Claroty xDome

面向工业网络安全之旅的模块化 XIoT 解决方案

XIoT 安全挑战

工业企业需要网络安全来维护网络和运营弹性。但是，这两个目标正变得越来越遥不可及。这些挑战的根源存在于扩展物联网(XIoT)的发展中。在数字化转型的推动下，这个庞大的互联网连接涵盖了从工业环境中的传统 OT 资产到“智能”照明和供热通风与空气调节系统，甚至是设施内连接互联网的自动售货机的一切。尽管有明显的商业利益，但这种网络物理连接也产生了新的安全盲点和日益增长的攻击面，对操作可用性、完整性和操作环境的安全构成了相当大的风险。

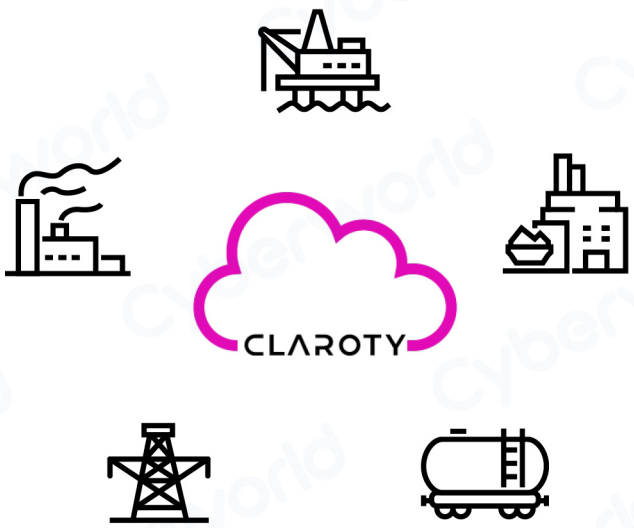
在 XIoT 具有挑战性的安全和风险条件下，实现并保持网络和运营弹性远非不可能 —— 但它确实需要一套强大的要求，传统解决方案或通用方法根本无法满足。Claroty xDome 跨越整个网络安全之旅，从为企业提供全面的资产可视化、识别、衡量和优先排序处理风险，到部署基于零信任的保护控制，再到通过庞大的集成网络优化威胁检测。

xDome 是一个模块化平台、SaaS 平台，通过以下方式明确 XIoT 网络安全决策：

- 资产发现
- 漏洞与风险管理
- 网络保护
- 威胁检测
- 资产管理
- 变更管理

xDome 优势一览

- 通过模块化、SaaS 驱动的工业网络安全平台，在整个 XIoT 中扩展网络安全。
- 支持从资产发现到全面网络安全集成和优化的完整工业网络安全之旅。
- 专为可扩展性、灵活性和易用性而设计，无论网络规模、架构或最终用户的多样性如何。
- 与安全解决方案无缝集成，将现有的网络安全控制扩展到工业环境中。

