白皮书

如何提升数据中心环境的网络弹性

目录

引言

AI技术的飞速发展以及当今社会日益增长的计算需求,正在推动对数据中心的需求。随着越来越多企业进行数字化转型,并且优先考虑可靠性、运营连续性和可持续发展。他们在保护支撑这些目标的网络化物理系统(Cyber Physical Systems, CPS)方面,面临着日益复杂的挑战。

保持正常运行时间对数据中心非常重要。不仅因为它们支持企业和消费者的基本服务,还因为它们需要满足高级认证框架,例如,Uptime Institute 制定的、全球公认的数据中心可用性和性能标准。达到 Tier III 和 Tier IV 等级,意味着单个设备故障对运营的影响降至最低。为了始终保持正常运行时间、抵御网络威胁,数据中心必须实施强大的 CPS 网络安全策略,有效降低风险并防止中断。

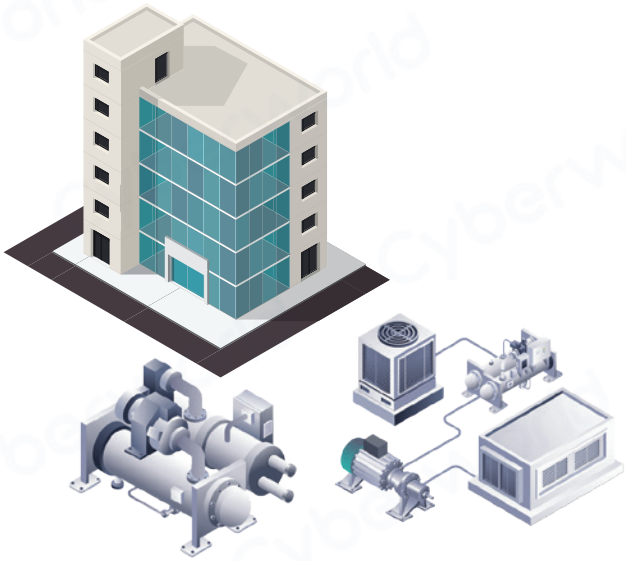
CPS对任何数据中心的网络安全计划都至关重要,因为它们把物理过程(例如,冷却、配电、访问控制)与数字网络和控制系统连接起来。与侧重于保护数据和数字服务的传统 IT 网络安全计划不同,数据中心内CPS的普及扩大了攻击面,需要密切关注物理过程的运行完整性和安全性。有效的CPS网络安全需要一种整体的方法,结合传统IT安全措施与专门的技术,以保护物理资产,确保安全性、运营连续性和业务弹性。

数据中心面临的 CPS 网络安全挑战

在数据中心环境中，大多数 CPS 可以分为两类，每类由不同的系统监管：数据中心基础设施管理（Data Center Infrastructure Management, DCIM）、楼宇管理系统（Building Management Systems, BMS）。

DCIM 和 BMS 的成效

DCIM	BMS
• 包含一套全面的流程和工具，旨在监控、跟踪和管理IT资产（例如，服务器和软件）以及数据中心的物理基础设施组件，例如，冷却系统、配电单元和机房空间。 • 可优化资源使用、降低运营成本。通过收集和分析关键指标（尤其是与电力消耗和数据中心环境相关的指标）来提高效率。	• 侧重于控制更广泛的建筑环境，维护设施元素，例如，安全系统、配电、照明、暖通空调（HVAC）系统。 • 通过自动化机械任务（微调温度设置、管理火灾探测系统）来保持人员舒适度并确保运营完整性。



虽然 DCIM 和 BMS 解决方案为关键过程提供了有价值的洞察，但不是专为CPS网络安全控制所需的CPS可视化而设计。这些系统通常依赖手动资产录入，可能导致资产清单不完整。即使供应商提供自动发现功能，这些功能通常仅限于识别自家设备，可能无法检测到其他制造商的设备。这一限制可能会导致未发现的资产，在数据中心的 CPS 环境中形成盲点，使漏洞未能得到解决。

