



WHITE PAPER

Enhancing Healthcare Compliance With The NIST Cybersecurity Framework

TABLE OF CONTENTS

What is the NIST CSF	3
The Healthcare Cybersecurity Landscape for Cyber-Physical Systems (CPS)	3
Current State of the Regulatory Landscape for Healthcare	4
The NIST CSF Functions	4
The NIST CSF & Claroty	5
How Claroty's Product Portfolio Supports the NIST Framework	6
Why Comply Now	12
About Claroty	12

What is the NIST CSF?

The US National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a comprehensive set of guidelines designed to help critical infrastructure owners and operators better manage and reduce cybersecurity risk. This document provides information on the NIST Cybersecurity Framework 2.0 and how Claroty can support your healthcare cybersecurity program's alignment with NIST.

The Healthcare Cybersecurity Landscape for Cyber-Physical Systems (CPS)

The pace of automation and connectivity within healthcare delivery organizations is constantly evolving. Hospitals, clinics, and medical offices are continuously adopting new and innovative technologies involved in patient care delivery such as stronger digital health, telemedicine, and patient engagement programs. As both clinical and non-clinical workflows in healthcare organizations become more interconnected and reliant on these new technologies, however, they are not always properly managed within traditional IT processes and controls.

The healthcare industry also is increasingly a target for data breaches and other cybersecurity incidents. As of May 2024, the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR) had received over 500 notices of data breaches affecting healthcare providers since 2023.¹ According to Claroty's 2023 global healthcare cybersecurity study, 78% of health systems have experienced at least one cybersecurity incident within the past year and 60% reported that these had an impact on patient care.² Additionally, nearly a third of respondents reported that their building automation systems (BAS) were affected.

When it comes to protecting and securing healthcare networks from cybersecurity breaches, medical devices have unique implications as they directly impact clinical workflows and patient safety. The reality is, however, they are often some of the most misunderstood and vulnerable devices on the network, making them particularly susceptible to malicious exploitation.

Claroty's internal research group, Team82, recently conducted an analysis of cybersecurity trends and events impacting medical devices and the overall healthcare industry. This research revealed the breadth of vulnerabilities and other exposures, in particular on medical devices, that significantly elevates healthcare delivery organization's exposure to external threats and impact on patient safety. Some key findings were:

14%

of connected medical devices are currently running unsupported or EOL

32%

of unsupported devices are among the most critical to patient care such as MRIs and CT scanners



PACs and imaging workstations tend to be among the top medical devices to contain vulnerabilities

4%

of devices used in surgeries operate on guest networks³

As new technology emerges and connected devices in the healthcare environment increase, healthcare organizations can no longer rely on traditional IT security tools to account for the complexity and regulatory pressures in these environments.

Current State of the Regulatory Landscape for Healthcare

In order to better protect and secure all connected assets across healthcare environments, many healthcare organizations are taking extra measures to protect their data by adopting and implementing cybersecurity frameworks and best practices such as the NIST cybersecurity framework (NIST CSF) and HICP, Healthcare Industry Best Practices.

According to recent research done by KLAS in the Healthcare Cybersecurity Benchmarking Study 2024, several industry regulations are top of mind for healthcare organizations this year. The top 3 regulations when it comes to healthcare cybersecurity are the following:



While NIST CSF is among the regulations top of mind, healthcare organizations tend to vary greatly when it comes to state of maturity and adoption levels per function. Most organizations tend to take a bit of a reactive approach and could benefit from understanding best practices, processes, and procedures to proactively adopt NIST thoroughly across their organizations. Even if NIST is implemented across existing IT security processes and controls, organizations may need additional approaches when it comes to protecting and securing CPS (cyber-physical systems).

The NIST CSF Functions

This section aims to familiarize you with the functions of the NIST framework. This NIST framework is categorized into 6 core functions, each including processes and procedures valuable in protecting and securing CPS (cyber-physical systems). Each function, or category, also includes sub-categories within it that enable organizations to implement the appropriate processes and procedures.

These core functions include:

Identify (ID)	Detect (DE)	Recover (RC)
Protect (PR)	Respond (RS)	Govern (GV)

CSF 2.0 now represents a significant update to the original framework. The updated framework retains the core structure of its predecessor, organized around the primary functions of Identify, Protect, Detect, Respond, and Recover, but introduces a new function: Govern. This addition emphasizes the importance of governance in managing cybersecurity risks effectively.

