DELL Technologies

增强网络安全并提高弹性成熟度

企业网络安全成熟度是每一家现代企业战略发展的重要杠杆

当下的网络威胁环境比以往更加复杂严峻，AI 驱动型攻击的频率、速度和复杂性都在持续攀升。企业已无法再依赖零散的防御措施或渐进式更新。

作为企业领导者，您必须将信息泄露视为不可避免，甚至就在眼前。在 Dell Technologies，我们帮助客户提升安全成熟度，增强企业在面对网络风险时稳健运营的信心。我们通过推行一套全面、分层的网络安全与业务弹性方案（该方案围绕三大关键实践领域构建），来实现这一目标。

公司必须具备以下能力：

- **减小受攻击面**
- **检测和响应网络威胁**
- **从网络攻击中恢复**

行之有效的网络安全防护，始于对当前安全态势与成熟度的客观评估。这种清晰认知让您能够优先开展关键改进，为更安全的未来进行布局投资。

减小受攻击面

组织的攻击面正动态延展、瞬息万变，同时 AI 更是引入了全新的攻击途径。再加上远程办公与老旧系统的叠加影响，这些因素进一步扩大了攻击面，为威胁行为者创造了更多可乘之机。因此，缩减攻击面已成为一项战略要务 — 用以降低风险、满足合规要求、捍卫组织弹性，并筑牢信任基石。

增强网络安全并提高弹性成熟度

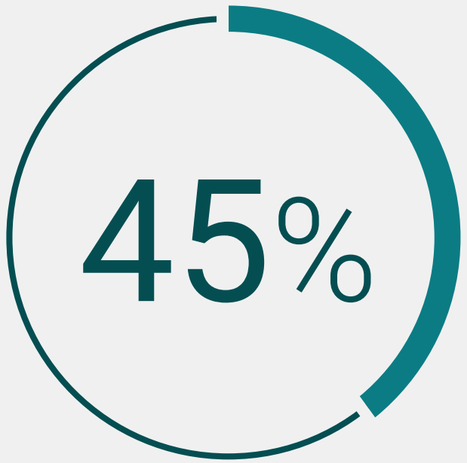
缩减攻击面有助于更大限度地减少攻击者可利用的切入点，从而全面降低整体风险。这样可以提高安全成熟度并简化合规性工作。最终，将能够实现更强的业务弹性、通过规避安全事件降低成本，同时能够更快速地行动、更自由地创新，并凭借从源头构建的安全能力，自信开拓新市场。这一切始于采用零信任原则“永不信任，始终验证”，并在用户、设备和应用程序之间强制实施最低权限。

在 Dell Technologies，我们秉持"安全原生设计"的理念。网络安全贯穿我们工作的始终 — 从构建安全的全球供应链，到为核心产品注入原生保护能力。这些保护措施从硬件层面启动，确保设备仅启动和运行受信任的软件。我们的解决方案遵循零信任原则，帮助您在攻击者利用漏洞之前将其消除。例如，我们的商用 AI PC 安全可靠[1]，可为现代化工作区提供基础防护。

减少攻击面可消除不确定性，从而提升安全成熟度 — 未知风险更少、入侵入口更少、意外状况更少。

关键客户成果：

- **更大限度地减少漏洞：**通过主动强化端点、基础架构和应用程序，您可以显著减少攻击者的机会。
- **简化的安全管理：**暴露的资产越少，需要管理的管控措施就越少，从而形成更精简、更高效的安全态势。
- **更坚实的创新基础：**借助可信赖的端点和受保护的数据，您可以更加放心地采用 AI 和边缘计算等新技术。



专注于减少攻击面的组织在管理外部风险时，可以将网络泄露风险降低 45%。[2]

检测和响应网络威胁

在网络安全领域，速度与情报需要双管齐下。高效的检测与响应能力，可助您快速识别并遏制威胁、缩短攻击滞留时间，并降低攻击造成的损失。最终，将能够实现成本下降、停机时间减少，让企业在持续威胁环境下仍能安心、安全地运营。

增强网络安全并提高弹性成熟度

但是，许多组织在面对混合环境的有限可见性和大量警报时感到力不从心。通常情况下，攻击者在被发现前，平均可在网络内部潜伏 11 天。为了应对这一挑战，您需要通过持续监测、威胁情报和自动化来实现对端点、网络和系统的实时可见性。

理想的安全合作伙伴可以提供威胁情报和事件响应方面的专业知识。戴尔将高级分析、AI/ML 驱动的威胁检测和 24x7 全天候托管服务与安全的硬件基础相结合，可识别和控制威胁，防止其造成中断。Managed Detection and Response (MDR) 等可选服务可提供安全专业知识，以扩大可见性并快速响应和缓解威胁。

强大的检测与响应能力可缩短威胁驻留时间，提升安全成熟度，让团队在威胁出现时能够果断应对、信心十足。

关键客户成果：

- **更快的检测速度和更短的驻留时间：**Managed Detection and Response (MDR) 可将检测和响应的平均时间缩短 25-49%，从而降低攻击变得更加严重的可能性。
- **减轻运营负担：**与专家合作进行主动威胁搜寻和持续监视，可减轻内部团队的负担，让他们专注于核心战略工作。
- **提高弹性：**成熟的检测和响应功能可减少安全事件，并有助于避免更高昂的漏洞相关成本。

444 万美元

2025 年，数据泄露事件的平均成本已达 444 万美元。[3]

从网络攻击中恢复

一旦发生最坏情况，组织的主要目标应是尽快恢复到正常状态，并尽可能快速地减少中断。从网络攻击中恢复可确保您快速恢复干净的数据和系统，从而减少声誉损害，并让您确信恢复是可靠的，不会再感染。

