网络弹性实践

在安全/检测/恢复方面对全球企业就绪性进行基准测试
洞察讨论
2026 年 1 月

DELL Technologies

内容安排

- 目标和企业统计数据
- 网络弹性差距
- 安全
- 检测
- 恢复
- 复杂性、组织文化及未来展望

业务目标

- 旨在将戴尔打造成为网络弹性领域的思想领导者和战略合作伙伴
- 重申从“数据保护”标签转向“网络弹性”的战略决策

研究目标

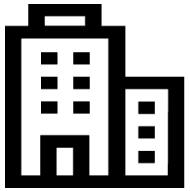
- 评估网络弹性战略的成熟度和集成水平
- 评估组织在安全、检测和恢复实践方面的有效性
- 了解提升网络弹性的主要障碍，包括技能差距、预算和复杂性
- 探索组织如何保护其 IT 环境并保护数据免遭勒索软件威胁

受访者有哪些?

受访者于 2025 年 7 月及 10 月接受了访谈

调研覆盖来自全球组织的 850 名 IT 决策者

拥有 1,000 名以上员工的组织



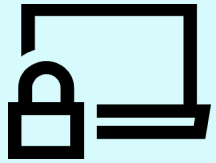
受访组织来自各类公共和私营行业

受访者包括：董事会成员、首席高级经理以及中层经理

主要研究成果

39%

的组织已建立完善并持续优化的网络弹性战略



持续优化至关重要 — 缺乏优化，策略将快速落后于不断演变的威胁，使组织面临更高风险

46%

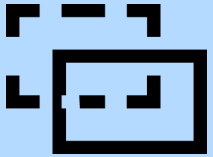
的组织意识到其备份数据的保护力度仍待加强

强化备份保护至关重要，以确保在主系统受损时仍能实现有效恢复。

安全可靠

30%

的组织跨网络、备份和主存储使用全面的威胁检测平台



缺乏统一检测机制，将导致威胁可见性降低、响应时间延长，并增加未检测到的漏洞风险。

检测

55%

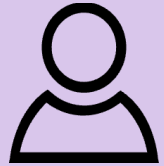
的组织成功从演练/真实事件中实现恢复 — 该数据来自每月或更频繁开展网络攻击模拟演练并成功恢复的受访企业

