



Enable Zero Trust model

ONTAP 9

NetApp
July 12, 2024

Table of Contents

- Enable Zero Trust model 1
 - NetApp and Zero Trust 1
 - Architect a data-centric approach to Zero Trust with ONTAP 2
 - NetApp security automation and orchestration controls external to ONTAP 6
 - Zero Trust and hybrid cloud deployments 7
 - Learn more about ONTAP Zero Trust content 7

Enable Zero Trust model

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-4015: NetApp and Zero Trust: Enabling a data-centric Zero Trust model*, which was previously published as a PDF, has been integrated with the rest of the ONTAP product documentation.

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 The concept of a secure outer perimeter is obsolete.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

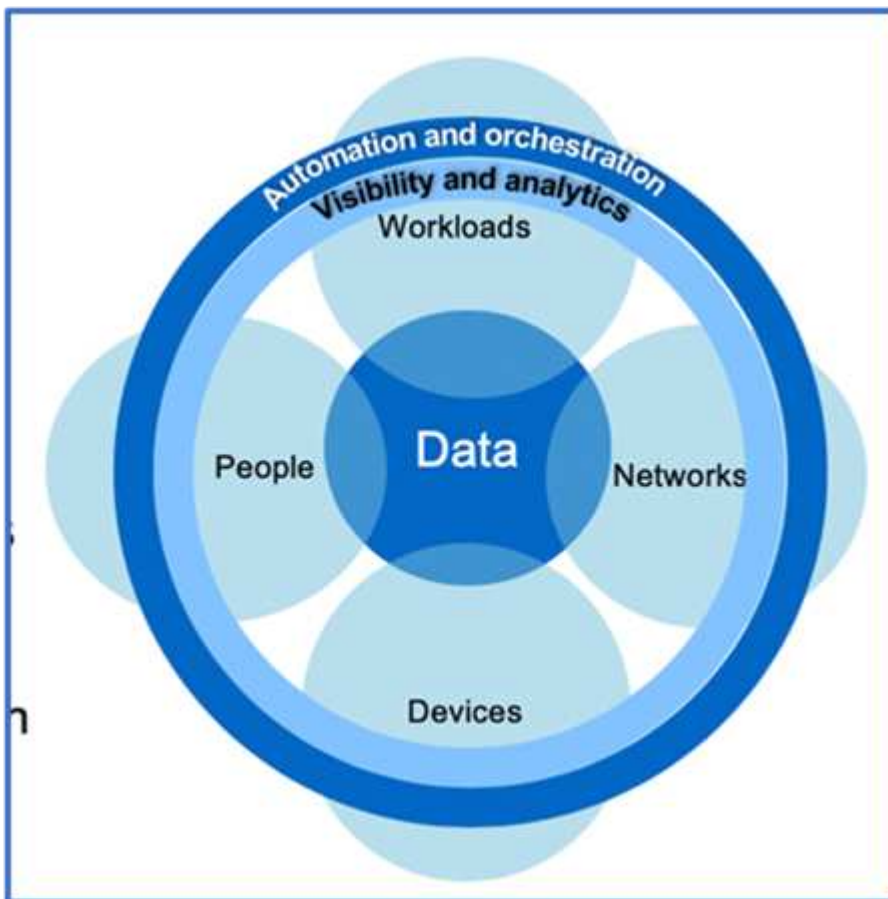
Security resources

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 [BlueXP 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 Snapshot copies is with ONTAP [Snapshot copy locking](#). Snapshot copy locking is a SnapLock capability where Snapshot copies are rendered indelible manually or automatically with a retention period on the volume Snapshot copy policy. Snapshot copy locking is also referred to as tamper-proof Snapshot copy locking. The purpose of Snapshot copy locking is to prevent rogue or untrusted administrators from deleting Snapshot copies on the primary and secondary ONTAP systems. Rapid recovery of locked Snapshot copies 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

