网络弹性洞察

探索欧洲、中东和非洲地区的网络弹性差距，剖析威胁演变，探讨 AI 驱动的防御与恢复策略

随着网络攻击激增与数据保护缺口凸显，业务中断风险持续攀升，网络弹性建设正面临日益严峻的挑战。对于拥有成熟网络弹性策略的组织*，其成功恢复的可能性是其他组织的近三倍。通过革新网络弹性策略、强化检测能力，并优先推进持续优化，IT 负责人能够显著降低风险，同时增强企业从容应对不断演变的威胁时的适应能力。

领导层过度自信

59% 的 IT 专业人士认为他们的领导层高估了对网络事件的准备程度。这种过度自信一旦占据主导，就会形成危险的盲区，不仅会使企业延迟关键投入，更会让安全漏洞长期悬而未决。

信心与能力的差距

99.8% 的组织已制定网络弹性策略

同时
59% 的组织无法从上次测试或事件中进行有效恢复

重防护，轻恢复：存在失衡之患

74%
的受访者认为其组织更注重防范攻击，而不是准备从攻击中恢复

然而，仅有
26%
的组织部署了能够全面覆盖主存储、备份存储及网络基础架构的威胁检测平台

仅
36%
对攻击或网络事件演练实现妥善处置并从中迅速恢复，使得影响甚微

因此，当数据泄露不可避免地发生时，许多组织在恢复阶段毫无准备，而这一阶段往往决定着企业的业务存续。

未来之路：
成熟的组织方能交付成果

拥有成熟网络弹性策略的组织，其成功恢复的可能性是其他组织的近 2.7 倍

三大核心支柱具有高度的战略成熟度，共同铸就牢不可破的网络弹性。

安全：
建立您的信任基础

拥有成熟网络弹性策略的组织具有以下优势：

使用固件/BIOS 级别安全控制措施保护设备的可能性提高了 **1.3** 倍

更有可能利用网络存储区来抵御不断演变的威胁，保障关键数据安全

然而，安全保障仅是起点。真正的优势源于智能检测。智能检测可精准识别威胁，从而避免您的宝贵资产受到侵害。

检测：
全天候安全智能

威胁可见性挑战：
仅有 26% 的组织在其备份存储、主数据存储及网络基础架构方面均具备稳健的威胁检测能力

AI 驱动型解决方案：

61% 的组织正优先投资部署基于 AI/ML 的威胁检测技术

40% 的组织利用 AI/ML 技术全面扫描备份数据，以探查潜在入侵痕迹

拥有成熟网络弹性策略的组织，其采用具备主动缓解与响应预案的 AI/ML 工具的可能性是其他组织的 **3.6 倍**

恢复：
准备充分方能展现卓越表现

测试优势：

在每月至少进行一次模拟网络攻击的组织中，有 **51%** 成功从事件中恢复了过来

在测试频率低于每月一次的组织中，有 **64%** 未能成功从事件中恢复

调查结果：
对于定期频繁进行测试的组织而言，其恢复时间目标与恢复点目标的达成率显著高于那些仅进行偶发性测试的组织。

您的网络弹性卓越之路

拥有成熟网络弹性策略的组织始终满足 SLA 的可能性是其他组织的 1.9 倍

奠定强大的基础
优先考虑预防和快速恢复。

- ✓ **安全：**通过 BIOS 级安全管控、数据加密及关键数据网络存储区，构筑纵深防线，有效降低风险。
- ✓ **监测：**运用实时 AI/ML 技术，对所有存储（包括主存储与保护存储）实现威胁的全景式监测与响应。
- ✓ **恢复：**为确保恢复目标的实现，组织应定期进行恢复测试，每月进行测试的组织更有可能达成恢复目标。

准备好提升您的网络弹性了吗？

准备好提升您的网络弹性了吗？请阅读戴尔 2026 年
网络安全弹性洞察研究的所有关键发现。

DELL Technologies

来源：Vanson Bourne 和 Dell Technologies 2025 年网络弹性调查

---

* 拥有成熟网络弹性策略的组织是指那些已建立完整策略并能够对其进行持续优化的组织，其策略优化会使用预测性分析、自动化及实时洞察（例如威胁情报数据源、基于机器学习的调整、以 KPI 为导向的改进机制）