Security and privacy of NetApp telemetry data

Brett Albertson
April 2026

version: 2.0

Abstract

NetApp® Active IQ® Digital Advisor displays information about your NetApp systems by aggregating telemetry data from the predictive technology built into those systems. As a NetApp customer, you should understand how this telemetry data is kept secure and private.

Table of Contents

Introduction *4*

Telemetry data overview 4

NetApp AutoSupport and Active IQ ecosystem components 4

Collection of telemetry data *6*

Data collected from ONTAP 6

Transfer of telemetry data *7*

Security in transit 7

When are AutoSupport messages sent to NetApp? 8

Reception, process, storage, access and retention of telemetry data *8*

Where does AutoSupport telemetry data reside? 8

AutoSupport Telemetry Data Masking and Encryption 8

Data reception and processing after encryption and masking 9

Data access 9

Data retention 9

Security compliance, certifications, and procedures *10*

Physical security 10

Product security 10

Data protection 10

Security incident management 10

Vulnerability and penetration testing 10

Security awareness training 10

Compliance 10

Secrets and secret rotation 11

Frequently asked questions *11*

Appendix *13*

Collection of telemetry data for other platforms 13

E-Series 13

StorageGRID 13

Cloud Insights 13

Active IQ Unified Manager 13

SANtricity Web Services (REST API) 13

Active IQ OneCollect 14

Items masked by the AutoSupport Encryption Service (AES) 14

Categories of protected data 14

© 2026 NetApp, Inc. All rights reserved.

© 2026 NetApp, Inc. All rights reserved.

Introduction

Telemetry data overview

NetApp brands its telemetry data as “AutoSupport”. AutoSupport telemetry data is machine-generated, system metadata automatically collected from NetApp products to support proactive operations, predictive analytics, and intelligent support services. This data includes configuration details, system health and status, performance metrics, and event-based logs. AutoSupport telemetry is generated on a regular schedule and in response to system events, enabling NetApp to detect, diagnose, and often resolve issues before they impact customers. Please note that **no data stored on customer systems is ever transferred to NetApp**.

AutoSupport telemetry delivers measurable operational, support, and business value to customers. By securely transmitting telemetry data to NetApp, customers enable automated support case creation, faster problem resolution, and predictive analytics through NetApp Active IQ Digital Advisor and other tools. Most support issues are detected or predicted by NetApp before customers are aware of them, significantly reducing unplanned downtime and operational disruption.

AutoSupport telemetry is the foundation for proactive support and AIOps-driven insights. The data powers Active IQ Digital Advisor capabilities such as health and wellness checks, upgrade planning, security risk identification (including known CVEs), and long-term system optimization recommendations. These insights help customers move from reactive firefighting to planned, data-driven operations, improving system availability, and lifecycle management.

Security and privacy are core to the AutoSupport design. Telemetry data is handled using strong security controls, encrypted transport, and rigorous access restrictions. Personally identifiable information (PII) and customer identifiable information (CII) are minimized, encrypted, and tightly controlled, with ongoing enhancements to further reduce data exposure. Customers retain control and transparency, while still benefiting from NetApp’s global analytics and support expertise.

Autosupport telemetry also allows the automatic update capabilities inside ONTAP. At present, that includes checking for new versions of disk, shelf, SP, and BMC firmware, Automated Ransomware Protection (ARP) updates, Disk Qualification Packages (DQPs), and time zone file updates. If a new version is found, it can be automatically updated without any downtime depending on the settings of the system.

In summary, AutoSupport telemetry transforms system data into actionable intelligence. For customers, this means greater uptime, faster resolution of issues, improved security posture, and reduced operational risk; all delivered with no additional infrastructure or operational overhead. AutoSupport is not simply a support mechanism—it is a critical enabler of smarter, more resilient NetApp environments.

NetApp AutoSupport and Active IQ ecosystem components

© 2026 NetApp, Inc. All rights reserved.

