DELL Technologies

提升网络安全和零信任成熟度

弥补资源和知识方面的不足，加强对网络攻击的防御。

如今，威胁瞬息万变，特别是随着 GenAI 的兴起，即使是最资深的网络安全专家也面临着意想不到的新挑战。
了解与经验丰富的安全专业人员合作如何帮助您避免网络攻击并始终遵循可靠稳妥的安全实践。

网络威胁就像野餐时出现的蚂蚁

您刚处理掉一只，另一只紧随其后。

在日益互联的世界中，组织高度依赖数字基础架构，而数据已成为一种影响广泛的商品，因此最好假设诡计多端的攻击者已经入侵了您的 IT 环境。

好消息是，有经验丰富的合作伙伴专注于技术和网络安全的交叉领域。

Dell Technologies 提供了可能在内部无法获得的创新解决方案和宝贵的专业知识，以帮助您应对不断变化的威胁环境。

- 硬件和软件安全性
- 对新兴风险的深入洞察
- 了解高级攻击技术
- AIOps 可应对快速变化的威胁
- 新的安全战略和最佳实践

构建防御层，以持续推进安全实践并采用零信任方法。

作为一家网络安全合作伙伴，Dell Technologies 致力于提供全面的专业服务、硬件和软件解决方案以及强大的合作伙伴生态系统，可限制攻击机会，识别并尽可能减少漏洞，并帮助您快速恢复业务运营。

减少
受攻击面 →

检测和响应
网络威胁 →

从攻击中
快速恢复 →

边缘 **核心** **多云**

专业服务

业务/技术合作伙伴生态系统 **安全供应链**

DELL Technologies

减少受攻击面

通过减少网络犯罪分子喜欢利用的途径，提高防御能力，减少受攻击面。

为了增强您的安全态势，您需要识别并尽可能减少漏洞和入口点，避免影响不同域（包括边缘、核心和云）的应用程序、系统或网络。

发现漏洞点

- 软件漏洞
- 错误配置
- 身份验证机制薄弱
- 未修补的系统
- 用户权限过多
- 开放式网络端口
- 物理安全措施薄弱

实施预防性措施

- 与安全的供应商合作
- 应用全面的网络分段
- 隔离关键数据
- 强制实施严格的访问控制
- 更新并修补系统和应用程序
- 利用 AI、定期评估和测试来识别和解决漏洞

采用零信任方法

零信任体系结构意味着您的组织不会自动信任其边界内部或外部的任何内容。相反，在授予访问权限之前，尝试连接到您系统的所有内容都会经过验证。

模型整合了 7 个相互关联的支柱，可系统地构建成熟度。

1. 用户信任
2. 设备信任
3. 数据信任
4. 应用程序和工作负载
5. 网络和环境
6. 可见性和分析
7. 自动化和编排

DELL Technologies

减少受攻击面

识别会削弱系统的薄弱环节，避免引发问题。

网络安全不是一次性任务，而是一个持续的过程。在经验丰富的安全服务合作伙伴的帮助下，定期执行审核、渗透测试和漏洞评估有助于识别和填补漏洞，从而降低风险。

安全的供应链实践	安全比您想象的更早开始。使用通过安全供应链、安全开发生命周期和严格的威胁建模设计、制造和交付的设备和基础架构，建立可信赖的基础。
内置安全性	使用具有基于硬件的内置安全性的设备和基础架构，提前捕获并击退攻击，避免造成损害。
定期修补和更新	通过应用最新的安全修补程序，确保应用程序、固件和操作系统保持最新状态，解决已知的漏洞，并尽可能降低被利用的风险。
最低权限	将用户和系统帐户限制为具有执行其任务所需的最低访问权限。此方法有助于控制攻击者获得未经授权的访问权限所带来的潜在影响。
网络分段	通过对关键数据、业务组和应用程序使用现代网络分段来隔离关键资产，以限制网络访问。这样可通过防止横向移动来控制攻击。
应用程序安全性	实施安全编码实践，定期进行安全测试和代码审查，并使用 Web 应用程序防火墙 (WAF) 来帮助保护防范常见的应用程序级攻击，同时减少 Web 应用程序的受攻击面。
专业服务与合作关系	与网络安全服务提供商协作，并与业务和技术合作伙伴建立合作伙伴关系，以提供内部可能不具备的专业知识和解决方案。
用户培训和认知	培训员工和用户，以识别和报告潜在的安全威胁、网络钓鱼企图和社会工程手段，以更大限度地降低利用人为漏洞的风险。

