

行业专题

数据中心 业务不间断

Claroty 赋能数据中心运营商,把全面的工业安全控制 扩展至其 网络化物理系统 (CPS, cyber-physical systems),包括 OT 和 楼宇管理系统 (BMS, building management systems),保障设施安全,并降低威胁。无论是占地极广、拥有数万台服务器的“超大规模数据中心园区”,还是靠近用户端、规模较小且位置分散的“边缘计算中心”,Claroty 都确保您的运营环境始终受到保护。

保护您的 OT 关键任务型基础设施

资产可视化与洞察

自动识别每一个 不间断电源 (UPS)、暖通空调系统 (HVAC) 控制器、分布式能源资源 (DER) 资产。在新收购或扩展的站点,从第一天起即可实现全面可视化,采用无 Agent 的 Dynamic Discovery (动态发现)方法,无需运输物理硬件,也不需要计划停机。

风险暴露管理

根据业务影响来划分风险优先级,并结合具体环境,减少互联设施(灰色空间)与 IT(白色空间)域的物理攻击面。针对无法立即进行补丁修复的供电或冷却单元,实施补偿性控制措施,增强系统安全性。

威胁检测

在制冷系统停摆之前检测事件。通过将 IT 安全事件与操作异常进行关联,实时捕获未经授权的逻辑变更和网络威胁,防止由网络攻击引发的物理损坏或代价高昂的非计划停机。

网络防护

把关键设施基础架构与 IT 及租户域进行隔离。实施虚拟分段,确保电力系统仅与其他电力系统通信,彻底消除多类风险,并防止威胁向控制系统进行横向移动。

安全访问

整合工程师和第三方维保供应商的远程访问。用灵活的无 Agent 网关替代高风险的传统 VPN,提供即时 (just-in-time) 授权、零信任控制、会话录制,以降低管理复杂性,确保 OT 网络的安全。



使用 Claroty 平台保护您的关键流程



xDome 平台

Claroty xDome 提供基于 SaaS 的模块化视图，覆盖整个数据中心资产。该解决方案可自动执行跨分散站点的资产发现与风险优先级排序，确保您的业务在高速增长的同时，保持安全性，并符合当地法规。



xDome Secure Access

Claroty xDome Secure Access 为本地工程师和全球 OEM 厂商提供可审计、无障碍的连接。它采用 专用网关 取代传统 VPN，防止未经授权的攻击向关键设施的电力与冷却控制系统进行横向移动。



持续威胁检测 (CTD)

Claroty CTD 为复杂的灰空间和白空间环境提供专门的监测。该解决方案可以辨识 BMS 的专有协议。在影响 SLA 保障的正常运行时间之前，识别出网络威胁或逻辑变更。

深受全球数据中心 领军企业的信赖



与三大自动化厂商合作

罗克韦尔自动化 (Rockwell Automation)、施耐德电气 (Schneider Electric)、西门子 (Siemens) 均是 Claroty 的投资者和客户。Claroty 的解决方案可兼容并支持数据中心核心系统。



获 35+ 项行业大奖

在安全性与运营弹性领域的卓越表现获得全球认可。Claroty 平台是保护关键 CPS 的黄金标准。



披露 700+ 个漏洞

Claroty 的 Team82 研究团队在识别 OT 风险方面处于世界领先地位。Claroty 率先发现漏洞，确保您的数据中心环境始终受到保护。

简化合规管理



支持全球合规框架

Claroty 助力您的运营符合国际标准，包括：ISO/IEC 27001、ISA/IEC 62443 及 NIS CSF。Claroty 可以自动完成 满足 网络化物理安全 全球基准 所需的 映射与报告，帮助您获得更有利的网络保险费率等级。



监管对齐

Claroty 平台可满足全球关键基础设施的特定监管要求，包括：

- **区域框架**：欧盟 NIS2、澳大利亚 SoCI、美国/英国 CISA/CNI、英国 NCSC / CAF、新加坡 CSA
- **特定行业义务**：GDPR、HIPAA、PCI DSS
- **安全框架**：ISA/IEC 62443、NIST CSF、ISO/IEC 27001



达到国际市场准入要求

向高要求的全球租户和监管机构展示严格、可审计的网络化物理弹性。保持全面的网络策略执行和第三方访问的可审计记录，确保您的设施符合最严格的国际准入“门槛”与合规标准。

Cyberworld
科明大同

中国区
总代理

公司网站 www.cyberworld.com.cn
业务联系 info@cyberworldchina.com
售后支持 support@cyberworldchina.com



关注公众号