DELL Technologies

网络安全生存指南：

# 如何应对现代网络威胁

数字世界已成为危机四伏的荒野，每次单击、下载或登录都可能触发隐藏的网络陷阱。

当今的网络环境比以往任何时候都更加危险，勒索软件、DDoS 攻击、网络钓鱼欺诈和备份渗透等威胁正日益升级。黑客如今利用 AI 来战胜传统防御，将原本的机会主义攻击转变为精心策划的持久威胁，并因此造成大规模破坏。

戴尔客户曾报告一起令人警醒的 AI 驱动攻击：黑客抓取社交媒体数据编造极具说服力的消息，甚至能欺骗网络安全意识最强的员工。

这些案例鲜明揭示了攻击者如何利用先进技术，以前所未有的精准度，实施操控、欺骗和组织渗透。

要在这种荆棘丛生的环境中前行，组织需要全面的网络安全战略 – 一个融合尖端工具、主动防御战略和警惕文化的救生包。本指南深入探讨了构建此类战略的各个要素，旨在帮助组织增强弹性能力，以抵御当今最严峻的网络威胁。

## 组织防护地图：零信任框架

在当今由 AI 驱动的威胁环境中，采用零信任框架已不再是可选项。攻击者正在利用 AI 来自动执行侦察、窃取凭据并快速调整攻击手段，以便削弱传统防御的有效性。零信任基于“假定已失陷”原则运作，持续验证每个访问请求并实施严格身份验证流程，以更大限度地降低风险。

通过主动监控用户、设备和应用程序，零信任可降低未经授权访问和数据泄露的可能性。这是一种现代化的统一身份管理方法。

## 保持营地安全：减少攻击面

减少攻击面对于防御 AI 驱动的威胁至关重要，因为攻击者通常会利用端点、API 和供应链漏洞。端点和 API 作为网络的入口点，经常成为部署恶意软件或窃取敏感数据的目标。

保护这些领域需要采用分层防御策略，包括强身份验证、传输中数据加密、定期漏洞测试、端点检测和响应 (EDR) 工具、修补程序管理以及设备强化。端点监控解决方案和持续威胁检测，可帮助实时识别并阻止恶意活动。

组织必须采取主动战略来保护其软件供应链和开发生命周期。实施最低权限访问可确保只有授权用户和应用程序才能与关键系统交互，而自动威胁检测和响应可在漏洞出现时快速解决漏洞。

## 跟随一位经验丰富的荒野追踪者：主动威胁检测和响应

AI 驱动的攻击利用漏洞、模仿合法行为并动态调整以绕过安全措施，使其难以被检测。为了应对这些复杂威胁，组织需要的不仅仅是被动措施，还需要高级威胁检测系统和快速响应功能。通过利用 AI 和机器学习，安全团队可以分析行为模式、检测异常并实时应对威胁，从而在发生重大损害之前解决问题。

一个有效的检测和响应系统需要处理大量运营数据，以便识别风险并触发自动化响应。这种 Threat Intelligence 还具有自我增强能力，从而使系统变得更智能，能够主动识别并应对新出现的对手策略。



DELL Technologies

## 未雨绸缪：事件响应和恢复

虽然预防攻击是第一步，但组织在运营过程中必须假设攻击是不可避免的。将攻击造成的损害降至最低是目标，而有效战略包含两个要素：

- 强有力的事件响应和恢复 (IRR) 计划。
- 以备份关键数据和应用程序为中心的技术措施。

事件恢复计划应当全面完善。由于严重攻击很可能会使公司大部分（若非全部）业务瘫痪，该计划应涵盖公司每个部门在遭遇网络事件时的应对措施。该计划还应明确组织对内对外的沟通机制，并预先准备好书面沟通模板。该计划也必须定期更新和维护。最终，该计划的价值取决于实践频率。当攻击发生时，所有人都必须本能地做好行动准备。

从技术角度来看，组织应首先确定最小可行公司 **(MVC)** 运营标准：哪些系统必须保持正常运行（即使这意味着要回归纸笔办公）？销售继续发挥作用是否至关重要？客户服务呢？

确定这些要素后，就应围绕它们构建备份和恢复机制。恢复到已知良好数据的能力不仅使组织能够快速恢复运营，还能剥夺恶意攻击者劫持数据的筹码。此外，现代 IR 战略必须超越传统方法，将聊天机器人和虚拟代理等 AI/LLM 系统视为与支付系统或客户数据相同的第 1 级资产，并给予同等恢复优先级。

为了应对高级威胁，IR 计划应在自动化与手动检查之间取得平衡。了解贵组织在整个系统中断的情况下将如何运作，这一点至关重要。万一你不得不退回到纸笔办公怎么办呢？

## 全员参与：员工安全意识

员工如同荒野求生的团队，是抵御网络威胁的第一道防线。每个成员都在识别风险和保护资源方面发挥着关键作用。为了强化这道防线，组织需要开展强效安全意识培训计划，例如包含 AI 特定威胁（如高级网络钓鱼和深度伪造）的攻击演练。

