DELL Technologies

DDoS：携手 Dell Technologies 加强网络安全和弹性

DDoS 攻击威胁不断攀升

分布式拒绝服务 (DDoS) 攻击已成为数字时代最普遍且破坏性最强的威胁之一。利用大量被入侵设备组成的庞大网络，DDoS 攻击会向目标系统、服务器或网络倾泻海量流量。这种持续不断的流量冲击会使运营速度骤降甚至完全瘫痪，往往在此过程中导致企业遭受重创。

随着 DDoS 攻击的持续蔓延，从初创企业到跨国公司，没有一家组织可以免遭威胁。由于企业越来越依赖数字基础架构，此类攻击会带来从财务损失到声誉损害等毁灭性后果。Dell Technologies 认识到这一挑战的严重性，提供可扩展的创新解决方案，帮助企业加强防御能力并抵御冲击。

DDoS 攻击是什么?

DDoS 攻击旨在通过来自多个来源的大量流量来破坏网络、服务或服务器的正常运行。这些攻击通过利用僵尸网络实施，即由攻击者远程控制受感染设备组成的网络。

DDoS 攻击的工作原理

1. **僵尸网络招募：**网络犯罪分子通过恶意软件感染成千上万台设备，组建可随时发动攻击的僵尸网络，这种攻击足以使企业陷入全面瘫痪。
2. **流量泛滥：**攻击者操纵僵尸网络向目标服务器发送海量请求，导致系统运行缓慢、崩溃或无法为合法用户提供服务。
3. **系统过载：**系统因非法流量而不堪重负，无法响应合法请求，从而导致服务中断或严重延迟。

常见手段

- **基于卷的攻击**利用海量流量来耗尽网络带宽。
- **协议攻击**利用 TCP/IP 等协议中的漏洞来消耗资源。
- **应用层攻击**针对特定应用程序（如网站或数据库），以破坏其功能。

这类攻击手段持续演变，使试图保障运营安全的企业面临严峻挑战。

对企业的影响

财务影响

单次 DDoS 攻击可能会造成数百万美元的收入损失、停机时间和恢复费用。即便是几分钟的服务中断，也可能对依赖实时交易的企业（如电子商务平台和金融服务机构）造成重大影响。

运营中断

DDoS 攻击导致的中断会降低生产力、延误关键流程，并阻碍对基础服务的访问。对于医疗或制造业等行业，运营停机可能会导致深远的后果。

声誉受损

当客户遇到服务中断时，信任度会削弱。长期或反复的攻击事件可能导致组织声誉长期受损，进而导致客户流失和市场信心下滑。

现实案例

2020 年曾发生一起典型案例：一家大型金融机构遭遇持续数小时的 DDoS 攻击，导致其网上银行服务全面瘫痪。直接收入损失加上声誉受损，共同造成超过 **5000 万美元**的损害。

触目惊心的统计数据

2024 年 2 月，Zayo Group 发布的 DDoS 洞察报告显示，未受保护的组织平均每分钟遭受 **6,000 美元的损失**，导致 2023 年每起事件的平均成本约为 **408,000 美元。**此外，此类攻击的频率不断升级，每年报告的攻击**超过 1000 万次。**这些统计数据凸显出建立强大预防机制的紧迫性。

2050 万起

2025 年第一季度的 DDoS 攻击拦截数据

来源：2024 年：CloudFlare DDoS 威胁报告

携手 Dell Technologies 抵御 DDoS 攻击

Dell Technologies 提供了一套高级解决方案，帮助企业提前预防、检测 DDoS 攻击并快速恢复。

通过戴尔可信设备，强化端点安全保护

端点是 DDoS 相关威胁的关键切入点。戴尔可信设备提供了内置在硬件中的强健安全功能，例如 Secure BIOS 和 SafeID，这些功能可以防止未经授权的访问并保持系统的完整性。

服务器安全性

戴尔服务器解决方案配备戴尔可信服务器技术等嵌入式安全措施，包括：

- **硬件信任根：**此功能可确保服务器的硬件组件在启动时得到验证，构筑防篡改或未授权修改的基础安全层。
- **内置安全功能：**戴尔服务器附带自加密驱动器和端到端启动验证，可防止未经授权的访问并增强对数据完整性的信心。
- **网络弹性：**该方法包括的功能可用于检测异常、漏洞和未经授权的操作，使组织能够快速从网络事件中恢复。
- **全面的数据保护：**戴尔的可信服务器解决方案采用集成的安全机制，可保护静态数据和传输中数据。其中包括高级加密技术和自动化恢复选项，以确保业务连续性。