增强网络安全并提高弹性成熟度

即便您要构筑最坚固的防线，也必须将攻击视为不可避免并进行规划。拥有全面的恢复计划和功能至关重要。这包括在隔离的恢复存储区中维护干净且不可更改的关键数据备份，以及使用洁净室环境验证还原的系统是否没有恶意软件，然后再使其恢复联机。

戴尔将恢复功能内置到了产品之中，当风险发生时，确保业务恢复正常是我们的首要要务。PowerProtect Cyber Recovery 存储区等解决方案可隔离和保护关键数据的干净拷贝，以实现快速恢复、减少丢失并避免勒索软件攻击者的利用。这种体系结构可帮助您快速将关键工作负载恢复在线状态，让您安心无忧。

恢复能力往往是安全成熟度的真正试金石 — 此时，信心取决于业务能否迅速且无痕地回归正常运营。

关键客户成果：

- **减少业务影响：**拥有经过精心练习的事件响应计划的组织可以将泄露成本降低约 61%。
- **更快速地恢复运营：**优先快速恢复业务，而不仅仅是消除威胁，有助于在恢复运营的同时尽可能减少中断和成本。
- **优化数据完整性：**通过隔离关键数据、使用不可变副本，并在恢复前验证数据完整性，可显著增强恢复流程的可靠性。

的组织承认很难在满足服务级别协议的同时从网络攻击中恢复。[4]

通过战略合作伙伴关系，加强安全成熟度

在当今快速变化且纷繁复杂的网络安全环境中，经验丰富的合作伙伴至关重要。由于网络威胁越来越复杂和频繁，单个组织几乎无法保持所需的专家知识、资源和技术，以保持领先地位。通过与戴尔等安全领导者合作，公司能够获得专业技能、尖端技术和值得信赖的合作伙伴网络。这些合作伙伴关系可提供有效检测、预防和响应威胁所需的支持和专业知识，确保企业在不断发展的数字环境中始终受到保护。

通过在这三大实践领域采取正确方法，企业能够提升安全成熟度，即便面临持续的网络安全压力，也能安心运营、大胆创新、稳健增长。戴尔整合了可信赖的基础架构、可信赖的工作区、高级服务和合作伙伴生态系统，帮助您的组织保持安全性、适应性和弹性，从容应对未来挑战。

探索安全解决方案

DELL Technologies

常见问题

1.为什么我的企业应将网络安全视为优先要务?
网络安全远不止防护本身，它是企业在凶险的网络安全环境中仍能创新与增长的坚实根基。强大的安全态势不仅涉及防御，还涉及支持。拥有成熟网络安全体系的企业能够行动更迅速、创新更自由、更有信心地开拓新市场。它们也更有能力应对监管变化、客户需求和竞争压力。

2.我们如何在严格的安全需求与创新自由度之间取得平衡?
您不必在安全和创新之间做出选择。稳固的安全体系实际上能够赋能创新。当您拥有"安全原生设计"的基石 — 即从源头将安全融入设备、基础架构与数据之中 — 您的团队便能满怀信心地拥抱 AI、边缘计算等新兴技术。

3.为何供应链安全至关重要?
真正的安全，早在设备启动之前就已开始。随着您的数字版图不断扩大，风险敞口也随之增大 — 此时，信任便成为您的第一道防线。供应链中的每个环节都必须得到保护，因为任何一个环节出现安全漏洞，都可能危及最先进的软件系统。因此，我们从根源构建安全体系，守护从生产到部署的每一步。从工厂生产线到您的使用场景，您所获得的科技产品均经过可信认证与严格验证，确保安心使用、稳定运行。

4.戴尔如何帮助我们在遭遇网络攻击后恢复运营?
当安全事件发生时，更大限度地减少停机与业务中断至关重要。准备工作是关键。通过我们的 PowerProtect Cyber Recovery 存储区，可为您的关键数据创建一份干净且不可变的副本，并且与您的主要环境安全隔离。一旦发生安全事件，您可快速、可靠地恢复业务运行，无需妥协，也无需支付赎金。
戴尔提供丰富的产品和服务，旨在帮助您实施全面的恢复战略。服务范围涵盖可制定恢复与培训方案的咨询服务，以及可保障核心数据安全的数据保护能力。戴尔坚持以人为本、技术为核的理念，让人员与技术协同发力，助力您快速恢复业务。

5.戴尔能否帮助进行实时威胁检测?
完全同意。应对网络威胁，速度就是一切。我们将内置安全功能与 Managed Detection and Response (MDR) 等高级服务相结合，为您的环境提供全天候持续监视。通过利用 AI/ML 驱动的洞察和专业人员经验，我们可帮助您即时发现异常和潜在威胁，让您能够在问题影响业务之前做出响应并有效处置。

来源

[1] 基于戴尔内部分析，2024 年 10 月（英特尔）和 2025 年 3 月 (AMD)。适用于搭载英特尔和 AMD 处理器的 PC。并非所有 PC 都提供所有功能。某些功能需要额外购买。Principled Technologies 验证的基于英特尔的 PC，2025 年 7 月 受信任的设备解读信息图
[2] Forrester Consulting，《The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight》，2024 年 10 月。
[3] IBM 和 Ponemon Institute，《Cost of a Data Breach Report 2025: The AI Oversight Gap》，2025 年。
[4] Dell Technologies，《Advance Cybersecurity Maturity: Technology Infrastructure is the Heartbeat of Every Modern Business》，2025 年 2 月。

关于 Dell Technologies

Dell Technologies（NYSE：DELL）帮助组织和个人打造数字未来，实现工作、生活和娱乐方式的转变。我公司为客户提供业界较为全面，而且具有创新意义的技术和服务产品组合，让他们为 AI 时代做好准备。

有关详情，请访问 Dell.com