DELL Technologies

检测和响应网络威胁

旧式安全实践就像拨号上网一样，在当今要求严苛的环境中不仅速度太慢，而且效率低下。

为了应对复杂的网络威胁，您需要更好的安全技巧，例如将 AI 和 ML 内置到应用程序和方法中，以识别和响应已知和未知的问题。

实施强大的入侵检测和防护系统

利用 AI 和 ML 进行异常检测

建立对网络流量和用户行为的实时监控

通过与经验丰富的专业服务团队合作来获得专业知识，从而提高弹性。

作为经验丰富的技术合作伙伴，Dell Technologies 可以帮助您建立主动式事件响应和恢复协议，明确角色和职责，并确保各成员之间无缝地进行沟通和协调。

通过使用以下先进技术，增强您主动检测和响应网络威胁的能力：

- 威胁情报
- 事件响应
- 安全信息和事件管理
- 终端保护
- 行为分析

通过以下方式促进高效、快速的恢复并更大限度地减少数据丢失：

- 明确定义的事件响应计划和协作
- 定期备份关键数据和系统
- 安全的异地存储解决方案和数据加密

DELL Technologies

检测和响应网络威胁

保持警觉并迅速采取行动。

检测和响应网络威胁意味着时刻保持警惕，并针对最坏的情况做好计划。制定持续更新并定期演练的响应和恢复计划，以便您的整个组织知道如何减少攻击的影响。这是一个持续迭代的过程，需要将技术、技能娴熟的人员、明确定义的流程和团队协作结合起来。

持续监视

入侵检测系统 (IDS)、入侵防护系统 (IPS)、日志分析和威胁情报等安全工具可帮助识别未经授权的访问、入侵、恶意软件感染和数据泄露的迹象。

威胁检测

利用 AI 和 ML 来分析数据，以确定可能指向威胁的模式、异常情况和感染指标 (IoC)。这包括识别已知的攻击签名和偏差行为。

警报和通知

发出早期预警，以便及时调查和应对。显示警报和通知，借助集成的安全性快速采取行动。在操作系统上方馈送设备级遥测数据，以帮助加快威胁检测速度，并在检测到潜在威胁或事件时调配安全人员或安全运营中心 (SOC)。

事件响应

启动响应计划以调查和缓解已确认的安全事件。这涉及到控制影响、确定根本原因以及实施必要的操作来恢复系统并防止造成进一步损害。

取证分析

对事件进行详细分析，以了解攻击方法、确定违规程度、识别受影响的系统或数据，并收集证据以查找和解决安全漏洞。

修复和恢复

采取措施修复漏洞、修补程序系统、删除恶意软件并实施增强的安全措施，以防止类似事件再次发生。将受影响的系统和数据恢复到正常状态，以完成恢复过程。

DELL Technologies

从网络攻击中恢复

全速前进，让您的企业重新进入快车道。

在当今数据驱动的世界中，网络弹性必不可少，也是客户和合作伙伴所期望具备的能力。为此，需要采用多层保护，以确保关键数据得到保护和隔离，在受到攻击后能够信心十足地快速恢复。评估网络弹性 ›

采取措施减轻网络攻击造成的损害

重建受损或中断的服务和设备

分析事件以防止今后受到攻击

满足业务 SLA 要求并使操作恢复正常

制定全面的网络安全战略，让您的组织可以高效地恢复。

从网络攻击中恢复需要 IT 团队、网络安全专业人员和管理层齐心协力，协调一致地开展工作，有时还需要外部专家的帮助。恢复的关键在于让系统和操作快速恢复正常，同时从事件中吸取教训，以减少中断和停机时间，恢复服务和数据完整性，尽量减少财务和声誉影响，并加强网络安全，防止将来受到类似的攻击。

