白皮书

Quantum 数据安全和数据隐私

策略及产品功能

Quantum

目录

引言

本文档概述了与安全和整体数据隐私相关的 Quantum 策略及产品功能。主要介绍的主题是对我们的客户至关重要的相关国家法律法规。

一般安全漏洞策略

所有 Quantum 产品均遵循 Quantum 计算机安全事件应急响应小组（Quantum Computer Security Incident Response Team，CSIRT）流程。该流程旨在确保 Quantum 产品免受安全漏洞的影响，并在发现新威胁时对产品进行更新。该流程包含检测阶段和应对阶段。

检测阶段

在 CSIRT 流程的这一阶段有 3 种形式的检测：

1. 漏洞监控：在这种检测形式下，CSIRT 流程监控 US-CERT 网络安全和基础设施安全局 (CISA) 是否报告了与 Quantum 产品或 Quantum 产品组件有关的威胁。
2. 漏洞扫描：在这种检测形式下，Quantum 运行安全漏洞扫描软件，以检测 Quantum 产品中是否存在已知的通用漏洞披露 (CVE)。
3. 社区报告：在这种检测形式下，如果 Quantum 产品中存在需要评估的潜在漏洞，Quantum 客户和合作伙伴将向 Quantum 服务团队报告。

应对阶段

应对阶段有 3 种形式的应对：

1. 告知：向客户和合作伙伴告知 Quantum 产品中存在已识别的漏洞。一旦发现漏洞，将生成一份服务公告，解释漏洞的性质、风险、解决方案以及修复时间表。服务公告会不定期更新，以包含可用的新的相关信息。
2. 修复：针对已识别的安全漏洞开发解决方案以及进行硬件和软件修复。请参阅下文 *“严重性评分”* 一节，详细了解何时对已识别的安全漏洞进行修复。
3. 修复版本分发：发布新版本的产品硬件和/或软件，对安全漏洞进行更正。

严重性评分

Quantum 使用通用漏洞评分系统（Common Vulnerability Scoring System）为安全漏洞分配严重性值。可访问以下网址获取 CVSS 计算器：https://www .first .org/cvss/calculator/3 .1 .分值有：零、低、中、高和临界。通过分值确定何时进行修复，如下所示：

- 临界：在一个月内进行修复
- 高：在下一个维护版本中进行修复
- 中/低：视情况需要，在下一次产品发布时进行修复

STORNEXT 文件系统

Quantum StorNext 是一个存储和保护数据的高性能文件系统和数据管理平台。虽然 StorNext 有与其他系统和云共享数据的功能选项，但必须由管理员进行配置。默认情况下，不会进行任何数据传输配置。默认情况下，StorNext 数据存储自包含在文件系统管理的硬件中。

1. 保护数据

   a .复制：StorNext 可将文件数据复制到其他 StorNext 系统以及其他非 StorNext 文件系统。管理员必须在 StorNext 上对此进行配置，以发送或接收数据。

   b .云：StorNext 可保护数据并将数据存档到多个受支持的云目标，例如 AWS、Azure、Google 或通用 S3 兼容目标，但管理员必须在 StorNext 上对其进行配置，才能进行数据发送。

2. 将数据传输往境外

   a .如果需要将数据传输往境外，则必须由管理员对 StorNext 进行专门配置，才能执行此操作。

3. 向 Quantum 报告的数据

   a .可将元数据和统计数据报告给目前在美国托管并由 Quantum 管理的 Quantum Cloud Based Analytics (CBA)。这是一个选择加入选项，需要 StorNext 管理员在将数据发送到 Quantum 之前对其进行配置。

      i .数据仅限于性能日志和统计数据，不包括由客户生成的任何数据。

      ii .维护产品的现场服务人员不会保留客户生成的数据。

4. 确保安全的产品功能

   a .StorNext 用户：StorNext 中有多种类型的管理用户。此类用户都需要进行身份验证。StorNext 7 GUI 和相应的 Web 服务使用基于角色的访问控制，可为 20 多项不同的用户责任和控制提供各种细分选项。

   b .为监控和记录前 6 个月的产品运行状态和网络威胁，StorNext 会维护多个日志以用于审计，然后管理员用户可以清除日志。日志不直接监控威胁，但可用于威胁的审计和人工评估。

   c .有关处理安全问题的补丁和部署，请参考上文详述的 Quantum 计算机安全事件应急响应小组（Quantum Computer Security Incident Response Team，CSIRT）流程。

ACTIVESCALE 对象存储

ActiveScale 是一个完全自包含的对象存储解决方案。除了特别需要激活的特定功能外，ActiveScale 不需要任何外部连接。唯一的例外是需要可在客户数据中心本地托管的 NTP 服务器。

