ESG 展示

网络弹性对于任务关键型存储至关重要

日期： 2022 年 10 月 **作者：** 业务实践主管 Scott Sinclair；高级研究分析师 Monya Keane

摘要： IT 环境已发生改变。数据现在成为了一种高价值资产，网络威胁也因此变得无处不在。所以，在选择任务关键型存储时，网络弹性是一项必须坚持的核心原则。通过 PowerMax，Dell Technologies 直接构建基本网络弹性功能并将其集成到这些系统中，进一步确立了自身在任务关键型存储领域的非凡地位。

概览

数据是一种至关重要且极具价值的商业资产。ESG 研究显示，59% 的受访组织认为数据基本等同于他们的业务，预计这一比例将在两年内增加到 81%。[1]任务关键型存储基础架构的作用是保留、保护和交付那些支持不能出现故障的工作负载和应用的数据。

数十年来，部署"任务关键型存储"即代表着提供必要性能和扩展，同时确保始终可用，以防止组件故障、站点故障、用户错误和自然灾害。如今，恶意攻击愈发普遍。因此，任务关键型存储的核心原则必须超越传统功能，将改善组织的网络弹性态势也纳入其中。

作为企业级存储领域的佼佼者，Dell Technologies 将继续发展其旗舰存储平台 PowerMax，致力于满足要求苛刻的 IT 环境的任务关键型需求。戴尔近期的创新工作集中在为 PowerMax 产品线注入一系列强大功能，帮助各组织提高其网络弹性，从而更好地保护其数据和重要应用程序、维护其品牌声誉并实现长期成功。

针对数据的网络威胁始终存在的时代

随着网络威胁的增加，IT 工作的复杂性也在增加。近一半 (46%) 的 ESG 调查受访者表示，如今的 IT 工作比两年前更加复杂。网络安全环境的快速发展（37% 的受访者提到）以及遵守新数据安全和隐私法规的工作（32% 提到）是导致 IT 工作复杂性的两个最常见因素。[2]

不仅如此，组织目前也在努力聘用技术娴熟的网络安全人才，力图克服这一复杂性问题。48% 的受访组织表示，他们没有足够多的网络安全专家，这是企业 IT 目前最常提到的技能短缺问题。[3]

[1] 来源：ESG 研究报告，*Data Infrastructure Trends*，2021 年 11 月。

[2] 来源：ESG 完整调查结果，*2022 Technology Spending Intentions Survey*，2021 年 11 月。

[3] 同上。

勒索软件和恶意软件盛行

企业面临诸多威胁，而外部勒索软件和恶意软件攻击其实已然无法避免。ESG 近期对 IT 和网络安全专业人员进行了一项研究调查，他们的职责是监督用于保护公司免受勒索软件攻击的技术和流程，其中 79% 的受访者表示在过去 12 个月内遭遇过勒索软件攻击。其中 30% 表示，攻击每周发生一次，甚至更加频繁。[4]

在遭遇过攻击的组织中，73% 至少遭受过一次成功的攻击。但在这种情况下，支付赎金并非最优选择，甚至谈不上是一种明智策略。56% 遭受成功攻击的组织支付了赎金。但是，在按要求支付赎金的组织中：

- **87%** 再次遭到了勒索，犯罪分子要求支付更多赎金。事实上，在第一次支付赎金的组织中，有 61% 最终会支付更多赎金。[5]
- 支付赎金后，也只有 **14%** 的组织完全拿回了他们的数据。
- **61%** 的组织在支付赎金后只拿回了 75% 甚至更少的数据。

显然，成熟的勒索软件保护需要一种更多面的策略，包含针对检测、预防和恢复的多种技术和工具。

现在，许多组织都在根据 NIST 网络安全框架提供的指导来建模其网络弹性战略，该框架建议组织识别并保护关键资源、检测故障和违规，以及规划针对网络事件的响应和恢复。组织广泛采用的另一个 NIST 框架组件是零信任体系结构，它不考虑防护网络边缘的概念，而是采用"从不信任，始终验证"的做法。在此模型中，必须重复定期验证用户（甚至组织内部人员）的安全配置，然后用户才能访问应用程序/数据。

存储系统必须是这种网络安全方法的一部分。毕竟，ESG 研究表明，勒索软件攻击最常瞄准的基础架构组件便是存储硬件。40% 的受访者提到了这一点。

任务关键型存储如何提高抗勒索软件能力

勒索软件攻击以访问和加密重要业务数据为主。许多网络弹性战略都以工具和技术为基础，这些工具和技术专注于防范威胁，防止威胁进入网络，并及早检测所有渗入的威胁。但是，因为勒索软件的存在，我们还必须注重加速恢复。

任务关键型存储系统位于数据路径的某个位置，这是帮助在发生攻击后快速恢复数据的主要位置。例如，随着勒索软件成功攻击次数的增加，一些存储系统已经能够利用其中包含的功能，通过保存并提供安全且不可变的数据卷拷贝来帮助实现快速恢复。