频繁测试能帮助团队为真实事件做好准备。准备不足的团队在关键时刻可能面临响应和恢复的延迟。

恢复

63%

的受访者认为，领导层高估了组织应对重大网络事件的准备程度



过度自信可能阻碍投资、延迟响应规划，并使关键漏洞得不到及时处理。

第 1 部分：网络弹性差距

了解问题及其发展的紧迫性

持续优化弹性战略可提升恢复效果，但成功并非必然

99.5%

的组织已制定某种
形式的网络弹性战略

39%

的受访者认为其策略已完全
建立并持续优化（即成熟战略）

57%

的受访者在上次测试或事件
中未能有效控制并恢复

拥有成熟网络弹性战略的组织，
其成功恢复的可能性要高出 2.6 倍

65% 与 **25%**

63%

的受访者认为**领导层高估了其对重大网络事件的准备程度**

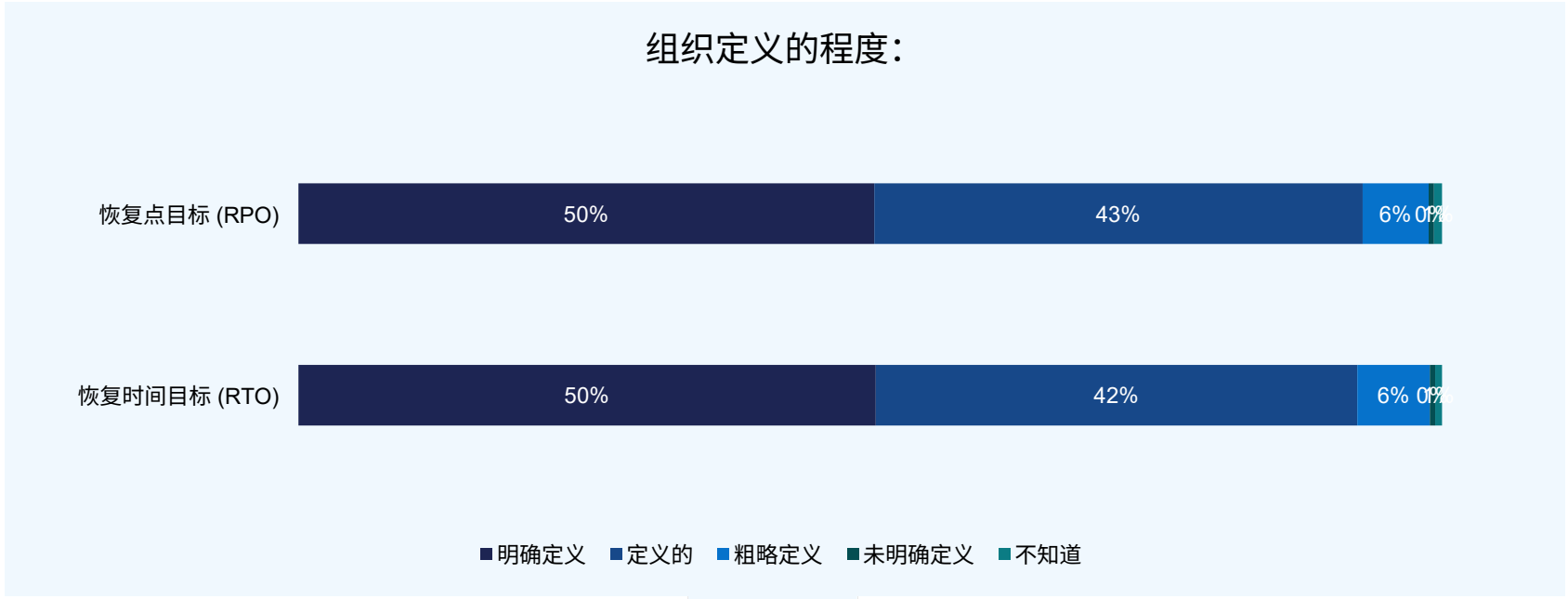
为何此刻至关重要

97%

的受访者认同其组织需随威胁演变而持续强化防护能力

