Akamai

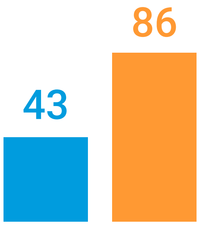
信息图

2023 年分段现状

事实证明，克服部署过程中的障碍意义非凡

面对勒索软件攻击数量翻倍的局面，只有那些采用更高级分段策略的企业转变了防御方式。

过去两年内，勒索软件攻击（包括得手和未得手的攻击）数量增加了一倍...



从 2021 年的平均 43 起增加到 2023 年的 86 起。

93%

的 IT 安全决策者一致认为，分段对于抵御破坏性攻击至关重要。

89%

的受访者表示微分段至少是他们的高优先级任务，34% 的受访者表示这是他们的首要任务。

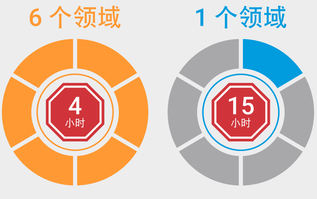
尽管企业十分信赖这项技术，但分段部署的进展一直较为缓慢。2023 年，只有 30% 的企业在两个以上的关键业务领域进行了分段（相较而言，2021 年为 25%），而 44% 的企业在两年前或更早便开始了网络分段项目，这表明此项工作已处于停滞状态。

采用 Zero Trust 框架是企业开始实施分段项目的主要原因之一，但只有五分之二 (40%) 的受访者表示他们的 Zero Trust 框架部署已完全定义且结构完整。

坚持不懈终有回报。那些对六个关键业务领域进行了分段的企业已经转变了防御方式。

扩展分段范围十分重要

若对全部 6 个领域进行分段，在遭到入侵时，全面拦阻勒索软件攻击的时间将会缩短 11 个小时。



如何加速完成分段部署？

确保您的解决方案：

- 针对整个 IT 环境中建立的所有连接创建交互视景
- 基于软件，以便覆盖所有操作系统和设备，而无论这些系统和设备实际位于何处
- 提供省时且 AI 驱动的策略建议和开箱即用的策略模板
- 提供出色技术支持，与您合作完成整个部署流程

下载完整报告

支持

发布时间：2023 年 10 月

扫码关注：获取最新 CDN 前沿资讯