

eyeInspect

全面的设备可见性

无代理

获得统一、完整的所连接IP和串行设备的实时OT资产清单。

准确

借助数千个OT特定的威胁指标和强大的基于机器学习的异常检测，为资产设立基线并保护您的网络。

有效

主动评估风险，发现威胁，衡量其商业影响并优先进行修复任务。

可靠

实时保证安全工具和合规控制正常运转。

高效

将时间密集型的合规和风险评估任务自动化，同时尽量减少人为错误，提高效率。

降低风险，自动化合规，优化ICS和OT环境的威胁分析

Forescout eyeInspect为OT (运营技术) 网络提供了深入的设备可见性，并能有效地实时管理各种运营和网络风险。

- 使用数千个ICS/OT特定威胁指标和查询建立可采信的网络行为基线
- 根据风险等级和原因，汇总数千条警报和数百万条日志
- 自动对设备进行分类和评估，以符合政策和法规合规性



可视化

在设备连接到网络的瞬间就看到设备。

随着设备进出持续监测。

获得实时资产清单，而不中断业务。



检测

识别不同类型的具有IP功能的串行OT设备。

为设备和设备组设立基线。

优化自动分类效力和持续监测。



响应

自动化合规评估。

用直观的风险分数评估风险。

获得对网络和运营风险的情境感知。



可视化

在一个屏幕上可视化上千台设备

- 看见一切。消除与新连接设备和非法设备相关的盲点
- 获得详细准确的实时资产清单
- 查看具有IP功能的串行设备，包括HMI、SCADA、PLC、控制器、传感器、仪表和I/O

检测

智能检测威胁并管理风险

- 借助数千个ICS/OT特定的威胁检查和受损指标，检测已知和未知的网络威胁
- 检测网络和运营风险，并根据紧急程度和对业务的潜在影响来确定其优先级
- 检测整个网络中的不合规设备和策略
- 检测网络的变化，包括新设备、基础架构的变更和不正常的运营活动

响应

采用世界上最智能的可扩展OT安全解决方案来响应

- 根据明确的分数响应网络和运营威胁
- 使用预先定义的自动化 workflows、规则和修复操作响应警报
- 使用资产基线定义的规则、参数和报告响应合规变化
- 查看楼宇管理系统 (BMS) 和楼宇自动化系统 (BAS) 设备，包括HVAC和门禁控制
- 查看其他实体和SDN基础架构，包括交换机、路由器、VPS、无线接入点和控制器
- 根据各种参数，包括时间、设备、网络位置和警报类型，查看警报和日志

企业指挥中心需求

最低要求	
硬件/管理程序	19"机架式服务器或最低VMware ESXi 5
处理器	12核(英特尔®)CPU 64位≥2.4GHz
内存大小	32-64GB
硬盘驱动器	500GB-1TB自动精简配置
网络接口	用于指挥中心通信和网络应用程序访问的接口

指挥中心要求

	小型部署 (≤5个传感器)	中型部署 (≤10个传感器)	大型部署 (>10个传感器≤100个)
管理程序	最低VMware ESXi 5		
形状因数	19"机架式服务器或虚拟设备		
处理器	4核CPU 64位	4/6-core (intel) CPU 64-bit	12-core (intel) CPU 64-bit ≥ 2.4 GHz
内存大小	16GB	32GB	64-256GB
硬盘驱动器	500GB	1TB	>1TB
	(按数据保留90天计算)		
网络接口	用于传感器通信和网络应用访问的接口		

被动传感器要求

	小型部署 (最高100Mbps)	中型部署 (最高500Mbps)	大型部署 (最高1Gbps)
硬件模型示例	Foxguard® IADIN-FS1	戴尔®嵌入式计算机5000	戴尔®PowerEdge R640
部署说明	小型网络和恶劣环境中的部署	中型网络、恶劣环境中的部署	大型网络和数据中心安装中的部署
形状因数	小型工业PC/DIN 钢轨配件	中型工业PC	19"1U机架式服务器
处理器	2核或4核(英特尔) CPU 64位	4核或6核(英特尔) CPU 64位, 8GT/s	6核(英特尔) CPU 64位≥2.4GHz
内存大小	4-16GB	16-32GB	64-256 GB
硬盘	工业PC64GB-500GB(应使用宽温SSD)		
监测接口	最多4个监测接口	最多8个监测接口	最多8个监测接口

主动传感器最低要求

与被动传感器集成	独立运行	虚拟
eyeInspect可直接集成到任何被动传感器上,用于小型、中型和大型部署。	处理器	4vCPU
	内存大小	4GB RAM
	网络接口	≥1

有关更多硬件要求信息,请访问:

<https://www.forescout.com/company/resources/command-center-and-sensor-hardware-guidelines/>

协议

有关所有标准OT、IT和专有OT系统协议的完整列表，请访问此链接：<https://www.forescout.com/company/resources/eyeinspect-protocols/>

协调、细分 和控制

Forescout通过一套产品扩展了eyeInspect和Forescout平台的价值，从而可以为资产管理、设备合规、网络访问、网络细分和事件响应设计并实施策略和自动化操作。请访问 www.forescout.com/platform/，了解Forescout的eyeSight、eyeSegment、eyeControl、eyeManage和eyeExtend产品。

eyeInspect可解决以下问题：

由以下原因引起的**OT可见性漏洞**：

地域分布和非同质设备网络

当补丁没有得到解决或应用程序被暴露时存在的**保护和漏洞挑战**

警报过载和修复任务优先级不当造成的**运营和网络风险**

对可防御策略的执行造成妨碍的不完整的威胁情报

使您的组织面临严重罚款的风险的**资源密集型合规任务**

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/eyeInspect

china@forescout.com

zh.forescout.com