Datasheet

Security Features in E-Series SANtricity OS

Securing the World's Most Vital Resource, Information

Key Benefits

Enhance data confidentiality, integrity, and availability
Leverage security features and associated controls in NetApp E-Series SANtricity to solidify the confidentiality, integrity, and availability of your organization's most important resource, data.

Create a security posture for your environment
Establish a secure foundation in your organization's data fabric and understand the visibility and security functions that create a secure infrastructure.

Leverage NetApp and industry best practices for security
Establish a vetted security footprint with help from NetApp experts, industry knowledge, and common practices.

Satisfy governance and compliance requirements
Leverage established security best practices to adhere to and support industry regulation and security compliance.

NetApp® SANtricity® storage management software continues to evolve, with security as an integral part of the solution. The many E-Series SANtricity security features and functions are invaluable for protecting an organization's security posture and adhering to industry best practices. These new features make data confidentiality, integrity, and availability a top priority.

Read about the E-Series SANtricity OS 11.50 receiving the Common Criteria certification for Network Device Collaborative Protection Profile (NDcPP).

To learn about NetApp's drive security and management security solutions, see TR-4474: NetApp SANtricity Drive Security and TR-4712: NetApp SANtricity Management Security.

The Challenge

Each day, the threat landscape becomes larger and more sophisticated, and the stakes grow higher. As administrators and operators of data and information assets, storage engineers are expected to manage data in a secure manner throughout its lifecycle.

The Solution

This datasheet is an overview of the new and existing security features and functions in SANtricity 11.50 and later releases. It describes the essential elements for creating an industry-proven security posture for your most important resource, data.

NetApp®

Certificate Revocation Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Revocation Checking Using Online Certificate Status Protocol (OCSP)	OCSP enables E-Series applications that use TLS communications, such as LDAP or TLS, to receive digital certificate status. The application receives a signed response signifying that the certificate requested is good, revoked, or unknown. The preferred setting for Common Criteria mode is to enable OCSP.	With OCSP enabled, certificate revocation checking is performed and certificates are validated.

Cryptographic Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Transport Layer Security for Management Interface	E-Series leverages TLS v1.2 for secure communication and administration functions in the management GUI, secure CLI, and REST API.	NetApp does not recommend TLS v1.0 or TLS v1.1 because their significant vulnerabilities make these versions incompatible with compliance standards such as PCI-DSS. NetApp recommends using TLS v1.2 because of its strength and integrity.
FIPS Compliant Encryption	E-Series uses Bouncy Castle, a collection of APIs used in cryptography, which is FIPS 140-2 Level 1 compliant, for all encrypted data.	FIPS 140-2 Level 1 is the industry standard for cryptography products and solutions.

Data Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Full Disk Encryption (FDE)	FDE is a hardware-based encryption mechanism to encrypt data on self-encrypting drives. With FIPS140-2 certified FDE-capable drives, FIPS140-2 compliant cryptographic algorithms are used by the disk to encrypt the data.	Data encryption at rest continues to be an industry focus. FDE satisfies this focus while also maintaining a strong security posture at the subsystem level through other security-related features.
FDE Internal Key Management	The FDE internal key management feature is a self-contained encryption solution for data at rest. Internal key management works with FDE, which performs full-disk encryption by using self-encrypting drives.	FDE internal key management is a self-contained solution for organizations that prefer not to invest in external key management servers, thereby reducing total cost of ownership. The feature also allows users to secure data at rest, a pivotal data security solution.
FDE External Key Management	FDE external key management is handled through the use of a third-party system in the storage environment that securely manages authentication keys used by encryption features in the storage system, such as FDE. The storage system uses an SSL connection to contact the external key management server (for example, Gemalto SafeNet KeySecure) to store and retrieve authentication keys through the use of the industry-standard Key Management Interoperability Protocol (KMIP).	FDE external key management offers the ability to centralize an organization's key management functions while ensuring that keys are not stored near the assets, decreasing the possibility of compromise.
Secure Erase for FDE-Capable Drives	Use the Secure Erase feature to sanitize disks by removing data from an FDE-capable disk or a set of FDE-capable disks so that the data can never be recovered.	Security protocols for retiring or repurposing drives often require you to make data unrecoverable.