DCIM 和 BMS 解决方案并非以安全为导向，缺乏评估资产风险暴露的能力。它们无法检查某个资产的版本信息，而版本信息对于识别相关漏洞和其他风险暴露相当重要。此外，这些系统无法提供资产在更广泛CPS环境中的关联性信息，而这一因素对于安全团队有效评估风险、确定修复优先级至关重要。

深入了解数据中心的 CPS

数据中心是一个复杂的运行环境，物理设备和数字系统高度融合并实时互联，其攻击面较广，传统的IT网络安全措施无法完全应对。为了有效地保护数据中心的CPS，第一步是获取完整的CPS资产清单。最佳的方法是：把CPS保护平台与现有的 DCIM 和 BMS 解决方案集成。

专门为CPS设计的平台，可以识别数据中心环境中的以下关键系统。下表详细说明了其功能、这些设备最常见的制造商、以及它们用于实现业务逻辑的通信协议：

系统	详情	制造商	常用协议
电力系统	为高可用性环境设计的不间断电源（UPS）、发电机、开关设备、配电系统。	Schneider Electric、Eaton、Vertiv、ABB、Fuji Electric、Mitsubishi Electric	SNMP、Modbus、专有协议、MMS、ICCP
冷却系统	采用液体冷却和气流管理等技术，维持高密度计算环境的最佳温度。	Trane、Vertiv、Stulz、Daikin、Munters、Airedale	Modbus、BACnet、LonWorks
安全系统	火灾探测和灭火机制、环境监测和泄漏检测、紧急断电（EPO）系统等。	Bosch、Siemens、Kidde、Halma、Honeywell、Nohmi Bosai	Modbus、专有协议、LonWorks
物理安全	用于保护物理资产和基础设施的监控、访问控制、入侵检测传感器。	Axis Communications、Hikvision、Genetec、Honeywell、Bosch	RTSP、HTTP、专有协议、SIP
楼宇自动化与管理系统	通常在设施层面管理暖通空调（HVAC）、照明、能源系统，以确保运营效率。	Siemens、Johnson Controls、Delta Controls、Honeywell、Tridium、Schneider Electric	BACnet、Modbus、KNX
数据中心基础设施管理系统	提供对电力、冷却、安全和 IT 基础设施在楼层、机架级别的集中控制和监控。支持运营效率、资产管理和容量规划。	Schneider Electric、Vertiv、Nlyte、Sunbird Software	BACnet、SNMP、Modbus、IPMI

表 1：包括了关键系统、制造商、协议，
还有暖通空调（HVAC）、照明、可再生能源、环境监测等系统。先进的分析工具或平台通常用于优化和预测性维护。

Claroty 为数据中心推荐的 CPS 网络安全之旅

本节概述 Claroty 推荐的数据中心 CPS 网络安全之旅，具体步骤如下：

1. **厘清资产**。利用全面、安全、高效、可扩展的资产发现方法，实现资产可视化，获取完整的资产清单。

2. 通过**风险管理**减少攻击面。这是一种主动的、以端点为中心的解决方案，专注于修复网络安全暴露问题。

3. 一旦数据中心完成了CPS网络安全之旅的早期里程碑，**网络保护**可作为进一步保护数据中心环境的选项。

CPS 网络安全之旅的早期阶段：厘清资产和风险管理

利用动态发现（Dynamic Discovery）技术创建 CPS 资产清单

围绕数据中心网络构建的全面CPS网络安全计划，第一步是厘清资产。被动流量检测和收集，已成为CPS环境中的架构标准。因为它可以在不干扰运营的情况下分析机器间通信。然而，该技术需要复杂的硬件部署、计划停机时间，还可能缺乏对特定资产详细信息的可视化，例如，补丁级洞察（Patch-level insights）。

