解决方案概述

遵守 NERC CIP

Claroty 如何支持北美电力可靠性公司关键基础设施保护（NERC CIP）标准

随着当今的电力公司不断对其运营和基础设施进行现代化改造，以提高效率、可靠性和需求响应，其信息技术 (IT) 和运营技术 (OT) 网络比以往任何时候都更加互联。智能电网技术、工业物联网传感器和其他现代互联网连接设备，现在与以前隔离的传统 OT 设备复杂地交织在一起。与此同时，工厂工作人员和第三方都转向远程访问，而非现场，对无人值守的发电机组和其他地理位置偏远的设施进行日常维护、维修与审计。尽管这些技术带来了效率提升、更高的安全性和更强的可持续性，以及许多其他好处，但它们也增加了安全团队难以缓解的复杂网络风险。

降低这些风险并进一步加强大容量电力系统 (BES, Bulk Electric System) 的弹性、安全性和完整性，是 NERC CIP 制定标准的基础。Claroty 的 OT 安全产品组合旨在支持责任实体 (RE, Responsible Entities) 实现和保持 NERC CIP 合规性。更具体地说，Claroty 为 RE 提供支持，以证明其在 BES 中的网络资产的安全性，从而确保发电和输电的安全性和可靠性。

Claroty 安全解决方案

Claroty 的产品组合不同于 IT 解决方案以及为 OT 重新设计的解决方案，其专为 OT 独特的安全和运营需求、支撑 BES 的更广泛的网络化物理系统 (CPS)、流程和网络而设计。Claroty 提供本地、基于云的和混合 OT 安全解决方案，以满足这些环境所需的广泛安全需求：

漏洞与风险管理	网络保护	威胁检测	资产管理	变更管理	远程访问
资产可视化					
灵活部署		特定角色的用户体验		集成生态系统	
持续威胁检测 (CTD)：本地部署		xDome：基于 SaaS 的平台		安全远程访问 (SRA)：可靠的内部和第三方安全远程访问	

NERC CIP 标准

上述 Claroty 的安全解决方案组合可支持 NERC CIP 合规性。
下表列出了最新的 NERC CIP 标准，特定的 Claroty 产品可以满足这些要求。

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-002-5.1a **BES 网络系统分类**	Claroty CTD 和 Claroty xDome 可以自动识别所有资产，并识别有关这些资产的配置参数（例如，型号、固件版本、配置等）。RE可以使用这些信息对 BES 网络系统进行高、中、低影响的分类标记。	CTD xDome
CIP-003-8* **安全管理控制**	CTD 和 xDome 可以协助安全计划对资产进行分类，并支持风险降低功能的管理。 SRA可支持远程访问功能，以降低风险并缓解访问问题，包括但不限于支持 OT 环境的第三方承包商的管理。	CTD xDome
CIP-005 **电子安全边界（ESP）**	Claroty的解决方案通过识别和映射控制网络（现场总线/串行和 IP 网络）上通信的所有资产，协助设计和验证这些网络。这些信息用于构建网络图，识别所有外部可路由的通信路径和接入点。 监察对 ESP 的入站和出站访问，以检测恶意活动。Claroty 独特的签名组合、专门构建的 OT 行为模型和专有的异常检测功能，可帮助 RE 实现这一目标。CTD 和 xDome 能立即检测并提供有关恶意活动的可操作信息。最重要的是，CTD 和 xDome 可以识别传统安全工具无法理解的OT协议中潜在的恶意通信，从而填补合规性方面的潜在差距。	CTD xDome

*请您注意，该标准已被 CIP-003-9 取代，计划 2026 年 4 月发布。

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-005 **R2** **第 2.4 和 2.5 部分** **安全远程访问**	(1) Claroty 安全远程访问 (SRA) 可防止发起连接的设备直接访问受保护的资产。远程访问通过 SRA 进行安全代理，确保只有始发设备上的授权用户才能访问。 (2) SRA 提供从始发设备到远程访问服务器之间的加密。通过 HTTPS 可以访问 SRA，HTTPS 是一个用于安全 Web 访问的行业标准协议。 (3) SRA 支持双因素身份验证，可以将用户帐户配置为：除了必需的用户密码，还需要一次性密码 (OTP, one-time password)。SRA 支持 Google Authenticator 和类似的 OTP 系统。 (4) SRA 可主动监察所有会话，并能够随时断开任何会话。 (5) CTD 和 xDome 支持身份提供商 (IdP) 的 SAML，用于多因素身份验证 (MFA)或 IdP 集成。	CTD xDome SRA
CIP-005 **R2** **第 2.4 和 2.5 部分** **供应链访问**	SRA可主动监察所有供应商远程访问会话，并能够随时断开任何会话。	SRA
CIP-005-7 **电子安全边界**	CTD 和 xDome 能自动识别进出 BES 的所有周边通信，可以自动识别关键通信和设备。CTD 和 xDome 能根据分类引擎自动识别关键通信流和设备。基于对“正常”流量的了解，CTD 和 xDome 可以阻止恶意的入站或出站通信，以协助阻止尝试利用漏洞的攻击。 SRA 可以控制所有进出 BES 系统的访问，创建相应的审计日志，记录谁访问了哪个系统，并强制执行审批要求。SRA可以在必要时确定并禁用供应商远程访问会话。	CTD xDome SRA