Message Logging Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Login and Message of the Day (MOTD) Banners (SANtricity OS 11.40.1 and later)	Login banners are printed in the output prior to authentication. These banners allow organizations and administrators to communicate with system users.	Login banners allow organizations to present operators, administrators, and even miscreants with terms and conditions of acceptable use for a system, and they also indicate who is permitted access to the system.
Secure Log Forwarding (Syslog over Transport Layer Security [TLS]) (SANtricity OS 11.40.1 and later)	The log-forwarding function allows administrators to provision targets or destinations, so they can receive syslog and audit information. Due to the secure nature of syslog and audit information, E-Series can send this information securely via TLS, using the TCP-encrypted parameter.	Log and audit information is invaluable to organizations from a support and availability standpoint. In addition, the information contained in logs (syslog) and audit reports and outputs is typically sensitive in nature. To maintain security controls and posture, log and audit data must be managed in a secure manner.
Simple Network Management Protocol (SNMP v2c)	SNMP is a standard protocol that allows network-attached devices (E-Series array) to report their status. E-Series supports SNMP v2c, which contains security improvements (community-based authentication). The preferred setting for Common Criteria mode is to disable SNMP.	This feature allows an SNMP management application to provide simple monitoring capabilities for NetApp E-Series storage arrays.

OS Authentication Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Digitally Signed SANtricity OS Firmware (SANtricity OS 11.40.2 and later)	Digitally signed controller firmware is required in version 8.42 and later. If the firmware is unsigned, download attempts are rejected. In addition, during array Start-Of-Day, it does a self-test to ensure that firmware is intact.	Prevents unauthorized or malicious users from downloading a non NetApp or modified code bundle.

User Access Control Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Role-Based Access Control (RBAC)	RBAC in E-Series allows administrators to limit or restrict users' administrative access to the level granted for their defined role. Administrators can manage users by their assigned role.	Access control is a foundational element for creating a security posture. Functions such as RBAC allow organizations to determine who has data access and to what extent they have access. This limits vulnerabilities and exploits, including data exfiltration and escalation of privileges.
Lightweight Directory Access Protocol (LDAP)	Ability to authenticate and authorize directory users is fundamental to deploying storage in enterprise IT environments.	Supports configuring and assigning users from LDAP to perform storage management functions on E-Series storage arrays.
Secure Lightweight Directory Access Protocol (LDAPS) for Directory Services Interactions	E-Series supports secure communication channel (LDAPS) when interacting with an LDAP server.	The LDAPS protocol helps to avoid transmitting sensitive information in clear text.
Multifactor Authentication (MFA) using SAML 2.0 Technology	The E-Series embedded SANtricity System Manager GUI supports SAML. Authentication can be managed through an identity provider (IdP) using SAML. An administrator establishes communication between the IdP system and the storage array, and then maps IdP users to the local user roles embedded in the storage array.	Support of the SAML standard enables implementation of multifactor authentication solutions, thereby complying with federal identity management guidelines.
Password Policy	This feature allows the administrator to set the number of login attempts to SANtricity System Manager for each controller before the user is locked out for a period of time. There are two lockout modes that the administrator can set: lockout based on the IP address (the default) and lockout based on the user account. The preferred method for Common Criteria mode is user-based lockout. E-Series allows configuring the password to require a minimum of 15 characters. The maximum length is 30 characters.	Reduces potential denial-of-service attacks because it prevents attackers from having unlimited attempts to try to gain access to the storage array. Setting to a larger minimum password length makes the password more difficult to crack and complies with federal requirements.

User Interface Security Features

SOFTWARE OR FEATURE	FUNCTION	IMPACT
Console Access via SSH	With E-Series, users can connect to the array console via SSH. The preferred setting for Common Criteria mode is to disable SSH access.	Console access via SSH is generally used to troubleshoot issues with the storage array. This task is usually performed with guidance from the NetApp Customer Support team.
Securing Protocols and Ports REST API Access over Secure HTTPS Protocol	E-Series supports the REST API, which provides a secure communication interface between the storage array and the management client over the secure HTTPS protocol. The preferred setting for Common Criteria mode is to disable SYMbol (a proprietary communication interface).	The REST API encrypted management interface helps to enforce confidentiality in communication between the storage array and the management client.
Secure Command-Line Access	E-Series implements the SMcli for communication to the storage array. Secure CLI introduces a secure communication channel used for CLI communication between client and server via the TLS protocol.	Establishing secure access to systems is a crucial part of maintaining a secure solution.

About NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations. For more information, visit **www.netapp.com**. #DataDriven