这些功能可确保服务器能够承受流量激增，同时保持运营稳定性。在攻击期间，存储解决方案可保护关键数据的可用性和完整性，从而尽可能减少中断。

存储安全性

Dell Storage 通过各种集成安全措施和先进技术，尽可能减少漏洞、及早检测威胁并确保在发生攻击时快速恢复，从而帮助防范 DDoS 攻击。主要方法包括：

- **主动威胁检测：**Dell Storage 解决方案采用智能监控和 AI 驱动的异常检测，识别可能指示 DDoS 攻击的异常访问模式。这些工具提供实时安全洞察，并可触发自动化威胁响应，以减轻攻击的影响
- **信任根体系结构：**此体系结构集成到存储控制器中，可确保固件真实性并防止未经授权的修改，从而增强存储硬件的安全性并降低在 DDoS 攻击期间受到损害的可能性
- **多因素身份验证 (MFA) 和访问控制：**实施 MFA 和基于角色的访问控制 (RBAC) 有助于防止对存储系统的未经授权访问，进一步防范与 DDoS 攻击相关的威胁
- **微分段和网络隔离：**戴尔通过隔离存储系统和限制工作负载之间的访问，更大限度地减少潜在的攻击载体，并在发生漏洞时保护存储系统免受横向移动攻击
- **安全快照和不可变日志：**Dell Storage 解决方案提供安全快照和不可变日志，可确保数据完整性，并帮助组织快速从 DDoS 攻击中恢复。通过这些功能，IT 团队可以更轻松地进行取证分析和事件调查，以便检测和分析攻击载体。
- **Cyber Recovery 数据避风港存储区：**Dell PowerMax 和 PowerProtect Cyber Recovery 等解决方案可创建不可变的 Air Gap 安全隔离备份，并且有效防范勒索软件和其他攻击。通过恢复这些备份，可以确保业务连续性，同时避免再次感染的风险。

通过集成这些全面的安全功能和技术，Dell Storage 和 Cyber Resilience 可有效帮助组织抵御 DDoS 攻击并维护具备弹性的安全 IT 环境。

通过 CrowdStrike，实现主动监控

实时监控和高级分析对于在上报之前检测异常流量模式至关重要。CrowdStrike 可与戴尔生态系统集成，利用行为分析和 AI 提供支持的洞察，将合法活动与攻击流量区分开来，从而实现快速补救。

通过 Dell PowerProtect，实现数据完整性

在 DDoS 攻击中，Dell PowerProtect 可确保关键数据安全无虞且可访问。不可变的备份功能和隔离的恢复环境使企业能够还原系统，并尽可能减少事件发生后的停机时间。

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。

现实实施

一家全球电子商务平台在近期利用 Dell PowerProtect 解决方案和主动检测功能来抵御复杂的 DDoS 攻击。通过隔离关键系统并部署紧急恢复流程，该企业在创纪录的时间内恢复了全面运营，从而减少了财务损失并维护了客户的信任。

多层安全方法

抵御 DDoS 攻击的成功之道在于构建分层式自适应防御体系。为了与其技术选项相辅相成，戴尔倡导以下策略：

增强防御的关键步骤

- **零信任体系结构**实施“从不信任，始终验证”模式，以仔细检查每个用户和设备
- **高级加密：**跨所有层加密通信，以保护潜在攻击尝试期间传输的敏感数据。
- **员工培训**指导员工识别可疑活动并遵循安全协议，以防止意外违规。
- **定期系统测试**执行例行评估，包括渗透测试和负载测试，以检验系统应对高流量负载的预备能力。

这些措施与 Dell Technologies 解决方案相结合，可创建强大的防御机制来抵御复杂威胁。

加强网络安全的合作伙伴关系

为了拓展技术能力，Dell Technologies 与 **Microsoft**、**CrowdStrike** 和 **Secureworks** 等行业领导者开展合作。这些合作伙伴关系提供了额外的保护层，将出色的威胁情报和高级检测方法融入戴尔的全面框架中。

利用 Dell Professional Services

除了技术解决方案，Dell Professional Services 还为面临 DDoS 挑战的企业提供专家指导。从事件响应到量身定制的安全体系结构咨询，戴尔团队确保组织能够快速恢复并强化未来的防御措施。

打造弹性未来

Dell Technologies 不仅仅是一家技术提供商，更是致力于保护您的业务免受 DDoS 攻击演变威胁的合作伙伴。戴尔将尖端技术、深入的合作伙伴关系和切实可行的洞察相结合，可帮助企业保护运营、维护客户信任并主动开拓增长机遇。

立即迈出第一步，踏上弹性重塑之旅。联系 Dell Technologies，强化企业 DDoS 威胁防护能力，为未来发展保驾护航。

Dell Technologies 助力企业克服 DDoS 网络安全的挑战，印证了安全根基才是在互联世界中取得成功的关键。

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