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-006-6 **BES网络系统的物理安全**	为了支持 1.10，CTD 和 xDome 能自动监察环境中的所有通信链路，可以监察通信链路的状态，发现通信故障或网络攻击，并发出相应的警报。这两款产品都提供了一种直接的方法来证明监察和警报的存在。	CTD xDome
CIP-007-6 **系统安全管理** **R1** **禁用不必要的逻辑网络可访问端口**	一般而言，对于此要求，Claroty 的 CTD 和 xDome 都可监察 BES系统的变更，提供审计跟踪。这两款产品还能检测和监察恶意代码。此外，与 R4 和 R5 相关，SRA 可以强制执行身份验证，控制对 OT 系统的远程访问。 CTD 和 xDome 监察网络通信，识别设备正在通信的端口。这些洞察可用于识别此要求所需的端口，或作为附加控制来识别配置错误的设备或潜在的安全事件。 在NERC CIP监管的网络中，对于Claroty产品，在默认情况下，xDome 要求端口 443 (HTTPS) 保持打开状态并可通过网络访问，而 CTD 需要端口 22 (SSH) 和端口 443 (HTTPS)。	CTD xDome SRA

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-007-6 **R2** **补丁管理**	CTD 和 xDome 都可以通过识别其监察的网络上设备的特定硬件和固件版本来提供帮助。这提供了一个可用于建立和跟踪补丁源的清单。此清单还可用于评估特定补丁的适用性，以确定哪些特定设备可能需要安装补丁。此外，这些产品可以自动生成企业设置的补丁策略与主机上实际安装的补丁列表之间的比较，从而识别和报告每个主机上缺少的补丁列表。这可以作为额外的控制措施，确保补丁已安装。 在 NERC CIP 监管的网络中，对于 Claroty 产品，其本身也符合范围，Claroty可通过为其软件和底层操作系统平台提供所有必要的补丁（包括安全补丁）来简化补丁管理合规性。这些补丁涵盖系统功能和操作系统安全性。底层操作系统的补丁在发布给客户之前由 Claroty 内部进行测试。	CTD xDome
CIP-007-6 **R3** **恶意代码防护**	CTD 和 xDome 安全结构可以监察受保护网络内的所有网络流量。凭借专为ICS网络和协议构建的高级深度数据包检测(DPI, deep packet inspection)功能以及高级机器学习算法，这些产品可自动将合法基线活动列入白名单，并在发生任何更改或异常时发出警报。这些功能提供了强大的能力来检测网络上发生的恶意软件活动。 当Claroty产品符合范围时，按照标准允许的情况，可通过产品安全强化来解决恶意代码风险。Claroty已经记录了完整的强化程序，作为系统部署过程的一部分。Claroty加固程序指南可根据要求提供。此外，Claroty会对所有软件更新和新软件版本进行加密和签名，再发送给客户。	CTD xDome

*自 2022 年 10 月起，CIP-010-4 取代 CIP-010-3。

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-007-6 **R4** **安全事件监察**	许多 ICS 设备的日志记录功能有限，可通过 CTD 和 xDome 中的功能解决此问题，即通过检查ICS网络流量识别相关安全事件。如果网络资产无法记录事件类型，Claroty 产品可以通过 DPI 识别事件。这包括网络资产通信连接、用户登录或注销、基线网络配置、固件更改、使用的命令和寄存器类型以及响应值。Claroty 产品能识别受监察资产中的事件，可根据需要通过管理报告进行审查。这两款产品还可以配置为捕获和存储网络流量，以支持安全事件事后的调查。CTD 和 xDome 均可针对已知与未知威胁、可疑活动、事件记录失败以及构成风险的更改提供可操作的实时警报，企业可以保护其资源免受ICS网络威胁。 对于不成功的登录尝试，Claroty 产品可以使用 DPI 在整个 ICS 网络中被动检测不成功的登录尝试。通过使用WMI、SNMP和日志收集，产品可以检测资产本地发生的不成功登录尝试。当连续无效访问尝试次数超过规定值时，它们会发出警报。对于许多设备来说，这是一种有效的附加控制，并且可能是某些 OT 设备唯一可用的控制。 当Claroty产品符合范围时，它们提供强大的日志记录功能并与现代安全信息和事件管理 (SIEM) 系统兼容。Claroty 提供广泛而强大的日志记录功能，包括对无处不在的syslog协议的支持，可轻松与企业 SIEM 部署集成。Claroty 的主要功能是生成大量安全相关的日志事件和警报，这些事件和警报超出了CIP标准的要求，并完全支持检测网络安全事件的根本目标。Claroty 的日志消息格式有详尽的记录。 Claroty产品还具有强大的警报功能，可以针对受监察网络上检测到的各种安全相关事件生成警报。这些警报可以直接通过电子邮件发送，也可以转发到 SIEM 进行集中警报和响应。	CTD xDome

