DELL Technologies
戴 尔 科 技 集 团

2022 年 1 月

集成式网络安全防御策略

抵御针对 PowerScale 数据的多方位攻击

简介

网络攻击已成为各种规模的企业和垂直领域持续面临的一项严峻威胁。每 11 秒就会发生一次网络攻击[1]，一次攻击造成的平均损失为 1300 万美元[2]，而这个数字还在不断增长。网络攻击也变得越来越复杂，甚至可以突破相当现代化的安全措施。事实上，“攻击创新”可以通过某些复杂的 DevOps 流程来突破最新的安全措施。攻击者会使用多方位攻击，此类攻击可寻找终端用户设备、应用程序和操作系统、网络以及数据存储基础架构中的漏洞。虽然 IT 生态系统的这些层都有相应的点式解决方案，但我们必须将这些层关联在一起，才能更大限度地加快检测和响应此类攻击的速度。

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[2] https://www.accenture.com/us-en/insights/security/cost-cyber-crimestudy

本白皮书说明了由 Superna 的 Ransomware Defender 和 Smart Airgap 技术提供支持的戴尔 PowerScale 网络保护解决方案如何通过 API 集成，利用来自 IT 生态系统不同层的安全情报来抵御网络威胁。API 集成可以触发自动响应，例如终止对数据避风港存储区的复制、拦截可疑用户、标记损坏的数据等，甚至可以在攻击者试图突破安全防御层的过程中做到这一点。这种方法可以大大缩短检测和响应时间，并使 IT 团队能够比攻击者先行一步。

适用于 PowerScale/Isilon 的 Dell Technologies 网络保护解决方案概览

戴尔 PowerScale 网络保护解决方案有两个主要组成部分：

通过 Smart Airgap 实现数据隔离

Smart Airgap 解决方案可将数据副本与所有内部和外部网络路径隔离开来，是作为最后一种手段的恢复副本。数据最初复制到数据避风港存储区后，生产环境与数据避风港存储区副本之间会保持网络阻断状态。要进一步进行增量复制，只能在确保没有已知事件表明生产站点上存在安全漏洞后，通过关闭网络阻断来间歇性地完成。

检测可疑的数据访问方式并触发广泛的响应

Ransomware Defender 是用于文件和对象数据的存储层保护解决方案，具有用户文件系统锁定、快照、文件和对象跟踪以及受感染主机 IP 跟踪功能，还有用于离线数据管理的全集成式网络存储区自动化功能，可监视用户行为并实时保护数据。

多方位攻击和多层检测

检测方位是一种专注于应用程序堆栈特定层的安全性监视，诸如操作系统、文件系统、网络数据包流、应用程序日志、防火墙、电子邮件日志、来自交换机和路由器的系统日志事件等，都是安全产品可以检测恶意行为的领域。大多数攻击主要涉及以下两个安全层：

网络层

许多攻击会通过网络来探测防御能力并寻找漏洞，并会使用机器侦听 SMB 和 NFS 等常见端口。在此阶段，攻击者会使用工具扫描网络，并利用发现的漏洞来制定针对预定目标的攻击计划。这是一个检测方位的示例，它可以在发起攻击之前发现此恶意活动。可利用网络检测解决方案来观察网络设备流，将此活动视为有关可疑活动的早期检测。这是攻击中的一个关键点，可以用来针对攻击做好准备并保护数据。

应用程序层

有人说：“如今，攻击者不需要实施入侵；只需登录即可。”可见身份和访问管理技术领域是网络安全战略的关键组成部分。这些技术利用人工智能和机器学习来检测授权用户的可疑活动。分布式拒绝服务 (DDoS) 攻击是另一种类型的应用程序层攻击，此类攻击会使用大量流量让 Web 服务不堪重负并导致服务器崩溃。我们可以使用内容交付网络 (CDN) 中的工具，以及嵌入到 Web 服务器中的工具，来检测和避免此类攻击。

