WHITE PAPER

Quantum Data Security and Data Privacy

Policies and Product Capabilities

Quantum

CONTENTS

INTRODUCTION

This document summarizes Quantum policies and product capabilities related to security and overall data privacy. It focuses on topics important to national laws and regulations that are important to our customers.

GENERAL SECURITY VULNERABILITY POLICIES

All Quantum products adhere to the Quantum Computer Security Incident Response Team (CSIRT) process. This process is designed to help protect Quantum products from security vulnerabilities and update them as newer threats are discovered. The process has a Detection phase and an Action phase.

Detection Phase

There are 3 forms of detection in this phase of the CSIRT process:

1. **Vulnerability Monitoring:** In this form, the CSIRT process monitors the US-CERT Cybersecurity & Infrastructure Security Agency (CISA) for reported threats that pertain to Quantum products or components of Quantum products.
2. **Vulnerability Scanning:** In this form, Quantum runs security vulnerability scanning software to detect whether the presence of known Common Vulnerabilities and Exposures (CVE) are present in a version of a Quantum product.
3. **Community Reporting:** In this form, Quantum customers and partners report to the Quantum service team that there is a potential vulnerability in a Quantum product that needs evaluation.

Action Phase

The Action Phase can take 3 forms:

1. **Communication:** This is the process of communicating the existence of vulnerabilities that have been identified in a Quantum product to customers and partners. Once a vulnerability has been identified, a Service Bulletin is generated explaining the nature of the vulnerability, the risks, any workarounds, and a timeline for remediation. Over time, Service Bulletins are updated to include new and relevant information as it becomes available.
2. **Remediation:** This is the act of developing workarounds and hardware and software fixes for identified Security Vulnerabilities. See the section below titled *Severity Scoring* for details on when to expect remediation for identified Security Vulnerabilities.
3. **Remediation Distribution:** This is the process of releasing new versions of product hardware and/or software, which has corrections for security vulnerabilities.

Severity Scoring

Quantum uses the CVSS (Common Vulnerability Scoring System) to assign a severity value to a Security Vulnerability. The CVSS calculator can be found here: https://www.first.org/cvss/calculator/3.1. The possible score values are: None, Low, Medium, High, and Critical. The value of the score can be used to determine when to expect remediation as noted below:

- Critical: Expect remediation within a month
- High: Expect remediation with the next maintenance release
- Medium/Low: Expect remediation at the next product release opportunity as needed

STORNEXT FILE SYSTEM

Quantum StorNext software is a high-performance file system and data management platform that stores and protects data. While StorNext has options to share data with other systems and the cloud, this MUST be configured by the administrator. Nothing is configured for data transfer by default. By default, StorNext data storage is self-contained on the hardware managed by the file system.

1. Protecting Data
    a. **Replication:** StorNext has an ability to replicate file data to other StorNext systems, and other non-StorNext file systems. This must be configured on StorNext by the administrator to either send or receive data.
    b. **Cloud:** StorNext can protect and archive data to several supported cloud targets, such as AWS, Azure, Google, or general S3 compatible targets, but it must be configured on StorNext by the administrator to send data out.
2. Allowing Data Transfer Out of Country
    a. If a transfer out of country is necessary, StorNext must be specifically configured by the administrator to accomplish this.
3. Data Reported to Quantum
    a. There is an option to report back metadata and statistics to Quantum Cloud Based Analytics (CBA) which is currently hosted in the US and managed by Quantum. This is an opt-in option which requires the StorNext administrator to configure it before it sends data to Quantum.
        i. Data is limited to performance logs and statistics and doesn't include any customer-generated data.
        ii. Customer-generated data is not retained by field service personnel maintaining the product.
4. Product Features to Aid Security
    a. **StorNext Users:** There are multiple types of administrative users within StorNext. These users all require authentication. The StorNext 7 GUI and corresponding web services use a role-based access control, which allows granular options for over 20 different areas of user responsibility and control.
    b. To monitor and log product operational status and cyber threats for the prior 6 months, StorNext has several logs maintained for audit purposes, but logs can be cleared by admin users. The logs do not monitor threats directly but can be used for audit and manual threat assessment.
    c. For patch and deployments to deal with security concerns please reference the Quantum Computer Security Incident Response Team (CSIRT) process detailed above.

