# 网络安全监控：消除可视性缺口

## 《ESG 网络安全监控趋势报告》的要点

2016 年，思科与 Enterprise Strategy Group (ESG) 合作，对 200 位 IT 和网络安全决策者做了问卷调查。我们的目标：评估网络安全监控的当前做法。《网络安全监控趋势》报告，可帮助读者深入了解网络监控属于重要安全实践的原因，其挑战所在，以及首席信息安全官做出重大投资的原因。

## 可视性缺口给网络安全监控工作带来挑战

安全专业人员对网络安全监控极为重视。其中，80% 的安全专业人员表示，网络安全监控对其组织的整体网络安全战略至关重要。

但是，网络安全监控却极为困难。大多数安全专业人员还表示，当前网络安全监控比两年前还要困难。其原因包括外部因素，例如恶意软件数量、网络流量和绕过传统安全工具的攻击数量的增加。

但是，内部组织因素也使网络安全监控困难重重。网络盲点和缺乏可视性首当其冲。

### 网络安全监控所面临的挑战


问题 12：对于网络安全监控，您认为以下哪一项是贵组织面临的最大挑战？

在对数据进行详细了解后，我们发现安全组织中正面临以下最大的可视性缺口：

### 网络安全监控可视性缺口


问题 13：关于网络安全监控，您认为贵组织在哪些方面存在最大的可视性缺口（例如，贵组织缺乏网络数据捕获、处理或分析的领域）？

消除网络盲点是成功实现网络安全监控和保护组织免受高级威胁的关键所在。但是，大多数安全工具无法提供这种可视性。要了解如何解决可视性缺口，请查看我们的白皮书《消除网络盲点》，并了解思科 Stealthwatch™ 系统和思科© 身份服务引擎 (ISE) 有关网络可视性和安全方面的信息。

阅读 ESG 的完整报告：
网络安全监控趋势。



(11/16/16-r02)