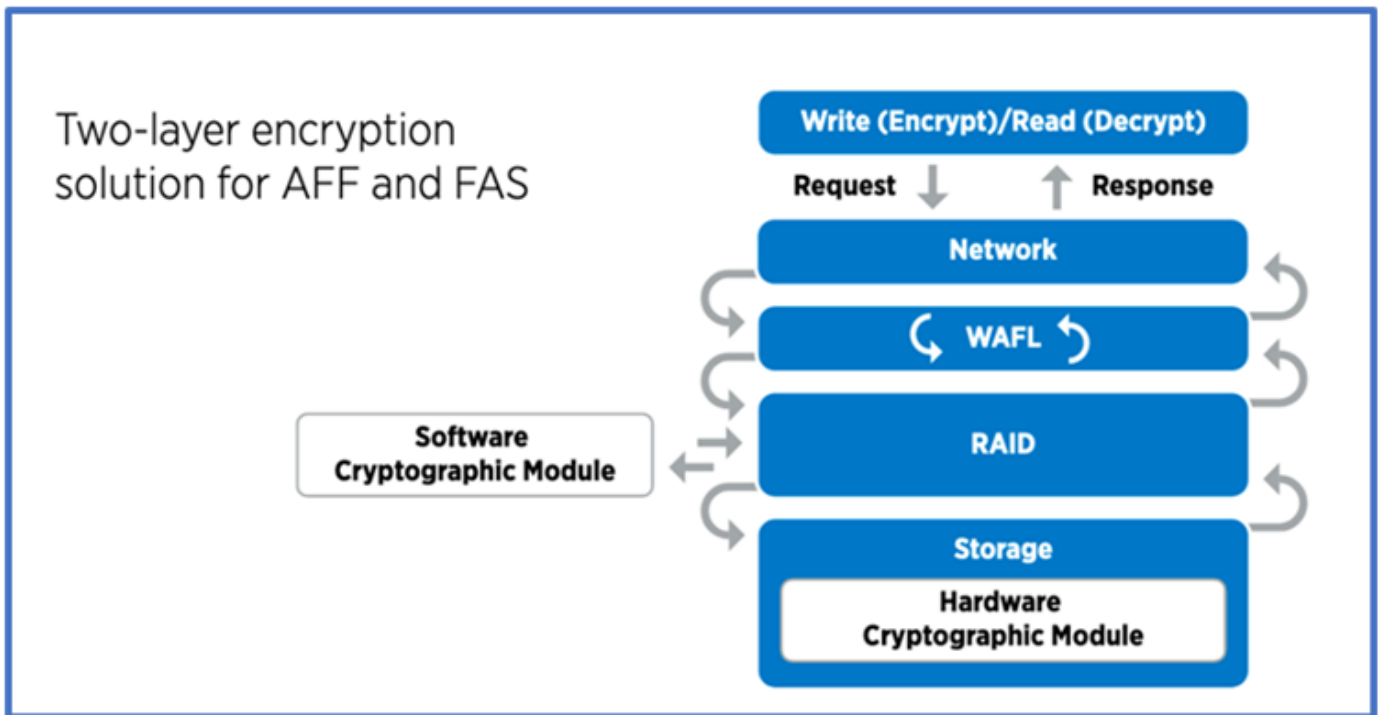
Data at rest encryption

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 in to 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.