Function	Description
Identify (ID)	The Identify function entails the understanding of the organization and its operational context, assets, resources, capabilities and risks so that cybersecurity efforts can be focused and prioritized in accordance with existing risk management and organizational objectives.
Protect (PR)	The Protect function involves developing and implementing appropriate safeguards to ensure the delivery of critical services. This function supports the ability to limit and/or contain the impact of a potential cybersecurity incident.
Detect (DE)	The Detect function encompasses developing and implementing appropriate activities and controls to enable the timely and accurate discovery of a cybersecurity event.
Respond (RS)	The Respond function is about developing and implementing suitable activities to act in response to a detected cybersecurity incident. This function supports the ability to contain the impact of such an incident.
Recover (RC)	The Recover function is about developing and implementing activities to maintain plans for resilience and restore capabilities that were impaired due to a cybersecurity incident. It supports timely recovery to normal operations to reduce the impact of such an incident.
Govern (GV)	The Govern function provides context that helps organizations establish and monitor their cybersecurity risk management, strategy, expectations, and policy. NIST describes the Govern function as “cross-cutting,” and it’s designed to help security teams prioritize the outcomes outlined in the other five functions.

The NIST CSF Functions

As Claroty aims to protect and secure connected assets across the world’s most critical infrastructure for healthcare environments, our solutions directly support the NIST CSF, these include:

- **Claroty xDome:** Claroty xDome is a SaaS-based healthcare cybersecurity platform that safeguards the connected devices that underpin patient care.
- **Claroty Secure Access:** Claroty xDome Secure Access delivers frictionless, reliable, secure remote access for internal and third-party OT personnel.

How Claroty's Product Portfolio Supports the NIST Framework

The following chart outlines the current categories of each function of the NIST CSF 2.0 framework, what they mean, and how Claroty's product portfolio helps to ensure compliance.

Category	Description	Claroty Support	Subcategories
Identify (ID)			
ID.AM: Asset Management	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Claroty ensures that all current cybersecurity risks are understood through industry-leading asset discovery across our entire product portfolio. This is done by discovering all network-connected devices on the network and in-depth device profiles, including criticality, impact, and device lifecycle information.	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	The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	The Claroty portfolio supports assessing risk across organizational operations across various departments. From customizable dashboards for security, compliance, and clinical engineering teams to tracking logging in surrounding admin activity, this helps to support an overall view of vulnerabilities and risks.	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

Category	Description	Claroty Support	Subcategories
ID.AM: Asset Improvements	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.	Claroty continuously updates support as new vulnerabilities are uncovered, ensuring improvements from a vulnerability management perspective are implemented immediately. Our platform also has metrics, easily enabling the ability to track security program improvements over time.	ID.IM-01 ID.IM-02 ID.IM-03 ID.IM-04
Protect (PR)			
PR.AA: Identity Management, Authentication, and Access Control	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.	Claroty Secure Access supports both IAM (Identity Access Management) and RPAM (Remote Privileged Access Management) providing security, control, and access to support a complete zero-trust approach.	PR.AA-01 PR.AA-03 PR.AA-04 PR.AA-05 PR.AA-06
PR.AT: Awareness and Training	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks with related policies, procedures, and agreements.	Claroty's implementation and customer success team takes a personalized approach to ensuring end users of the product are fully trained and know how to use the product. The user interface is largely intuitive.	PR.AT-01 PR.AT-02
PR.DS: Data Security	Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Claroty xDome maps all device communication and continuously monitors for anomalous behavior, helping prevent data leakage. The ability to enforce policies across your industrial network to protect confidentiality, integrity, and availability.	PR.DS-01 PR.DS-02 PR.DS-10

Category	Description	Claroty Support	Subcategories
PR.PS: Platform Security	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.	Claroty xDome's asset discovery provides comprehensive device profiles helping to identify outdated firmware, operating systems and more in order to ensure continuous monitoring of devices to ensure platform security.	PR.PS-01 PR.PS-02 PR.PS-03 PR.PS-04 PR.PS-05 PR.PS-06
PR.IR: Technology Infrastructure Resilience	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.	Claroty xDome supports infrastructure resilience through the ability to implement zero-trust architectures and enforce network segmentation ensuring only the necessary communication is required.	PR.IR-01 PR.IR-02 PR.IR-03 PR.IR-04
Detect (DE)			
DE.AE: Adverse Event Analysis	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.	Claroty xDome's Advanced Anomaly & Threat Detection module consists of a robust alerting engine that detects anomalous behavior, device communications, and device changes that are customizable to your organizational risk tolerance. Our solution offers an end-to-end workflow for identification, detection, and remediation.	DE.AE-02 DE.AE-03 DE.AE-06 DE.AE-07 DE.AE-08
DE.CM: Continuous Monitoring	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.	Claroty xDome's Advanced Anomaly & Threat Detection module doubles as a solution for continuous threat monitoring that detects anomalous behavior, network threat signatures, and other indicators of compromise like communication with known-malicious entities.	DE.CM-01 DE.CM-02 DE.CM-03 DE.CM-06 DE.CM-09