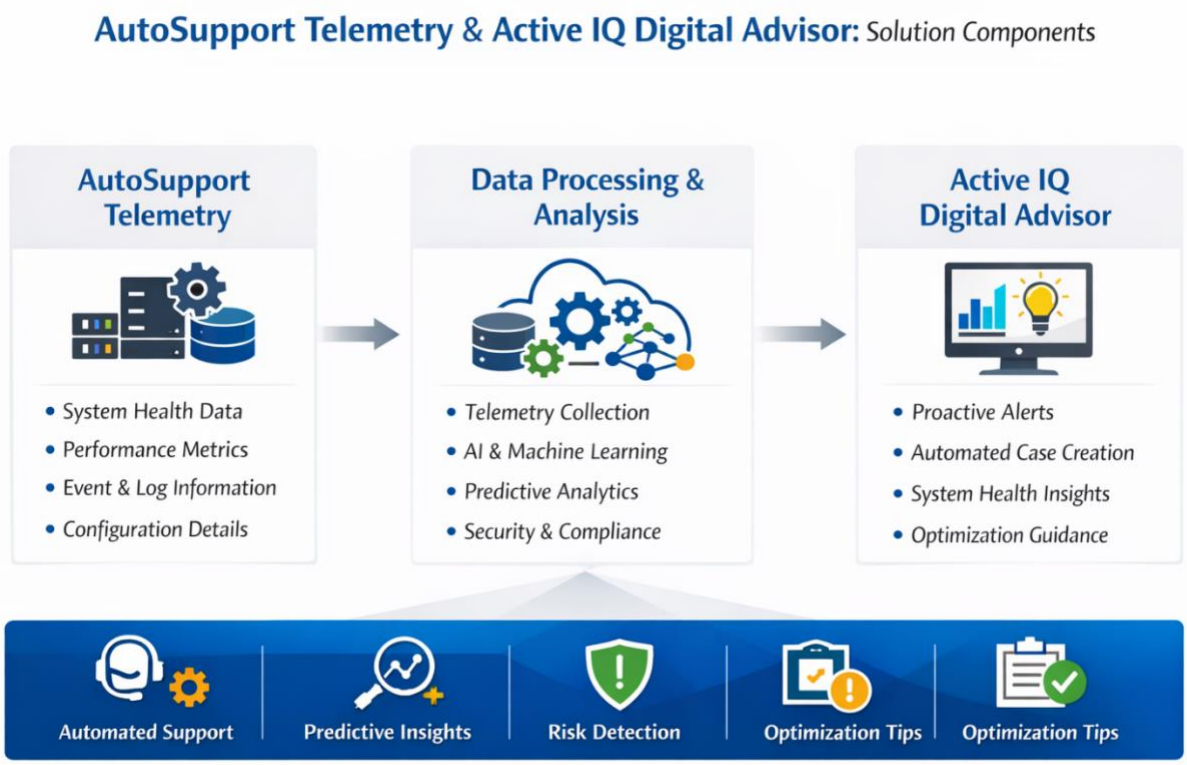

Figure 1.1 AutoSupport and Active IQ ecosystem components

© 2026 NetApp, Inc. All rights reserved.

Collection of telemetry data

AutoSupport collects functional data such as configuration, status, and performance information about your systems. You can disable sending telemetry data to NetApp if you choose; however, doing so affects your access to predictive analytics and proactive support, such as automatic case creation. The procedure for disabling AutoSupport depends on the platform. See the product documentation for information about how to perform this action.

AutoSupport is enabled by default on most NetApp systems. You may have to either configure a proxy or change your firewall settings to allow AutoSupport messages to be sent to NetApp.

For ONTAP, you also have the option to mask sensitive information from AutoSupport messages, but doing so can impact support as well. This option is disabled by default. AutoSupport telemetry data is handled using security best practices and controls that address privacy regulations. NetApp also offers a Customer Data Processing Addendum (available here) that commits NetApp to compliance with any applicable legal requirements related to privacy and data protection. Review the section on access and retention of telemetry data before deciding to limit any data sent to NetApp. Doing so will make it more difficult to manage, monitor, maintain, and support your systems.