ACTIVESCALE OBJECT STORAGE

ActiveScale is a completely self-contained object storage solution. Except for specific features that specifically need to be activated, ActiveScale does not need any external connection. The only exception is the need for an NTP server, which can be hosted locally in the customer data center.

While ActiveScale has options to share both data logs and metrics with the outside world, all of these features are opt-in and are controlled by the customer. Examples of these are:

- Replication to another ActiveScale system or AWS S3
- Monitoring through Prometheus, syslog, SNMP
- Home phone and email
- ActiveScale Cloud Manager

ActiveScale can be deployed as software running on appliances. The system can be supported, such that no drives containing data have to leave the premises for warranty fulfillment. Support operations, including through managed services, happen through looking at monitoring data that only includes metrics and events about hardware or software malfunctions. It never includes customer data or metadata.

The system comes with extensive auditing options. Next to the typical auditing of management operations, ActiveScale keeps a log of every data operation executed on the system, including write, read, list operations, etc. Audited information includes, but is not limited to: username, IP address, type of request, parameters, payload, etc. This enables the user of the system to use that information not only for auditing reasons but also as input for a billing system.

ActiveScale also supports a hierarchy of roles to keep your data protected:

- **Admin user or group** used to manage and monitor the systems hardware and the data users' logins and credentials. The admin users can be linked to an external AD or LDAP system.
- **Data account owners:** These users create and manage buckets. This includes managing access rights to the data users and setting retention policies. An important feature supported for these users is the S3 Lock feature. This enables the account owners to set a policy which enforces that no data written to the system can be physically removed from the system in a given time window.
- **Data users:** These users typically are only allowed to read/write data. They have the option to virtually delete data. Physical deletion of data typically happens by the account owners or by policies set by them.

As already indicated above, the combination of having these different roles with the S3 Lock feature, allows for setting up the system in a ransomware protected mode: even if the application writing the object store or the user with data rights to the object store has been compromised, data cannot be physically removed from the system before the expiration of the retention window.

In combination with Quantum CSIRT policy, ActiveScale has a 1-click rolling upgrade procedure that can be applied when reacting to security threats. During the upgrade the system stays operational and is designed to serve any request without downtime.

SCALAR TAPE STORAGE

Quantum Scalar Tape Storage systems provide low cost, secure data storage for long-term retention and archiving. Quantum Scalar Tape Libraries do not access customer data. Customer data is stored on media that is managed by the customer selected host/application.

1. Allowing Data Transfer Out of Country

   a. If a transfer out of country is necessary, the customer selected host/application would need to be configured by the customer to transfer data, not the Quantum Scalar tape library.

   b. If a Scalar Tape Library or Drive needs repair, there is no customer data that is returned with the hardware since the data is on the tape.

   c. If a cartridge is requested by a customer to be replaced under warranty, the customer can request degaussing of the defective cartridge to remove all data for leaving the region.

2. Data Reported to Quantum

   a. There is an option to report back metadata and statistics to CBA currently configured on Amazon Web Services (AWS) as well as an option to send statistics and trace logs back to Quantum tech support via emails that are configurable just like CBA. This is operational data to support the health of the Scalar tape library, not customer data. These options require the Scalar Library administrator to configure for it to take place.

      i. Data is limited to performance logs and statistics and doesn't include actual customer-generated data.

      ii. Likewise, actual customer-generated data is not accessed by field service personnel maintaining the product.

