FORESCOUT
Active Defense for the Enterprise of Things™

eyeSight
全面的设备可见性

无代理
获得联网设备的统一、实时清单。

准确
剖析所有设备，获得建立主动安全和合规的情境

有效
识别非法、有漏洞或不合规的设备并建立策略限制风险

可靠
实时保证安全工具和合规控制正常运转。

高效
自动衡量并报告合规态势及网络风险暴露情况，同时尽量减少人为错误，提高效率。

持续发现、分类并评估您企业中所有连接的事物

Forescout eyeSight为您的整个物联企业（EoT）提供绝无仅有的洞察，而且不会中断关键业务流程。

- 发现每台IP连接设备
- 自动分类设备并获取全面
- 评估策略合规性和设备安全态势

发现
在设备连接至网络时即进行查看

随着设备短暂进出持续监测

获取实时资产清单而不会中断业务

分类
识别不同类型的IT、IoT和OT设备

利用Forescout设备云的力量

提高自动分类效率和速度，扩大其范围

评估
识别安全风险和合规漏洞

评估对内部和外部指令的遵守情况

获取对网络和运营风险的情境感知

发 现

持续的无代理发现

消除盲点并最小化运营风险，同时您的EoT具备完全的可见性：

- 笔记本电脑、平板电脑、智能手机、BYOD/访客系统、在家办公设备
- 园区网络、数据中心、分支机构、远程站点和边缘网络中的IoT设备
- AWS、Azure和VMware环境中的公有云和私有云实例
- 操作技术（OT）系统，包括医疗、工业和建筑自动化
- 实体和SDN基础架构，包括交换机、路由器、无线接入点和控制器

将20多种主动和被动监测技术的灵活性用于有线、无线、VPN、虚拟和软件定义网络。避免破坏对主动扫描技术敏感的设备。

对基础架构被动	对终端设备被动	对终端设备主动
SNM陷阱	网络基础架构轮询	无代理Windows检查 • WMI • RPC • SMB
SPAN网络流量分析 • NetFlow • 灵活的NetFlow。 • IPFIX • sFlow	SDN集成 • Meraki • 思科ACI	无代理macOS、Linux检查 • SSH
DHCP请求	公有云/私有云集成 • VMware • AWS • Azure	NMAP
HTTP用户代理	查询目录服务（LDAP）	SNMP查询
TCP指纹识别	查询网络应用（REST）	HTTP查询
协议解析	查询数据库（SQL）	SecureConnector®
RADIUS请求	eyeExtend协调	

分 类

智能自动分类

零信任策略只有在处于完整的设备情境时才能执行。手动收集这种情境几乎是不可能的，在没有完整设备情境时实施零信任策略可能会使运营面临风险。通过对超过150种IT和OT协议的深度数据包检测，eyeSight可对所有IT、IoT和OT设备进行深度剖析。多维度分类法可识别设备功能和类型、操作系统和版本以及供应商和型号，包括：

- 600多个不同的操作系统版本
- 5,700多个不同的设备供应商和型号
- 来自400多家领先医疗技术供应商的医疗设备
- 用于制造业、能源、石油和天然气、公用事业、采矿业和其他关键基础设施行业的数千个工业控制系统和自动化设备

EYESIGHT可解决以下问题：

孤立的团队和不同的安全工具造成的**可见性漏洞**

源于容易出错的人工流程的运营和业务风险

妨碍可防御零信任策略执行的**不完整的设备情报**

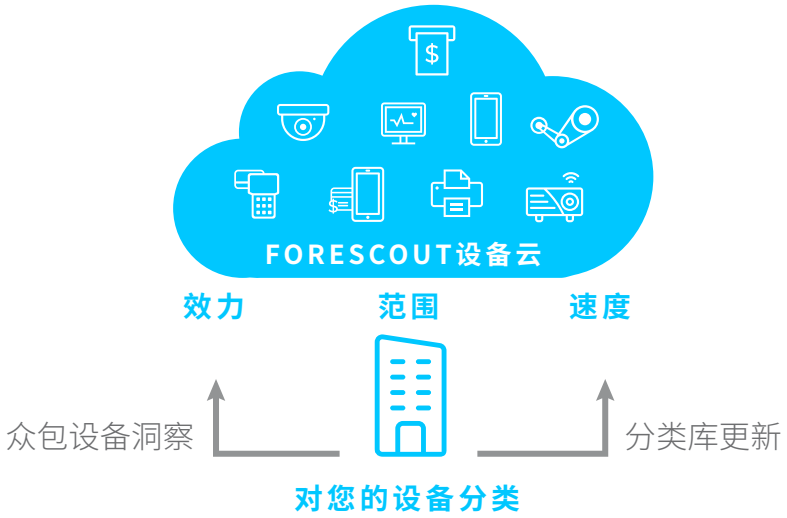
基于代理的工具没有正常更新或运行时存在的**安全漏洞**

未检测到的非法设备或欺骗设备

可能会在时间点扫描之间迅速出现的**不合规**

由Forescout设备云提供的自动分类

设备云是全球最大的众包设备智能数据湖，可以最全面、最准确地了解任何组织情境内的所有设备风险。



功能		+	操作系统		+	供应商和型号	
• 平板电脑	• 销售点		• Windows 7	• iOS		• 苹果iPad	• GE水处理器
• 无线接入点	• X射线		• Windows服务器2016	• CentOS		• 苹果iPhone	• 日立动力系统
• 打印机	• HVAC系统		• OS X 10.7 Lion	• 安卓		• 苹果机场	• Hoana医疗
• VoIP服务器			• OS X 10.10 Yosemite			• 3M控制系统	

评 估

设备态势评估

零信任策略的另一个基本要素是结合连接设备的安全卫生和风险状况。eyeSight持续监测网络，评估连接设备的配置、安全态势和风险指标，以及它们是否遵守合规规定和安全标准。零信任策略可以基于风险和合规性条件，如：

- 安全软件是否已安装运行，并更新至最新的补丁？
- 是否有设备运行未授权的应用程序或违反配置标准？
- 设备（尤其是IoT和OT系统）是否使用默认或弱密码？
- 是否已经检测到非法设备，包括欺骗合法设备的设备？
- 您的哪些连接设备最容易受到最新威胁的影响？

监 测

EoT可见性和合规性

从开箱即用和可定制的仪表板中获取可操作的洞察，快速确定您的联网设备风险，并确定其优先级和主动缓解风险。动态视图有助于安全分析师和SOC团队

- 评估所有或任何策略子集的风险和合规进度
- 识别易受攻击和受损的设备，加速事件响应
- 一段时间内跟踪合规趋势
- 个性化并分享高管和审计师对风险和合规的看法
- 按策略或设备属性快速搜索和过滤EoT资产

细分、协调和执行

通过一套Forescout产品扩展eyeSight的价值，从而可以为网络访问控制、IoT安全、网络细分和OT安全设计和实施零信任策略。

访问www.forescout.com/platform/
了解更多关于Forescout eyeSegment、eyeControl、eyeInspect和eyeExtend的产品

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/eyeSight　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