白皮书

Claroty与NIST网络安全框架(NIST CSF)

使用NIST CSF保护网络化物理系统(CPS)

目录

什么是 NIST CSF ?

美国国家标准与技术研究院网络安全框架（National Institute of Standards and Technology Cybersecurity Framework, NIST CSF）是一套全面的指南，旨在帮助关键基础设施所有者和运营商更有效地管理、降低网络安全风险。本白皮书介绍了NIST CSF 2.0、Claroty如何支持企业网络安全计划与 NIST 标准对齐。

网络化物理系统（CPS）的监管环境

数字化转型极大地改变了制造业和关键基础设施企业的运营方式。互联技术的快速应用推动了连接性的提升，从而提高效率并降低成本。这一变化体现在一项预测数据中："到2029年，全球物联网（IoT）连接数将接近400亿，是当前数量的两倍以上。"然而，互联技术的发展扩大了这些关键环境的攻击面，带来了新的风险和漏洞，可能会被恶意行为者利用。

恶意网络活动的激增促使各国政府和国际组织采取行动，制定并完善监管框架，包含保护关键基础设施中网络化物理系统（Cyber Physical Systems, CPS）的明确规定。这些框架包括广为人知的 IEC-62443 标准，以及一些法规，例如，美国运输安全管理局（TSA）针对交通运输的指令、欧盟 NIS2 指令。随着这些标准的采用率不断提升，它们将促使关键基础设施企业优化其网络安全计划，以保持合规性，提高其弹性，并避免运营中断或影响人员安全。

许多关键基础设施企业已在 IT 流程和控制措施中实施了 NIST 等监管标准。但在 CPS 设备的管理中，可能需要独特的方法。本白皮书概述了 NIST 框架、Claroty 的产品组合如何支持这一监管标准。

NIST CSF 的功能

本节可让您熟悉 NIST 框架的功能。NIST 框架分为 6 个核心功能，每个功能都包含保护和保障 CPS 安全的、有价值的流程及程序。此外，每个功能（或类别）还包括子类别，可帮助企业实施适当的流程和程序。
这些核心功能包括：

识别 Identify (ID)	**检测 Detect (DE)**	**恢复 Recover (RC)**
保护 Protect (PR)	**响应 Respond (RS)**	**治理 Govern (GV)**

NIST CSF 2.0是在原有框架的基础上进行更新，保留了原来的核心结构，围绕识别（Identify）、保护（Protect）、检测（Detect）、响应（Respond）、恢复（Recover）这五个主要功能进行组织，新增了一个功能：治理（Govern），治理在有效管理网络安全风险方面非常重要。

功能	描述
识别 **Identify (ID)**	识别功能涉及了解企业及其运营环境、资产、资源、能力和风险，以便根据现有的风险管理和企业目标，确定网络安全工作的优先级。
保护 **Protect (PR)**	保护功能涉及制定和实施适当的防护措施，以确保关键服务的交付。该功能支持限制、遏制潜在网络安全事件的影响。
检测 **Detect (DE)**	检测功能包括制定和实施适当的活动（activities）与控制措施，以便及时准确地发现网络安全事件。
响应 **Respond (RS)**	响应功能旨在制定和实施适当的措施，以应对检测到的网络安全事件，并支持控制其影响。
恢复 **Recover (RC)**	恢复功能涉及制定和实施活动，以保持弹性计划，恢复因网络安全事件受损的能力，从而支持及时恢复正常运营，并减少事件影响。
治理 **Govern (GV)**	治理功能提供关联性信息，帮助企业建立和监察网络安全风险管理、策略、目标和政策。NIST 把治理功能描述为“横跨（cross-cutting）”，它不仅限于单一功能，而是与识别、保护、检测、响应、恢复功能相互关联，贯穿整个网络安全框架。

NIST CSF 与 Claroty

Claroty 致力于保护全球关键基础设施环境中的互联资产，其解决方案可直接映射到 NIST CSF ：

- **Claroty xDome**：SaaS 网络安全平台，专为工业和关键基础设施企业打造，用于保护 OT 和运营环境中的互联设备。
- **Claroty xDome SA（Secure Access，安全访问）**：为内部和第三方 OT 人员提供顺畅、可靠、安全的远程访问。
- **Claroty 持续威胁检测（CTD）**：一款本地部署解决方案，擅长发现 CPS 资产。通过风险管理和威胁检测功能，识别可能影响 OT 网络的风险。

