ForeScout CounterACT®

获得实时监控、控制和基于策略修复受管、未受管以及非传统设备的能力。

ForeScout CounterACT® 是一个无代理安全设备，可动态识别和评估网络端点以及应用程序，联网即可见。CounterACT 迅速确定用户、所有者、操作系统、设备配置、软件、服务、修补程序状态以及是否存在安全代理。完成确定后，它可提供修复、控制和连续监控。

CounterACT 在公司分发的、个人拥有的自带设备 (BYOD) 端点以及非传统设备上执行这些操作 - 无需软件代理或对设备的了解。它可迅速部署到您的现有环境并几乎不需要更改基础设施、升级或重新配置端点。

客户选择 CounterACT 的原因

异构支持。可用于流行的网络基础设施、操作系统、端点软件和第三方解决方案。

无代理。在身份验证和网络访问控制上无需端点代理。

出色的可见性。监测其他解决方案无法看到的设备：

- 台式电脑、笔记本电脑、服务器、路由器、智能手机和平板电脑
- 有线/无线 LAN 和打印机
- IoT 设备 (投影仪、工业控制、医疗保健、制造、POS 设备等)

自动控制。自动进行一系列操作：

- 根据设备情况和安全策略授予、拒绝或限制网络访问
- 隔离并修复恶意/高风险端点

快速实现价值。快速部署，数小时获得网络可见性。

策略执行。执行网络访问控制、端点合规性以及移动设备安全保护。

生产率。向人员和设备授予适当的网络访问权限 - 无需干扰性干预或人工参与。

可靠性。通过确定并移除未授权基础设施改善网络稳定性。

成本削减。针对访客访问，消除和打开/关闭网络端口相关的手动操作。

合规性。自动确定政策违规、修复端点缺陷并根据合规性强制要求进行衡量。

网络安全风险和盲点

传统网络安全关注的是通过防火墙和防入侵系统阻止外部攻击。但是这些安全工具对于防止您的网络受到内部人员威胁无能为力，而这些威胁所导致的安全事件和违规正不断增多。威胁包括：

- **访客：**将计算机带到您企业当中的访客和承包商。这二者都需要访问互联网，并且承包商可能需要其他资源。如果您将不受限的访问权限授予这些访客，会让您的网络面临危险。
- **无线和移动 (BYOD) 用户：**员工希望在您的网络上使用其个人拥有的智能手机、平板电脑和笔记本电脑。如果没有足够的控制，这些设备可感染您的网络或造成数据丢失。
- **物联网 (IoT) 设备：**非传统设备继续扩大您的攻击面，这是因为添加了未受管的设备，例如 IP 连接投影仪、恒温器、灯控件、安全摄像头等等。
- **未授权设备：**出于好意的员工可通过经济的接线集线器、部门服务器、路由器和无线接入点扩展您的网络，但是这会造成网络不稳定以及漏洞。
- **恶意软件和僵尸网络：**一旦您的网络受到威胁，联网的设备可在“透视攻击”中被利用，在该攻击中外部人员可扫描您的网络并窃取数据。
- **合规性：**不当配置的端点和虚拟机可包括不正确的设置或不适当的软件。此外，它们可能被用户或恶意软件有意禁用，从而停用安全控制。

您无法保护看不见的东西

可见性受限导致安全盲点。大多数端点安全系统需要每台设备上有最新的代理，以对它们进行查看和管理。IT 安全经理通常对于未受管自带设备端点的存在与否以及每天在网络上数目不断增多的 IoT 设备没有可见性。

分析师、客户和合作伙伴选择 CounterACT

- ForeScout 在 Gartner 网络访问控制魔力象限中**以其执行能力和视野的全面性而被评为领先者（四个连续报告中获得此评价）
- SC Magazine 最佳 NAC 解决方案，2015 年 6 月
- SC Magazine 最值得购买奖，2014 年 10 月

> 我们需要可快速部署的 NAC 解决方案，不存在干扰业务的风险。此外，它需要支持我们混合的 Aruba® 和 Cisco® 基础设施。ForeScout CounterACT 为我们提供这一切还有更多 - 包括令人印象深刻的与我们现有 FireEye® 和 ArcSight® 安全工具集成的功能。这是我们将 CounterACT 誉为我们信息安全部门“瑞士军刀”的原因，因为它以最有效的方式促进了多种自动化安全检查及合规性管制。”
>
> **— Ali Kutluhan Aktaş, KKB 的信息安全/风险管理主管**