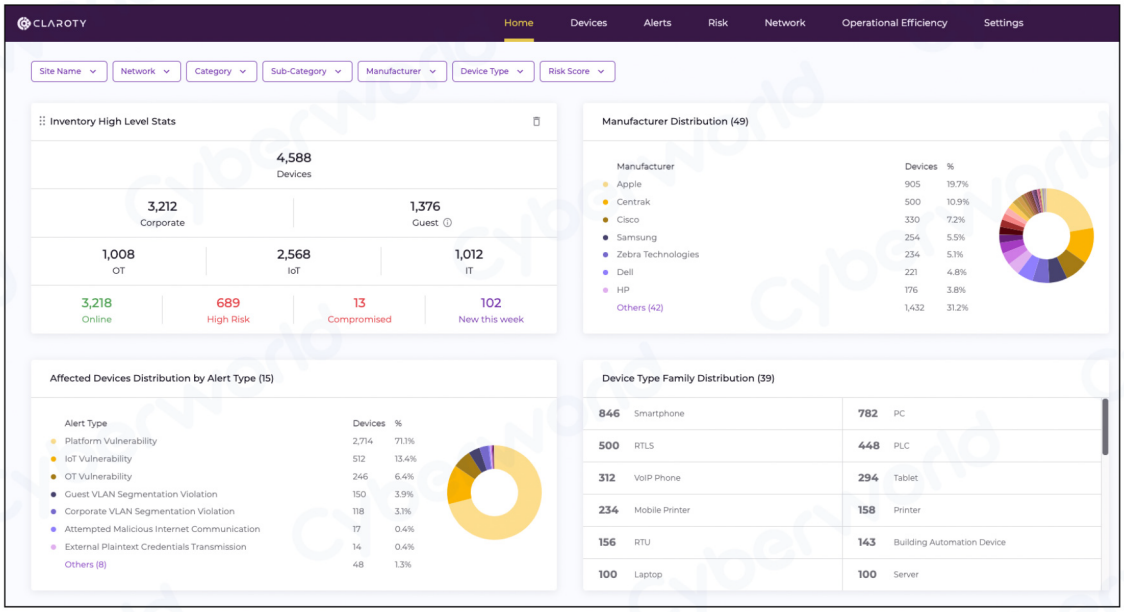


© 2022 Claroty Ltd. All rights reserved

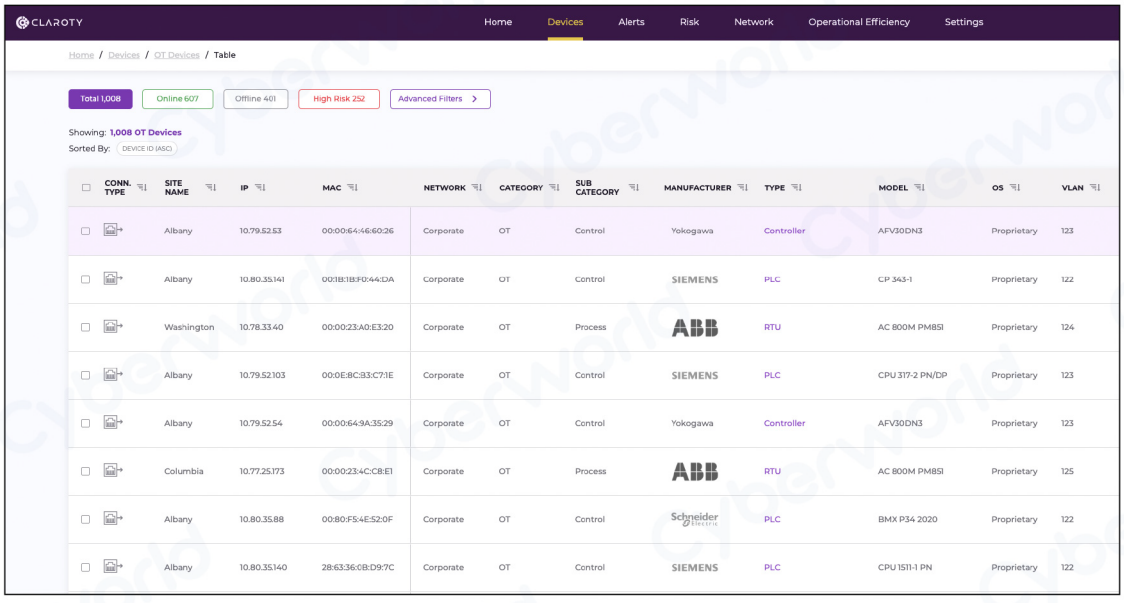
资产发现

有效的工业网络安全始于了解需要保护的内容，这就是为什么全面的 XIoT 资产清单是工业网络安全之旅的基础。Claroty xDome 利用最广泛和最深入的 XIoT 协议覆盖范围组合、Claroty Team82 对这些协议的特定领域研究，以提供高度详细、集中的 XIoT 资产清单。Claroty 是唯一一家能够通过三种不同的、高度灵活可视化的供应商，这些方法可以根据每个环境的独特需求进行组合或单独使用：

- **被动监控：**持续监控网络流量，以识别和丰富资产细节和通信配置文件。
- **Claroty Edge：**战略性地放置，快速安全地查询网络中困难或无法访问的部分。
- **集成生态系统：**与常用的配置管理数据库(CMDB)和资产管理工具无缝集成，进一步丰富资产细节，优化企业资产管理。



Claroty xDome 主页仪表板



Claroty xDome OT 资产列表

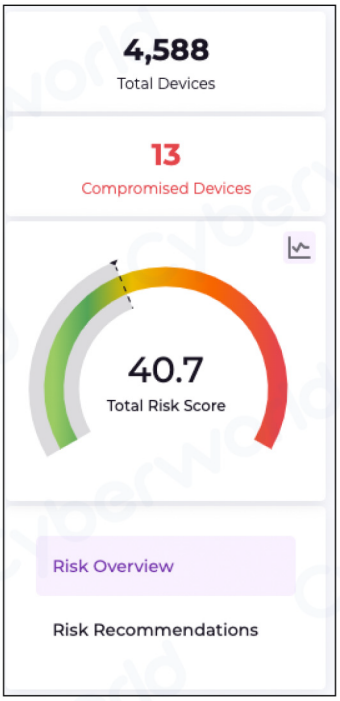
© 2022 Claroty Ltd. All rights reserved

漏洞与风险管理

xDome 自动关联每个 XIoT 资产、Claroty 屡获殊荣 Team82 研究团队的最新漏洞发现、 Claroty 庞大的通用漏洞披露(CVE)数据库和其他弱点。xDome 完全能够自定义企业的风险承受能力，可为全网络的降低风险措施提供量身定制的风险评分和建议。亮点包括：