Claroty 的产品组合如何支持 NIST 框架

下表概述了 NIST CSF 2.0 框架每个功能的当前类别、描述、以及 Claroty 的产品组合如何帮助合规。

类别	描述	Claroty支持	子类别
识别 Identify (ID)			
ID.AM: Asset Management (资产管理)	识别并管理支持企业实现业务目标的数据、人员、设备、系统和设施，确保其管理方式与其对企业目标的相对重要性及企业的风险策略一致。	Claroty业界领先的资产发现功能，涵盖整个产品组合。通过发现网络中所有连接设备，并生成详细的设备配置文件（关键性、影响和可利用性信息），识别所有网络安全风险。	ID.AM-01 ID.AM-02 ID.AM-03 ID.AM-04 ID.AM-05 ID.AM-07 ID.AM-08
ID.RA: Risk Assessment (风险评估)	帮助企业了解其网络安全风险，包括对企业运营（使命、职能、形象或声誉）、企业资产、相关人员的影响。	Claroty的产品组合支持跨部门评估企业运营中的风险。可为安全团队、合规团队、OT团队提供定制化仪表板，并通过日志跟踪管理员活动，帮助全面了解漏洞和风险。	ID.RA-01 ID.RA-02 ID.RA-03 ID.RA-04 ID.RA-05 ID.RA-06 ID.RA-07 ID.RA-08 ID.RA-09 ID.RA-10
ID.IM: Asset Improvements (资产改进)	跨所有CSF功能，持续识别和改进其网络安全风险管理的流程、程序、活动。	Claroty持续更新支持，以应对新发现的漏洞，并从漏洞管理的角度立即实施改进。Claroty平台还提供可视化指标，便于长期跟踪安全计划的改进情况。	ID.IM-01 ID.IM-02 ID.IM-03 ID.IM-04

类别	描述	Claroty支持	子类别
保护 Protect (PR)			
PR.AA: Identity Management, Authentication, and Access Control（身份管理、身份验证和访问控制）	对物理和逻辑资产的访问仅限于授权用户、服务和硬件，并根据未经授权访问的风险评估进行管理。	Claroty Secure Access（安全访问）支持IAM（身份访问管理）和RPAM（远程特权访问管理），提供安全性、控制和访问权限，全面实现零信任策略。	PR.AA-01 PR.AA-03 PR.AA-04 PR.AA-05 PR.AA-06
PR.AT: Awareness and Training（意识与培训）	对企业员工进行网络安全培训，培养其网络安全意识。让他们可以按照相关策略、程序和协议执行网络安全任务。	Claroty 的实施和客户成功团队（implementation and customer success team）采用个性化方法，确保最终用户充分掌握使用方法。产品用户界面设计直观易用。	PR.AT-01 PR.AT-02
PR.DS: Data Security（数据安全）	信息和记录（数据）的管理应与企业的风险战略保持一致，以保护数据的机密性、完整性和可用性。	Claroty映射所有设备通信并持续监察异常行为，帮助防止数据泄露。Claroty可在工业网络上执行安全策略，以保护数据的机密性、完整性和可用性。	PR.DS-01 PR.DS-02 PR.DS-10
PR.PS: Platform Security（平台安全）	物理和虚拟平台的硬件、软件（例如，固件、操作系统、应用程序）、服务，都应该根据企业的风险策略进行管理，以保护其机密性、完整性和可用性。	Claroty的资产发现功能提供全面的设备配置文件，帮助识别旧版本固件、操作系统等，确保对设备进行持续监察，保障平台安全。	PR.PS-01 PR.PS-02 PR.PS-03 PR.PS-04 PR.PS-05 PR.PS-06
PR.IR: Technology Infrastructure Resilience（技术基础设施弹性）	安全架构的管理应符合企业的风险策略，以保护资产的机密性、完整性和可用性，并提高企业弹性。	Claroty通过支持零信任架构和创建网络分段（仅允许必要的通信）来增强基础设施弹性。	PR.IR-01 PR.IR-02 PR.IR-03 PR.IR-04