ForeScout CounterACT® 的工作方式

ForeScout CounterACT 提供独一无二的能力，可监测 IP 连接网络设备，对它们进行控制并在不同的安全工具当中协调信息共享和操作。具体方法如下：

监测 CounterACT 设备在您的网络上以带外形式部署。由此它持续监控网络流量并和您的网络基础设施集成，一旦设备访问网络即对其进行确认。CounterACT 具备独有的能力，可监测各种 IP 连接端点、用户和应用程序。实际上，CounterACT 精密的技术可发现竞品无法看见的设备。

CounterACT **不仅如此，**它接下来可通过被动和主动询问技术对网络上的端点进行准确分类。CounterACT 可确定设备类型、位置、用户以及设备是否是您域的成员，以及其他基本信息。它还通过使用管理凭据查询公司拥有的设备来获得有关设备安全情况的详细信息。

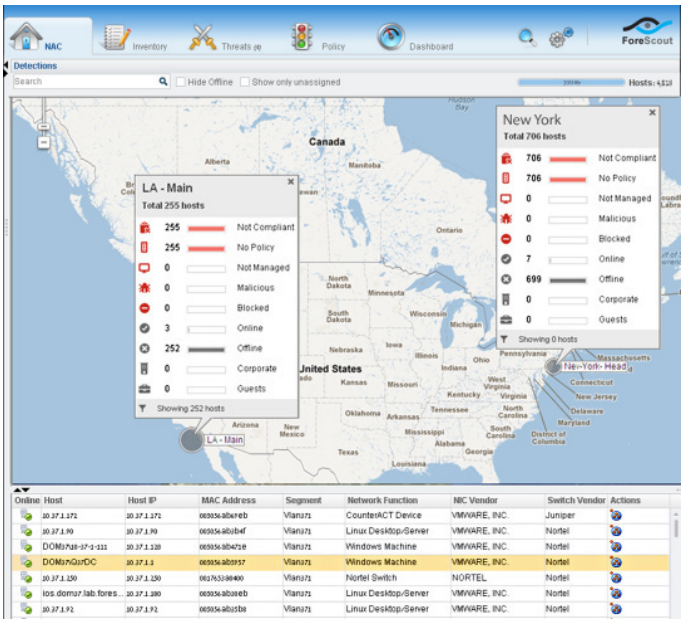

图 1: ForeScout CounterACT 提供有关您网络上设备的高度概括性和详细的信息。

控制。一旦 CounterACT 在端点上发现安全问题，其精密的策略管理器就可根据问题严重程度自动执行一系列响应。不严重的违规可能导致向最终用户发送警告消息。自带设备的员工和承包商可被重定向至自动登入的门户。严重的违规可导致阻止或隔离设备、重新安装安全代理、重新启动代理或进程、触发端点以获取操作系统修补程序或执行其他修复措施的操作。

ControlFabric 架构的价值

ControlFabric 架构是 ForeScout CounterACT 功能与第三方网络、安全性、移动性和 IT 管理产品之间的纽带。它消除了安全管理孤岛，从而：

- 统一系统范围安全管理
- 实现更高的运营效率
- 加快威胁响应
- 加快安全投资回报
- 大幅改善您的网络安全性以及合规性情况

图 2: ForeScout CounterACT 处理全部控制操作。

协调。 CounterACT 利用 ForeScout ControlFabric® 架构以在您已经拥有的安全和系统管理工具中协调信息共享以及操作。ControlFabric 架构可让您通过自定义集成或即插即用软件模块实现这点。同 ForeScout 技术合作伙伴共同开发的 ForeScout 基本和扩展模块将 CounterACT 的功能带给 70 多个领先的网络、安全、移动和 IT 管理产品*，从而：

- 与 IT 安全和管理系统共享上下文见解
- 跨系统将一般工作流程、IT 任务和安全流程自动化
- 加快系统范围响应以迅速缓解风险和数据违规

特性

常规

带外部署在您的网络上以带外形式部署，不会造成延迟或潜在的网络故障点。

可见性： 资产清单功能提供实时、多维网络可见性和控制，可让您跟踪并控制用户、应用程序、进程、端口、外部设备等等 (参见图 1) 。

开放的互操作性： CounterACT 可用于受欢迎的交换机、路由器、VPN、防火墙、端点、操作系统 (Windows®、Linux、iOS、OS X 和 Android) 、修补程序管理系统、防病毒系统、目录以及标签系统 - 无需更改基础设施或升级设备。