[4] 来源：ESG 研究报告：*The Long Road Ahead to Ransomware Preparedness*，2022 年 6 月。除非另有说明，否则本展示中所有的 ESG 研究引用均来自此研究报告。

[5] 来源：ESG 完整调查结果：*The Long Road Ahead to Ransomware Preparedness*，2022 年 6 月。

这种支持对于加速恢复极具价值。系统可以快速将快照识别为"已知良好"的卷，并由 IT 快速恢复，将数据集恢复到之前的原始状态。但是，对于任务关键型应用程序环境，*存储技术则必须更加强大*。

戴尔 PowerMax 可改善组织的网络弹性态势

数十年来，产品名称不断变化，功能不断增加，但自 20 世纪 80 年代后期 EMC 将企业级存储确定为单独的 IT 类别以来，Dell Technologies 的任务关键型基础架构存储系统一直在这一领域中保持前列。如今，戴尔 PowerMax 具有多种功能，旨在满足任务关键型工作负载的细致要求，包括：

- 全 NVMe 多控制器横向扩展体系结构，可大规模实现一致的强劲性能。
- 大规模工作负载整合，支持各种数据块和文件应用程序环境，包括大型机工作负载、裸机系统、虚拟机、容器等。
- 高级别的安全性、可用性和弹性。据戴尔表示，PowerMax 提供 99.9999% 的可用性，支持从主机到 PowerMax 的端到端数据加密、静态数据加密和安全快照，确切地说，它支持*每个阵列多达 6,400 万个快照*。此外，戴尔的 Symmetrix Remote Data Facility (SRDF) 灾难恢复软件使用高级拓扑和自动化功能，为出色的弹性奠定了坚实基础。借助 SRDF，组织甚至可以创建安全隔离的存储区。在该存储区中，数据互相隔离，与存储区的连接是间歇性的且高度受限。

戴尔精心构建 PowerMax，助力实现出色弹性

最近，戴尔专注于在 PowerMax 中构建和整合更多安全功能。例如，PowerMax 现在针对基于戴尔七大零信任支柱的零信任安全环境而设计，包括通过以下方式对系统本身进行固有安全防护/保护，使其免受攻击：

- 不可变的硬件信任根功能 — 这些功能可跨节点、介质存储模块和控制台验证硬件和软件更改。戴尔制造部门将嵌入式不可变组件级加密密钥物理融入内存中。
- 安全启动信任链功能 — 这些功能可建立并扩展固件"信任链"，针对性地防范恶意启动、内核和驱动程序 Rootkit。安全启动信任链对基于戴尔签名的后续固件加载/启动加载程序使用加密身份验证。
- 数字签名固件更新 — PowerMax 还利用戴尔的数字签名身份验证来防范未经授权的固件更新。它使用加密身份验证密钥扫描节点、介质和控制台组件。

除了这一值得信赖的设计之外，PowerMax 还提供其他功能，以改进对勒索软件攻击和其他网络安全威胁的预防、检测和恢复。

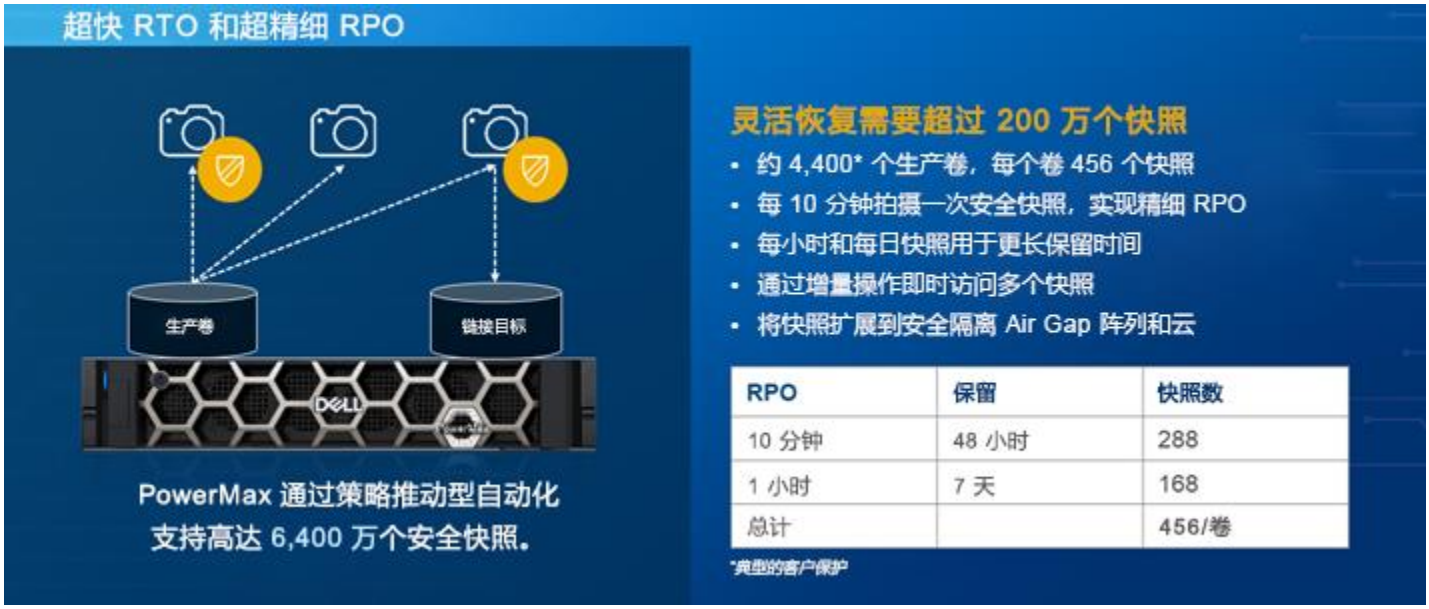
在预防方面，除了具有内置硬件安全性外，PowerMax 还凭借其防止未经授权的用户访问这一高级安全功能帮助防止攻击，支持通用标准、STIG 强化/APL、FIPS 140 认证的安全认证，以及受信任管理员访问控制机制，例如：

