FORESCOUT
Active Defense for the Enterprise of Things™

制造业

工业物联网的网络安全和风险管理

近来网络物理系统的广泛采用已导致网络的高度异构和扁平化。因此，制造商的运营风险增加，为难以控制和修复的网络事件铺平了道路。在与保护制造业网络相关的众多挑战中，三个最困难的是:

- 获得实时网络可见性
- 主动评估和管理网络风险
- 识别联网和运营问题实施正确的OT（运营技术）网络监测解决方案可以帮助制造业组织实现上述三个目标。

制造商的网络恢复能力平台: eyeInspect

Forescout eyeInspect（前身为SilentDefense™）是一个OT网络监测解决方案，可提供工业网络的完整可见性，同时还可保护工业网络免受各种威胁。

eyeInspect将专利的深度数据包检测（DPI）和异常检测技术与一个含成千上万的IoC的库结合起来，用于检测高级网络攻击、网络错误配置和操作错误，所有这些都可以帮助检测已知和未知威胁。

“到2021年，70%的OT安全将由CIO或CISO直接管理，而不是现在的35%。” [1]

高德纳

eyeInspect的图形界面提供了实时网络地图、网络可视化和通信分析，为资产通信或主机变更行为提供全面的可见性。通过持续监测和分析网络通信，并将其与合法运营的基线和我们专有威胁库中定义的“已知不良”特征进行比较，eyeInspect可实时识别和报告网络和运营威胁。

用于制造业网络的eyeInspect用例

实现实时网络可见性

eyeInspect通过被动（或选择性主动）收集各种OT设备信息，为整个ICS网络提供持续更新的资产清单。
发现的详情包括：

- 网络地址
- 主机名称
- 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

eyeInspect还提供了对背板模块、串行设备和资产配置更改的全面可见性，同时记录更改以进行安全分析和操作取证。eyeInspect会自动构建一个详细的网络地图，其中包含大量的设备详细信息、每个资产的基线、

通信可视化以及按网络和/或角色自动分组。分组以多种格式提供，包括普渡级别和通信关系。eyeInspect的主动技术ICS Patrol可安全、有选择性地查询网络上的特定主机，提取更多的资产详细信息。

威胁情报借助EYEINSPECT

威胁环境正在快速演变，因此安全解决方案需要能够快速引入新的检测特征和算法。eyeInspect提供可操作的威胁情报的一些方式包括：

- 实现对OT和IIoT网络的被动、实时网络监测和细分
- 提供eyeInspect主动传感器，这是一种非入侵式的主动技术，可提供深入的资产可见性
- 通过与ServiceNow的丰富集成，简化IT-OT开发运营，实现安全策略
- 通过高级警报汇集优化威胁分析和修复
- 通过资产风险框架提高SOC和分析师的效率，实现风险分析的自动化
- 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

主动管理网络风险

大多数网络监测工具迫使用户单独查看风险因素。eyeInspect是第一个自动评估风险因素和单个数据点的解决方案，为每个资产提供安全和运营风险评分。该安全风险评分可

使安全分析人员立即识别出很可能受到攻击，且有实际证据表明潜在的攻击正在进行的资产。用户可以深入了解风险评分，了解该资产处于风险中的原因以及可以采取的措施。

eyeInspect使用特征以及行为和获得专利的异常检测技术，从最初阶段到实际使用时检测已知和未知威胁。以下是在现场检测到的一些威胁例子：

- L2服务器和现场机器人从外部服务器通信和下载固件
- 细分不力，使易受攻击的设备暴露在互联网上
- 工厂里的类似WannaCry的恶意软件
- 广泛使用默认密码

eyeInspect的交互式地图可识别事件的来源和传播，其数据包捕获（PCAP）中提供的数据可支持根本原因分析，加快响应工作。

识别网络和运营问题

偶尔出现网络和运营问题是不可避免的，但这些问题不一定会导致严重的系统停机。上述运营风险评分使OT工程师能够快速发现需要立即关注的资产，包括出现配置错误或故障迹象、可能导致意外停机的设备。eyeInspect的高级警报汇集功能使用户能根据事件的原因和紧急程度将威胁关联起来。

已识别的威胁包括：

- 使用不安全的协议
- 路线/网关问题
- 以不合规格式发送的数据
- 与现场设备的连接问题
- 关键设备的故障
- 不稳定的程序价值
- 不正确的过程测量
- 开关和设备配置错误

