WHITE PAPER

How Claroty Secure Remote Access (SRA) Maps to CISA's Cross-Sector Cybersecurity Performance Goals

Critical infrastructure has long been a highly sought-after target for state-sponsored and other cyber actors due to its potential to fuel widespread disruption if compromised. The risk of such compromises has escalated in recent years amid the growing embrace of digital transformation — and, thus, cyber-physical connectivity — across critical infrastructure sectors that now face even larger, more vulnerable attack surfaces as a result. Recognizing the crucial need to minimize these areas of risk exposure, the Cybersecurity Infrastructure & Security Agency (CISA) and the National Institute of Standards and Technology (NIST) recently partnered to release Cross-Sector Cybersecurity Performance Goals (CPGs) that aim to assist critical infrastructure organizations in establishing the cybersecurity practices that matter most.

How Claroty Secure Remote Access (SRA) helps organizations to achieve CPGs

Among those practices are various controls that share a distinct focus: operational technology (OT) remote access. As both an integral element of operational continuity and an exceedingly common — and risky — cybersecurity gap, OT remote access certainly warrants this caliber of attention. Claroty commends CISA and NIST for ensuring the CPGs accounted for related controls, most of which also underpin a core component of our portfolio: Claroty Secure Remote Access (SRA). By providing secure, reliable, and frictionless access to OT environments for internal and third-party remote users, the solution reduces exposure to cyber and operational risks, improves visibility and control, and strengthens detection and response. SRA's capabilities closely align with the CPGs, making it uniquely suitable for critical infrastructure organizations seeking to eliminate cybersecurity gaps without impeding operational workflows.

This document demonstrates Claroty SRA's capabilities with Claroty's industrial cybersecurity portfolio, which includes the SaaS-based xDome platform and its on-premise counterpart, Continuous Threat

Detection (CTD) solutions. The guide map shows how Claroty can help organizations in critical infrastructure and all sectors to effectively and efficiently implement the recommendations set forth by CISA and NIST via the CPGs.

Out of the eight CPGs, six pertain in some capacity to OT remote access, thereby underscoring its fundamental role in critical infrastructure cybersecurity. Details about each of these six CPGs and how Claroty SRA can help you achieve them are as follows:

1.0 Account Security

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	1.1	**Detection of Unsuccessful (Automated) Login Attempts** *Protect organizations from automated, credential-based attacks.*	Claroty SRA helps prevent unauthorized access and other credential-based attacks by enabling administrators to define thresholds for failed login attempts and automatically detecting, alerting on, and blocking any users who exceed this threshold.	PR.AC-7
✓	1.2	**Changing Default Passwords** *Prevent adversaries from using default passwords to achieve initial access or move laterally in a network.*	Claroty SRA eliminates default passwords as an attack vector for OT environments by managing all credentials for OT remote access in a manner that obfuscates the underlying credentials while binding them to end-user identities. It also enforces stringent password hygiene requirements and offers the ability to integrate with SAML- and OIDC-based identity providers.	PR.AC-1
✓	1.3	**Multi-Factor Authentication (MFA)** *Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.*	Claroty SRA offers multiple options for multi-factor authentication, including Single Sign On (SSO) and application-based authentication, with advanced security policies such as password length, complexity, and history. For customers requiring further integration, Claroty has developed SAML support for third-party identity and access management (IAM) providers, as well as integrations with user directories such as Microsoft Azure AD.	PR.AC-7

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	1.4	**Minimum Password Strength** Organizational passwords are harder to guess or crack by adversaries.	Claroty SRA enforces advanced unique credential policies such as password length, complexity, and history. It also supports the enforcement of password hygiene requirements and offers the ability to integrate with SAML- and OIDC-based identity providers.	PR.AC-1
✓	1.5	**Separating User and Privileged Accounts** *Make it harder for adversaries to gain access to administrator or privileged accounts, even if common user accounts are compromised.*	Claroty SRA supports least-privilege policies and separation of duties (i.e. secondary approval). SRA administrators can create highly granular user profiles that grant access only to the devices to which each user requires access during a specified window.	PR.AC-4
✓	1.6	**Unique Credentials** *Attackers are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.*	Claroty SRA eliminates credential reuse as an attack vector for OT environments by enforcing advanced unique credential policies such as password length, complexity, and history.	PR.AC-1
✓	1.7	**Revoking Credentials for Departing Employees** *Prevent unauthorized access to organizational accounts or resources by former employees.*	Claroty SRA allows administrators to automatically disable accounts with no user activity for a specified number of days. Claroty SRA's integration with various identity providers also assists administrators in automatically enforcing their existing user-access and password policies for SRA users, making it easier to invalidate SRA user accounts and revoke the credentials of former employees.	PR.AC-1

2.0 Device Security

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	2.1	**Hardware and Software Approval Process** *Increase visibility into deployed technology assets, and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.*	Claroty SRA assists with establishing a change control process by managing administrative access and ensuring only authorized users can access assets and make configuration changes. SRA also collects details of all assets and locations accessed and configuration changes made during a session.	PR.IP-3
✓	2.3	**Asset Inventory** *Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.*	Claroty SRA, with its native integration with Claroty's industrial cybersecurity portfolio, including the xDome and CTD solutions, offers comprehensive support for asset inventory control in OT environments. Integrating SRA with xDome or CTD enables advanced threat detection and ensures accurate and up-to-date asset inventory. xDome and CTD each provide a centralized management console from which to streamline the asset inventory control process. The combination of SRA and xDome or CTD provides organizations with increased visibility and control over the assets in the OT networks. To learn more, visit here.	ID.AM-1