ActiveScale 可与外界共享数据日志和指标，不过此类功能都是可选的，由客户进行选装。例如：

- 复制到其他 ActiveScale 系统或 AWS S3
- 通过 Prometheus、syslog、SNMP 进行监控
- 家庭电话和电子邮件
- ActiveScale 云管理平台

ActiveScale 可以部署为在设备上运行的软件。提供系统支持，因此包含数据的驱动器不必离场进行保修。通过查看仅包含硬件或软件故障指标和事件的监控数据来支持操作（包括通过托管服务）。不包括客户数据或元数据。

该系统有广泛的审计功能选项。除了管理操作的典型审计之外，ActiveScale 还会保存系统上执行的每项数据操作的日志，包括写入、读取、列表操作等。经审计的信息包括但不限于：用户名、IP 地址、请求类型、参数、有效负载等。系统用户不仅可以出于审计原因使用该信息，还可以将其用作计费系统的输入数据。

ActiveScale 还支持角色层次结构，以保护您的数据：

- 管理员用户或组，用于管理和监控系统硬件以及数据用户的登录和凭据。可以将管理员用户链接到外部 AD 或 LDAP 系统。
- 数据帐户所有者：此类用户创建和管理存储桶。包括管理数据用户的访问权限和设置保留策略。面向此类用户的一项重要支持功能是 S3 锁定功能。帐户所有者能够设置策略，强制在给定的时间窗口内不能从系统中物理删除写入系统的任何数据。
- 数据用户：此类用户通常只被允许进行数据读写。其可以选择虚拟删除数据。数据的物理删除通常由帐户所有者或依据其设置的策略执行。

如上所述，将这些不同的角色与 S3 锁定功能相结合，允许在勒索软件保护模式下设置系统：即使写入对象存储的应用程序或对对象存储具有数据权限的用户受到威胁，数据也无法在保留窗口到期之前从系统中物理删除。

依据 Quantum CSIRT 的策略，可在应对安全威胁时应用 ActiveScale 的一键式滚动升级程序。在升级过程中，系统将保持运行状态，并且可以在不停机的情况下处理任何请求。

SCALAR 磁带存储

Quantum Scalar 磁带存储系统提供低成本、安全的数据存储，以实现长期保留和存档。Quantum Scalar 磁带库不会访问任何客户数据。客户数据存储在由客户选择的托管平台/应用程序管理的介质中。

1. 将数据传输往境外

a .如果需要将数据传输往境外，则客户需要配置客户选择的托管平台/应用程序以传输数据，而不是 Quantum Scalar 磁带库。

b .如果 Scalar 磁带库或驱动器需要维修，客户数据不会随硬件返回，因为数据位于磁带上。

c .如果客户要求在保修期内更换盒带，客户可要求对有缺陷的盒带进行消磁以擦除所有数据，然后盒带方可离场。

2. 向 Quantum 报告的数据

a .可向当前在 Amazon Web Services (AWS) 上配置的 CBA 报告元数据和统计数据，以及通过电子邮件将统计数据和跟踪日志发送回 Quantum 技术支持团队，此类电子邮件与 CBA 一样可配置。此类数据为支持 Scalar 磁带库运行状况的操作数据，而不是客户数据。此类选项由 Scalar 库管理员进行配置，以便执行操作。

i .仅限于性能日志和统计数据，不包括客户生成的实际数据。

ii .同样，维护产品的现场服务人员无权访问客户生成的实际数据。

3. 确保访问安全、有效事件应急响应和灾难恢复计划的产品功能

Quantum Scalar 库功能丰富，旨在防止安全攻击和保护客户的隐私。以下是 Quantum Scalar 库支持的安全功能的详细列表：

a .验证用户身份。

i .Scalar 库通过登录 ID 和密码支持 RBAC（基于角色的访问控制）。

1. 管理员 - 具有访问所有库配置和操作功能的权限。
2. 用户 - 具有访问一个或多个分配的分区的权限，并可在一个分区内执行操作。用户无法执行配置更改，仅具有操作权限。
3. 服务 - 除用户访问配置外，具有与管理员相同的功能访问权限。每个库只有一个服务帐户。管理员可以限制为仅在设备本地用户界面进行访问，并为访问设置时间限制窗口或完全禁用服务登录访问。

