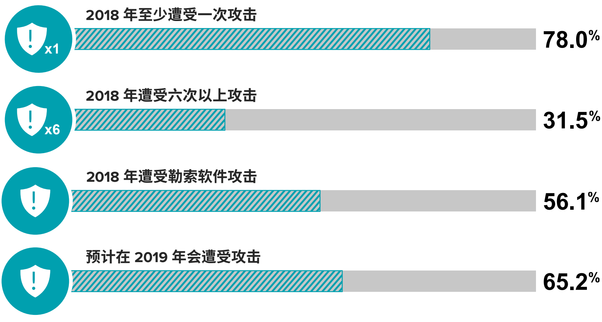
Gigamon

2019 网络威胁防御报告

CyberEdge Group 的第六个年度网络威胁防御报告揭示了 IT 安全专家对其组织安全态势的看法、在建立有效网络安全防御时面临的挑战以及他们必须克服这些挑战的计划。继续阅读以了解今年报告中的一些关键发现。

仍然受困

组织受到网络攻击的速度令人吃惊...
未来这种情况会越来越多。



关键挑战

近年来，即便在预算较为充足的情况下，多数组织在应对关键挑战方面仍然力不从心，难以有效防御网络威胁。

影响防御的第一大障碍

要分析的数据太多

影响防御的第二大障碍

84%

组织正在遭受技能 IT 安全人才短缺

威胁捕捉的第一大障碍

难以实施或集成威胁捕捉工具

将近四分之三的受访者指出，

74%

高效解密 SSL/TLS 流量进行检查是一大问题

有助工具

尽管一些新技术有望帮助 IT 安全团队克服安全数据过载产生的干扰...

#1

46.9% 的受访者认为：
安全分析工具位居 2019 年计划采购安全技术的榜首

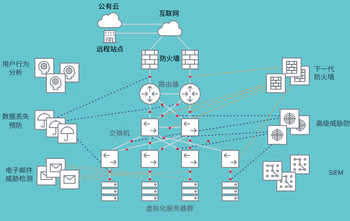
81%

81% 的受访者同意：
机器学习和人工智能技术能够抵御高级网络威胁

...但不幸的是，它们不能解决根本原因。

一个潜在问题

多年来添加的大量平行的安全工具层已形成一个临时的安全架构。
除了导致安全数据泛滥，此类设计还有下列缺点...



- 网络流量接入不可靠
- 不能高效检查加密流量
- 安全堆栈复杂性和成本增加
- 误报和警报重复出现
- 对测试新安全工具的支持较差

有效的解决方案

要克服这些挑战，就需要新的解决方案能够提供普遍的可视化，
还要最大限度地减少元数据的冗余分布和处理工作，以避免安全事件的发生。
这一切都依赖于向工具和团队提供正确的情报和见解，
而不是让他们不堪重负，具体为：

1. 向工具提供优化流量（从物理、虚拟和云环境）
2. 集中化管理资源密集型流程（如解密）并卸载
3. 加速全新安全工具的部署和集成
4. 实现协调和自动化（以提升运营效率）

若要下载完整报告，请访问：
www.gigamon.com/cdr2019

CYBEREDGE GROUP