For platforms other than ONTAP, see the appendix for details of what is collected.

Data collected from ONTAP

The following list is a representative sample of what is included in an AutoSupport message for ONTAP.

Note: You can identify the exact content sent in an AutoSupport message by reviewing the manifest for that message. To do so, use the *system node autosupport manifest show* command.

- Date and timestamp of the message
- ONTAP software version
- Serial number of the storage system
- Encrypted software licenses
- Host name of the storage system
- SNMP contact name and location (if specified)
- Console encoding type
- Output of commands that provide system information
- Checksum status
- Error-Correcting Code (ECC) memory scrubber statistics
- The following information, if a high-availability (HA) configuration is licensed:
  - System ID of the partner in an HA pair
  - Host name of the partner in an HA pair
  - HA node status, including the HA monitor and HA interconnect statistics
- Contents of non-privacy-related files under the /etc directory
- Expiration date of all NetApp SnapLock® volumes on the system
- Registry information
- Usage information
- Service statistics
- Boot time statistics
- NVLOG statistics
- NetApp WAFL® check log
- Modified configurations

© 2026 NetApp, Inc. All rights reserved.

- X-header information
- Information about the boot device (such as the CompactFlash card)

Certain portions of this data, either alone or in combination with other external data sources, may identify an individual or company, or contain confidential information. See the section on encryption, for information about encryption of sensitive information in AutoSupport when it is received by NetApp. To give our customers additional control over the data they send to NetApp, ONTAP offers a solution that protects the privacy of sensitive customer-identifying data by masking or filtering that information with the *–remove-private-data* parameter of the *node autosupport modify* command. When enabled (set to true), this parameter removes, encodes, or masks sensitive data from AutoSupport attachments and headers. Note: see below about the encrypting and masking that is done upon reception before deciding to enable this option.

Eliminated data includes the following items:

- IP addresses
- MAC addresses
- URIs
- DNS names
- E-mail addresses
- Port numbers
- Node names
- SVM names
- Cluster names
- Aggregate names
- Volume names
- Junction paths
- Policy names
- User IDs
- Group IDs
- LUNs
- Qtree names

You should remove private data only if you have a compliance reason requiring the most robust security. Removing the data has the following significant functional impacts:

- Limited system information visibility and functional capability in Active IQ Digital Advisor (for example, when viewing the inventory, capacity, performance, and wellness dashboard views)
- Reduced value to customers from other NetApp services that depend on AutoSupport content analysis such as assessment services and storage optimization and efficiency reports
- Increased support resolution times compared to complete AutoSupport information messages

Transfer of telemetry data

Security in transit

By default, NetApp products use the HTTPS protocol to send telemetry data to NetApp. HTTPS connections to NetApp are encrypted and authenticated using TLS 1.2 or later. Extremely old and unsupported versions of ONTAP sending AutoSupport over HTTPS which pre-date TLS 1.2 are not

© 2026 NetApp, Inc. All rights reserved.

accepted by NetApp. HTTPS connections are supported through a proxy (see product documentation to configure a proxy). NetApp strongly recommends using HTTPS because it is more secure; it enables NetApp to provide better support, and it provides better analytics through Active IQ Digital Advisor. However, SMTP is also offered for customers that cannot use HTTPS. NetApp does support encrypted SMTP transfers.

When are AutoSupport messages sent to NetApp?

AutoSupport telemetry data is generally sent according to a schedule. Messages are sent daily and weekly. There are three cases where they can be sent at other times.

1. Emergencies and critical issues on the system can generate a message triggering a proactive support case to reduce the time to resolution for these important issues.
2. Customers can initiate a manual AutoSupport at any time. For example, it is recommended that customers send a manual AutoSupport at the end of a software version update so that their dashboards are updated with the new information.
3. NetApp support and support partners chosen by the customer can initiate an AutoSupport on Demand (AOD) during a support case. These contain more granular information and can also transmit a performance archive for performance troubleshooting cases. The use of AOD is strictly controlled with RBAC, and all uses are logged. Note: AOD depends on transmission over HTTPS.