类别	描述	Claroty支持	子类别
检测 Detect (DE)			
DE.AE: Adverse Event Analysis (不良事件分析)	对异常情况、入侵指标（IoC）、其他潜在的不良事件进行分析，以描述这些事件，并检测网络安全事件。	Claroty解决方案包含强大的警报引擎，可检测异常行为、设备通信、设备变更，还可根据企业的风险容忍度进行定制。Claroty解决方案提供端到端的工作流程，涵盖识别、检测和修复。	DE.AE-02 DE.AE-03 DE.AE-06 DE.AE-07 DE.AE-08
DE.CM: Continuous Monitoring (持续监察)	对资产进行持续监察，以发现异常、IoC、其他潜在的不良事件。	Claroty解决方案提供持续的威胁监察，可检测异常行为、网络威胁特征、其他入侵指标（例如，与已知恶意实体的通信）。	DE.CM-01 DE.CM-02 DE.CM-03 DE.CM-06 DE.CM-09
响应 Respond (RS)			
RS.MA: Incident Management (事件管理)	对检测到的网络安全事件进行管理。	Claroty平台中的漏洞、暴露和警报可被优先级排序，并在平台中 分配给负责人或工作组，以便在事件发生时迅速解决问题。	RS.MA-01 RS.MA-02 RS.MA-03 RS.MA-04 RS.MA-05
RS.CO: Incident Reporting and Communications (事件报告与通信)	根据法律、监管或政策要求，与内部和外部利益相关方协调响应活动（response activities）。	Claroty提供预定义报告和自动化风险建议功能，有助于事件报告和跨职能沟通。这些报告可自定义，设定定期生成，并按照预定的时间间隔发送给利益相关方。	RS.CO-02 RS-CO-03
类别	描述	Claroty支持	子类别

RS.AN: Incident Analysis（事件分析）	开展调查，以确保有效响应，并支持取证和恢复活动（recovery activities）。	Claroty可识别已知和未知的IoC，并提供任何可疑行为的详细信息，以便在事件发生时进行全面识别和分析。	**RS.AN-03** **RS.AN-06** **RS.AN-07** **RS.AN-08**
RS.MI: Mitigation（缓解）	执行活动（activities）以防止事件的扩散，减轻其影响，并解决事件。	Claroty的产品组合支持端到端网络安全管理。Claroty平台提供全面的、与事件相关的信息，包括：了解资产及其通信情况、实施网络分段策略、限制因第三方凭证泄露造成的损害、把这些洞察输入到额外的事件响应工具中。	**RS.MI-01** **RS.MI-02**
恢复 Recover (RC)			
RC.RP: Incident Recovery Plan Execution（事件恢复计划执行）	执行并维护恢复流程、程序，以确保受网络安全事件影响的系统或资产得以恢复。	Claroty xDome SA 恢复机制结合访问封锁与基于需求的受控启用，确保恢复过程中安全性与可用性的平衡。	**RC.RP-01** **RC.RP-02** **RC.RP-03** **RC.RP-04** **RC.RP-05** **RC.RP-06**
RC.CO: Incident Recovery Communication（事件恢复通信）	恢复活动需要与内部和外部相关方进行协调。	Claroty可与SIEM（安全信息与事件管理）系统或其他安全平台集成，并支持导出事件数据，以有效协助恢复通信。	**RC.CO-03** **RC.CO-04**
类别	**描述**	**Claroty支持**	**子类别**

