ForeScout

ForeScout

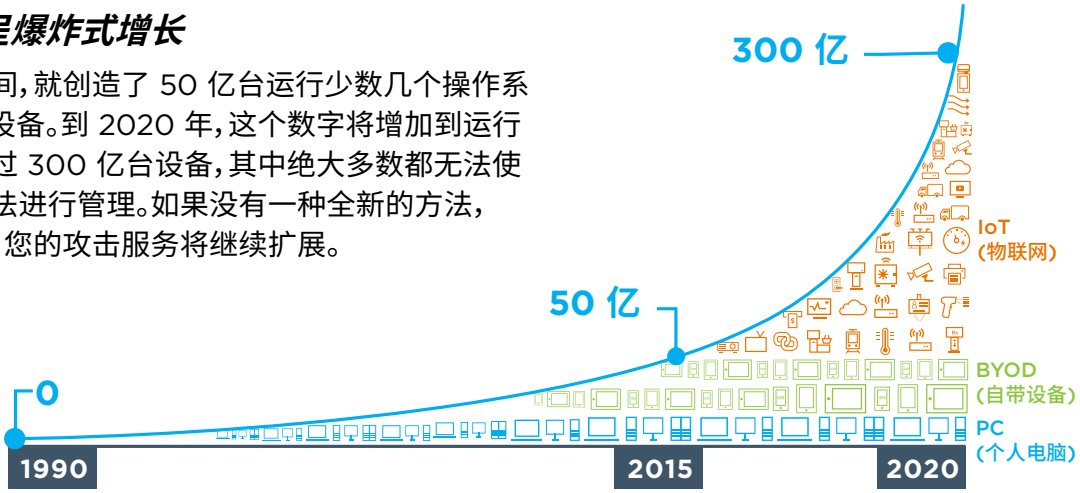
可视化浪潮下的安全新趋势

可视

挑战：

平台和 IoT 设备呈爆炸式增长

仅仅用了二十五年时间，就创造了 50 亿台运行少数几个操作系统 (OS) 的网络连接设备。到 2020 年，这个数字将增加到运行数百个操作系统的超过 300 亿台设备，其中绝大多数都无法使用基于代理的安全方法进行管理。如果没有一种全新的方法，网络盲点将成为常态，您的攻击服务将继续扩展。



ABI Research, 2017

物联网 (IoT)、新操作系统和移动性的高速发展正在引发非受管设备的爆炸式增长。

解决方案：

无代理可见性和控制

ForeScout 开创了一种无代理的安全方法，可实时发现设备并对设备进行分类、评估和监控，让您可以看到网络上的全部设备（从校园到云），并对其进行安全管理。

应对措施：

当前的业务不是在标准、一成不变的网络上运营的，而是随着时间不断地发生动态变化。在 ForeScout，我们推出了为整个网络提供可见性的**异构安全性**，范围从校园内设备到数据中心和私有/公共云环境中的工作负载。我们的方法**高度灵活**且**与供应商无关**，可支持 Cisco、Aruba、Juniper Networks 和运行 802.1X、非 802.1X 或同时运行二者的其他有线和无线网络。

安全性的前提是要了解您的网络上有什么。我们会**发现**您的基础设施、物理/虚拟系统、受管/非受管端点、IoT 和未授权设备，而无需使用软件代理或了解以前的设备。接下来，我们的解决方案将**评估**设备安全性，并**持续监控**安全状态。

我们的**适应性数据收集**功能**支持您选择数据集**，并使用右侧列出的高级的主动和被动技术获得深入的可见性。我们的解决方案可快速评估设备和应用程序，确定设备用户、所有者、操作系统、配置、软件、服务、修补程序状态和是否存在安全代理。了解这些信息可让您执行准确的访问控制、实施和修复策略。

ForeScout 如何帮助您监测更多情况

1. 轮询交换机、VPN 集中器、接入点和控制器，以提供连接设备的列表
2. 从交换机和控制器接收 SNMP 陷阱
3. 监控对内置或外部 RADIUS 服务器的 802.1X 请求
4. 监控 DHCP 请求，以检测新主机何时请求 IP 地址
5. 可以有选择地监控网络交换机端口分析器端口以查看网络流量，例如 HTTP 流量和横幅
6. 运行网络映射器 (Nmap) 扫描
7. 使用凭据在设备上运行扫描
8. 接收 NetFlow 数据
9. 导入外部媒体访问控制地址分类数据或请求 LDAP 数据
10. 监控公共/私有云中的虚拟机
11. 使用以太网供电和 SNMP 对设备进行分类
12. 使用可选代理