Reception, process, storage, access and retention of telemetry data

Where does AutoSupport telemetry data reside?

AutoSupport data is sent to one or more NetApp data centers in the United States. The data is not archived at an offsite location. Some data processed or derived from AutoSupport is stored in Amazon Web Services.

AutoSupport Telemetry Data Masking and Encryption

When AutoSupport telemetry data is received by NetApp, the AutoSupport Encryption Service (AES) processes message content to identify and protect personally identifiable information (PII) and customer identifiable information (CII).

The AES uses a rules-based configuration that defines, for each known file or data structure within an AutoSupport message, which fields to protect and how. The system applies two primary protective actions:

- Encryption - sensitive field values are encrypted in place, preserving the ability for authorized personnel to decrypt the data when required for support or analytics. All decryptions are logged.
- Masking - values are replaced with a fixed mask value (for example, XXXXXX), irreversibly removing the original data.

Encryption enables NetApp to retain the ability to correlate and analyze data for support purposes while protecting it at rest. Masking is applied to fields where the original value is not needed for downstream analysis. The AES processes over 130 distinct file types and data structures within AutoSupport messages, covering structured formats including line-oriented log files, XML, SMF (Structured Message Format), and JSON.

© 2026 NetApp, Inc. All rights reserved.

Data reception and processing after encryption and masking

When data arrives, data from certain governmental entities is separated from the rest of the data and is stored separately from all other data. This data has additional security controls placed on it, including that only verified NetApp employees and contractors who are U.S. citizens and on U.S. soil can use it during support issues.

The data is stored in an encrypted database, which has strong security controls and auditing placed on it. Only customers and specially authorized people can decrypt the data when needed, and then those decryptions are logged and audited. All data is encrypted at rest and in transit.

Data access

Access to NetApp telemetry data is secured by a data access layer that requires positive identification of each user requesting access. All requests for data must include a verifiable reference to the individual who is requesting access. The data access layer is implemented using the following:

- NetApp uses Microsoft Entra ID as our central identity provider. NetApp also allows customers to federate so that they can use their own Azure/Microsoft logins. NetApp allows security policies like MFA. At the end of this login process, your session is given a SAML (Secure Assertion Markup Language) token to show who you are and that you have been authenticated.
- Your SAML token allows us to know your authenticated user attributes (employing company, geographic location, citizenship, etc.) which allows us to limit access to data based on that.
- Role-based access control (RBAC) based on job function also limits access to data for NetApp employees.

The following people and job roles at NetApp can access AutoSupport telemetry data:

- **NetApp customer success (support) and account teams**. NetApp employees and approved agents in these roles can access telemetry data for customer support and sales uses, which allows them to better help their customers.

- **Customers**. Any user from a company that has registered with the NetApp Support site can access data for all their installed systems that have AutoSupport enabled and have active support contracts. Users are only able to view systems that are registered with their company. Active IQ uses the product registration and support registration credentials from the NetApp Support site to control access.

- **Partners**. Partners who have registered with the NetApp Support site can access data for all systems for which they are the “partner of record” and have an active support contract. Partners are the “partner of record” for systems that they sold or currently support. Customers can remove their access or change partners at any time.

Note: For systems that have the “secure for government” support level or that are owned by the United States government, NetApp access to telemetry data is restricted to employees and contractors who are United States citizens working in the United States.

Data retention

NetApp will retain AutoSupport telemetry messages for seven years. Processed data for use in tools like Active IQ Digital Advisor is retained for less time, usually less than one year. Customers can

© 2026 NetApp, Inc. All rights reserved.

request that their data be deleted at any time by opening a support case.

Security compliance, certifications, and procedures

Physical security

AutoSupport telemetry data is stored in datacenters in the United States in buildings with locks or keys on the doors.

