FORESCOUT
Active Defense for the Enterprise of Things™

OT的网络安全和风险管理

降低风险，自动合规，优化ICS和OT环境的威胁分析

信息技术（IT）和运营技术（OT）网络的不断融合，正在增加

工业控制系统（ICS）网络的复杂性和脆弱性，而这些网络原本是孤立的。同时还有工业物联网（IIoT）设备的爆炸性增长，这就造成了巨大的可见性差距，并使合规执行更加困难。企业需要一个可以提供深入的OT和ICS网络可见性，并实现对运营和网络风险的有效实时管理的安全工具。

> **“到2021年，80%的IIoT项目将有OT特定的安全要求。”[1]**
>
> **高德纳**

OT环境中的主要挑战

随着组织升级基础设施，采用新技术，并将OT和IT网络结合在一起，高度脆弱的OT和ICS系统必须在现代异构的网络环境中得到维护和保护。因此，安全和运营团队面临着新的挑战，包括：

- 识别、分类和控制所有连接的IT设备、IIoT系统和OT资产——无论是否托管
- 分析警报，确定威胁的优先级，及时响应事件，将业务中断降到最低程度
- 确保所有连接的设备——即使是遗留的OT系统——都符合监管要求和政策
- 保持准确、最新的资产清单

Forescout eyeInspect：IIoT和OT基础设施的网络恢复能力和风险管理

Forescout eyeInspect（前身为SilentDefense™）可保护OT和ICS网络免受各种威胁，提供被动和主动发现功能，创建自动、实时的资产清单，并根据潜在的业务影响采取有针对性的修复操作。

- 实现被动、实时的网络监测和细分
- 通过高级警报汇集优化威胁分析和修复
- 提供与ServiceNow®的丰富集成，并与SIEM解决方案、防火墙、IT资产管理、沙盒和认证服务器自然连接
- 提高SOC和分析师的效率，实现和资产风险框架的风险分析自动化
- 将Forescout平台卓越的设备可见性、分类和剖析功能从云端扩展到边缘设备

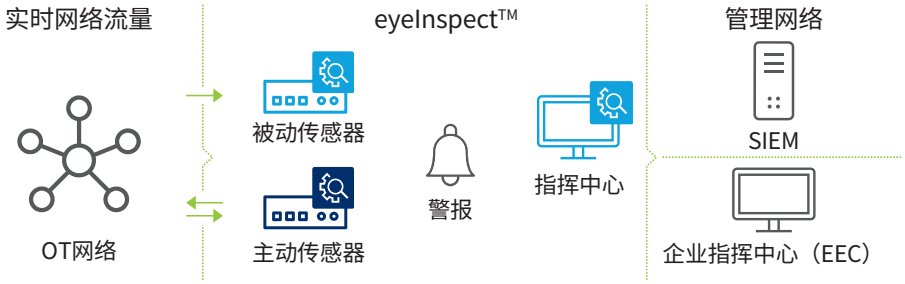

图1：基本的eyeInspect部署模式

完整的可见性和威胁检测

eyeInspect将Forescout平台业界领先的设备可见性、分类和剖析功能扩展i到更深层的OT和ICS环境。它可以识别和有效修复各种网络和运营威胁，包括：

- 网络攻击（DDoS、MITM与扫描等）
- 未授权的网络连接、通信
- 可疑的用户行为/策略变化
- 设备故障或配置错误
- 新的和无响应的资产
- 损坏的信息
- 未授权的固件下载 不安全的协议
- 默认凭证和不安全的认证
- 逻辑变更
- 对具有IP功能的串行设备的可见性

eyeInspect使用案例

资产可见性和监测

eyeInspect提供OT网络和站点内的持续资产可见性。eyeInspect自动构建详细的网络地图，其中包含丰富的资产详情，并可按网络/角色自动分组，以多种格式（如普渡级别和通信关系）提供。eyeInspect使用广泛的发现功能，包括：

- 150多个IT和OT协议的专利深度数据包检测
- 持续、可配置的策略和行为监测
- 自动评估设备漏洞、威胁暴露、网络问题和运营问题
- 可选的非入侵式主动组件，可选择性地查询特定主机

资产配置管理

eyeInspect自动收集各种OT资产信息，记录所有配置变更，进行安全分析和操作取证。发现的详情包括：

- 网络地址
- 主机名称
- 资产的供应商和型号
- 序号
- OS版本
- 固件版本
- 硬件版本
- 设备模块信息

自动化合规

借助eyeInspect主动传感器，资产所有者可以

根据特定的合规策略轻松确定资产和资产组的基线，自动检测偏离既定基线的情况。这些基线允许您根据组织的需要，或NERC CIP、ISA99/IEC 62443、NIS和NIST CSF，以及FDA和

FIPS等合规指南来自定义基线策略。资产所有者可以就这些合规框架的基线生成可采信的证明/报告。

网络访问控制和细分

eyeInspect利用Forescout平台的ACL和VLAN分配功能，为运营网络带来基于策略的细分和访问控制，支持

跨IT、IoT和OT的统一实时资产管理。借助eyeInspect，资产所有者可以对IT、OT和医疗保健环境中资产之间的关系（通信模式）进行情境感知（即协议感知/DPI）映射和可视化，并可与其他现有的流量遥测系统/产品（Medigate、NetFlow、SPAN等）集成