78%

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



32%

在两方面均有明确定义

的组织拥有成熟的网络弹性战略

58%

具有明确定义的 RTO 和 RPO

第 2 部分：安全

保护数字资产，防止攻击和加强防御

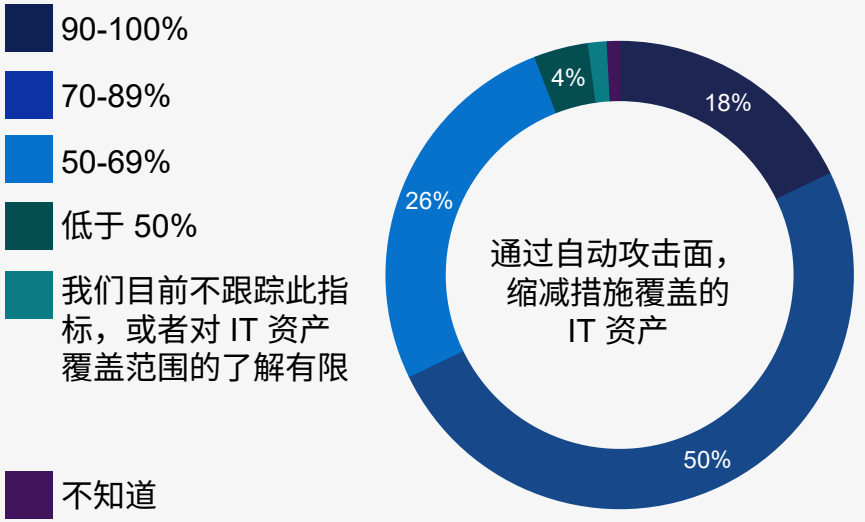
可见性差距和防护短板

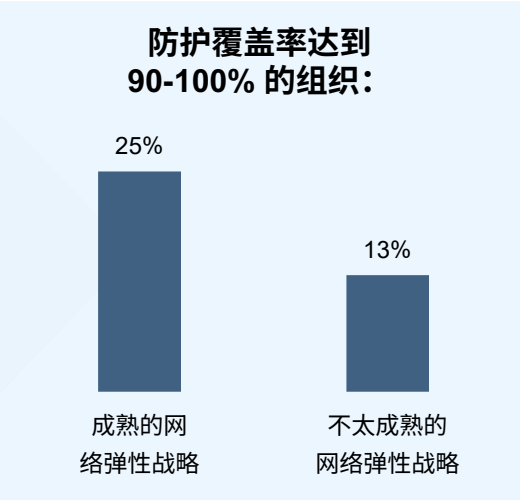
46%

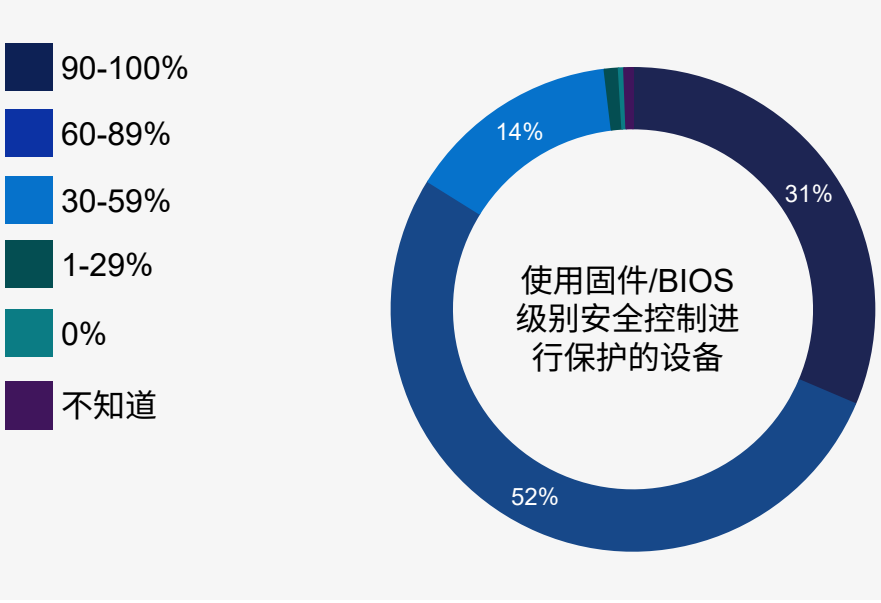
的组织承认其备份数据未得到应有的充分保护

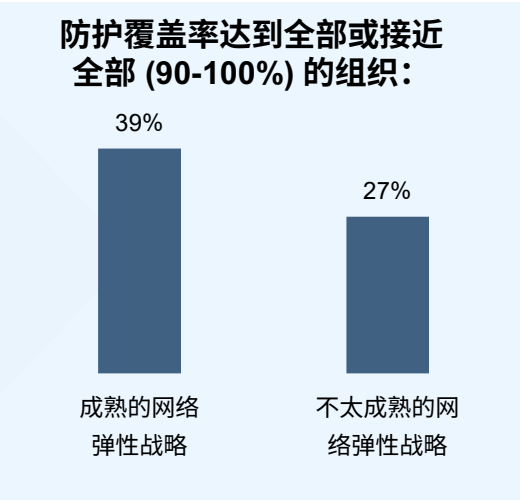
不适用	**59%**
欧洲、中东和非洲	**43%**
拉丁美洲	**41%**
亚太及日本地区	**39%**