解决最棘手的使用案例

物联网 (IoT)：

在 IoT 设备连接到您的网络时立即发现该设备，而无需使用代理。对设备、用户、应用程序和操作系统进行分类和分析，并自动分配设备以保护虚拟局域网 (VLAN) 段并监控行为。

网络访问控制：

在设备、用户、应用程序和操作系统访问您的网络时获得实时可见性。将问题通知给用户和 IT 工作人员，并自动应用适当的访问控制，例如限制、阻止、隔离设备，或将设备重新分配给 VLAN 段。

访客联网：

自动完成访客、承包商和合作伙伴注册，并使用适当的登入选项实施策略合规性。与企业移动管理和端点保护工具共享设备安全状态详细信息并协调实施操作。

BYOD 安全：

在员工将自己的笔记本电脑、平板电脑和智能手机连接到您的网络时提供无代理可见性。实施访问控制和端点合规性策略，从而消除与打开或关闭网络端口相关的手动操作。

端点和法规合规性：

在设备进出网络时监控设备，并向用户通知策略违规情况，例如过期或不合标准的安全软件、操作系统和配置设置。自动将用户重定向到自修复门户。

安全的云计算：

将校园中设备和虚拟机的可见性和控制扩展到您的私有和公共云环境中。在物理环境和虚拟环境中使用单一窗格视图，从而可以利用现有安全操作的团队技能和流程。

控制

> **“到 2020 年，利用实时发现、可见性和控制机制来保护 IoT 的组织将从今天的 5% 至少上升到 25%。”**
>
> —Gartner，*实时发现、可见性和控制对 IoT 安全至关重要*，Saniye Burcu Alaybeyi 和 Lawrence Orans，2016 年 11 月 3 日

挑战：

安全警报太多，实施能力不足

大多数安全工具在发送警报方面非常出色，但却没有能力实施操作。因此，安全团队因必须手动评估和处理大量警报而不堪重负。有些警报会生成误报并被忽略，而其他警报则会由于资源限制而蒙混过关。

解决方案：

基于策略的分段和实施

ForeScout 可对设备、用户和应用程序自动完成基于策略的访问控制和实施，从而允许您限制对适当资源的访问、自动完成访客登入、查找和修复端点安全漏洞，并帮助维护和改进行业法规合规性。

应对措施：

ForeScout 允许您根据策略和情况的严重程度，将广泛的主动操作或被动操作**自动化**，并**对连接实施控制**。为了实现这一点，我们使用策略引擎来**持续地**基于一组策略检查设备，这组策略指示并实施网络上的设备行为。与其他供应商定期检查或查询设备的产品不同，我们的策略引擎可以**实时**监控单个部署中超过一百万台设备的行为。

策略是基于特定设备上发生的事件而被触发的。这些事件可以是网络准入事件（插入交换机端口或 IP 地址更改）、身份验证事件（由 RADIUS 服务器接收或通过网络流量检测）、**用户/设备行为更改**（禁用防病毒软件、添加禁用的外围设备、打开/关闭端口）以及特定的**流量行为**（例如设备通信方式以及所使用的协议。）

通知

- 电子邮件用户/管理员
- 发送屏幕通知
- 重定向到网页
- 请求最终用户响应
- 发送系统日志/CEF 消息
- 开立帮助台票证
- 与 IT 系统共享情境

确认

- 移动到访客网络
- 更改无线用户角色
- 分配给自修复 VLAN
- 限制未授权设备
- 启动应用程序/进程
- 更新防病毒/安全代理
- 应用操作系统更新/修补程序

限制

- 隔离设备
- 关闭交换机端口
- 阻止无线或 VPN 访问
- 使用 ACL 限制访问
- 终止未授权的应用程序
- 禁用 NIC/外围设备
- 触发修复系统