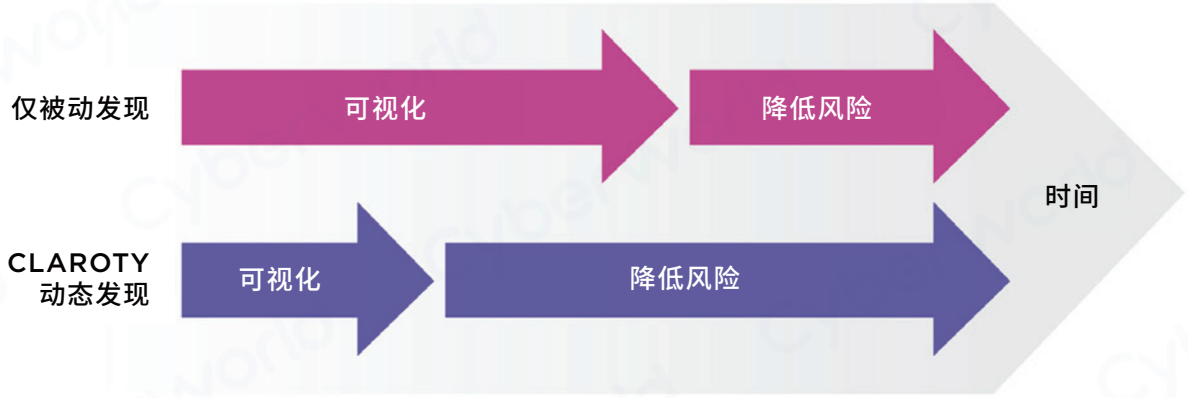
基于上述原因，仅采用被动发现方法，会延长数据中心的价值实现时间（TTV），增加总体拥有成本（TCO）。虽然被动通信是实现完整CPS可视化的重要环节，但Claroty的非被动发现方法已发展成熟，无需硬件即可提供深度可视化和资产发现。

Claroty 的**动态发现（Dynamic Discovery）**提供了一种主动的资产识别和分析方法，无需依赖被动的网络流量监察。Claroty的多种动态发现方法为数据中心提供了灵活性，可根据其CPS可视化需求，轻松组合资产发现技术：

被动监察 (Passive Monitorning)	安全查询 (Safe Queries)	Claroty Edge	项目文件分析 (Project File Analysis)	集成 (Integrations)
持续监察网络流量以识别资产特征	使用资产的原生协议，进行针对性资产发现	通过本地化查询，进行快速的、基于主机的资产分析	定期摄取离线配置文件，以丰富资产信息	无需更改硬件或配置，即可提升可视化

在数据中心环境中，垂直化的动态发现策略，可以通过BMS、DCIM网络协议（例如，BACnet、Modbus和LonWorks）安全地查询 CPS 资产，并将这些结果集成到 BMS 和 DCIM 平台中，例如，Schneider Electric 的 EcoStruxure IT、Siemens 的 Desigo CC 、Johnson Controls 的 Metasys。通过动态发现技术，提供准确、细致、全面的资产清单，为数据中心的风险管理奠定了坚实基础。

采用专门的方法来实现CPS可视化，可以让数据中心运营商实现更低的TCO和更快的TTV，还可以降低整体风险。



通过风险管理减少攻击面

为了跟上数字化转型的步伐，数据中心必须越过传统的CPS漏洞管理，打造一个更广泛、更动态的计划来管理其整体风险暴露。传统的漏洞和风险管理策略，在数据中心CPS环境中存在不足。因为传统的漏洞管理工作流程很少考量容易出现风险的暴露，例如，错误配置、使用不安全协议、使用默认密码。

风险管理框架

Claroty建议企业转向持续威胁暴露管理（Continuous Threat Exposure Management, CTEM）计划，该计划需要实施更成熟、由策略驱动的预防性控制措施，并具备检测和响应能力。Gartner® 将 CTEM 定义为："持续威胁暴露管理（CTEM）计划是一套流程和功能，让企业能够持续、一致地评估其数字和物理资产的可访问性、暴露程度、漏洞的可利用性。"[1]

