DELL Technologies

# 恶意内部威胁：携手 Dell Technologies 加强网络安全和弹性

## 恶意内部攻击威胁不断增加

恶意内部攻击已成为当今业务环境中最紧迫的网络安全威胁之一。与外部威胁不同，恶意内部威胁已经在组织内部拥有一定程度的信任和访问权限，这使得其行为更具破坏性且更难被察觉。从访问敏感数据到破坏系统，内部攻击可能会削弱关键运营，并导致严重的财务和声誉影响。

Dell Technologies 认识到这些攻击带来的日益严重的危险，开发了可扩展的创新解决方案，帮助企业识别、预防和降低恶意内部威胁的风险。通过将先进技术与专家主导的服务相结合，戴尔可帮助组织防范这些内部威胁。

## 恶意内部攻击是什么？

恶意内部攻击指组织内部人员滥用访问权限，为达成个人、经济或竞争目的而破坏数据、干扰运营或窃取敏感信息的行为。该人员可以是员工、承包商、合作伙伴或任何有权合法访问公司系统和网络的人员。

## 恶意内部攻击的工作原理

恶意的内部威胁利用其受信身份绕过传统的安全防御措施。常见手段包括：

1. **数据失窃**：泄露机密客户数据、知识产权或财务记录。
2. **蓄意破坏**：故意损坏 IT 系统以中断业务运营或损害声誉。
3. **凭据滥用**：使用被盗或滥用的凭据提升访问权限或创建虚拟账户。
4. **与外部攻击者勾结**：与外部网络犯罪分子共享访问权限或敏感知识，以换取经济收益。

相比外部攻击者，这种兼具信任地位与内部知识的双重优势，使得恶意内部威胁具有异常危险性。

## 对企业的影响

恶意内部攻击造成的危害影响深远，其破坏性远超财务损失范畴。企业可能会面临以下后果：

### 财务损失

窃取敏感信息、欺诈或蓄意破坏等行为可导致企业蒙受高达数百万美元的收入损失与恢复支出。

### 运营中断

系统破坏或数据销毁可能会导致运营中断，从而造成业务延误、机遇错失及生产力下降。

### 声誉受损

内部威胁引发的数据泄露或攻击会损害客户和利益相关者的信任，从而影响客户忠诚度与市场声誉。

### 监管不合规性

基于行业特性，如果医疗或金融等敏感数据遭泄露，内部威胁的攻击可能引发高额罚款和处罚。

## 现实案例

在 2020 年，一家大型金融机构的 IT 承包商蓄意删除了关键系统配置，导致网络中断超过 **10 小时**。这种破坏行为导致**数百万**美元的财务损失、巨额恢复成本和声誉损害。诸如此类的事件揭示了内部威胁的破坏潜力，也凸显了采取强效检测与预防措施的紧迫性。

## 预估费用

2024 年 Ponemon Institute 的一项研究显示，内部事件的平均成本估计为 **499 万美元**，占所有漏洞的近 **55%**。该数字涵盖了检测、恢复和缓解费用，凸显了组织迫切需要投资于预防内部风险的先发制人防御措施。

**83%**

的组织在过去一年中报告至少发生过一次内部攻击

来源：2024 年：网络安全内部威胁报告

## 携手 Dell Technologies 打击恶意内部威胁攻击

Dell Technologies 提供全面的工具和服务生态系统，可抵御恶意内部威胁，确保贵组织为意外事件做好准备。

### 通过戴尔可信设备，为端点提供保护

端点通常充当内部威胁的入口点。戴尔可信设备将先进的安全功能集成到硬件中，以强化端点并保护敏感数据。

- **Dell SafeBIOS** 可确保固件完整性，阻止在硬件级别操纵系统操作的企图。
- **SafeID** 可保护凭据数据，防止未经授权的访问和凭据滥用。
- **SafeData** 提供端到端敏感数据加密，确保被截获或窃取的信息对恶意内部威胁始终保持不可读状态。