ii .支持 LDAP 和确保安全的 LDAP (LDAP and secure LDAPS is supported）。

iii .多重身份验证 (MFA) 可用于通过二次身份验证提供额外保护。轻型目录访问协议 (LDAP) 未启用此功能。

iv .复杂密码支持。

v .登录超时或者多次登录失败后执行登录失败锁定。

vi .用户若不执行活动，系统会自动退出登录（会话超时）。

b .防止计算机病毒/入侵威胁（包括勒索软件），确保网络安全

i .仅允许库控制固件上的 Quantum 经验证数据进行数字签名。固件更新过程中将进行数字签名测试，以拒绝非正版固件更新。

ii .Active Vault 功能将分区与应用程序或网络的可见性隔离开来。

iii .可配置会话长度以限制访问。

iv .限制可以访问库 UI 的 IPv4/v6 地址。

v .用于支持访问的可配置限时反向隧道。

vi .ICMP 禁用可防止通过“ping”发现磁带库。

vii .支持 LTO 一次写入多次读取 (WORM) 介质，可确保数据一旦写入就不会被篡改。

c .监控和记录前 6 个月的产品运行状态和网络威胁

i .操作性和意外介质删除事件的介质安全通知。

ii .日志用户活动和库配置更改报告的审计报告。

iii .通过多个安全扫描器对固件版本进行测试。

iv .在安装之前对新的库固件版本进行身份验证。

v .当更新的固件可用时，库会提醒操作员。

vi .通过简单网络管理协议 (SNMP) 对安全和健康信息进行监控。

d .启用重要数据的数据分类、备份和加密

i .支持磁带加密，包括 FIPS 验证的加密。

ii .支持基于应用程序或库管理的 SKM 或 KMIP 加密。

iii .加密密钥使用策略，可为每个磁带、分区或库选择一个密钥。

e .及时部署安全威胁/补丁修复

i .有关处理安全问题的补丁和部署，请参考上文详述的 Quantum 计算机安全事件应急响应小组（Quantum Computer Security Incident Response Team，CSIRT）流程。

DXi 备份设备

DXi 备份设备是提供重复数据删除和复制的备份存储系统。虽然 DXi 有与其他系统和云共享数据的功能选项，但必须由管理员进行配置。默认情况下，不会进行任何数据传输配置。默认情况下，DXi 是一个自包含的 (self-contained) 存储设备。

1. 保护数据

a .复制：DXi 能够将数据复制到位于任何位置的任何服务器，但必须在 DXi 上进行配置以发送或接收数据。

2. 将数据传输往境外

a .如果需要将数据传输往境外，则必须由客户对 DXi 进行专门配置，才能执行此操作。

3. 向 Quantum 报告的数据

a .可向当前在 Amazon Web Services (AWS) 上配置的 CBA 报告元数据和统计信息。这是一个选择加入选项，需要 DXi 管理员对其进行配置。

i .数据仅限于性能日志和统计数据，不包括客户生成的实际数据。

ii .同样，维护产品的现场服务人员无权访问或保留客户生成的实际数据。

4. DXi 设备包括一项称为“安全快照”的功能，可在非网络可寻址层中隔离选定的备份。

a .DXi 用户：DXi 中有多种类型的用户。

i .管理员和系统用户：受密码保护。未通过 LDAP 或 Active Directory (AD) 进行身份验证且未在系统之间共享的本地用户。

ii .可以装载备份驱动器的数据访问用户：受密码保护，可通过 AD 进行身份验证。

iii .备份访问用户：由备份应用程序专门创建的用户，用于从该特定备份应用程序（即 NetBackup 或 Veeam）写入数据。备份应用程序确保用户的安全。

iv .操作员: 操作员被授予访问特定备份共享的权限，并且具有有限的访问控制权限。其为本地用户，未经 LDAP 或 AD 进行身份验证。

b .DXi 系统的“root”用户通过重命名得到充分保护，并且可从 GUI 禁用。

i .为监控和记录前 6 个月的产品运行状态和网络威胁，DXi 会维护多个日志以用于审计，然后管理员用户可以清除日志。

c .数据分类由备份服务器管理，但在 DXi，可以通过以下方式进行分层：

i .选择复制以复制到其他系统。

ii .将数据备份到“安全快照”共享，以便定期创建和保护数据的受保护快照。

iii .如果在购买时选择了 SED 系统，则磁盘上的所有数据都会被加密

1 .对于虚拟系统，磁盘加密功能取决于客户购买的磁盘。

iv .所有数据都在磁盘上和飞行模式下（如果启用）加密。

d .有关处理安全问题的补丁和部署，请参考上文详述的 Quantum 计算机安全事件应急响应小组（Quantum Computer Security Incident Response Team，CSIRT）流程。

结语

阅读完本文档，希望您对 Quantum 产品的安全功能有了深入了解。如果有其他疑问，请联系您的 Quantum 销售代表或经销商。