持续优化虽无法完全消除覆盖盲区，但能为组织的弹性带来关键优势









从部署前完整性到攻击后恢复：增强安全性的两端

组织用于确保 IT 硬件/软件完整性的流程/方法

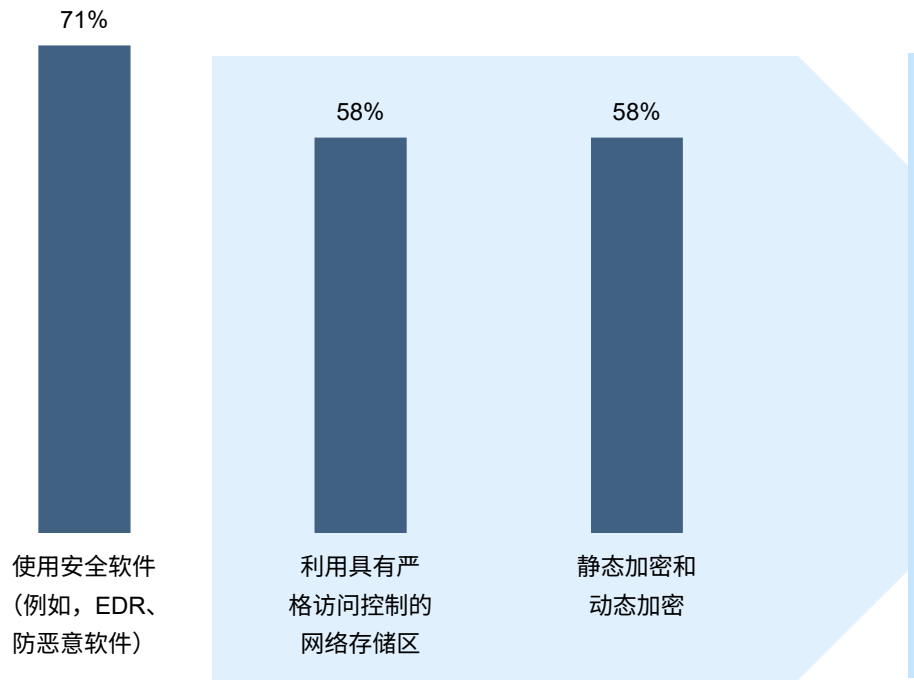
72%

的组织依赖供应商提供的资质认证与证明，以及搭载嵌入式工具（具有组件完整性验证功能）的系统

64%

在暂存/部署期间执行内部审核或手动审查

组织用于保护关键数据免遭勒索软件攻击的方法



拥有成熟弹性战略的组织更倾向于采用：

- **数据加密（59% 对 57%）**
- **网络存储区（63% 对 55%）**

与那些没有成熟抗风险战略的组织相比

第 3 部分：检测

在受到影响之前发现和响应威胁

利用 AI 和自动化可以在威胁影响备份之前发现威胁

38%

的组织采用 AI/ML 工具，
并结合使用主动缓解和响应行动手册

拥有成熟网络弹性战略的组织采用此措施的可能性**高出 3.1 倍**

65% 与 **21%**

48%

的组织广泛使用 **AI/ML 来扫描备份数据**
以发现潜在的入侵迹象

广泛使用 AI/ML 的情况，**在拥有成熟网络弹性战略的组织中出现的频率是其他组织的 2.3 倍**

72% 与 **32%**

83%

受访者认为在勒索软件攻击中，
威胁行为者**正越来越多地针对备份进行攻击**

62% 的组织正优先投资于自动化和 AI/ML 驱动的威胁检测

可见性不完整会增加风险

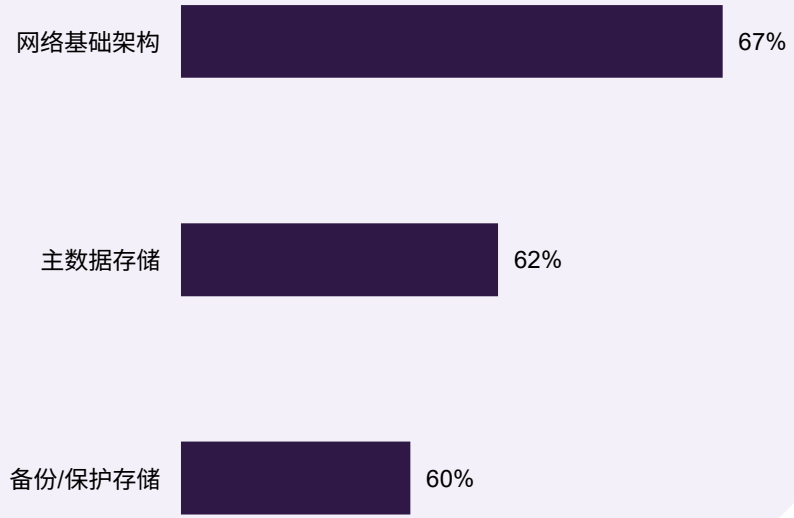
54%
的受访者称其对备份系统中的可疑活动或泄露数据具有高度可见性

74% 拥有成熟网络弹性战略的组织

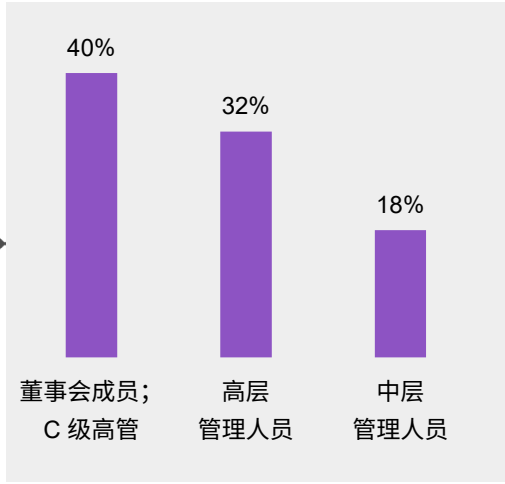
与

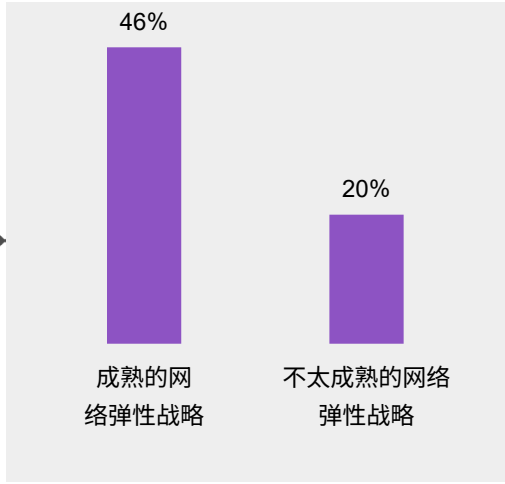
42% 的组织拥有不太成熟的网络弹性战略

在以下领域拥有稳健威胁检测平台的组织



30%
的组织拥有**涵盖所有 3 个领域**的全面平台





第 4 部分：恢复

快速恢复并满足 SLA 预期

恢复现状：多数组织能达到目标，但为应对不断演变的威胁态势，必须持续改进

40%

成功控制和恢复，
且影响极小

董事会成员 (53%) 比**中层管理人员 (30%)** 更倾向于认同此观点

54%

的组织达到
RTO/RPO 目标

按职位：董事会成员 (66%)
对中层管理人员 (45%)