Gartner®指出："在任何成熟阶段，CTEM周期都必须包含五个阶段——界定范围、发现、优先级排序、验证、动员。构建CTEM计划的企业需要使用工具来厘清、分类资产及漏洞，模拟或测试攻击场景以及其他形式的态势评估流程和技术。重要的是，CTEM计划必须为基础设施团队、系统和项目负责人提供一个有效且可操作的路径，以对发现的问题采取行动。"[1]

由于 CPS 环境的独特性，需要一种专门的方法，让数据中心能够构建一个暴露管理计划，该计划需考虑到资产的复杂性、针对性的治理方法、数据中心环境的运营成果。Claroty提供了一系列量身定制的功能，支持 CPS 暴露管理流程：

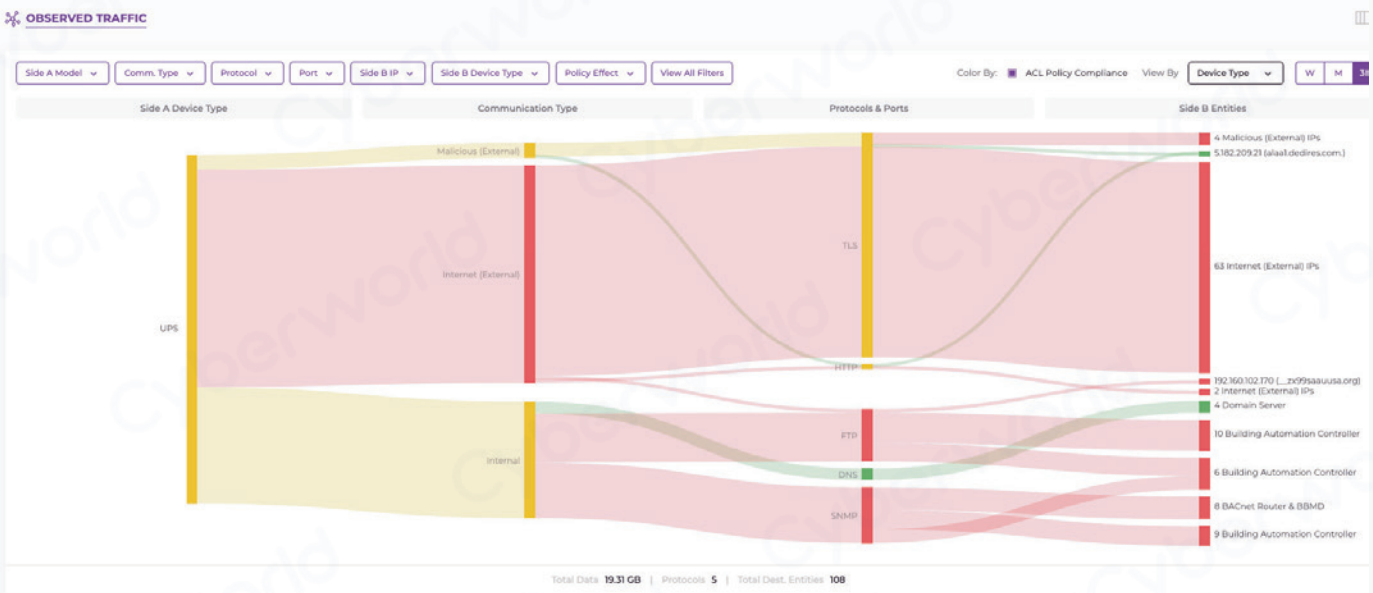
持续暴露管理流程阶段	Claroty的产品功能与CTEM周期的每个阶段对应如下：
界定范围（Scoping）	Claroty解决方案专为CPS设计，帮助识别和优先考虑业务关键运营。Claroty界定并映射所有相关的CPS资产，包括运营技术（OT）、物联网（IoT）和楼宇自动化系统（BAS），以设定安全目标和风险容忍度。
发现（Discovery）	CPS需要专业知识来有效识别和评估风险。Claroty的动态发现技术可以分析CPS资产、映射网络通信，并关联漏洞和其他风险。
优先级排序（Prioritization）	Claroty的风险框架、来自 CISA 的 KEV（已知被利用漏洞目录）和EPSS（漏洞利用预测评分系统）的数据馈送、多重风险暴露考量，能够突出特定的攻击向量，评估漏洞的可利用性和影响，并提供量化的修复建议。在数据中心环境中，电力、冷却、物理安全最为敏感。因此，Claroty根据业务关键性，对风险暴露进行优先级排序。
验证（Validation）	确认漏洞的可利用性需要深入了解相关CPS和环境。Claroty会模拟攻击场景，并利用广泛的威胁情报来验证潜在的漏洞利用。
动员（Mobilization）	Claroty提供可操作的修复执行指导，推荐有针对性的措施来缓解高优先级风险，并提高系统弹性。Claroty与多种企业解决方案集成，提供详细的报告，帮助实现顺畅的风险暴露修复工作流程。

