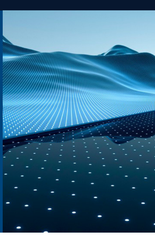
10 大网络安全建议

当今技术发展迅速。我们采用新的工具和系统来增强自身能力，而这也为试图利用漏洞的网络威胁创造了新的机会。在这种环境下，必须实施强有力的网络安全措施，以防范这些新兴威胁，确保在安全的环境中卓有成效地开展创新。当今组织都在积极应对新风险，Dell Technologies 的网络安全专家建议采取 10 项基础性行动来提升网络安全成熟度。



1 了解您的威胁风险环境。

经验丰富的网络安全合作伙伴可提供宝贵的专业知识和资源，助您应对瞬息万变的威胁环境。

- 执行全面的漏洞评估和渗透测试，确定需要应对的潜在薄弱环节，并找出策略中的任何漏洞。
- 利用内部可能不具备的专业技能和知识，例如对新出现的风险、高级攻击技术以及全新安全战略和最佳实践的见解。
- 定义访问权限及其依据，帮助您建立适当的安全框架，以实施业务控制和治理。

2 制定全面的网络安全战略。

确保网络弹性需要 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。

- 倡导整个公司齐心协力 — 安全人人有责。
- 尽可能利用自动化技术。
- 确保制定的 IRR 计划经过反复演练，以便适当的人员都能了解在什么情况下会发生网络攻击。

3 与具有安全供应链的供应商合作。

安全始于早期阶段，可能比您预想的更早。值得信赖的供应商会在设备和基础架构的设计、制造和交付过程中优先考虑安全性，与这些供应商合作可确保奠定坚实的基础。如果供应商能够提供安全的供应链、安全的开发生命周期和严谨的威胁建模，就能助您比攻击者先行一步，有所防范。

- 确保描述或传输于 IT 供应链的信息，以及有关 IT 供应链各参与方信息的机密性、完整性和可用性。
- 确保 IT 供应链中的 IT 产品或服务是真实、未经篡改的，并符合买方的规范，没有任何其他不必要的功能。
- 减少可能限制组件预期功能、导致组件故障或提供入侵机会的漏洞。

4 采用零信任原则。

零信任是一个安全概念，其核心理念是组织不应自动信任其边界内外的任何内容，而是必须验证尝试连接到其系统的所有内容，然后才能授予访问权限。

- 摒弃基于边界的安全模式，采用零信任原则。
- 实施最低权限原则来对用户和系统账户加以限制，使其仅具有执行相应任务所需的最低访问权限。这种方法可以减少受攻击面，以及攻击者未经授权的访问带来的潜在影响。
- 整合微分段、身份和访问管理 (IAM)、多因素身份验证 (MFA) 和安全分析等解决方案。

5 减少受攻击面。

受攻击面是指可能被恶意攻击者利用的潜在漏洞和切入点。为了增强安全态势，组织必须尽可能减少受攻击面，从而降低风险并增强整体网络防御能力来应对新兴威胁。

- 为员工和用户提供培训，让他们能够识别和报告潜在的安全威胁、网络钓鱼企图和社会工程策略，助力更大限度地降低利用人为漏洞成功发起攻击的风险。
- 实施预防性措施，例如全面的网络分段、关键数据隔离、实施严格的访问控制，以及定期更新和修补系统与应用程序。
- 确保系统、网络和设备按照安全最佳实践进行正确配置，例如禁用不必要的服务、使用强密码和实施访问控制。

6 检测和响应网络威胁。

传统的安全措施已不足以应对各种复杂的威胁。组织应利用先进的威胁检测技术和方法，有效识别和响应已知和未知威胁。

- 监视和分析网络流量、系统日志和其他方面以及安全数据，以主动识别未经授权的访问、入侵、恶意软件感染、数据泄露或其他网络威胁的迹象。
- 实施响应计划以快速调查和缓解已确认的安全事件。这包括遏制影响、确定根本原因，以及实施必要的操作来还原系统并防止进一步造成损害。
- 利用 AI/ML 实时分析异常数据模式或行为，快速检测网络威胁。利用这些技术，还可以评估威胁严重性、预测产生的影响，自动执行某些防御措施并扩展安全实践，助力快速做出响应，从而尽可能减少潜在损害。

7 从网络攻击中恢复。

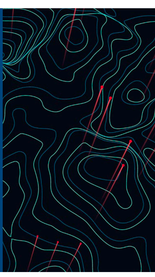
即便主动采取了关键应对措施，组织也应始终假设已遭到入侵，并必须具备弹性功能。他们应经常对这些功能进行测试，以确保在网络攻击得逞后有效地从中恢复。

- 立即采取措施进行隔离并遏制影响，减轻网络攻击造成的损害。
- 断开受影响系统与网络的连接、禁用遭到入侵的账户，并采取措施防止进一步发生蔓延或造成损害。
- 使用 AI/ML 可以快速识别受影响的系统和数据并自动执行备份还原流程，从而加速恢复。

8 与经验丰富的合作伙伴合作。

没有一家供应商具备提供端到端安全性所需的所有必要能力，包括人员、流程或技术；这需要多家供应商通力合作。因此，有必要与多个经验丰富的合作伙伴开展合作。

- 与经验丰富的网络安全合作伙伴开展合作，他们可提供宝贵的专业知识和资源，助您应对瞬息万变的威胁形势。
- 从内部可能不具备的专业技能和知识中获益，包括对新出现的风险、高级攻击技术以及全新安全战略和最佳实践的见解。
- 利用经验丰富的专业服务提供商的专业知识并与值得信赖的业务合作伙伴建立合作关系，从而建立全面的安全态势，以有效防范不断变化的网络威胁。



9 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，各种环境已成为关键的漏洞点。无论应用程序如何进行部署，它们都需要相同的安全性级别并符合业务策略，以确保应用程序用户获得一致的体验并实现管理一致性。

- 确保将零信任原则扩展到边缘和云环境，提供强有力的访问控制、持续的身份验证以及对网络流量的全面可见性和控制。
- 在核心网络和云环境中实施网络分段、加密和持续监视等安全措施，以防范潜在威胁。
- 与专注于边缘、核心和云安全性的经验丰富的专业服务提供商合作，运用他们的专业知识实施有效的措施，助力全方位保护您的组织。

10 实施主动式管理，提高端到端抗风险能力。

通过管理威胁情报、事件和响应及安全运营，可以增强组织检测和响应网络威胁的能力。

- 建立主动事件响应和恢复协议，明确相应角色和职责，确保团队成员之间顺畅地进行沟通和协调。
- 增强环境可见性，使组织能够主动监视和响应网络中存在的威胁，同时在必要时提供警报以进行恢复。
- 利用高级威胁情报、安全信息和事件管理 (SIEM)、端点保护解决方案和行为分析，增强主动检测和响应网络威胁的能力。

不要让安全问题扼杀创新。
访问 dell.com/SecuritySolutions，了解如何提升网络安全和零信任成熟度。

DELL Technologies