虽然 IT 生态系统的多个层都有相应的检测机制，但成功的关键在于更大限度地加快检测和响应速度，以下是其中涉及的一些挑战：

- ✓ 从时间线的角度来看，攻击者探测设备的时间窗口可能很短暂，我们需要立即响应即将发生的攻击，并做好准备。
- ✓ 操作人员收到来自网络安全设备的警报的时间点可能太晚，无法发挥作用，导致攻击者可能会在安全人员看到警报之前就已经发起了攻击。
- ✓ 并非所有组织都能够配备安全人员来全天候监视网络安全事件，这使攻击者能够在没有人查看和响应安全警报时发起攻击。
- ✓ 此外，在网络层检测到警报并不意味着可在存储层提供主动保护，而存储层才是攻击的目标。

这些挑战可以通过自动化的多方位集成式防御解决方案来克服，此类解决方案可以自动执行网络层防御和存储层防御之间的流程。即使是标记为警告的低级别可疑活动，也可用于准备自动响应措施。

用于集成式检测和响应的 Smart Airgap API

戴尔 PowerScale 网络保护解决方案是一个完整的解决方案，可主动保护生产数据，同时还可以使用来自外部安全工具的信息，来拦截针对数据避风港存储区的复制行为，并维护干净、完好的数据副本。Smart Airgap API 支持利用多个层的传感器信息，还提供使用戴尔 PowerScale 的集成式 Smart Airgap 数据避风港存储区。

Smart Airgap API 提供集成点来连接网络层或其他层的检测系统，例如电子邮件网关、入侵检测系统、防火墙、SIEM 工具、端点保护等。将网络检测威胁警告连接到智能存储层防御后，Smart Airgap API 可向存储层传递决策和响应，以便在即将发生的攻击开始之前采取主动措施来保护数据。

下图显示了网络安全层的集成如何向 Ransomware Defender 传递网络警告。此类 API 请求可以是一般警告，也可以传递更具体的信息，例如用户名和主机 IP 地址。

Smart Airgap API 功能

以下是使用入站 API 触发器提高响应速度的方法：

- ✓ 来自外部设备的威胁警告通知可帮助 Ransomware Defender 主动获取关键数据的快照。
- ✓ 或拦截针对数据避风港存储区的复制，以确保存储区内的数据完整性。
- ✓ 或从网络层请求用户锁定。这使网络层能够使用 Ransomware Defenders 独特的用户感知存储锁定，来请求禁止用户访问存储。

除入站 API 调用之外，Smart Airgap 还提供出站触发器：

- ✓ 在存储层检测可疑用户行为时，可将相应用户名和主机 IP 地址发送到外部安全工具。这使网络层设备可以在收到 Smart Airgap API 的通知后自动采取措施，如监控主机或断开主机与网络的连接、禁用 AD 帐户或隔离电子邮件。

Smart Airgap 的综合审核日志

首要目标是确保可疑或受损数据不会进入安全的网络存储区。通过文件级的审核日志来确定哪些数据受损以及事件发生时间，从而缩短恢复时间。Ransomware Defender 和 Easy Auditor 提供全面的追溯能力，可确定数据泄露的相关地点、时间和人员。

如果解决方案无法追溯攻击发生之前生产系统中的用户和文件级历史信息，则恢复时间将延长，因为从存储区选择数据将是一个漫长的试错过程。如果使用的是较早版本的存储区数据，则误报的干净数据会在重新启动大规模恢复流程时，进一步增加不必要的成本和时间。这种不断试错的过程会大幅增加恢复时间。这就是完整的用户审核日志历史数据对于快速准确地识别攻击开始时间如此重要的原因，而 Superna Easy Auditor 产品可提供用于取证分析的长期审核数据。

总结

快速变化的威胁形势需要更先进的威胁响应系统，并在响应中消除人为影响，从而针对产生于基础架构各种位置的威胁，实现快速多方位的检测响应。

务必要注意，数据避风港存储区解决方案本身并不能改善安全态势，它只能解决网络灾难发生后的清理问题。

企业应着眼于大局，为基础架构提供检测和响应解决方案并长期保留审核数据，因为这样才能在网络攻击后进行取证审核，无论是否配备了数据避风港存储区，均可帮助恢复数据。

在 Superna 的 Ransomware Defender、Easy Auditor 和 Smart Airgap API 的支持下，戴尔 PowerScale 可将安全性与智能、主动的数据保护相结合，以跟上当今时代网络攻击不断变化的复杂性和速度。