- 简化漏洞识别，管理修复计划和执行。
- 安全地使用扫描漏洞程序和编排工具来识别工业环境中的 IT 风险。
- 根据真实和模拟的影响结果确定缓解风险的优先级。

这转化为对风险、漏洞的潜在影响以及最有可能被利用领域指标的整体、特定于企业的观点。因此，用户可以更有效地识别、优先排序处理和修复工业环境中的漏洞。



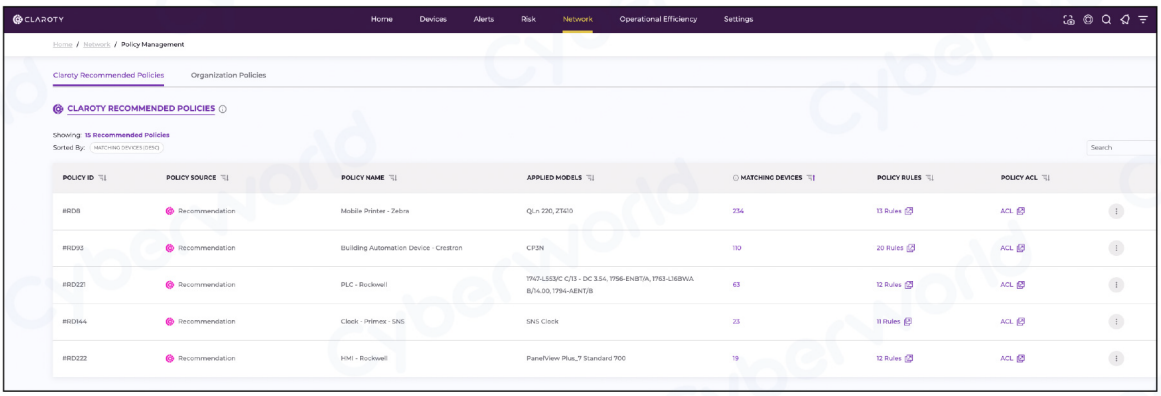
网络风险评分

网络保护

在 Claroty 深厚专业的领域知识支持下，xDome 利用它提供的XIoT资产及其行为模式的可见性来自动定义和推荐网络通信策略。此自动化解决方案使现有安全基础架构更轻松地监控、优化和实施这些策略，不会影响运营操作。这些策略也是动态的，可以在实施之前进行模拟，以展示网络影响，从而帮助企业跟上不断变化的复杂环境。

作为一种网络分段方法，Claroty xDome 的网络保护功能有助于为零信任实践奠定基础，这是改善企业工业网络安全态势的核心：

增强网络架构中资产可视化 | **提供正常网络通信基线视图** | **通过策略监控和实施降低风险**



Claroty xDome 推荐策略视图

© 2022 Claroty Ltd. All rights reserved

威胁检测

xDome 认识到针对工业环境威胁的频率和影响不断上升，因此采用了弹性检测模型来持续监控您的环境，以获取已知和新出现的威胁的最早指标。Claroty xDome 会自动分析所有 XIoT 资产及其通信模式，以便为正常网络行为生成基线，描述合法流量以清除误报异常，并实时向用户发出已知、未知和新出现的威胁警报。亮点包括：

- **统一警报系统：**Claroty xDome 通过无与伦比的设备深度可视化和修复工作流功能，提供自动化的方法来监控、优先排序处理和响应警报。
- **特定于域的威胁情报：**作为 一个 SaaS 驱动的解决方案，Claroty xDome 至少每周都会收到自动检测更新，因此企业始终是在最新的威胁情报上运行。
- **广泛的集成机会：**Claroty xDome 通过与安全信息与事件管理(SIEM)、端点检测与响应(EDR)和其他安全解决方案的集成，将现有的系统级芯片(SOC)功能扩展到运营环境中。

资产与变更管理

在发现、丰富和分析整个工业环境中的所有 XIoT 资产后，Claroty xDome 使企业能够简化资产和变更管理。通过强大的基于角色的访问控制，企业可以自动执行特定用户和组的资产管理工作流，从而节省管理时间并减少操作人员的维护窗口。xDome 为用户提供管理各种资产需求所需的工具：

- **监控资产更新：**xDome 持续监控漏洞、过时软件、产品寿命结束(EoL)指标和其他需要更新的变化，以帮助保持资产可用性。
- **简化服务级别协议(SLA)合规性：**xDome 通过可用性、位置数据和自定义属性，可以轻松识别和报告特定资产的服务级别协议(SLA)合规性状态。
- **识别资产更改：**网络中的新增功能、配置更改和异常是 xDome 为支持变更管理(MoC)程序而进行的众多变量监视器中的一部分。
- **支持审计请求：**高级报告功能以及与版本控制和备份工具的集成增强了通过 xDome 与利益相关者的沟通。

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平台可以与客户现有的基础设施集成，提供可视化、漏洞和风险管理、威胁检测、安全远程访问的全方位控制。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。

Cyberworld
广州科明大同科技有限公司
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

© 2022 Claroty Ltd. All rights reserved