通过部署这些解决方案，组织可以确保其端点受到保护，无论威胁来自内部还是外部。

### 通过 CrowdStrike，实现主动威胁检测

识别内部威胁需要具备对用户行为的可见性与监控能力。戴尔解决方案中集成了 CrowdStrike，可利用人工智能和行为分析来检测指示内部威胁的异常情况。

例如，在非工作时间传输异常数据或未经授权访问网络关键区域会立即被标记，从而快速启动应急响应。一家美国医疗组织最近利用主动威胁检测，成功识别并终止了一名员工试图泄露患者数据的行为，从而避免了一起代价高昂的数据泄露事件。

### 通过 Dell PowerProtect，增强数据保护

Dell PowerProtect 可提供安全备份、Air Gap 安全隔离存储和关键数据的不可变拷贝，从而构建强大的防线。通过确保敏感信息不被篡改或删除，针对数据完整性的内部攻击可能会彻底失效。

典型案例：一家制造公司遭遇心怀不满的员工试图篡改设计文件。Dell PowerProtect 的恢复存储区使该公司能够在数小时内恢复运营，从而避免中断并保持业务连续性。

### 通过 Dell Professional Services，实现快速事件恢复

当内部威胁升级为事件时，快速恢复至关重要。Dell Professional Services（包括远程数据恢复和事件响应）确保企业能够快速恢复数据和系统。戴尔专家负责主导整个流程，尽可能减少停机时间并减轻影响。

以上仅是戴尔解决方案体系中可应对恶意内部威胁的部分案例。

### 通过 Dell PowerSwitch Networking 和 SmartFabric OS，实现高级网络安全性和微分段

在整个基础架构中提供高级网络分段、严格的访问控制和实时流量分析，从而增强对零日攻击的防御能力。

## 多层安全方法的重要性

有效防范内部风险需要多层保护。实施多层安全策略可确保系统不存在任何可能被利用的薄弱环节。主要步骤包括：

### 增强防御的关键步骤

- **零信任原则：**持续验证所有访问请求，即使在边界内，也不假定任何实体是固有的可信实体。
- **基于角色的访问控制 (RBAC)：**限制员工仅访问其角色所需的系统和数据。
- **高级加密解决方案：**对静态数据和传输中数据进行加密，从而有效消除数据盗窃。
- **员工意识和培训：**采用频繁的安全意识计划，防范员工无意参与恶意活动。
- **定期系统测试：**执行渗透测试和漏洞扫描，以确保防御保持可靠。

结合戴尔解决方案，这些实践构建起抵御恶意内部威胁的完整防护框架。

## 通过战略合作伙伴关系，加强防御

戴尔与 **CrowdStrike** 和 **Secureworks** 等网络安全提供商开展合作，进一步强化其解决方案。CrowdStrike 可增强端点安全性，并提供有关入侵指标的宝贵威胁情报，而 Secureworks 可提供高级威胁检测和响应服务。这些合作确保戴尔的客户能够受益于一个集成尖端技术的生态系统。

## 为何携手 Dell Technologies 来实现网络安全

Dell Technologies 持续树立多层网络安全解决方案的黄金标准。戴尔卓越的专业知识、深厚的合作伙伴关系和创新型产品套件，可适应当今不断变化的威胁环境，让企业从中受益。从端点安全性到内部威胁检测再到事件恢复，戴尔提供了一个完整的弹性框架，可激发信任并促进发展。

## 携手 Dell Technologies 打造弹性未来

借助 Dell Technologies 可扩展的全面解决方案，保护贵企业免受恶意内部威胁的侵害。与戴尔合作，您不仅能够保障运营安全，还能确保业务的持续发展、赢得客户的信任，并为贵组织的未来发展打下坚实的基础。立即联系我们，了解有关实施主动防御的更多信息。

Dell Technologies 是您值得信赖的盟友，可帮助您抵御内部威胁、保护关键资产，并帮助贵企业在动态数字环境中蓬勃发展。安全无忧，未来可期 — 戴尔护航，智启新程。

如需了解如何应对当今一些主要的网络安全挑战，请访问 **Dell.com/SecuritySolutions**

详细了解戴尔解决方案

联系 Dell Technologies 专家

查看更多资源

加入 #HashTag 对话



DELL Technologies