报告： 完全集成的报告引擎可助您监控自己合规性级别、履行合规性审核要求，并生成实时的资产清单报告。

可扩展性： 在端点数超过 1,000,000 的客户网络中经过证明。CounterACT 设备有各种大小可用。

认证： CounterACT 是军事级方案，获得了以下认证：

- USMC 运作权 (ATO)
- U.S. Army CoN (Networthiness 证书)
- UC APL (统一功能批准产品清单)
- 通用标准评估保证等级 (EAL) L4+

非破坏性： 部署不会影响用户或设备。当您希望通过自动化控制继续工作时，可逐步进行，从问题最明显的位置开始，并选择适当的执行措施。

策略管理： 创建最适合您的企业的安全策略。由于内置的策略模板、规则和报告，配置和管理迅速而方便。

ControlFabric 架构： ControlFabric® 架构提供丰富的第三方互操作性以及开放的集成架构。

端点

无代理：无需代理，对网络访问进行确定、分类、验证和控制。只要 CounterACT 在端点上具有管理凭据，可在没有代理的情况下执行深入的端点检查。在 CounterACT 没有管理凭据的情况下，例如对于自带设备的情况，则可借助我们可选的 SecureConnector 代理执行深入检查，该代理免费随 CounterACT 附送。

端点合规性：确保您网络上的端点符合您的防病毒策略、正确应用了修补程序并且没有非法软件。CounterACT 自动确定政策违规、修复端点安全缺陷并根据法规强制要求进行衡量。

威胁检测：持续监控可比时间点漏洞扫描提供更加及时、准确的见解，因为某些设备可能进入网络后又离开。

未授权设备检测：检测未授权基础设施，例如未授权交换机以及无线接入点。CounterACT 甚至可检测没有 IP 地址的设备，例如专门用来窃取敏感信息的隐秘数据包获取设备。

访问

访客注册：允许访客访问您的网络，而不会危及您内部网络的安全。数个访客注册选项可让您根据组织的需求定制访客进入过程。

基于角色的访问：CounterACT 确保具有正确设备的正确的人获得正确网络资源的访问权限。它利用您在其中向用户身份分配角色的现有目录。

灵活控制选项：和过多采用手动控制并且会干扰用户的“老旧”NAC 产品不同，CounterACT 提供全面的执行选项，可让您针对具体情况量身打造响应。通过向最终用户发送通知或自动修复安全问题解决低风险违规；这可让用户在进行修复时保持高效（参见图 2）。

802.1X 身份验证或其他技术：可选择 802.1X 或其他身份验证技术，例如 LDAP、Active Directory®、RADIUS®、Oracle® 和 Sun。混合模式可让您同时使用多种技术，加快大型、多样化环境中的 NAC 部署。

内置 RADIUS：内置 RADIUS 服务器让 802.1X 的推行更加便利。或者通过配置 CounterACT 以作为 RADIUS 代理工作来利用现有 RADIUS 服务器。

可扩展模型

CounterACT 在端点数目超过 1,000,000 的客户网络中拥有业经证实的良好业绩记录。它可用在一系列物理和虚拟设备选项中，满足您业务的具体要求。可集中通过 CounterACT Enterprise Manager 管理需要多个设备的大型网络。每个 CounterACT 设备具有永久的许可证，用于指定数量的网络设备。有关许可政策的详细信息，请访问 www.forescout.com/licensing。

集中管理和控制

CounterACT Enterprise Manager 可以物理或虚拟设备的形式部署，提供集中管理以及对于 CounterACT 实施的控制。它可以监视 CounterACT 的活动和策略，并收集每个设备上恶意活动的信息，以及 CounterACT 执行的识别、通知、限制和修复操作的信息。该信息可在 CounterACT 控制台上显示和报告。

访问 **www.ForeScout.com**
了解更多信息

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

免费电话（美国） 1 -866-377-8771
电话（国际） +1-408-213-3191
支持电话 1-708-237-6591
传真 1-408-371-2284

*截至 2016 年 1 月。
**Gartner, Inc.，“网络访问控制魔力象限”，Lawrence Orans 和 Claudio Neiva，2014 年 12 月 10 日Gartner 公司不推荐任何在其研究出版物中所述的供应商、产品或服务，也不建议技术用户只选择排名最高的供应商或指定其他供应商。Gartner 公司的研究出版物仅代表 Gartner 研究机构的观点，不应理解为对事实的声明。Gartner 公司对该研究不承担任何明示或暗示担保，包括任何适销性或适用于某一特定用途的担保。

版本 6_16