网络恢复能力的底线收益

Forescout eyeInspect可以通过改善其运营系统的安全性和恢复能力，同时大幅提高管理效率、风险管理和合规性，对组织的盈亏底线产生积极影响。

例如，Forescout最近研究了OT网络监测 对美国一家著名食品生产公司财务业绩的贡献，该公司的17名FTE专注于ICS网络安全和合规性。2 该研究发现：

- 每年节省820,336美元，降低了人工成本，提高了管理效率
  提高了与资产和网络可见性相关的威胁猎取能力。
- 与可操作的威胁管理更新、更快的事件响应和减少的停机风险相关的成本每年节省346,456美元，
- 所有这些都与改善的网络威胁检测和响应能力有关。
- 与ICS安全和资产管理解决方案的内置集成相关的合规成本每年节省158,120美元。

威胁检测和事件响应

- 使用eyeInspect的警报调查和响应工具自动进行威胁检测、控制和修复。仪表板和小组件加强用户协作。丰富的警报详情支持根本原因分析，并加速有效、高效的响应。企业指挥中心(EEC)允许用户放大来自其任何多站点或地理分布网络的警报，从而详细分析事件，包括涉及的设备和警报情境。

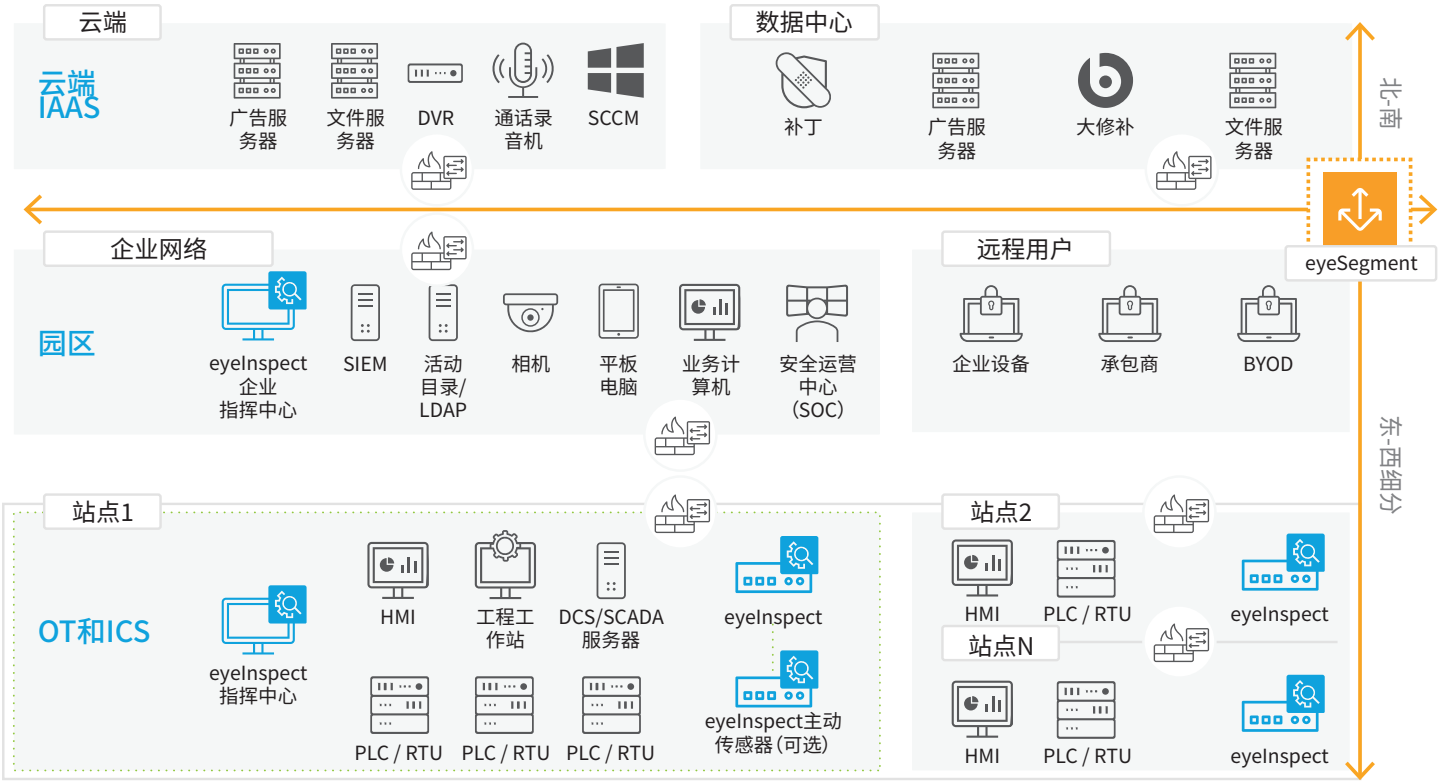

图2：eyeInspect是Forescout的统一IT-OT安全平台的一部分，该平台可在整个扩展企业中提供对网络和运营风险的情境感知和自动控制。

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。

1. SRM领导者在技术选择过程中没有问OT安全供应商的7个问题，Saniye Alaybe yi，高德纳，2018年，https://www.forescout.com/gartner-report-7-questions-for-OT-security-providers

2. 基于标准化客户数据的预测。实际节省可能因多种因素而有所不同。

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