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-007-6 **R4** **安全事件监察** （续）	当监察接口出现故障时，Claroty 可以发出警报，支持 CIP-007 R4.2.2 下日志丢失警报的要求。 Claroty能够保留所需的90天间隔的日志。此外，所有日志都可以发送到 SIEM，可以集中维护日志保留，以轻松实现合规性。 日志审查要求可以通过两种方式满足。通过 Claroty 的 SIEM 集成，实体的分析师团队可以在单一平台上执行日志审查。此外，Claroty 产品本身可以生成报告，重点介绍与运营环境相关的特定事件。这使工作人员能够轻松审查安全事件，为这项关键任务提供相应的专业知识。	CTD xDome
CIP-007-6 **R5** **密码猜测攻击**	如 R4 所述，对于不成功的登录尝试，CTD 和 xDome 均可使用 DPI 在整个ICS网络中被动检测不成功的登录尝试。通过使用WMI、SNMP和日志收集，产品可以检测资产本地发生的不成功的登录尝试，包括密码猜测。当连续无效访问尝试次数超过规定值时，它们会发出警报。对于许多设备来说，这是一种有效的附加控制，并且可能是某些ICS设备唯一可用的控制。 对于用户身份验证，Claroty产品包含一个内置功能，通过SAML 2.0集成，根据内部用户数据库或外部 IdP 对用户进行身份验证。 当Claroty产品符合范围时，它们满足此标准的要求，其中包含几个帐户管理和密码相关项目： **用户身份验证：** Claroty产品包含一个内置功能，通过SAML 2.0集成，根据内部用户数据库或外部 IdP 对用户进行身份验证。 **默认帐户：** Claroty 产品强制用户在首次登录时更改默认密码。 **密码控制：** Claroty 产品支持强密码控制，满足或超出标准要求。 **帐户锁定：** Claroty 产品支持控制措施，以阻止密码猜测攻击。登录尝试失败次数达到可配置的次数后，系统将自动禁用用户帐户。	CTD xDome

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-008-06 事件报告和响应计划	CTD 和 xDome 均通过其监察、分析和报告网络通信与系统活动的多种功能，协助识别潜在的网络安全事件，包括针对可疑、未经授权或已知恶意活动生成警报。 CTD 和 xDome 通过快速简易地报告其监察系统中的通信和采取的行动来支持事件响应，为调查人员提供见解。用户能从这两款产品中导出信息，用于调查。这两种工具的输出可以与其他工具（如SIEM）集成，以支持调查。这两款产品还可以通过与防火墙或网络准入控制 (NAC) 技术集成来支持主动响应。 因此，此功能可让实体快速有效地识别事件、响应或采取行动，在需要时传递重要见解。	CTD xDome
CIP-009-06 BES网络系统的恢复计划	CTD 和 xDome 都可以识别需要进行恢复过程的事件的根本原因，并会自动保存该数据以供日后调查。这将生成网络事件的记录和警报，以确保适当的审计能力。	CTD xDome
CIP-010-4* 配置变更管理和漏洞评估	在整体上遵循这一标准时，Claroty CTD 和 xDome 都可以识别、建立和记录预期流量的基线，并针对此基线活动的变化生成警报。这两款产品可以通过主动检测和被动监察来实现这一点。 当 Claroty 产品符合范围时，产品的软件安装将利用 Linux 更新系统。Claroty 提供所有必需的软件包，并在强化的、最小化的基于 Linux 的平台上运行，使变更管理更加简单。	CTD xDome