Product security

NetApp follows the security development lifecycle to embed security into everything we do. Change management procedures and policies define when and how changes occur and help maintain the stability of the production environment. Any impactful changes are formally communicated, coordinated, properly reviewed, and approved before their release into the production environment. The AutoSupport and Active IQ team follows a strong software development process, including activities like threat modelling, penetration testing, SAST, 3rd party software scans and secret scanning.

Data protection

The AutoSupport and Active IQ production environment is a highly redundant infrastructure using NetApp's own products following best practices. In addition to a highly available and redundant computing infrastructure, the entire infrastructure and data is mirrored to another NetApp site and is ready to run a disaster recovery at any time.

Security incident management

AutoSupport and Active IQ is integrated with NetApp's Product Security Incident Response Team (PSIRT) process to find, assess, and resolve known vulnerabilities. PSIRT intakes vulnerability information from multiple channels, including customer reports, internal engineering, and widely recognized sources such as the CVE database. If the engineering team detects an issue, it will initiate the PSIRT process, assess it, and potentially remediate it.

Vulnerability and penetration testing

The AutoSupport and Active IQ team follows industry best practices and performs regular vulnerability and penetration testing using internal and external security professionals and companies.

Security awareness training

All NetApp personnel undergo security training developed for individual roles to ensure each employee is equipped to handle the specific security-oriented challenges of their roles.

Compliance

NetApp undergoes independent third-party audits performed by external firms to validate its security practices and processes. The published audit reports can be found on the trust site. At the time of

© 2026 NetApp, Inc. All rights reserved.

publishing NetApp maintains the following certifications: CCPA, Common Criteria, Cyber Essentials, HIPAA, ISO 9001:2015, ISO 14001:2015, ISO/IEC 27001:2022, PCI DSS, SOC 2 Type 2, TX-RAMP Level 2, and NIST 800-218. Please see the trust site for current information.

Secrets and secret rotation

For the code that runs AutoSupport and Active IQ, no secrets are stored in code or configuration files. All secrets are stored in a third-party application in an encrypted database. Those secrets are programmatically rotated on a 30-day basis. RBAC and logging are applied to any use of the secrets.

Frequently asked questions

Does AutoSupport contain any data stored on my storage array?

No, it only sends information about how the storage array is running.

Can I keep my AutoSupport telemetry data locally or within my country?

No, the data pipeline for AutoSupport is in NetApp data centers inside the United States.

Did NetApp use customer telemetry data to train an AI?

No, NetApp does not do AI training currently.

Can my competitors see my telemetry data?

No, NetApp uses mandatory authentication and RBAC.

Do Active IQ's APIs have the same security as the Active IQ Digital Advisor GUI to access telemetry data?

Yes, all APIs use the same mandatory authentication and RBAC as the GUI.

Can I manually upload AutoSupport data when needed?

Yes, but it is not the recommended way to do it because you lose out of all the key benefits like proactive support case automation and much more. To upload an AutoSupport manually, go to https://upload.netapp.com/ .

Can I copy my partner on an AutoSupport message?

Yes, see the product documentation to configure AutoSupport to do that.

I want to remove potential PII and CII from my AutoSupport messages with the "-remove-private-data" option. What effects will it have?

It will make support cases harder to resolve. The data shows that setting that option will approximately double support case resolution time. Some case automation will break without the names of volumes or aggregates. Customer facing tools like Active IQ Digital Advisor, Console, and the support site will have a lot of broken features. Internal tools your account team and partners use to better take care of you will be broken, for example the ability to easily quote add-ons and tech

© 2026 NetApp, Inc. All rights reserved.

refreshes.

Can I use a web proxy to send AutoSupport data?

Yes, see the product documentation for details on how to do it.

© 2026 NetApp, Inc. All rights reserved.

