DELL Technologies

解决方案简述

Dell PowerScale 网络保护和恢复

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。网络攻击每 11 秒钟就发生一起，一次攻击造成的平均损失为 1300 万美元，这个数字还在不断增长。网络攻击会扰乱运营、损害声誉，并可能导致与数据保护法规相关的法律诉讼。虽然完全规避网络攻击不现实，但 IT 组织可以做很多工作来显著提高系统的网络弹性，以保护业务关键型数据和设置系统，从而更快地恢复业务运营。

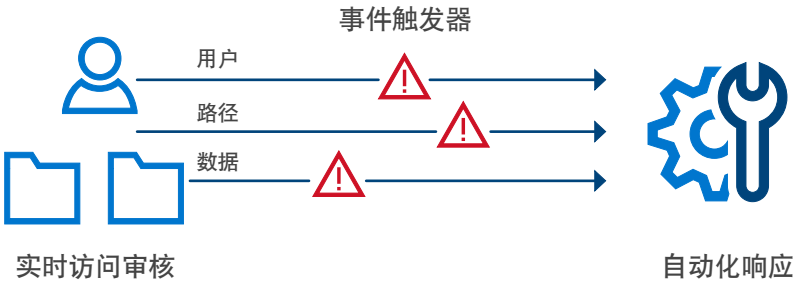
适用于 Dell PowerScale 和 ECS 系统的 Superna Eyeglass Ransomware Defender 可为客户提供全面的功能来保护数据、实时检测攻击事件以及从网络攻击中恢复，从而提高非结构化数据的网络弹性。

利用智能网络阻断技术进行保护

强大的网络弹性战略涉及使用数据保护方面的所有最佳实践：正确级别的访问控制、不可变的数据拷贝、防病毒和反恶意软件。除这些功能外，Ransomware Defender 还提供出色的保护，即存储保险库的数据拷贝与生产环境隔离。数据最初复制到存储保险库后，生产环境与存储区拷贝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。

实时检测网络攻击

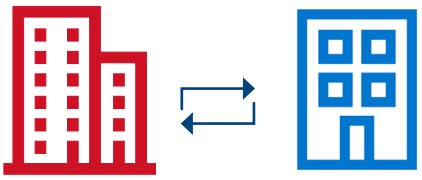
团队越早检测到攻击，就越能更好地作出响应并从中恢复。Ransomware Defender 能够基于表明存在网络攻击的数据访问模式来配置事件触发器。这些模式包括检测大规模数据删除、大规模数据加密、未经授权的网络访问或明显背离历史数据访问模式的用户行为等。这些事件可以通过警报进行捕获并用于对安全漏洞进行根本原因分析。用户可以设置自动化任务来响应那些表明极有可能发生了网络攻击的事件，这些任务包括终止向存储保险库的复制、拒绝某些用户的访问，以及为数据存储区拷贝制作更多快照。用户还可以启用学习模式，让系统能够更准确地预测问题。



运营和数据恢复

故障切换和故障恢复无需操作手册

如果网络攻击未被发现，导致数据访问被拒绝或对开展业务运营必不可少的关键服务访问被拒绝，客户可以选择故障切换到存储保险库。Ransomware Defender 与 Eyeglass DR Edition 的功能集成，其中包括持续监视故障切换就绪性，从而实现不需要复杂或过时操作手册的一键式故障切换。



经过流程编排的到存储保险库的
故障切换和到生产环境的故障恢复

数据恢复快如闪电

对于数据恢复，您可以利用存储保险库中的不可变快照，将数据精确还原到其上一个干净版本。并非所有存储区拷贝都相同。PowerScale 上的存储保险库拷贝可为 1 PB 数据提供短至几小时的 RPO，而使用典型的对象存储则可能需要数周时间。

从存储保险库中的
不可变快照执行数据恢复

Superna Eyeglass Suite

为了更充分地利用 Superna Eyeglass Ransomware，需要安装 Superna Eyeglass Suite 中的下列产品：

- Superna Eyeglass DR Edition
- Superna Eyeglass Easy Auditor

网络阻断解决方案可以采用两种配置进行部署，具体取决于群集的规模和安全功能：

- **基本**网络阻断配置，可在受保护的主群集之一上部署 Ransomware Defender 代理
- **企业**网络阻断配置，可在存储保险库群集上部署 Ransomware Defender 代理。此解决方案具有更高的可扩展性和附加安全功能。

了解有关 PowerScale 平台的更多信息

详细了解我们的 PowerScale 平台

在 Twitter 上关注 Dell 存储

联系 Dell Technologies 销售或支持专家

DELL Technologies