ForeScout 可以根据您的安全策略实施适当的控制级别，从适中到严格。

自动化

挑战：

分段安全

大型企业会有数十个未连接、分散的安全系统。这种孤立的方法阻止了协调一致、企业范围的安全响应，从而使攻击者有更多的时间来利用系统漏洞。

解决方案：

安全自动化

ForeScout 使用领先的 IT 和安全管理产品来协调信息共享和基于策略的安全实施操作，以便在无人干预的情况下实现安全工作流自动化并加快威胁响应速度。

> **“在深夜，或者当我的工作人员睡觉时，ForeScout 正在与我们的其他安全解决方案合作，发现威胁并立即采取行动。这种自动化功能的价值是无法用金钱来衡量的。”**
>
> — Michael Roling，首席信息安全官，密苏里州

应对措施：

通过将可视化和控制作为基本功能，ForeScout 可以**打破安全壁垒**，并可利用您现有的安全投资。使用 ForeScout 模块能够持续交换设备安全性、威胁、行为和合规性数据，使您现有的安全工具和分析更智能、更具有情境感知能力。您的安全基础设施可以获得关键的控制功能，允许您**自动实施手动策略**、**加快响应速度**并显著**改善您的安全状态**。以下是几个示例，说明如何通过 ForeScout 将您的工具放到我们的工具上层，以实现系统范围的安全协调：

高级威胁检测 (ATD)：检测到恶意软件和感染指标 (IOC) 后，领先的 ATD 产品立即通知 ForeScout 平台。然后，ForeScout 解决方案根据策略隔离被感染的设备，并执行修复操作。它还会扫描现有设备和新设备以查找 IOC，并启动缓解。

安全信息和事件管理 (SIEM)：当有设备连接到网络时，ForeScout 平台检测到并分析该设备，然后与 SIEM 共享设备详细信息，使其更加智能。SIEM 根据收集的事件和日志对设备进行评估。ForeScout 根据您的安全策略将此洞见转化为操作，允许、拒绝或隔离设备。

动态网络分段：通过与领先的防火墙、交换机和路由器供应商产品深度整合，我们的策略引擎可以自动应用 VLAN 或访问控制列表 (ACL)，将设备和用户放到或分配给适当的网段。对访客、承包商、特定员工和 IoT 设备进行分段有助于防止透视、横向、内部和 DDoS 攻击。

有关协调功能的完整列表，请访问 **forescout.com/modules**。以下是一些与我们合作的合作伙伴：

amazon web services · Check Point SOFTWARE TECHNOLOGIES LTD · CYBERARK · FireEye · IBM · McAfee · MobileIron · paloalto NETWORKS · QUALYS · RAPID7 · servicenow · splunk> · Symantec · tenable · vmware

“ForeScout 在网络访问控制 (NAC) 技术方面取得的成就显然具有变革性。”

— Frost & Sullivan 最佳网络安全 2016

“ForeScout 为摩根大通提供了增强的可见性和控制能力，可以监控连接到我们公司网络的数十万台设备。”

— 摩根大通公司全球首席信息安全官 Rohan Amin

公司概况

行业：网络/物联网安全

客户：全球 60 多个国家/地区内的 2000 家企业和政府机构*

市场：金融服务、政府和国防、医疗保健、制造、教育、零售和关键基础设施

成立时间：2000 年

CEO：Michael DeCesare

2016 年荣获的奖项和赞誉：

- 摩根大通变革性安全技术名人堂创新奖
- Gartner IoT 安全市场先锋
- Gartner NAC 市场先锋
- 福布斯 100 强云技术公司
- Deloitte 科技发展最快 500 强
- Nanalyze 9 大热门网络安全创业公司之一
- CRN（电脑经销商新闻）杂志最强安全公司
- Inc. 成长最快 5000 公司之一
- SC Magazine 欧洲最佳 NAC 解决方案

安全框架/合规性要求：

领先的安全标准体系和框架有一个共同的基本原则：安全性从可见性开始。ForeScout 可以帮助企业和政府机构遵守以下要求：

- 互联网安全 CSC（关键安全控制）中心
- CDM（持续诊断与缓解）
- FISMA（联邦信息安全管理法案）
- HIPAA（健康保险携带和责任法案）
- HITECH（健康信息技术促进经济和临床健康法案）
- ISO/IEC 27001（国际标准化组织和国际电工委员会）
- NIST（国家标准与技术研究所）风险管理框架
- PCI-DSS（支付卡行业数据安全标准）
- SCAP（安全内容自动化协议）
- SOX（萨班斯-奥克斯利法案）

ForeScout®

全球办事处：
加州圣何塞（总部）
达拉斯
伦敦
纽约
悉尼
特拉维夫
华盛顿特区

截至 2016 年 12 月 31 日