Appendix

Collection of telemetry data for other platforms

E-Series

AutoSupport messages for E-Series storage systems contains the following information:

- System log files
- Configuration data (formatted XML and unstructured command output)
- State data (subsystem up/down and capacity used)
- Performance metrics
- System inventory data

StorageGRID

AutoSupport messages for StorageGRID contains the following information:

- StorageGRID software version
- Operating system version
- System-level and location-level attribute information
- All alarms raised in the last 7 days
- Status of all grid tasks, including historical data
- Events information as listed on the SSM > Events > Overview page
- Admin Node database usage
- Number of lost or missing objects
- Grid configuration settings
- NMS entities
- Active ILM policy
- Provisioned grid specification file

Cloud Insights

AutoSupport messages for Cloud Insights contain the following information:

- Basic information about the Cloud Insights instance
- The licensed modules and protocols
- The arrays that the Cloud Insights instance is monitoring (serial number, manufacturer, model number, capacity, etc.)
- The virtual disks that the Cloud Insights is monitoring (data source, location, object identifier, capacity, etc.)

Active IQ Unified Manager

AutoSupport messages for Active IQ Unified Manager contains the following information:

- Basic configuration information about the systems managed by a Unified Manager instance
- Log files
- Diagnostic contents from command outputs

SANtricity Web Services (REST API)

AutoSupport messages for SANtricity Web Services contain the following information:

- A configuration file of systems being managing

© 2026 NetApp, Inc. All rights reserved.

- Logs for the application
- Application-specific counters
- A web server configuration file

Active IQ OneCollect

AutoSupport messages for OneCollect contain the following information:

- Configuration information from the hosts, hypervisors, switches, and storage arrays from which a collection was run

Items masked by the AutoSupport Encryption Service (AES)

Categories of protected data

The following categories of data are identified and protected:

- Usernames and identifiers
- Usernames, login IDs, user accounts, group memberships, and related identity fields are encrypted or masked across all supported products. This includes fields such as usernames, user IDs, Windows usernames, CHAP usernames, proxy users, privileged user lists, job usernames, contact names, and directory service bind identifiers. Generic or system-level accounts (such as admin, root, ndmp, guest, monitor, and System) are excluded from masking to preserve supportability.
- Email addresses
- Email addresses found in AutoSupport configuration, notification settings, and audit logs are encrypted or masked. This includes AutoSupport sender and recipient addresses, user email fields, creator and discovery email addresses, and mail-from/mail-to fields. The NetApp internal address autosupport@netapp.com is excluded from masking.
- IP addresses (public)
- Public IPv4 and IPv6 addresses are encrypted. The AES distinguishes between public and private IP address ranges; private and link-local addresses (RFC 1918, RFC 3927, and RFC 6598 ranges) are not encrypted. Protected IP address fields include cluster management IPs, node management IPs, client IPs, server IPs, DNS server addresses, KDC addresses, proxy IPs, remote IPs, device IPs, and switch IP addresses.
- Customer identifiable information (CII)
- Customer-specific identifiers that could reveal the identity of a customer or their environment are encrypted. This category includes:
- Domain names and DNS zones
- Hostnames and fully qualified domain names (FQDNs)
- Company and site names
- Active Directory domains and trusted domains
- NIS domains and servers
- Aggregate and volume names
- Broadcast domain names
- URLs and proxy URLs
- Syslog server destinations
- System names and discovered device identifiers
- Backup names and zone names
- Base DN and bind DN values from directory service configurations
- Domain values matching netapp.com are excluded from encryption. In addition, 35 of the processed file types apply a global domain replacement to systematically identify and

© 2026 NetApp, Inc. All rights reserved.

encrypt domain names appearing anywhere in the file content, beyond specifically named fields.

- Passwords and credentials
- Passwords, passphrases, and credential fields are masked rather than encrypted, ensuring the original values are permanently removed and cannot be recovered. This includes administrative passwords, proxy passwords, CHAP passwords, SVM passwords, Active Directory passwords, and outbound passphrases.
- Other sensitive fields
- Additional fields that may contain sensitive information are protected, including:
- Phone numbers (primary and secondary, including alternate numbers)
- Contact names and full names
- Physical location descriptions
- File paths and directory names
- Source system identifiers
- Scope of protection

© 2026 NetApp, Inc. All rights reserved.

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

Copyright information

Copyright © 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, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

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

NetApp