#4

网络安全投资的主要驱动因素是：
组织**最近发生的网络事件或未遂事故**

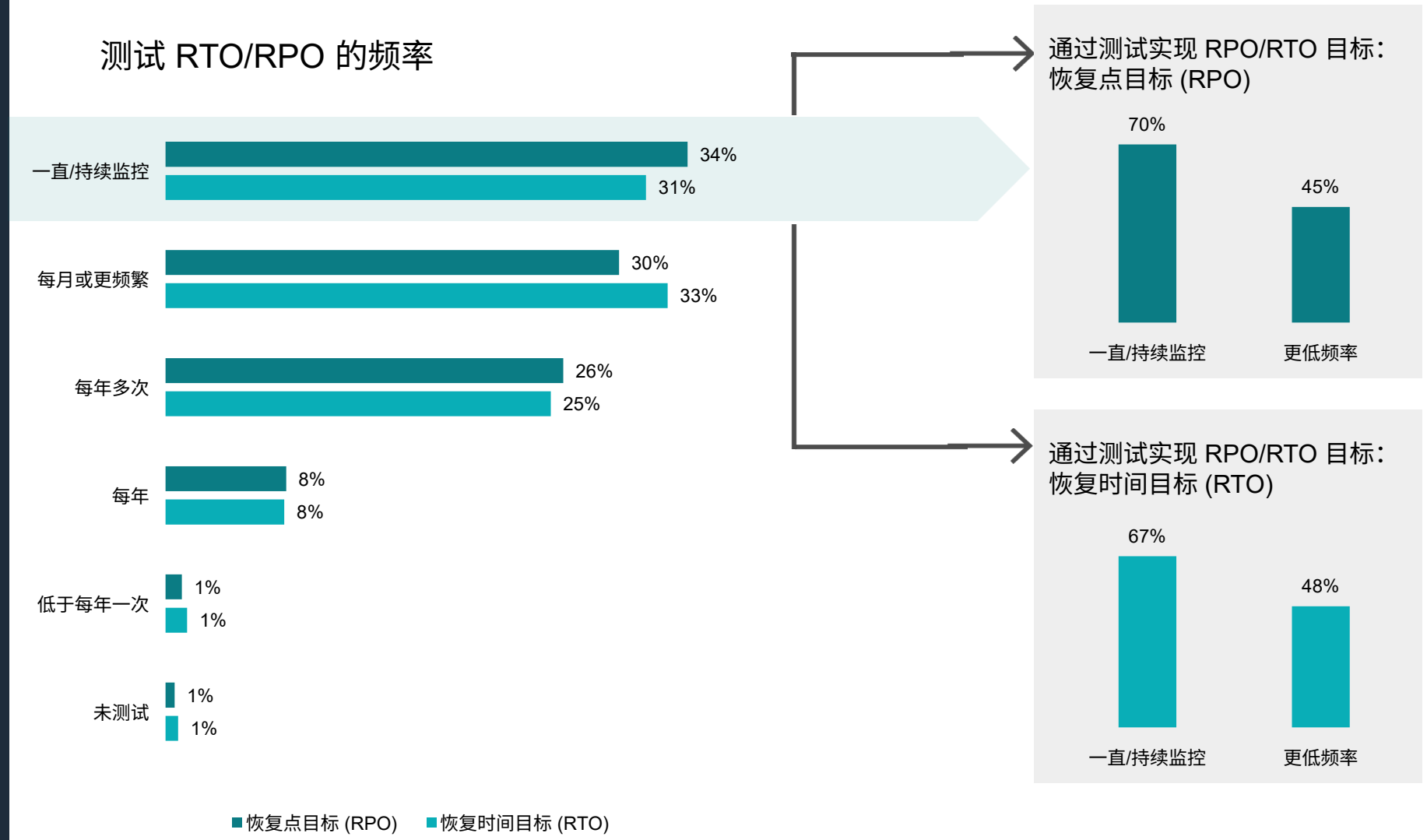
57% 的组织正在增强弹性能力，
以**满足法规或合规性要求**

频繁测试可以提高恢复能力

最终，警醒的文化与持续的改进才是铸就弹性的根本。

SNR 经理，巴西消费者服务组织

测试对于弹性至关重要，能为组织提供更高的恢复成功率



测试是弹性的基石

48%

的受访者表示其组织的网络安全测试并未真实模拟现代攻击技术

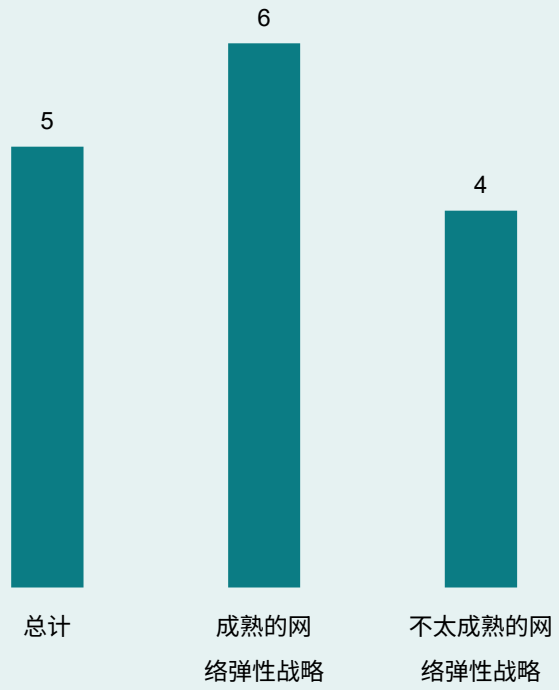
53% 的董事会成员；C 级高管

与

48% 的中层管理人员

常规演练是提升恢复能力的关键，但组织应持续为不断演变的威胁做好规划

