# Claroty Edge

## 一种快速简单的解决方案，可在几分钟内实现 XIoT 可视化

### XIoT 安全挑战

有效的工业网络安全需要厘清企业工业环境中所有 OT、IoT 和 IT 托管和非托管资产。但是，实现这种可视化是非常困难的，原因有很多，包括：

- 标准化的 IT 解决方案和扫描方法一般与工业网络都是不兼容的，而且对于工业网络是不安全的。
- 传统的工业资产管理解决方案通常所要求的硬件成本昂贵、复杂而且部署过程非常耗时。
- 许多工业网络在地理位置上是孤立，或是 air-gap 网络，从而使其难以访问，无法安装硬件。
- 传统的工业资产管理方法，比如被动数据收集和离线文件分析，在针对所有情况下的网络和用例时，可能不兼容或是不适用。

### 解决方案

Claroty Edge 是一种高度灵活的、基于 Windows 的数据收集器，可在几分钟内实现工业网络完全可视化，无需更改网络，不使用传感器，在较低的网络级别上没有任何物理足迹。

这种快速简便的解决方案可以部署在本地或通过 SaaS 运行，以揭示有关托管和非托管工业资产的深入细节，如果有其他的方法的话，在针对所有情况下的全部网络和用例时，可能不是最理想的或是不适用的。

### Edge 优势一览

**完全可视化**

Claroty Edge 提供您所托管和非托管的 XIoT 资产完整清单，以及影响到这些资产的所有风险与漏洞。

**零更改和无硬件**

Claroty Edge 安全地利用您现有的架构，无需您在网络的较低级别部署硬件。

**在几分钟内得到结果，而不是几天内**

Claroty Edge 在不到 10 分钟的时间，部署并提供对任何工业网络的全面可视化。

**高弹性部署**

Claroty Edge 灵活的云和本地部署选项使其解决方案完全适用于互联的、air-gap 的和云化的网络。

## 关键功能和用例

### XIoT 资产发现

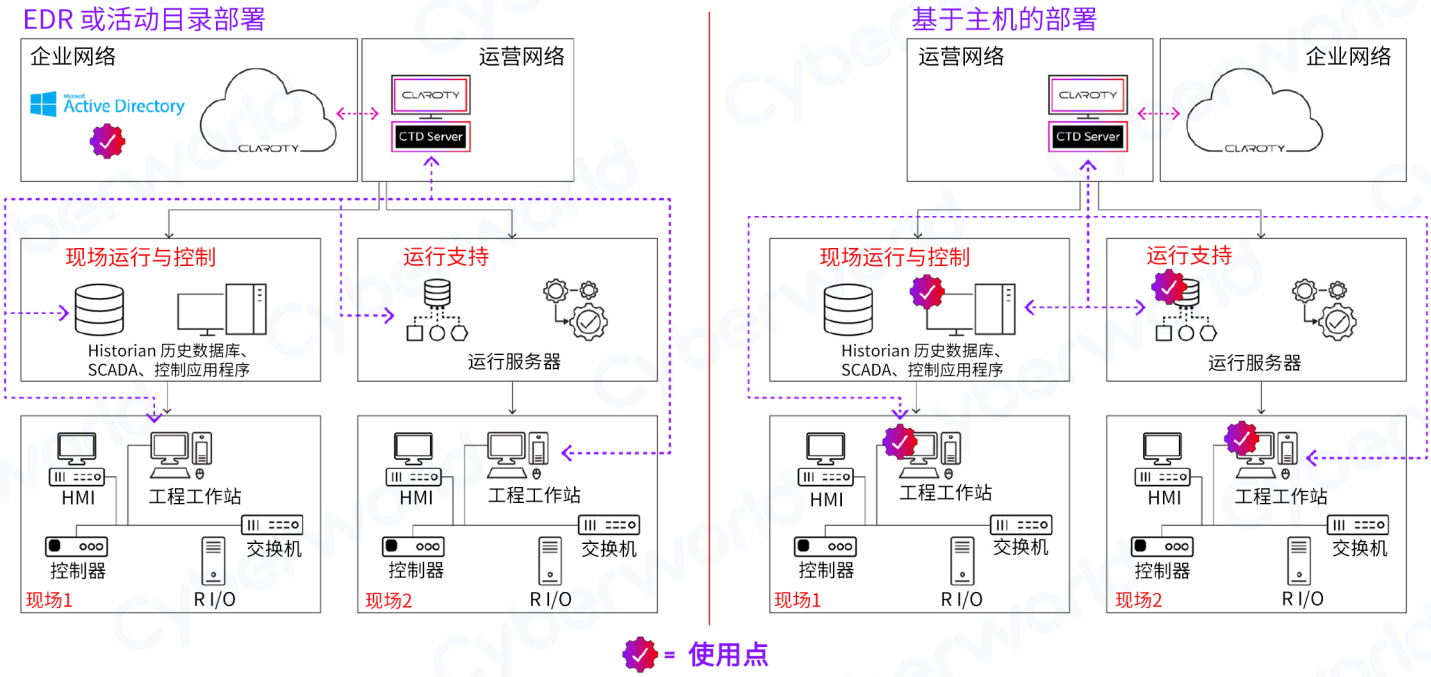
- 获得对所有 OT、IoT 和 IT 托管和非托管资产的完整且近乎即时的可视化。
- 这种可视化为有效的工业网络安全奠定坚实的基础，并且为广泛的相关用例提供支持。

### 风险与漏洞管理

- 轻松地识别和管理各种风险与漏洞，比如重要补丁的缺失、EoL 指标和 CVE 等，这些风险与漏洞都会对您所托管和非托管的资产产生影响。
- 这些功能可以更好地保护工业网络，减少风险。

其他用例包括：

- **审计与合规：**轻松、快速、有效地支持审计请求，并且报告您的工业网络的合规性，从而增强您对报告的信心，降低审计失败的风险，并增强合规性和整体安全态势。
- **M&A 尽职调查：**更轻松、更快速、更有效地对目标企业的工业网络进行 M&A 尽职调查，从而高效地履行 M&A 的各项要求，并且清晰地洞察运行中的风险态势。所有这些都遵循 LOI 规格的要求。
- **事件响应：**立即为安全团队的响应成员提供受感染环境的完整清单，以及风险和漏洞评估，从而优化事件响应工作，包括工业网络的影响评估、范围界定和取证。




## 关于 Claroty

Claroty 使工业、医疗保健和商业机构能够保护其环境中的所有网络化物理系统，扩展物联网 (XIoT)。Claroty 统一平台可以与客户现有的基础设施集成，为可视化、漏洞和风险管理、威胁检测和安全远程访问提供全方位的控制。Claroty 得到了全球领先的工业自动化供应商的支持和采用，拥有广泛的合作生态系统以及屡获殊荣的 Team82 研究团队。