最优方案需融合持续教育、开放沟通、现实演练和共担责任的文化。当从一线员工到高管都理解传统威胁及 AI 驱动的威胁时，整个组织就能形成高度警觉、信息富足的防御单元。通过培养团队协作和防范意识，贵组织方能领先于不断演变的网络风险，构筑抵御潜在攻击的弹性防线。

## 抵御 AI 驱动型攻击以保持弹性的最佳实践

为了保持抗风险能力，组织需要采取主动和战略性的方法来抵御 **AI** 驱动的攻击。以下是 **10** 项最佳实践：

零信任体系结构
需要持续验证、严格的访问控制和网络分段，以确保在授予访问权限之前对每个用户和设备进行身份验证，从而帮助阻止和遏制快速发展的 AI 驱动型攻击。

强化身份和访问管理：
部署强大的身份验证（MFA、RBAC）并实施强大的凭据策略，以减少网络钓鱼和凭据填充的成功率。

自动资产发现和资源清点：
持续发现和监控所有资产，包括云、物联网和影子 IT，以避免隐藏的风险。

微分段和网络访问控制：
对网络和工作负载进行分段隔离，防止攻击者横向移动并遏制威胁扩散。

终端与 **API** 加固：
使用高级端点保护 (EDR/XDR) 和安全 API 网关；实施强身份验证、速率限制、输入验证和加密。

严格的漏洞和修补程序管理：
自动扫描和快速修补，适用于操作系统、固件、应用程序、API 和第三方软件。

**AI** 驱动的威胁检测和监控：
运用 AI/ML 驱动的行为与异常检测技术，实时捕捉隐蔽或自动化威胁。

自动化事件响应：
使用自动化手册，快速隔离、遏制和补救威胁，从而更大限度地减少攻击者的停留时间。

定期实战演练与持续改进：
执行桌面演习、红队测试和网络钓鱼演练；根据结果更新 IR 计划和检测模型。

不可变的安全隔离 **Air Gap** 备份和恢复：
保留防篡改备份（理想情况下，采用安全隔离 Air Gap 且定期测试），以确保干净、快速的恢复。



DELL Technologies

## Dell Technologies：您探索未知领域的向导

为了保护贵组织免受高级网络威胁的侵害，需要合适的工具和专业知识来防范不断变化的风险。在当今复杂的网络安全环境中，稳健的战略对于保护您的数据、系统和声誉至关重要。Dell Technologies 致力于提供一整套解决方案，专为满足各种规模组织的需求而量身定制。

从安全的供应链、高级威胁检测和端点保护到安全的数据管理，戴尔可以为贵企业提供所需的技术，防御现代网络攻击。依托行业领先的专业实力，戴尔团队将与您紧密合作，制定定制化安全战略。通过实时监控、自动化威胁响应和零信任体系结构等功能，戴尔可帮助贵组织保持主动防御与业务弹性。

无论是应对勒索软件、网络钓鱼攻击，还是实现监管合规性，Dell Technologies 都可帮助您放心应对当今的威胁环境。与戴尔合作，保护您的业务并在数字时代蓬勃发展，确保您的运营安全、高效，并为未来发展做好准备。

> 您的事件响应计划必须打印纸质版本，因为在攻击期间，您的系统可能无法访问。”
>
> ***Rachel Tyler***
> 网络安全咨询顾问，戴尔服务

## 戴尔产品和解决方案，可以助您一臂之力

| 精选戴尔解决方案 | 说明 |
| --- | --- |
| 戴尔可信基础架构 | 戴尔服务器、网络、存储和网络弹性解决方案相结合，共同为创新奠定现代化、安全且有弹性的基础。 |
| 网络弹性 | 全面的解决方案产品组合，旨在保护您的数据并确保安全恢复。包括设备、软件和“即服务”产品。 |
| 网络安全服务 | 一套可帮助您制定并实施跨工作负载的全面安全战略的服务组合。服务内容包括咨询服务、vCISO、Managed Detection and Response、渗透和漏洞测试，以及事件响应和恢复。 |
| Dell Trusted Workspace（端点安全性） | 内置和可选附加功能的组合，旨在保护商用 PC。基于安全供应链实践构建，内置功能包括采用 TPM 技术的 SafeBIOS 和 SafeID。可选附加组件包括安全组件验证、SafeID 与 ControlVault，以及合作伙伴软件 CrowdStrike 和 Absolute，以更大限度地提高工作区的安全性。 |

了解如何应对当今一些主要的网络安全挑战：**dell.com/cybersecuritymonth**