Pulse Secure®

# Pulse Profiler 评估报告

发现、识别和监控连接到企业网络的端点

## 安全访问所面临的挑战


移动。云。物联网。当今的数字时代打破了传统网络最佳实践的核心原则。最终用户的访问需求正随着他们高要求的 24/7 工作方式而快速发展。员工工作效率正随着项目范围的演变而迅速变化。跨不同媒体、从移动设备到云端进行的数据和应用程序访问，正对传统的 IT 流程和策略带来新的挑战。凭借我们集成式的安全访问解决方案，Pulse Secure 可轻松保护数据中心、提供移动访问以及启用新的云服务。采购、部署和管理，从未变得如此轻松。

## 数字时代面临的挑战


[1] SkyHigh 云端采用与风险情况报告 (SkyHigh Cloud Adoption and Risk Report)
[2] Gartner - http://www.gartner.com/newsroom/id/3165317
[3] https://www.ft.com/content/0e9afdce-cdb6-11e6-b8ce-b9c03770f8b1

您的网络上都有哪些内容？此前想要回答这一问题并不困难。然而现在，您的数据中心和应用程序正使这一问题变得日趋复杂。数据中心正将云服务（例如 Office 365 和 Box）与您的现有应用程序进行融合。用户需要对信息进行 24x7 形式的访问，这意味着需要能够通过从笔记本电脑到智能手机，甚至是电话亭中的浏览器等的任意平台进行连接。BYOD、承包商和启用 WiFi 的设备，只是您最新的网络安全策略所涵盖的部分内容。如何掌控所有的这些变化？这一切都可以从 Pulse Profiler 及其企业级的可见性特征开始。

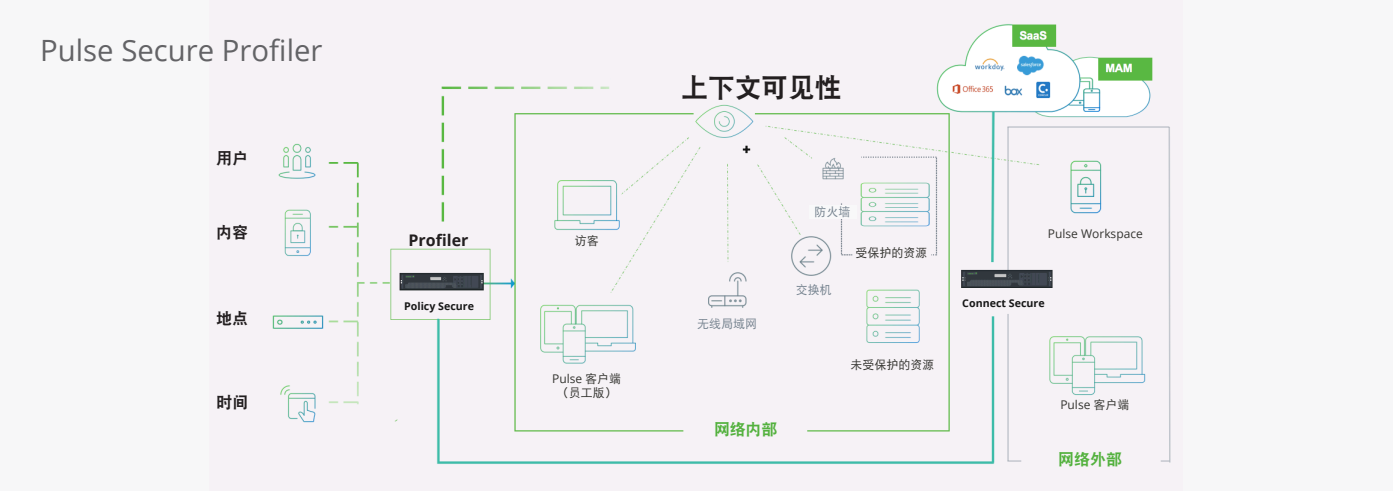
## 可见性的主要优势

- 了解网络使用情况和风险
- 创建针对性的安全策略
- 为合规性审计做好准备
- 启用异常/事件的主动检测和调查

## Pulse Profiler - 在 Pulse Policy Secure 中提供

通过 Pulse Policy Secure，可以使用集成的 Pulse Profiler 功能获得企业级的网络可见性**（请参阅“数据中心及其他”图表）**。网络管理员现在能够发现和跟踪连接到数据中心和云的所有 LAN 连接端点和远程端点的位置和类型。

# 数据中心及其他




## Profiler 的其他优势还有哪些?

- 收集端点设备分析信息并维护动态、上下文相关的联网设备清单
- 简化对于基于 802.1x 的基础架构的部署和管理
- 通过自动化设备识别和身份验证流程以及减轻管理任务来简化 Pulse Policy Secure 部署
- 监控并管理设备行为异常，例如端口交换、MAC 地址欺骗以及配置文件更改
- 保护所有公司自有的端点，包括不进行身份验证的设备（例如打印机和 IP 电话）
- 将设备清单用于资产管理、故障排除和可见性用途

## 立即尝试 Profiler 并访问以下快速报表：

- 设备操作系统图表
- 设备类别图表
- 设备供应商图表
- 设备更改配置文件报表

要了解更多关于企业级网络可见性的信息并分析您网络上所存在的内容，请联系您的 Pulse Secure 解决方案提供商，以获取 Profiler 评估报告。