多因素威胁检测

OT网络监测工具需要让用户和分析人员能够尽早检测出现已知和未知的威胁，以实现快速响应和修复操作。eyeInspect将特征与行为和获得专利的异常检测技术相结合，从最初阶段（发现）到实际利用时检测已知和未知的威胁，包括可能会暴露关键设备的不安全配置。

eyeInspect可以识别并帮助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/策略变更
- 设备故障和配置错误
- 新的和无响应的资产
- 尝试中使用的畸形信息
- 未授权的固件下载
- 使用不安全的协议
- 路线/网关问题
- 以不合规格式发送的数据
- 与现场设备的连接问题
- 关键设备的故障
- 不稳定的程序价值
- 不正确的过程测量
- 开关和设备配置错误
- 使用不安全的协议
- 默认凭证和不安全的认证
- PLC逻辑变更

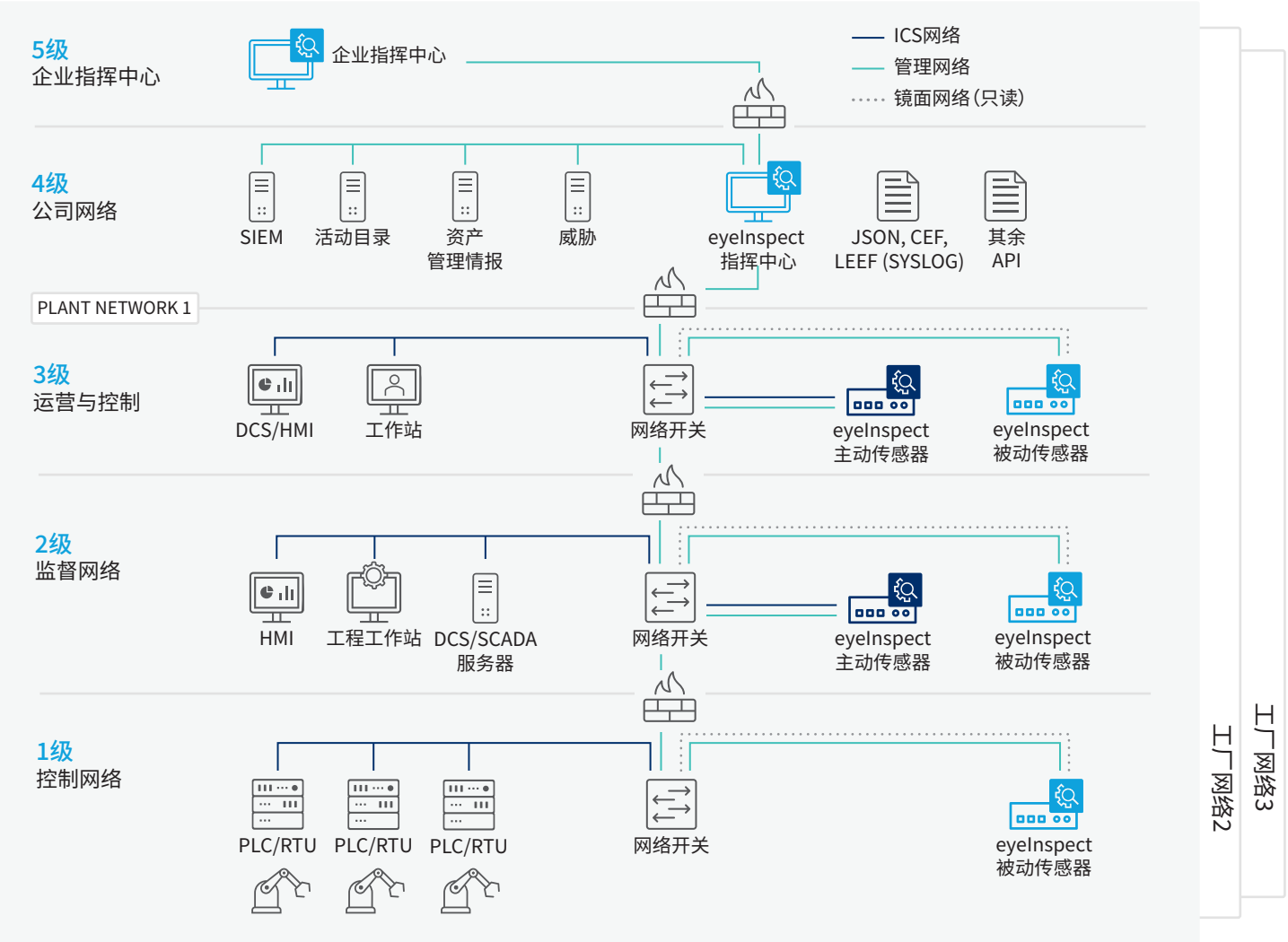

图1：eyeInspect是Forescout统一的IT-OT安全平台的一部分，该平台可在整个扩展企业中提供对网络和运营风险的情境感知和自动控制。

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 Alaybeyi，https://www.forescout.com/platform/operational-technology/gartner-report-7- questions-for-ot-security-providers/

forescout.com/platform/eyeInspect　　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