CPS 网络安全之旅的进阶阶段：网络保护

CPS网络安全计划日趋成熟，在资产识别和风险暴露管理方面奠定了坚实的基础。许多企业开始实施网络保护控制措施。被动监察（Passive Monitoring）是实现这种控制水平的先决条件。它可以实时监察网络流量，确保通信策略根据实际网络行为进行定制。

网络保护计划的一个重要组成部分是制定网络分段策略，这涉及到围绕特定资产区域定义通信策略。通过这种方式对网络进行分段，您可以创建更精确的边界和控制措施，从而提升保护关键业务资产的能力，减少攻击面。这种方法确保允许正确的通信流，阻止不必要的或恶意的流量。

有效分段数据中心网络，可能是一个繁琐且容易出错的过程，需要定义并不断调整适合您独特环境的策略。因此，应该与专业的CPS保护供应商合作，该供应商需要提供推荐的分段策略，还要模拟网络策略，展示其对环境的潜在影响。



依托Claroty深厚的专业知识，Claroty xDome 利用其资产可视化，自动定义并推荐通信策略所需的网络区域。动态策略可在实施前进行模拟，展示其对网络的影响，帮助数据中心适应其复杂环境中不断变化的条件。

总结

保护数据中心免受网络威胁，需要采取全面的CPS网络安全方法。Claroty致力于应对数据中心CPS带来的挑战，从基础步骤开始，创建详细完整的CPS资产清单和实施风险管理。Claroty作为一个全面的CPS保护平台，支持更专业化的应用需求，例如网络保护，并随着数据中心在其CPS网络安全之旅中的进展，而不断优化。通过遵循结构化、分阶段的方法，数据中心可以有效管理风险、提升可视化，保持安全性和可靠性，以支持其关键任务运营。

参考来源：

[1] Gartner 于 2023 年 10 月 11 日发布的《Implement a Continuous Threat Exposure Management (CTEM) Program》，作者：Jeremy D'Hoinne、Pete Shoard、Mitchell Schneider。
GARTNER 是 Gartner, Inc. 及其在美国和国际上的关联公司的注册商标与服务标志，在此经许可使用，保留所有权利。

关于 Claroty

Claroty 凭借无与伦比的、以工业为主的平台重新定义了网络化物理系统 (Cyber Physical Systems, CPS) 防护，该平台旨在保护关键任务型基础设施。Claroty平台提供市场上最深入的资产可视化和最广泛的CPS安全解决方案，包括风险管理、网络保护、安全访问和威胁检测，可以搭配 Claroty xDome 在云端使用，也可以搭配 Claroty CTD 在本地部署使用。Claroty平台以屡获殊荣的威胁研究和技术联盟为后盾，让企业能够有效地降低CPS风险，以最快的时间实现价值并降低总体拥有成本。在全球范围内，已有数百家企业在数千个站点部署了Claroty。