FORESCOUT
Active Defense for the Enterprise of Things™

现代NAC

无代理、灵活且非破坏性的零信任安全，适用于您的物联企业。

今天的企业需要一种方法来实施和维护零信任访问，用于其多种网络类型和一系列连接事物——园区计算机、访客设备、在家办公笔记本电脑、IoT、OT和智能设备。他们需要一个现代网络访问控制（NAC）平台来完成以下事情:

- 持续识别所有连接的事物
- 评估其态势
- 执行访问策略
- 自动对不合规或异常行为实施控制

零信任，说起来容易做起来难

控制所有连接到企业网络的事物很令人头疼。实施这些系统的IT和安全架构师面临着以下挑战：

- 早期的NAC解决方案由于复杂性或对业务运营产生负面影响的风险而失败
- 企业网络上激增的IoT和OT设备无法通过传统代理进行认证或控制
- 基于802.1X的控制在多供应商网络中不可行
- 计划中的网络扫描没有考虑到欺骗尝试和其他随时可能出现的威胁
- 许多零信任访问替代方案成本太高和/或需要太多人工投入

> **曾有人告诉我们可以在一个下午部署Forescout平台。我看着我的一个团队成员，我们俩都翻了个白眼。然后我们却真的部署了，就在几个小时内！**
>
> **MIKE ROLING**
> **首席信息安全官，密苏里州**

Forescout：同类最佳的现代NAC解决方案

如果上述挑战听起来耳熟，那么现在就是从Forescout评估网络访问控制的绝佳时机。我们可以通过以下方式满足您的需求并超出您的预期:

最全面的可见性

我们的20多种主动和被动技术，使连接到您的扩展网络的所有设备都100%可见，且实时同步。

用于所有连接设备的零信任

通过持续的无代理监测和统一的策略引擎控制违规影响，该引擎动态分割和隔离所有连接到您企业的事物。

非破坏性部署，为您的网络提供快速价值

无代理软件无需基础架构升级或802.1X配置，可在数天内获得全面可见性，并在数周内实现自动化控制。

经过验证的企业级扩展网络

我们数以千计满意的财富1000强客户，其中一些拥有200万个端点，他们证明了Forescout在保护网络安全方面的能力和给予客户的信心。

扩展您的安全和IT投资价值

大多数安全工具仅仅是标记违规行为并提醒您的员工。Forescout平台包括即插即用的模块，将可见性和控制功能扩展到：

- 与您的安全和IT管理工具实时共享设备情境
- 协调工作流并自动化响应操作
- 持续评估安全态势并执行自动修复设备的合规行为

“今天的NAC工具最适合帮助隔离设备和未经批准的实体（用户、细分、设备等），使其无法“接触”网络。使用这些来自Forescout等供应商的较新的NAC技术，帮助将未知的和可能未打补丁的项目从您的零信任网络中删除。”[1]

CHASE CUNNINGHAM
首席分析师，FORRESTER Research

识 别

发现所有连接设备并对其分类、列出清单

有了Forescout平台，安全和IT运营团队可在所有IP连接的设备访问网络时即实时获得100%的可见性，从而创建准确实时的资产清单。

- 从20多种主动和被动发现和剖析方法中选择，匹配您的业务环境，并帮助确保持续的网络可用性
- Forescout设备云中的12M+设备指纹为您提供了高保真的三维设备分类功能，可以确定设备功能、OS、供应商和型号等
- 获得所有地点、网络和设备类型的全面覆盖——无盲点——无论是否有802.1X认证

合 规

评估安全态势和合规性

基于代理的安全工具对代理缺失、损坏或无法使用的托管设备视而不见。另外，由于IoT设备无法支持安全代理，这些工具无法对其进行评估——进一步扩大了受攻击面。但通过Forescout平台，您可以在连接时自动对所有基于IP的设备进行态势评估和修复，并在之后持续进行。

- 从您现有的安全工具中查找并修复代理缺失、损坏或无法使用的托管设备
- 检测设备不合规性、态势变化、漏洞、弱凭证、IoC、欺骗尝试和其他高风险指标，所有这些都不需要代理
- 评估并持续监测非托管设备，包括不能接受代理的设备，以执行安全合规

我们从Forescout平台上得到的信息量是不可思议的。它确实是我用来正确寻找、识别和控制系统最好工具。它对我们来说无比宝贵。

JOSEPH CARDAMONE
SR.信息安全分析师，
HAWORTH INTERNATIONAL

连 接

在异构网络执行访问策略

Forescout平台基于设备和用户身份、设备卫生和实时合规状态实施零信任安全，而不需要对基础架构进行硬件或软件升级。

- 根据用户角色、设备类型和安全态势，提供对企业资源的最低权限访问
- 防止未授权、非法和冒充的设备连接
- 在有线、无线和VPN基础架构上实施灵活的控制——无论是否有802.1X

1. 零信任扩展生态系统：网络战略计划：安全架构和运营手册，弗雷斯特研究，2019年1月2日
2. Forrester Wave™: 零信任扩展平台提供商，2019年第4季度

Forescout]平台以及IoT/OT安全能力远高于竞争对手。最大的可见性，带来最大的运营控制和最终的安全，是Forescout零信任方法的核心。[2]

FORRESTER RESEARCH

不要视而不见。要保护。

马上联系我们，主动保护您的物联企业。

forescout.com/platform/eyeControl　　china@forescout.com　　zh.forescout.com

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
美国加利福尼亚州圣何塞，95134

电子邮件 china@forescout.com
电话（国际）+1-408-213-3191
支持+1-708-237-6591

访问Forescout.com了解更多