Category	Description	Claroty Support	Subcategories
Respond (RS)			
RS.MA Incident Management	Responses to detected cybersecurity incidents are managed.	Vulnerabilities, exposures, and alerts within Claroty xDome can be prioritized and assigned to owners or working groups in the platform to resolve incidents as they arise.	RS.MA-01 RS.MA-02 RS.MA-03 RS.MA-04 RS.MA-05
RS.CO: Incident Reporting and Communications	Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.	Predefined reports and automated risk recommendations within Claroty xDome aid in incident reporting and cross-functional communications. These reports can be customized and scheduled to run, and sent to key stakeholders on predefined intervals	RS.CO-02 RS.CO-03
RS.AN: Incident Analysis	Investigations are conducted to ensure effective response and support forensics and recovery activities.	Claroty xDome identifies known and unknown IoCs with detailed information on any suspicious behavior for comprehensive identification and analysis of incidents as they arise.	RS.AN-03 RS.AN-06 RS.AN-07 RS.AN-08
RS.MI: Mitigation	Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.	Claroty's product portfolio was built to support an end-to-end cybersecurity program. Claroty Secure Access and Claroty xDome give full breadth of context around incidents which as understanding assets and grow they are communicating, implementing segmentation policies, limiting damages from compromised third-party credentials, and feeding these insights into additional incident response tools.	RS.MI-01 RS.MI-02

Category	Description	Claroty Support	Subcategories
Recover (RC)			
RC.RP: Incident Recovery Plan Execution	Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Claroty Secure Access recovery includes a combination of access lock-down, followed by controlled enablement on an as-needed basis during recovery.	RC.RP-01 RC.RP-02 RC.RP-03 RC.RP-04 RC.RP-05 RC.RP-06
RC.CO: Incident Recovery Communication	Restoration activities are coordinated with internal and external parties.	Claroty xDome enables integration into SIEMs or other security platforms and the ability to export incidents to efficiently aid in recovery communications.	RC.CO-03 RC.CO-04
Govern (GN)			
GV.OC Organizational Context	The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood.	Claroty xDome's risk scoring and vulnerability assessment reporting provide support to align with organizational expectations and goals. The platform provides asset visibility to support the inclusion of CPS governance of legal, regulatory, and contractual requirements.	GV.OC-01 GV.OC-02 GV.OC-03 GV.OC-04 GV.OC-05
GV.RM: Risk Management Strategy	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.	Claroty xDome provides tailored risk scoring per organization, site, and device. The ability to assess overall security postures, as well as other forms of measurements of risks and threats in each unique environment, enables organizations to prioritize their risk tolerance to support operational risk decisions and tailor their CPS risk appetite in alignment with existing IT security controls.	GV.RM-01 GV.RM-02 GV.RM-03 GV.RM-04 GV.RM-05 GV.RM-06 GV.RM-07

Category	Description	Claroty Support	Subcategories
GV.RR: Roles, Responsibilities, and Authorities	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	Claroty xDome supports the establishment and support of cybersecurity roles and program improvements. The platform supports role-based access controls to enable the right data and access based on the end user's roles and responsibilities. The platform also supports the creation of customized dashboards and reporting to support tailored performance assessment and improvement based on role.	GV.RR-01 GV.RR-02 GV.RR-03 GV.RR-04
GV.PO: Policy	Organizational cybersecurity policy is established, communicated, and enforced.	Claroty xDome supports the creation and enforcement of policies across CPS devices. From risk reduction approaches to network segmentation enforcement across NAC & Firewalls, this policy enforcement can be done directly in the program and carried over into organizational policies.	GV.PO-01 GV.PO-02
GV.OV: Oversight	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	Each aspect of the Claroty xDome platform, from network segmentation projects to medical device operational efficiency metrics, can be tracked directly within the platform.	GV.OV-01 GV.OV-02 GV.OV-03
GV.SC: Cybersecurity Supply Chain Risk Management	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.	As CPS devices are typically part of organizations' supply chain operations, Claroty xDome provides specific expertise on keeping supply chains secure and establishing effective processes.	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

Why Comply Now

As the healthcare industry strives to protect and secure connected assets, new industry regulations and best practice guidance help steer direction as healthcare delivery organizations build out and mature their cybersecurity programs. With recent enhancements to the NIST CSF framework and the introduction of the governance function, now is a good time to align processes and procedures to the best practices outlined here

If you are interested in learning more on how Claroty's product portfolio supports the NIST cybersecurity framework, contact us or [request a demo](#).

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. Claroty is deployed by hundreds of organizations at thousands of sites globally. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America. To learn more, visit claroty.com.

¹ U.S. Department of Health and Human Services Office for Civil Rights Breach Portal

² The Global Healthcare Cybersecurity Study, 2023

³ State of CPS Security Report: Healthcare 2023