组织每年进行模拟网络攻击的平均次数



55%

的组织成功从演练/真实事件中实现恢复 — 该数据来自**每月或更频繁开展网络攻击模拟演练并成功恢复的受访企业**

35%

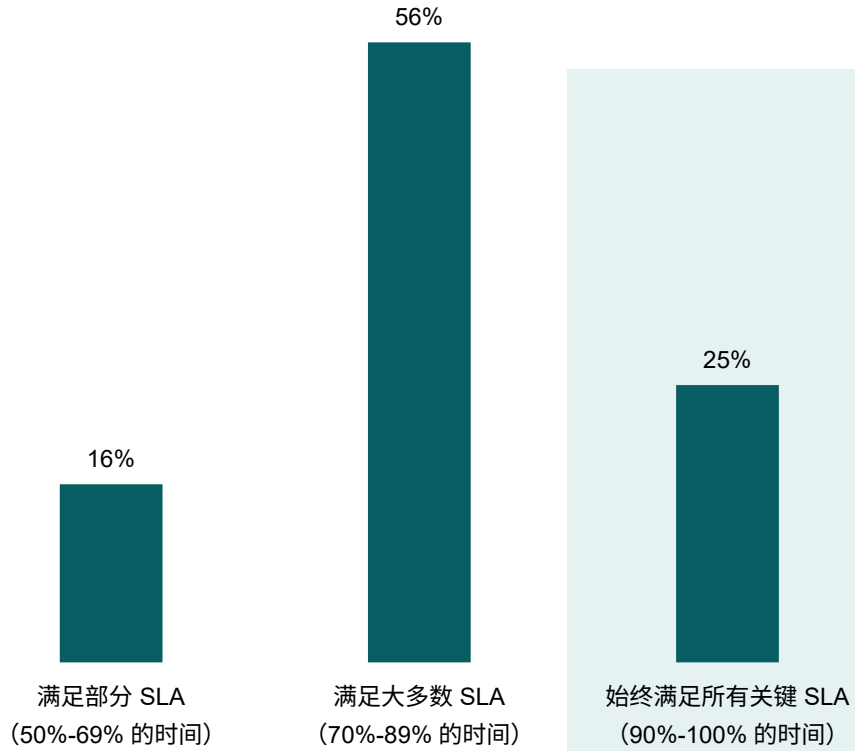
的组织成功从演练/真实事件中实现恢复 — 该数据来自**低于每月频率开展网络攻击模拟演练并成功恢复的受访企业**

> *需要对所有潜在威胁面进行整体测试和评估，而非仅关注单点覆盖测试。*
>
> SNR 经理，英国 IT 技术和电信部

> *网络攻击提醒我们进行定期安全演练的重要性。*
>
> *安全意识培训得到了加强，使每位员工都能够识别潜在威胁。*
>
> 董事会成员，澳大利亚建筑和房地产部