治理 Govern (GN)			
GV.OC: Organizational Context (企业关联性信息)	了解企业网络安全风险管理决策的关联性信息，包括：使命、利益相关方的期望、依赖关系、以及法律、监管和合同要求。	Claroty的风险评分和漏洞评估报告功能，有助于企业调整其网络安全目标和策略。Claroty平台还提供资产可视化，支持CPS的治理，符合法律、监管和合同要求。	GV.OC-01 GV.OC-02 GV.OC-03 GV.OC-04 GV.OC-05
GV.RM: Risk Management Strategy (风险管理策略)	企业的优先事项、约束条件、风险容忍度、风险偏好声明、假设需要被确立、传达，用于支持运营风险决策。	Claroty针对企业、站点和设备，提供定制化风险评分。支持：评估整体安全态势；量化每个独特环境中的风险和威胁；帮助企业优先考虑风险容忍度，以支持运营决策；调整 CPS 风险偏好，使其符合现有 IT 安全控制要求。	GV.RM-01 GV.RM-02 GV.RM-03 GV.RM-04 GV.RM-05 GV.RM-06 GV.RM-07
GV.RR: Roles, Responsibilities, and Authorities (角色、职责和权限)	明确网络安全的角色、职责和权限，以促进责任落实、绩效评估和持续改进。	Claroty支持网络安全角色的设立、安全计划的优化。Claroty平台支持基于角色的访问控制，根据最终用户的角色和职责提供适当的数据和访问权限。Claroty平台还可自定义仪表板和报告，支持按角色调整绩效评估和改进措施。	GV.RR-01 GV.RR-02 GV.RR-03 GV.RR-04
类别	**描述**	**Claroty支持**	**子类别**

GV.PO: Policy（策略）	创建、传达和执行企业网络安全策略。	Claroty支持跨CPS设备创建和执行策略。包括：降低风险的方法、通过网络访问控制（NAC）和防火墙实施网络分段。	GV.PO-01 GV.PO-02
GV.OV: Oversight（监督）	整个企业范围内的网络安全风险管理活动和绩效结果，用于告知、改进和调整风险管理策略。	Claroty平台提供全方位跟踪功能，包括：网络分段项目、风险缓解措施。	GV.OV-01 GV.OV-02 GV.OV-03
GV.SC: Cybersecurity Supply Chain Risk Management（网络安全供应链风险管理）	企业的利益相关方需要识别、建立、管理、监察、改进网络供应链风险管理流程。	CPS设备通常是企业供应链运营的一部分。Claroty提供专业技术，确保供应链安全，并建立有效的管理流程。	GV.SC-01 GV.SC-02 GV.SC-03 GV.SC-04 GV.SC-05 GV.SC-06 GV.SC-07 GV.SC-08 GV.SC-09 GV.SC-10

如何做到合规

众多工业组织正在努力保护和保障其互联资产的安全。新的行业法规和最佳实践指导，为企业构建和完善其网络安全计划提供了方向。随着NIST CSF 2.0的推出，现在是时候把流程、程序与本白皮书概述的最佳实践进行对齐。

使用 Claroty 保护 CPS

Claroty在制造业和其他关键基础设施领域，拥有无与伦比的行业专业知识，并非常了解CPS，这些构成了Claroty全面网络安全解决方案的基础。Claroty认识到，没有两个CPS网络是完全相同的，每个CPS网络都是独特的。因此，不能实施通用的方法来发现和保护它们。

被动监察 (Passive Monitorning)	安全查询 (Safe Queries)	Claroty Edge	项目文件分析 (Project File Analysis)
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

Claroty CPS 发现方法

Claroty采用多种发现方法，识别运营网络中的所有资产，包括使用独特或专有协议、Air Gap 或通过仅被动方式无法访问的资产。这些功能使Claroty能够提供广泛的、专为CPS设计的解决方案，涵盖风险管理、网络保护、安全访问、威胁检测。

风险管理	利用对暴露资产的可利用性洞察、这些风险对业务运营的潜在影响，来制定一种程序化的方法，专门针对 CPS 进行持续的风险管理。
网络保护	通过深入了解运营环境和最佳实践，为不同的 CPS 制定与生产环境相符的区域划分和通信策略建议。这些建议旨在推动网络分段和异常检测。
安全访问	专为安全访问设计的解决方案。利用详细的资产配置文件和策略，在一个统一的平台上，提供特权访问、身份管理和治理。
威胁检测	通过持续监察资产行为和动态威胁情报源，检测已知和未知的威胁、运营变化，保护 CPS 环境的运营完整性。

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。