack-detail.shtml?packUuid=c3ef31a1-65f3-4d57-8945-0b8af258e31e&packVersion=1.0.0
- Get Started with Automating your Dev Work Flows with NetApp and Ansible
  https://www.netapp.com/us/getting-started-with-netapp-approved-ansible-modules/index.aspx
- Ansible module specific to the NetApp DoD Unified Capabilities (UC) Deployment Guide (NetApp TR-4754).
  https://github.com/NetApp/ansible/tree/master/nar_ontap_security_ucd_guide
- Administrator Authentication and RBAC Power Guide
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-adm-auth-rbac%2Fhome.html
- NetApp Encryption Power Guide
  http://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.pow-nve%2Fhome.html

- TR-4569 Security Hardening Guide for NetApp ONTAP 9
  https://www.netapp.com/us/media/tr-4569.pdf
- Certificate-Based Authentication with the NetApp Manageability SDK for ONTAP
  https://netapp.io/2016/11/08/certificate-based-authentication-netapp-manageability-sdk-ontap/

Version History

Version	Date	Document Version History
Version 1.0	April 2020	Initial release.

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.

TR-4829