安全漏洞无处遁形，优先要务成竹在胸

攻击面不断扩大，新漏洞层出不穷，戴尔助您掌握全局

Vulnerability Management

Dell Technologies 安全专业知识与先进的漏洞扫描和优先顺序排列技术相结合

超过 50% 的组织经历过由第三方造成的数据泄露，而且 44% 的数据泄露事件发生在过去 12 个月内。[1]与此同时，披露的漏洞数量一直在增加 — 2021 年披露了将近 22000 个新漏洞。[2]由于漏洞数量不断攀升，对于大多数组织而言，想要修复所有的漏洞或者确定迫在眉睫的高危漏洞几乎难于登天。因此，IT 组织需要一种解决方案来识别其环境中的漏洞，并确定其修复优先级。

Vulnerability Management

戴尔 Vulnerability Management 可提供经验丰富的专家，他们利用先进的技术定期扫描您的 IT 环境，使您全面了解存在于端点、网络基础架构和云资产内的漏洞，还可为您提供一份报告，此报告会指明各个漏洞并标注有低、中、高或严重的优先度等级。此外，戴尔专家能够利用机器学习查明正被外部攻击者大量利用且近期更有可能成为攻击目标的漏洞，从而助您优先修补风险最高的漏洞和关键资产。

戴尔团队可为您提供季度审查和漏洞趋势信息，并且在修补活动安排方面给与指导。与戴尔合作，贵组织整体的安全态势将得到显著提升。

关键优势

- 按月定期扫描和管理漏洞，让您的防护措施保持及时更新
- 全面了解存在于端点、网络基础架构和云内的漏洞
- 清楚应修复哪些关键漏洞，避免其被利用
- 充分利用戴尔安全团队的丰富知识和专业技能，识别漏洞并确定其修复优先级
- 个性化报告可对漏洞的严重程度进行排序，指导您针对性地进行修补
- 借助季度修正计划，为您改善安全态势

主要特性

- 扫描客户环境以查找漏洞，包括端点、网络和基础架构、云
- 至少每月进行一次漏洞扫描，且由戴尔团队与客户共同商定是否进行额外扫描
- 如有必要，比如发现严重的新漏洞时，可由戴尔主导进行按需扫描
- 识别并创建资产清单，戴尔将根据已知漏洞数据库对其中的资产进行检查，以查找弱点和所需更新
- 提供反馈，告知客户亟需修复的高危漏洞，并给与其修补指导
- 进行季度审查，向客户简要介绍其环境和业内的漏洞趋势
- 由经验丰富、已获认证的戴尔网络安全专家提供服务
- 使用基于 ML 的高级平台执行扫描
- 以分层定价的订阅形式提供，具体定价取决于环境规模

选择戴尔，立即扫描您的环境，主动出击，让漏洞无处可逃

戴尔 Vulnerability Management 可以为您识别漏洞并确定其修复优先级，让您安心集中精力实现自身的核心业务目标。数据泄露事件愈加频繁，由此带来的成本也在不断上涨，Vulnerability Management 将在帮助贵组织持续改善安全态势方面提供宝贵价值。

立即联系您的销售代表。

[1]《A crisis in third-party remote access security》，源自 SecureLink（2021 年），检索日期 2022 年 8 月，网址为 https://www.securelink.com/wp-content/uploads/2022/08/SL_ResearchReport-Third-Party-Security.pdf

[2]《Tenable's 2021 Threat Landscape Retrospective》，源自 Tenable（2022 年 1 月 13 日），检索日期 2022 年 8 月，网址为 https://static.tenable.com/marketing/research-reports/Research-Report-2021_Threat_Landscape_Retrospective.pdf