3. Product Features that Contribute to Access Security, Effective Incident Response, and Disaster Recovery Plans

   Quantum Scalar Libraries have a rich set of features designed to prevent security attacks and to protect the privacy of our customers. Here is a detailed list of the security features supported by Quantum Scalar Libraries:

   a. Authenticate user identity.

      i. Scalar Libraries support RBAC (Role-based access control) via login ID and password.

         1. **Administrators -** Have access to all library configuration and operation functionality.

         2. **Users -** Have access to one or more assigned partitions and can perform operations within a partition. A user cannot perform configuration changes and is restricted to operations only.

         3. **Service -** Has access to the same functionality as administrators except for user access configuration. Each library has only one service account. Administrators can restrict to local on-device UI only and set time-limited window for access or completely disable service login access.

      ii. LDAP and secure LDAPS is supported.

      iii. Multi Factor Authentication (MFA) is available to add an additional layer of protection with a second authentication. This feature is not enabled with Lightweight Directory Access Protocol (LDAP).

      iv. Complex password support.

      v. Login Failure Lockout after time-period or failed attempts.

      vi. Inactivity will log out user (session timeouts).

b. Prevent computer viruses and cybersecurity/intrusion threats (including ransomware)

i. Will only allow Quantum authenticated data on library control firmware digitally signed. The firmware update process will reject non-authentic firmware updates by testing the digital signature.

ii. Active Vault feature that isolates partition(s) from visibility to applications or network.

iii. Configurable session lengths to limit access.

iv. Limit IPv4/v6 address that can access the library UI.

v. Configurable time-limited reverse tunnel for support access.

vi. ICMP disable prevents discover of the tape library via 'ping'.

vii. Support for LTO Write once read many (WORM) media that affords assurance that data cannot be tampered with once written.

c. Monitor and log product operational status and cyber threats for the prior 6 months

i. Media Security notifications on expected and unexpected media removal events.

ii. Audit reporting for log user activity and library configuration change reports.

iii. Firmware release is tested with multiple security scanners.

iv. New library firmware release is authenticated prior to being installed.

v. Library alerts operator when updated firmware is available.

vi. Security and health information may be monitored via Simple Network Management Protocol (SNMP).

d. Enable data classification, backup, and encryption of important data

i. Supports Tape encryption, including FIPS-validated.

ii. Support for application-based or library-managed SKM or KMIP encryption.

iii. Encryption key usage policy with choice of one key per tape, partition, or library.

e. Promptly deploy security threat/patch remediation

i. For patch and deployments to deal with security concerns please reference the Quantum Computer Security Incident Response Team (CSIRT) process detailed in previous section.

DXi BACKUP APPLIANCES

DXi Backup Appliances are backup storage systems that provide deduplication and replication. While DXi has options to share data with other systems and the cloud, this MUST be configured by the customer. Nothing is configured for data transfer by default. By default, the DXi is a self-contained storage appliance.

1. Protecting Data

a. **Replication:** DXi has an ability to replicate data to any server anywhere, but this must be configured on the DXi to either send or receive data.

2. Allowing Data Transfer Out of Country

a. If a transfer out of country is necessary, the DXi must be specifically configured by the customer to accomplish this.

3. Data Reported to Quantum

a. There is an option to report back metadata and statistics to CBA currently configured on Amazon Web Services (AWS). This is an opt-in option, so DXi admin must configure it for it to take place.

i. Data is limited to performance logs and statistics and does not include actual customer-generated data.

ii. Likewise, actual customer-generated data is not accessed or retained by field service personnel maintaining the product.