*自 2022 年 10 月起，CIP-010-4 取代 CIP-010-3。

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-010-4* **R1** **记录基线配置**	CTD 和 xDome 均可使用被动监察和主动检测来识别和记录设备的基线配置。这两款产品记录了ICS网络上资产的配置基线。每个资产的历史数据都存储在一起，使企业能够审查和报告偏离授权基线的变更。可以对资产执行报告，以验证已接受的变更。这些报告可以发送给指定的审批机构，然后将文档放入企业的变更控制数据库中。这些功能支持在 NERC CIP 审计期间回答审计员的证据请求。 如上所述，Claroty 在发送给客户之前，对其所有软件更新和新软件版本进行加密和签名，提供支持 R1 第 1.6 部分的强大安全性。	CTD xDome
CIP-010-4* **R2** **配置监察和未经授权的更改调查**	当 CTD 和 xDome 检测到资产偏离其记录的、已批准的基准时，都会发出警报。如果未经授权的组件连接到 ICS 网络或 ICS 网络上发生未经授权的通信，这两款产品都会为指定的权限创建警报。	CTD xDome
CIP-010-4* **R3** **漏洞评估**	通过被动和主动监察和检测技术，CTD 和 xDome 能获取网络配置、网络上的设备以及设备之间通信的详细信息。这为开展漏洞评估提供了丰富的信息。 这两款产品通过对网络流量的分析，生成大量见解。这些见解按优先级排序，并通过一系列标准报告提供。这些见解可识别系统设计或防御中的潜在漏洞或薄弱环节，例如未修补的漏洞、不安全的协议和外部通信。	CTD xDome

*自 2022 年 10 月起，CIP-010-4 取代 CIP-010-3。

NERC CIP 标准	Claroty 支持	Claroty 产品
CIP-010-4* **R3** **漏洞评估** （续）	这两款产品还可以生成一份汇总的风险评估报告，快速简易地概述系统安全性。CTD 和 xDome 深入洞察 ICS 环境，使用户能够主动识别并修复配置和其他可能导致网络易受攻击的网络卫生问题。利用专有情报，这两款产品持续监察网络中是否存在新的已知漏洞，为工业设备的固件版本提供精确的 CVE 匹配。 使用精确的资产清单和经过清理的CVE数据库，这些是唯一能够提供实际确凿漏洞的解决方案。其他解决方案要么无法收集完整的资产清单（例如，型号和固件），要么无法彻底清理其CVE数据库，这会增加警报疲劳，导致宝贵的资源浪费在追逐错误警报上。	CTD xDome
CIP-010-4* **R4** **瞬态网络资产和可移动媒体**	Claroty产品可以通过各种不同的方法识别连接到网络的瞬态资产，并对这些资产发出警报，以识别异常或恶意流量。	CTD xDome
CIP-012-1** **控制中心之间的通信**	CTD 和 xDome 可以监察控制中心之间的流量，并专门查找该流量中的恶意或异常活动。	CTD xDome
CIP-013-2 **供应链风险管理**	CTD 和 xDome 能自动识别漏洞，并显示哪些资产受到哪些漏洞的影响。此外，这两款产品提供了方便的功能，让用户可以实时查看哪些资产存在供应商披露的信息。	CTD xDome

**本标准修改中。请参阅 NERC 标准了解更多信息。

结论：简化 NERC CIP 合规性并保护所有电力服务

在 Claroty，我们了解 RE 在保护其关键网络资产方面负有重大责任。我们还了解，从合作社到市政当局等所有发电、输电和配电实体都必须确保其操作系统、设备和流程的整体安全。Claroty提供安全解决方案能够满足这些运营网络和流程所需的广泛安全需求。

Claroty 的不同之处

Claroty为不同规模的公共或私营电力公司提供以下服务：

- **灵活部署** OT 安全解决方案：本地、云端或混合
- **在整个 OT 安全过程中提供支持：**从资产可视化、资产管理、漏洞和风险洞察，到所有访问方的远程访问安全
- **深度协议支持**，提供您需要的 450 多种相关协议
- 在 OT、楼宇管理、IoMT 和其他 IoT 环境中，无论这些环境如何演变，都提供相同的解决方案和**保持一致**的定价
- 与您使用的供应商进行**广泛且相关的集成**，扩展您的防御、安全运营中心 (SOC) 和响应以及IT网络的价值

Claroty 认识到，保护支撑发电、输电和配电的 OT 环境是一项复杂的工作。Claroty 根据以下三个原则，定制了网络安全产品组合，以简化这一过程：

1. 了解 OT 环境中的所有 CPS

可视化是确保 OT 安全的基础。Claroty 可帮助公用事业公司获取所有电网、变电站、输电线路等的所有 OT、IoT 和其他 CPS 的完整清单。

2. 将 IT 工具与 OT 集成

这些环境中的许多设备和系统都使用专有协议和陈旧系统，与 IT 解决方案不兼容。但这并不意味着这些解决方案在 OT 中没有立足之地。Claroty 无需客户扩展其已经广泛的技术堆栈，而是与他们集成。客户可以轻松地将其 IT 工具和工作流程扩展到 OT 。

3. 将 IT 控制扩展到 OT

对于那些缺乏一些基本安全控制和一致治理的企业，在提供可视化、与 IT 工具和工作流程集成之后，Claroty 可帮助将现有的 IT 控制扩展到 OT，这能统一安全治理并提高 IT 和 OT 的弹性，包括以下用例和治理控制：

关于 Claroty

Claroty使工业、医疗保健、商业机构、大型企业和公建部门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。