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	2.4	**Prohibit Connection of Unauthorized Devices** *Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.*	Claroty SRA with xDome or CTD provides protection against unauthorized devices by using network segmentation, advanced device identification and authentication techniques, and continuous threat detection. This ensures that critical infrastructure is protected from cyber threats and that the industrial network remains secure at all times.	PR.PT-2
✓	2.5	**Document device configuration** *More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.*	Claroty SRA supports backup & recovery capabilities for all network devices by documenting device configuration. It also monitors, records and stores remote user video sessions to enable organizations to efficiently manage, respond to, and recover from cyberattacks to minimize downtime and restore critical services.	PR.IP-1

3.0 Data Security

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	3.1	**Log Collection** *Achieve better visibility to detect and effectively respond to cyber-attacks.*	Claroty SRA collects logs of any remote user activity performed during a remote session and employs multiple encryption techniques to ensure all user access and asset data are encrypted in the Claroty DB. Claroty SRA employs password vaulting that ensures all user access and asset data at rest are encrypted in the Claroty DB using AES-256 and hashed as SHA 256-bit. SRA encrypts its data in transit using SSL to encrypt user data and activities via TLS v1.2+ and SSH2 encryption with RSA 4096-bit authentication keys.	PR.PT-1
✓	3.2	**Secure Log Storage** *Organizations' security logs are protected from unauthorized access and tampering.*		PR.PT-1
✓	3.3	**Strong and Agile Encryption** *Effective encryption deployed to maintain the confidentiality of sensitive data and integrity of IT and OT traffic*		PR.DS-1, PR.DS-2
✓	3.4	**Secure Sensitive Data** *Protect sensitive information from unauthorized access.*		PR.DS-1, PR.DS-2, PR.DS-5

5.0 Vulnerability Management

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	5.1	**Mitigating Known Vulnerabilities** *Reduce the likelihood of adversaries exploiting known vulnerabilities to breach organizational networks.*	Claroty SRA establishes change control processes by managing administrative access and logging admin activity, reducing the risk of a threat actor to reduce exploiting known vulnerabilities and breaching the OT network remotely. Claroty SRA enforces secure architecture and uses encrypted tunnelling for Data-in-transit to isolate critical assets in your OT network while aligning with the Purdue model. It integrates with antivirus solutions to limit potential damage from compromised third-party credentials to a minimum number of assets. Claroty SRA with xDome or CTD provides comprehensive support for vulnerability management in the OT environment. xDome and CTD each automatically identify vulnerabilities affecting OT assets, assess the risk based on granular scoring mechanisms, and inform prioritization and remediation efforts based on the assessed risk. SRA can then use this information to determine and implement compensating control for known vulnerabilities, limit remote access to critical assets, and enforce granular policies.	PR.IP-12, ID.RA-1, DE.CM-8, RS.MI-3
✓	5.4	**No Exploitable Services on the Internet** *Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in public-facing assets.*		PR.PT-4
✓	5.5	**Limit OT Connections to Public Internet** *Reduce the risk of adversaries exploiting or interrupting OT assets connected to the public internet.*		PR.PT-4

7.0 Response and Recovery

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	7.3	**System Back-Ups** *Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.*	Claroty SRA performs regular backups and retains logs of all the remote user activities and live video sessions to retain any OT system changes made during a remote session.	PR.IP-4

8.0 Other

	ID	Security practice	Claroty SRA Support	NIST Control Mapping
✓	8.1	**Network Segmentation** *Reduce the likelihood of adversaries accessing the OT network after compromising the IT network.*	Claroty SRA's architecture preserves network segmentation by providing granular access controls and limiting the scope of access to specific assets or groups of assets. SRA's multi-layered architecture ensures secure access to industrial assets without compromising network segmentation. It monitors for unauthorized personal network connections (baseline deviation), devices (in-scope asset inventory) and software (ICS/PLC firmware changes). It also monitors the personnel activity of internal and external users for remote access to each industrial system and creates logging of configuration alterations on industrial systems to perform protection updates. *Continued on following page*	PR.AC-5, PR.PT-4, DE.CM-1

			Claroty SRA integration with CTD or xDome enhances its network segmentation controls by automatically mapping and segmenting industrial networks into virtual zones. At the same time, it leverages asset visibility to define and recommends network communication policies. This integration enables SRA to leverage these controls and policies to ensure secure access to industrial assets without compromising network segmentation.	

Jumpstart your journey to achieving CISA's CPGs with Claroty Secure Remote Access (SRA)

As the only remote access solution truly purpose-built for OT, Claroty SRA empowers thousands of engineers, plant managers, and other security and operations personnel globally to reduce risk while optimizing workflows and driving resilience.

To learn more about how Claroty SRA portfolio maps to CISA's CPGs, contact us for a demo.