SLA 是验证标准：拥有成熟战略的组织能够兑现恢复承诺

组织满足关键系统恢复 SLA 的频率

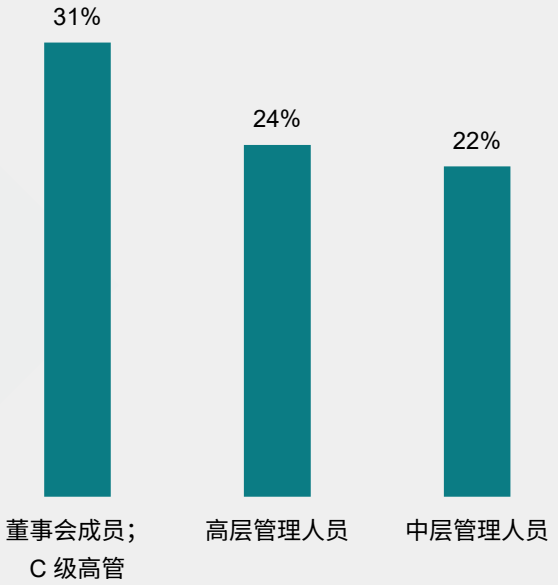


2倍

拥有成熟网络弹性战略的组织始终
满足 SLA 的可能性是其他组织的 2 倍

36% 与 **18%**

按职位：



第 5 部分：复杂性、文化及未来展望

组织障碍和未来投资计划

复杂性、技能差距和过度自信威胁着网络弹性，但 AI 和培训可以助您一臂之力

主要挑战：

复杂的 IT 环境	49%
预算限制	42%
缺乏具有相关技能的人才	39%
供应商/工具碎片化	38%
管理层优先级低	23%

大型组织更可能面临以下挑战：

- 50% 5,000 名或更多员工
- 50% 3,000 至 4,999 名员工
- 46% 1,000 至 2,999 名员工

63%

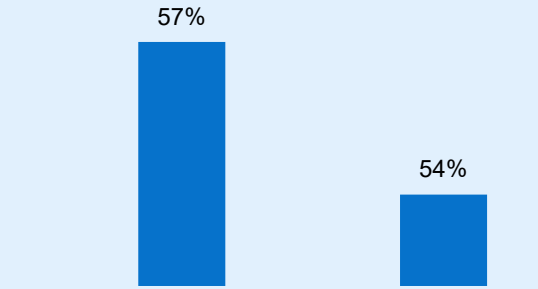
的受访者认为，领导层高估了组织应对重大网络事件的准备程度

96%

承认其在网络安全技能或专业知识方面存在不足

不过...