4. The DXi appliance includes an ability called “Secure Snapshot” that allows the isolation of select backups in a non-network addressable tier.

a. **DXi Users:** There are multiple types of users within DXi.

i. Admin and system users: Protected by password. Local users that are not LDAP or Active Directory (AD) authenticated and are not shared between systems.

ii. Data Access users that can mount backup drives: Protect by password and can be AD authenticated.

iii. Backup Access Users: Users specifically created by backup applications for writing data from that specific backup application (i.e., NetBackup or Veeam). Security for these users is controlled by the backup application.

iv. Operators: Operators are granted access to specific backup shares and have limited access control. These are local users and not LDAP or AD authenticated.

b. The “root” users for DXi systems are well protected by being renamed and can be disabled from the GUI.

i. To monitor and log product operational status and cyber threats for the prior 6 months DXi has several logs maintained for audit purposes, but logs can be cleared by admin user.

c. Data Classification is managed by the backup server, but within DXi can be tiered by:

i. Selecting replication to replicate to other systems.

ii. Backing up data to a “secure snapshot” share so that protected snapshots of data are regularly created and protected.

iii. All data on disk is encrypted if SED systems are selected at purchase

1. For Virtual system encryption on disk depends upon the disk purchased by the customer.

iv. All data is encrypted on disk and in flight (if enabled).

d. For patch and deployments to deal with security concerns please reference the Quantum Computer Security Incident Response Team (CSIRT) process detailed above.

CLOUD-BASED ANALYTICS (CBA)

CBA is a cloud-based monitoring and management tool that enables Quantum administrators, the Quantum support organization, and authorized service providers to remotely monitor the system health of Quantum products as well as provide insightful information on just how those systems are being utilized. There are 2 fundamental components with CBA, which requires special attention to detail to ensure the security of data and how that data is accessed.

1. Communication between the Quantum product and CBA to transfer performance data and logs to the cloud infrastructure.
2. End-user browser access to the CBA portal.

To facilitate remote support of Quantum products, CBA supports a reverse tunnel feature, which provides customers a mechanism to allow, on an as needed basis, Quantum service team members to remotely access the product for troubleshooting and repair. This reverse tunnel functionality is controlled entirely by the customer.

The below describes the levels of security used by CBA.

Secure Communication With the Product and CBA

- All communication between the product and the CBA is SSL/TLS2.0 secured to prevent eavesdropping.
- The product maintains an HTTPS certificate that uniquely identifies CBA. If the certificate cannot be verified, the product will not transmit data to the cloud server. This prevents man-in-the-middle, DNS, and other attacks to gain access to the product's data.
- Each product is assigned a unique "identity" by CBA, which includes a unique random key. The identity key is used to generate a cryptographically secure request signature using an algorithm similar to the AWS v4 signing algorithm - providing verification and protection of the communication channel between the product and the CBA cloud to prevent spoofing or replaying product communications.
- Agents have rules defining which data can be sent to the cloud and which data cannot. Only performance, component health, and log data are sent to the cloud. There is no mechanism for customer generated data to be transmitted.

Secure User Access to the CBA Portal

- All communications between the CBA portal and a user's browser are protected by SSL/TLS2.0.
- The CBA portal uses role-based access control with password-based authentication. Roles include: Quantum Administrator, Quantum Service, Service Partners, and End Customers.
- The CBA portal is a multi-tenant solution managed by qualified Quantum support staff who implements access-controls to ensure that a user only has access/visibility to the features and products that they own.
- The CBA portal has a documented and scheduled patching process to prevent exposure/vulnerabilities.
- The Quantum support organization monitors CBA portal 24/7 for availability and for expected performance of internal services.
- The CBA portal uses stateful firewalls to protect the servers from attacks.
- All customer telemetry data is backed up and retained for up to 3 years.

- Critical database fields are encrypted for an extra layer of protection.
- Quantum uses several scanning and endpoint protection tools on the cloud infrastructure to protect the servers from malicious behavior, viruses, vulnerabilities, etc.
- Quantum system administrators of the CBA portal rotate their keys to protect administrative access to the infrastructure.
- The CBA portal is deployed in the AWS US East data center, which provides physical security to the infrastructure.
- Quantum performs ongoing and regular internal IT audits of the cloud infrastructure as part of its continuous improvement program.

CONCLUSION

This document should have given you a strong understanding of the security capabilities of Quantum products. For additional questions, please contact your Quantum sales representative or reseller.