- 评估攻击对业务运营的影响
- 确定关键服务的优先级
- 部署数据保护系统
- 及时沟通任何事件和恢复进度
- 制定计划并反复演练，以确保连续性

DELL Technologies

从网络攻击中恢复

在事件发生后，及时地恢复系统、网络和数据，及早恢复正常运营。

实施网络弹性战略可将人员、流程和技术纳入一个整体框架，为整个组织提供保护。

控制事件发展态势	第一步是隔离并控制网络攻击的影响。这涉及断开受影响系统与网络的连接，禁用受感染的帐户，并采取措施防止进一步传播或产生更多损害。
系统或设备还原	一旦事件得到控制，受影响的系统和网络将恢复到干净、安全的状态。这可能涉及重建受损系统、重新安装软件以及应用安全修补程序和更新。自动化和自我修复在恢复运营方面起着重要作用。
数据恢复	必须恢复在攻击期间可能遭到入侵、加密或删除的数据。这可能涉及从备份恢复数据，或采用专门的数据恢复技术来重新获得丢失或加密的文件。
取证分析	在攻击之后，务必了解违规是如何发生的、利用了哪些漏洞以及采取哪些步骤来防范类似攻击。安全信息和事件管理 (SIEM) 等系统以及主机外 BIOS 比较等功能提供了有用的见解。
事件响应评估	恢复后，必须评估事件响应流程并确定需要改进的方面。从攻击中吸取经验教训，据此改进安全实践、更新事件响应计划并提供更好的保护，避免今后发生同样的事件。
专业服务与合作关系	网络安全服务提供商和技术合作伙伴提供宝贵的专业知识和资源来帮助您的组织实现恢复。他们可以协助执行取证分析等任务，识别违规的发生情况，并建议采取哪些措施来防范今后发生类似的事件。

DELL Technologies

将网络安全扩展到边缘和云环境

随着网络从核心扩展到边缘，再到云端，各种环境已成为关键的漏洞点。

在您推进网络安全战略时，您的组织应将零信任原则扩展到边缘和云，以确保严格的访问控制、持续的身份验证以及对网络流量的全面可见性和控制。随着威胁形势不断演变，明智的做法是将 AI 功能部署为第一道防线。此外，只有当核心网络和云环境具有网络分段、加密和持续监视等安全措施时，战略才是完整的。

网络安全专业服务可以帮助您采取整体方法。

连接各种安全解决方案可能是一项挑战。与专注于边缘、核心和云安全性的专业服务团队合作，为您提供专业知识，助力您采取有效措施，全方位地保护您的组织。

边缘

在边缘、网络以及硬件和软件中建立多个安全层。

核心

使用 AI、ML 和自动化将您的基础架构与零信任方法保持一致。

多云

保护任何环境中的任何工作负载，包括公有云、容器和云原生工作负载。

DELL Technologies

GenAI：就网络安全而言，它是一把“双刃剑”

在下一代 AI 的推动之下，我们加快了发展步伐，但在提高安全性的同时也面临着许多新的风险。

作为 AI 的下一个阶段，GenAI 包含可跨一系列任务了解、学习、调整和实施知识的系统。

一方面，它有望改进威胁检测和响应、预测功能和运营效率。另一方面，它带来了新的挑战，需要不断完善网络安全战略，通过强大的安全措施、持续监控、定期更新和修补，以及不断发展的兼顾数据隐私和道德规范的方法来应对各种风险。

借助 GenAI 保障组织安全

GenAI 已成为网络安全的重要盟友，为如何保护组织开辟了新的途径。

- 提高了威胁检测和响应的有效性。
- 能够预测未来威胁或识别潜在漏洞。
- 自动执行威胁检测并提高效率。
- 取证分析，以快速识别模式、异常和感染迹象。
- 量身定制安全意识培训。
- 通过更快地获得更丰富的见解来扩展安全运营。

保护 GenAI 系统

虽然 GenAI 可提供巨大的安全优势，但如果不加以适当保护，其功能可能会被恶意使用。

- 保护数据隐私和完整性。
- 缓解旨在欺骗 AI 系统以造成故障的恶意攻击。
- 检测并响应来自恶意 AI 的系统滥用。
- 审核并减少道德问题和偏见。
- 对 AI 系统实施强有力的访问控制。
- 保护和恢复大型语言模型 (LLM)。

DELL Technologies

现代网络安全应该是智能化、可扩展且自动化

Dell Technologies 可以帮助您建立全面的安全性，防范不断变化的网络威胁。随着技术的进步，我们的网络安全方法始终先行一步，利用 AI 和 ML 的力量来保护您的数字基础架构并保持对数字领域的信任。无论您处于网络安全之旅的哪个阶段，我们都愿意与您合作，在为您的组织保驾护航的同时，采取措施来确保您富有敏捷性和弹性。

DELL Technologies

Dell.com/SecuritySolutions

请求回电

与安全顾问交谈

请致电 1-800-433-2393