组织正通过以下方式采取行动：



未来投资展望

遥遥领先的

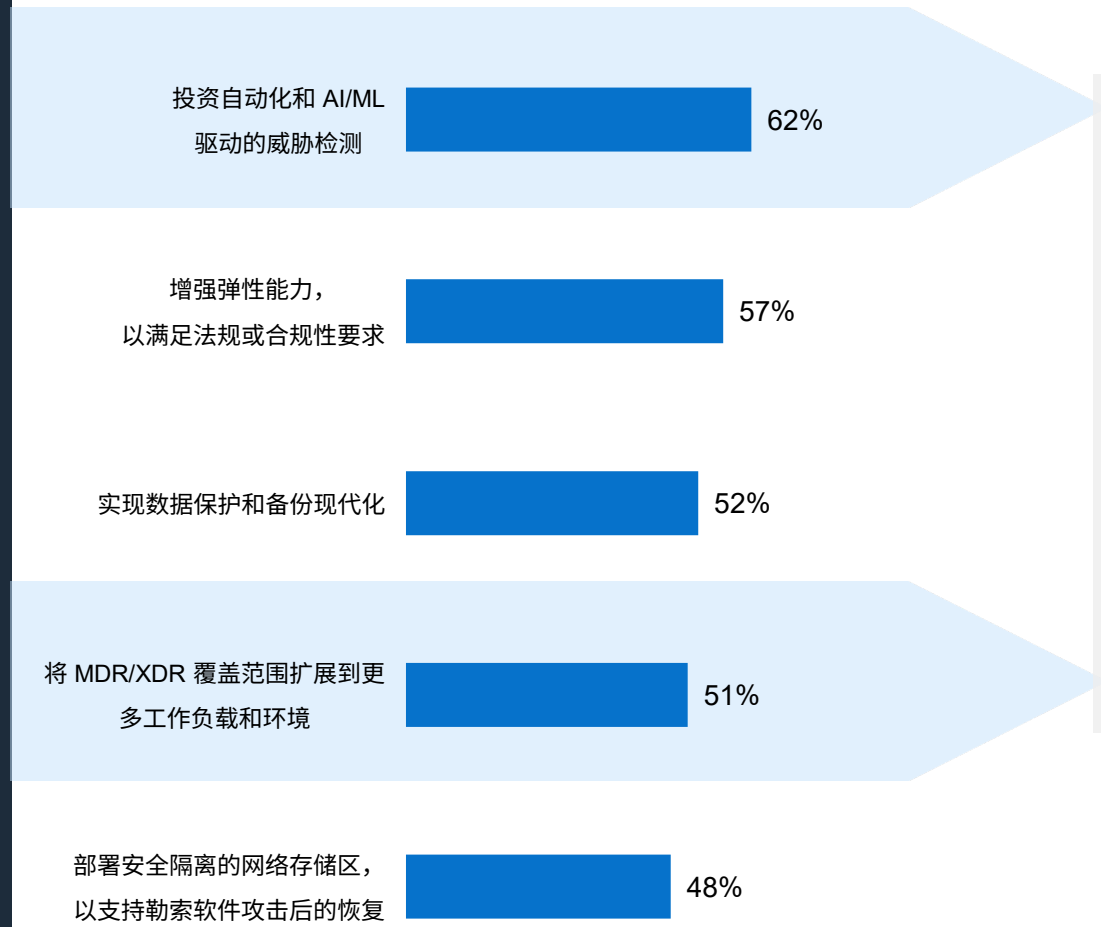
投资的主要驱动力是
不断演变的威胁形势

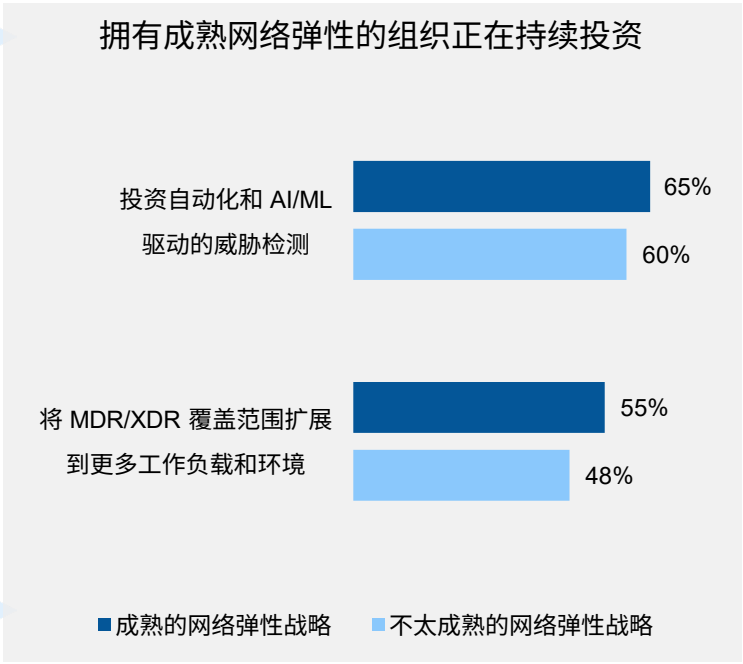
97%

“随着威胁的演变，我的组织需要不断加强安全性”

为保持成熟状态，持续投资与优化是必由之路

未来 12 个月优先考虑的网络弹性投资领域



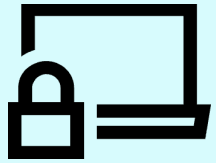


关键要点

主要研究成果

39%

的组织已建立完善并持续优化的网络弹性战略



持续优化至关重要 — 缺乏优化，策略将快速落后于不断演变的威胁，使组织面临更高风险

46%

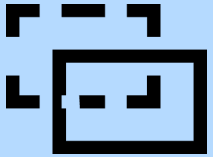
的组织意识到其备份数据的保护力度仍待加强

强化备份保护至关重要，以确保在主系统受损时仍能实现有效恢复。

安全可靠

30%

的组织跨网络、备份和主存储使用全面的威胁检测平台



缺乏统一检测机制，将导致威胁可见性降低、响应时间延长，并增加未检测到的漏洞风险。

检测

55%

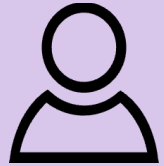
的组织成功从演练/真实事件中实现恢复 — 该数据来自每月或更频繁开展网络攻击模拟演练并成功恢复的受访企业

频繁测试能帮助团队为真实事件做好准备。准备不足的团队在关键时刻可能面临响应和恢复的延迟。

恢复

63%

的受访者认为，领导层高估了组织应对重大网络事件的准备程度



过度自信可能阻碍投资、延迟响应规划，并使关键漏洞得不到及时处理。

DELL Technologies