- SecurID 多因素身份验证，用于验证管理员身份。
- 包含证书/私钥的 CAC/PIV 智能卡支持，用于访问美国联邦政府的在线资源。
- 基于角色的访问控制 (RBAC)、LDAP 支持和 zDP 2 Actor（需要两个人执行特定 zDP 命令），仅允许授权用户执行指定操作，例如存储资源调配。

在检测方面，PowerMax 硬件和 Dell CloudIQ AI 软件均提供恶意软件异常检测。这是基于网络安全警报协议的合规性警报，以及安全系统日志警报和导出。具体而言，CloudIQ 通过监视异常 PowerMax 存储利用率和可疑活动指标来快速检测网络攻击。然后，它会提醒管理员注意由于可能的加密而出现的任何重大变化。它还可以持续监视存储基础架构，自动识别错误配置的系统设置带来的网络安全风险，然后提供详细的建议来纠正这些问题。

在恢复方面，PowerMax 安全快照技术将数据安全和保护提升至新的水平。根据企业的服务级别目标，IT 可以在每个 PowerMax 上配置多达 6,400 万个快照拷贝（参见图 1）。

图 1.PowerMax 如何支持快速网络恢复



资料来源：Dell Technologies

此功能使 PowerMax 支持攻击成功前几分钟的恢复点目标 (RPO)。同时，由于支持这么庞大的快照数量，IT 将拥有足够的拷贝来妥善保护大型整合任务关键型存储环境，从而实现任务关键型应用程序的几乎即时恢复。这种级别的保护灵活性正在大规模地颠覆生产环境。据戴尔表示，PowerMax 可大规模提供极精细的网络恢复，以便优化 RPO。

戴尔还可以为需要远程存储区安全隔离恢复选项 (SRDF) 的组织增加 PowerMax 网络恢复存储区选项，并为开放系统和大型机存储等提供编排存储/恢复。PowerMax 网络恢复存储区产品将于本月晚些时候正式上市，并使用 SRDF 远程复制来创建安全隔离 Air Gap。此解决方案专为需要在其生产网络外使用快速恢复 (RTO) 进行数据拷

贝的客户而设计。虽然 PowerMax 客户已经手动部署此配置一段时间，但本月发布的公告包含部署编排自动化和 Dell Professional Services，可以简化安装。

更重要的事实

提到安全供应商时，人们通常并不会首先想到戴尔。这种认知需要改变。恶意攻击者越来越有组织性，他们造成的威胁也变得愈发复杂。戴尔正在并将继续进行大量投资，帮助应对这些威胁、保护数据，并简化全面地管理安全性和弹性。

数据是组织最重要的资产，必须受到妥善保护，并且始终可用。而这种可用性面临的新威胁则源于勒索软件、恶意软件和其他网络攻击。而 PowerMax 在支持高端任务关键型工作负载方面具有强大的背景优势。多年来，戴尔一直坚持如此，但 PowerMax 的新功能尤其适用于如今几乎所有的存储购买者。每个人都担心勒索软件、恶意软件，害怕登上新闻头条。

这并不仅仅是防范渴望横财的窃贼。这些黑客可能为外国政府工作，窃取知识产权以增强其自身的国家安全或军事实力。除了剥夺您对数据的访问权之外，如果他们还可以加密您的数据，那么谁也不知道他们会用这些数据做些什么。

如果您有什么业务信息决不能落入坏人之手，您就需要与戴尔讨论如何正确保护存储基础架构。