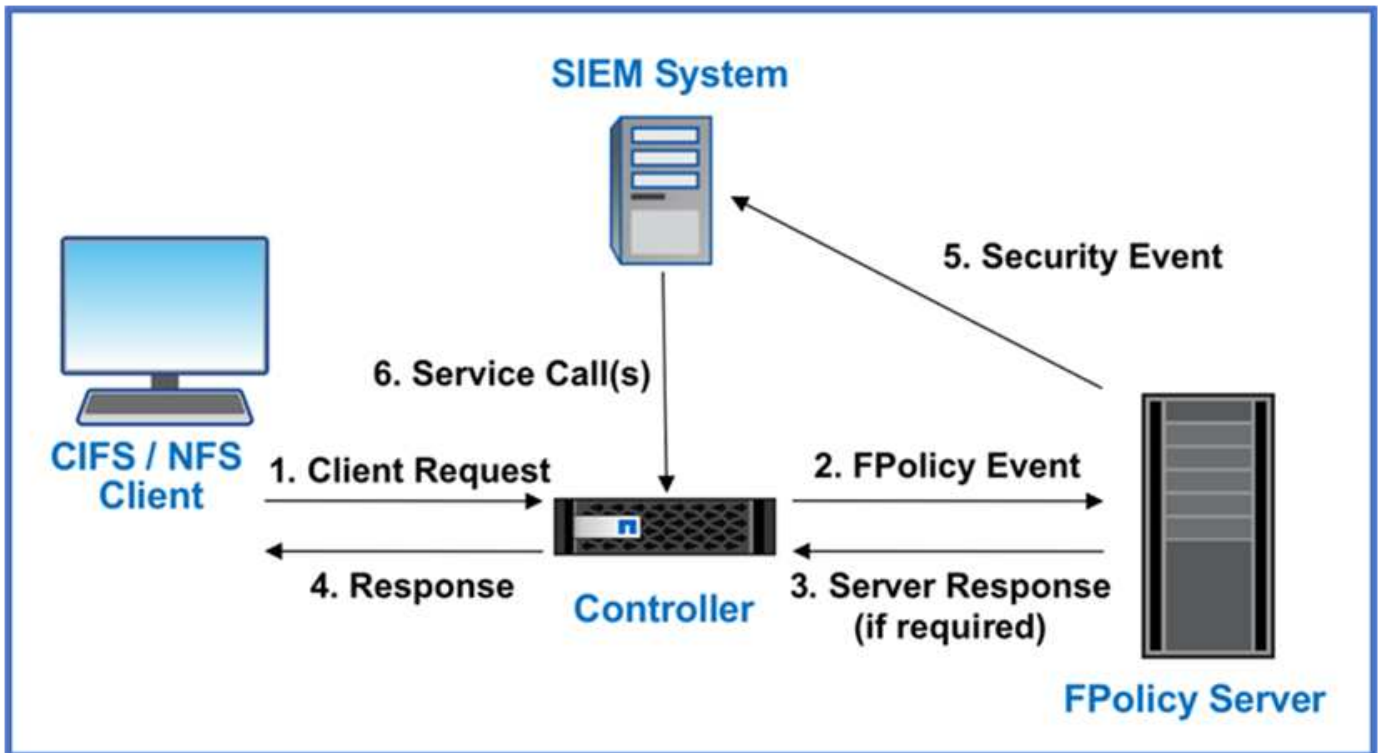
Data-in-flight encryption

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 Storage Workload Security (formerly known as [Cloud Secure](#)) 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 Snapshot copies 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 Cloud 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 copy and alert to administrators. Storage Workload Security integrates with ONTAP to receive ARP events and provides an additional analytics and automatic responses layer.

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.

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.

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 Storage Workload Security 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, 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 Platform (GCP), 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 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.

Learn more about ONTAP Zero Trust content

To learn more about the information described in the ONTAP Zero Trust content, refer to the following documents and/or websites:

- [Verizon Data Breach Investigations Report](#)
- [DoD Digital Modernization Strategy](#)
- [NIST SP 800-207 Zero Trust Architecture](#)
- [NetApp Partner Connect: Security Alliance Partners](#)

- [Using FPolicy for file monitoring and management on SVMs](#)
- [PCI-DSS 3.2 ONTAP 9](#)
- [General Data Protection Regulation \(GDPR\)](#)
- [Summary of HIPPA Privacy Rule](#)
- [NetApp BlueXP Classification](#)
- [Multi-admin verification](#)
- [Tamperproof Snapshot copy locking](#)
- [Multifactor authentication in ONTAP 9](#)
- [NetApp Storage Encryption, NVMe Self-Encrypting Drives, NetApp Volume Encryption, and NetApp Aggregate Encryption](#)
- [NetApp Storage Encryption](#)
- [NetApp Volume Encryption and NetApp Aggregate Encryption](#)
- [NetApp Cryptographic Module FIPS-140-2 Certificate](#)
- [Quantum Ready Data-At-Rest Encryption by NetApp](#)
- [Innovating with Security: NetApp and Ontrack win Flash Memory Summit Award](#)
- [Enabling onboard key management](#)
- [NetApp Interoperability Matrix Tool](#)
- [Configuring external key management](#)
- [Commercial Solutions for Classified](#)
- [ONTAP IPsec](#)
- [Security config modify to enable FIPS mode](#)
- [Enabling cluster peering encryption on an existing peer relationship](#)
- [Storage Workload Security \(Cloud Secure\)](#)
- [Get Started with Automating your Dev Work Flows with NetApp and Ansible](#)
- [Ansible module specific to the NetApp DoD Unified Capabilities \(UC\) Deployment Guide](#)
- [Administrator Authentication and RBAC](#)
- [ONTAP Data-at-Rest Encryption](#)
- [TR-4569 Security Hardening Guide for NetApp ONTAP 9](#)

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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