无处不在的安全保护覆盖您的整个扩展网络

全球网络犯罪市场规模预计达 **4500 亿 – 10000 亿**（美元）

- 财务风险巨大
- 响应速度缓慢

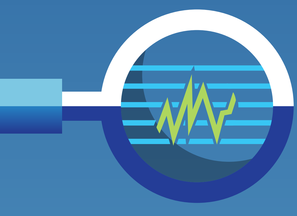
100%
的思科分析的企业网络中都有流向存在恶意软件的网站的流量。

54%
的组织曾因安全漏洞而受到公众关注

每个网络都存在某种形式的恶意流量。使您的网络成为安全传感器和执行器，借助思科安全解决方案迎难而上战胜高级威胁。

充分利用网络基础设施增强保护。

安全效力全面超越您目前的安全措施。



网络即传感器。

更快地识别威胁，获得深入而广泛的可视性。检测可疑流量、策略违规和受侵害的设备

网络即执行器。

缩小受攻击面，遏制威胁。借助软件定义网络分段技术应用您的安全策略

如何才能战胜安全攻击并加强安全性？

战胜安全攻击的最佳方法之一在于网络本身。通过以下 5 个步骤，确保您的组织在攻击前、攻击中和攻击后安全无虞：

1 使用 Cisco NetFlow、身份服务引擎和 Lancope® StealthWatch® 检测未发现的攻击。

- 了解您的正常网络流量
- 检测异常行为
- 近乎实时地识别各种攻击并对其进行分类

2 通过 Cisco TrustSec 和身份服务引擎实现软件定义分段

- 实施基于角色的方法进行分段
- 跨有线和无线网络不受限制地访问
- 阻止并遏制攻击

3 使用基于标准的方法对整个网络的数据进行加密

- 保护数据在整个网络中安全移动
- 跨有线络、无线络、广域网和移动网络进行加密
- 利用 CISF 和 CleanAir 技术防止各类欺骗

4 部署智能广域网和保护分支机构

- 确保分支机构进行直接互联网接入
- 应用集成云 Web 安全技术
- 借助下一代防火墙和入侵防御系统提供保护

5 使用 Cisco APIC EM 加强安全性
（应用策略基础设施控制器企业模块）

- 缩短网络补救时间
- 识别交换机和路由器配置不一致性
- 近乎实时地更新网络基础设施

实施这 5 项功能，构建更安全、更智能的网络。

每个网络都存在某种形式的恶意流量。使您的网络成为传感器和执行器，加强安全性并提供更出色的数据保护！

- 身份被盗
- 中间人攻击
- 网络攻击者
- 恶意软件
- 拒绝服务
- 邮件攻击
- 网络漏洞
- 非法设备

攻击者可通过多种方式进入您的网络。
思科安全解决方案采用一流的安全技术，专为保护企业数据而设计，可确保您的企业在攻击前、攻击中和攻击后安全无虞。

如需了解适合您企业的最全面的安全解决方案，请访问以下网址：
www.cisco.com/go/networksecurity

CISCO