FORESCOUT
Active Defense for the Enterprise of Things™

物联网安全

选择灵活的零信任
非传统方法
物联网企业中的设备

物联网(IoT)设备在企业网络上往往是隐形的。与传统系统不同，它们不易被跟踪，而且几乎不支持软件代理。这些设备扩大了受攻击面，并大大增加了组织的风险，因为它们可以被破坏，当作漏洞的进入点进入脆弱的企业网络。企业需要一种安全解决方案来持续识别和细分异构网络上的每台IoT设备，并强制其合规。

IoT设备：风险是否值得回报？

IoT设备很宝贵，它们往往是关键的企业资产。它们推动了生产力，改善了产品和服务质量，提高了底线。事实上，63%的企业期望在三年内实现其IoT项目的财务回报。[2] 老练且资金充足的危险分子一直在寻找组织中可利用的领域，如IoT可见性和安全性方面的漏洞——这些漏洞会导致停机、数据泄露、知识产权损失和声誉受损。想想看：

- 在波耐蒙研究所最近的一项调查中，近十分之九的受访者预计他们的公司将在未来两年内遭遇由不安全的IoT设备或应用程序引起的网络攻击或数据泄露。[3]
- 到2023年，首席信息官要负责的平均端点数量将是他们在2018年所管理端点的三倍以上。[4]

在当今的物联企业（EoT）中，无数的IT、IoT和OT（运营技术）事物互联交叉，企业需要一个安全解决方案，使IoT和所有IP连接的设备可见和可控，并符合零信任的联网方法。
否则，任何设备都可能被入侵并被恶意利用。

零信任定义

FORRESTER　research的信息安全零信任模型是一种保证企业安全的概念和架构方法。在其最简单的形式中，零信任就是建立信任，方法就是确保您在一个拥有可信访问权限的可信设备上拥有一个可信的用户。访问仅限于每个用户完成其工作所需的企业资产。弗雷斯特认为，[1] 要实施有效的零信任策略，必须：

- 将网络重新设计成安全的微边界
- 利用混淆技术加强数据安全
- 限制与过度用户权限和访问有关的风险
- 利用分析和自动化大幅提高安全检测和响应能力

Forescout零信任方法

Forescout认为，IoT安全必须基于零信任方法，将完整的设备可见性、主动的网络细分和对所有数字资产——设备、用户、应用和工作量的最低访问权限控制结合起来。Forescout平台通过以下方式让您有效管理整个EoT环境中的网络、运营和合规风险：

- 为未托管的IoT、医疗物联网（IoMT）和OT设备以及所有IP连接系统提供完整的可见性
- 评估和识别出厂默认或弱凭证的IoT设备，并自动执行强密码的策略操作
- 提供对IoT设备在扩展环境中的通信和风险行为的实时洞察
- 通过零信任策略执行最低权限访问，将设备划分进受信任区域
- 在多供应商环境和多个网络管区中自动编排统一的零信任策略
- 打破安全管理孤岛，加快响应速度，并且最大化您在其他安全解决方案上的投资价值
- 通过与Medigate的密切合作，帮助医疗健康组织（HDO）主动检测和减少漏洞/威胁，精细执行细分和网络访问规则，并立即遏制医疗设备威胁，同时推进补救措施

Forescout是提供零信任专注IoT/OT安全的供应商。IoT/OT设备安全是企业内部最难解决的问题之一。这是Forescout的甜蜜点，该供应商在IoT/OT安全方面的平台能力远超其竞争者。

FORRESTER WAVE：零信任扩展生态系统平台供应商，FORRESTER RESEARCH，2019年10月

图1：Forescout通过识别和细分每个连接的事物并强制其合规，主动保护您物联企业中的所有设备。

发现全部IP连接设备并对其分类

要获得异构环境中所有IoT、OT和关键基础架构端点的完整可见性和设备描述表，这一点至关重要。Forescout平台：

- 从所有IP连接设备（无论是实际的还是虚拟的）进入您网络时起，就持续发现它们——无需软件代理
- 使用20多种主动和被动发现、收集和分类技术，提供所有设备的深度可见性
- 利用Forescout设备云——世界上最大的众包设备智能数据湖，为1200多万台设备的指纹、行为和风险状况提供跨行业的单一信息源

实施动态网络细分，自动化控制

在当今的异构EoT环境中，采用零信任模式的企业必须能够在所有EoT领域进行网络细分和精心编排的事件响应。通过Forescout，您可以：

- 将访问与用户身份相关联（谁在做什么、在哪里、何时和为什么）
- 根据策略和实时情境将设备配置到动态网络细分
- 绘制数据流以设计细分策略，并模拟它们进行非破坏性部署
- 自动化细分，降低网络和运营风险

精心确保安全并强制合规

大多数组织都充斥着昂贵的、单一目的的安全解决方案，这些方案无法共享知识或协调事件响应。Forescout提供了解决这种低效的方法。Forescout eyeExtend产品可在Forescout平台与其他IT和安全产品之间共享设备情境，以便在不同的解决方案中自动执行工作流程和策略。这些协调功能可以帮助您：

- 提高IoT安全和整体设备合规性
- 缩短检测和响应的平均时间
- 提高现有工具的ROI
- 自动化您的配置管理数据库（CMDB）更新过程，消除耗时和容易出错的手动盘点

“今天我们知道我们的网络上有什么——包括IoT 设备，比如打印机、网络电话和监控摄像头。Forescout对设备进行分类，并将其分至恰当的VLAN细分。”

– KEN COMPRES，高级网络安全和集成工程师/CSO，西尔斯波洛社区学院

1. 零信任网络的五个步骤，路线图报告，Forrester Research，2018年10月
2. 物联网：释放真正的商业潜力，高德纳
3. 第三方IoT风险管理的新路线图，基准研究，波耐蒙研究所，Sabine Zimmer，2020年6月3日
4. 到2023年，IoT趋势和技术的主要战略，高德纳，2018年9月

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/IoT　　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