OSNEXUS

QuantaStor 6 - Security Features Overview

QuantaStor has a comprehensive set of security features to meet needs of organizations with high security compliance requirements. The breadth of security features in QuantaStor spans from authorization and authentication features, to end-to-end encryption, to immutability and snapshots to help protect against ransomware.

Distributed Security Enforcement with Storage Grid Technology
QuantaStor's grid technology enables IT organizations to link their QuantaStor storage systems together into a distributed control plane called a "storage grid". Once a grid is formed new users, roles and security policy changes are applied immediately across all systems within a grid. This makes it easy for IT security administrators to apply and enforce security policies and standards within and across sites.

Encryption-at-Rest
QuantaStor provides both hardware and software encryption for scale-out and scale-up configuration. Hardware encryption is available for us on SED media that is Opal/Ruby compliant. Software encryption can be used on all media types and is accelerated using the AES-NI features of the Intel and AMD CPUs.

Encryption-on-the-Wire
File protocol access via SMBv3 is configured with mandatory encryption by default which is inline with the default SMB protocol policies set within Windows Server. Additionally, S3-compliant object storage access uses HTTPS with TLS 1.2 and newer to ensure all object storage traffic is encrypted. For other storage protocols like iSCSI, FC, NVMeoF and NFS there are ipsec tunnelling options available for encrypting these protocols on the network.

256-bit AES

KMIP Integrated
QuantaStor supports the use of Key Management Interoperability Protocol (KMIP) to externally store and manage ones storage encryption keys. By leveraging the industry leading KMIP client library from Cryptsoft, QuantaStor is OASIS KMIP compliant to the latest standards and supports all commercial KMIP servers.

CRYPTSOFT

NIST Standards Compliant
Most of the major security compliance standards for industries such as health-care with HIPAA and law enforcement with CJIS are built on top of standards specified by the National Institute of Standards and Technology (NIST). The most important NIST standards around security compliance are NIST 800-53 (fed) and NIST 800-171 (non-fed) and QuantaStor has a rich set of security features specifically added to help organizations gain compliance to these standards. Separately, NIST has security standards for cryptographic modules which falls under the Federal Information Processing Standard (FIPS) 140-2 compliance. QuantaStor was FIPS 140-2 L1 certified in 2022. The L1 is a software level certification which enables QuantaStor to be operated in FIPS mode an a broad spectrum of hardware.

NIST

Immutability / WORM
QuantaStor supports Immutability for object storage and file storage which helps protect data from ransomware and other cyber attacks. In addition, file storage snapshots are immutable and when combined with the Long Term Snapshot Retention rules which can be specified in Replication and Snapshot Schedules it is easy to recover modified and/or deleted files.

Advanced Role Based Access Controls (RBAC)
A key tenant of security management is following the ‘Principle of Least Privilege’ so that each management user is assigned a Role that limits their access rights to the resources and operations needed for their job function.   QuantaStor has a patented (US-9953178-B2) RBAC system which makes creation of new Roles easy and adds powerful multi-tenancy features.

Single-Sign-On / LDAP Integrated
To simplify management of the grid management Roles within a QuantaStor storage grid may be associated with LDAP groups so that user accounts in LDAP may be given permission to directly login to the QuantaStor grid using ones LDAP user account. This will cause the a new DOMAIN\user account to be added to the storage grid automatically and LDAP associated accounts do all authentication through LDAP to enable single-sign-on functionatity.

LDAP

Active Directory (AD) Integration
For SMB protocol access to Network Shares one can assign ownership and access to specific Active Directory users and groups. This makes it easier to manage file and folder access in Windows and macOS environments especially.

Audit Logging
All management operations are recorded into an internal audit log that tracks all user activity from the QuantaStor web management interface, QuantaStor CLI, and QuantaStor API use. Additionally, QuantaStor also has file level audit logging for user access to Network Shares via the SMB protocol.

Multi-factor / 2FA Authentication
QuantaStor integrates with Cisco Duo to provide multi-factor authentication options with support for Google Authenticator in QuantaStor 6.2 and newer.

GDPR Compliance
To ensure security and protection of customer data QuantaStor systems do not send any automatic telemetry or other information from QuantaStor systems to OSNexus. Additionally the Send Log Report feature used to send logs to OSNexus does a pre-scrubbing of the generated logs files to remove all user names, IP addresses and any other user identifiable information before encrypting the logs and sending to support.osnexus.com. This pre-scrubbing of the logs provides IT organizations with additional protections and provides compliance to EU GDPR regulations for data retention. QuantaStor also provides and offline log collection and upgrade process for organizations with networks configured with no public internet access.

GDPR.EU

Firewall Management
QuantaStor has a built-in firewall management system to make it easy to disable unused protocols and features. Firewall management is granular such that enables specific protocols to be enabled or disabled on specific interfaces or system wide.

About OSNexus

Founded in 2010, OSNexus enables organizations to manage their storage as a distributed storage grid with its industry-leading QuantaStor Software Defined Storage (SDS) platform. QuantaStor systems combine together to deliver highly available and unified file, block, and object storage that deploys on standard hardware from all major manufacturers. For more information visit osnexus.com or write us at info@osnexus.com.