Security Principles of Claroty Secure Remote Access

About Claroty SRA

Claroty Secure Remote Access (SRA) is a core component of The Claroty Platform that delivers frictionless, reliable, and highly secure remote access to OT environments. Unlike traditional remote access solutions, SRA is purpose-built for the specific operational, administrative, and security needs of industrial networks. The result is a unique solution that reduces your mean-time-to-repair (MTTR), minimizes the cost and complexity of administering access for your OT remote users, and diminishes your OT environment's exposure to the risks posed by unmanaged, uncontrolled, and unsecured access.

Integral to its ability to deliver these capabilities and benefits, SRA is inherently secure-by-design. The following table illustrates the solution's security principles across three core areas:

Security Infrastructure

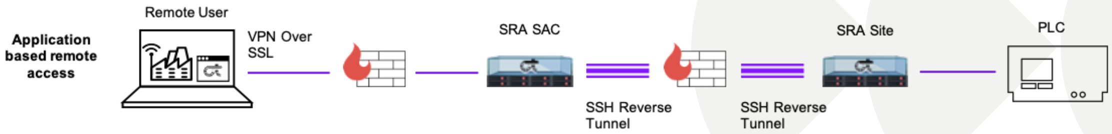
Data at Rest

SRA employs password vaulting that ensures all user access and asset data is encrypted in the Claroty DB using AES-256 and hashed as SHA 256-bit. When such data is pulled for use, credentials are not cached or stored in any decrypted form. All data related to each SRA session—such as user, session length, session purpose, etc.—can also be encrypted if desired.

Data in Transit

SRA splits all data in transit between two encrypted tunnels:

- One tunnel is between the user and the SRA Secure Access Center (SAC) and utilizes the benefits of SSL to encrypt user data and activities via TLS v1.2+.
- The other tunnel is between the SAC and the site device and utilizes SSH2 encryption with RSA 4096-bit authentication keys. This funnels different remote access protocols through one encrypted port between the SAC and SRA site device.



Breaking the encrypted tunnel in this manner enables SRA to remove direct connectivity between remote users and industrial assets, thereby reducing the number of devices connected to the network, the number of open ports in the firewall, and, ultimately, the attack surface.

Security Features

Purdue Model Preservation

SRA's multiple implementation options all support the Purdue Model by only interacting one layer up or down in the industrial network. All options comply with ISA/IEC 62443.

Authentication

SRA supports 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.

Principle of Least Privilege (PoLP) Support	SRA administrators can create user profiles that grant access only to the devices to which each user requires access. User profiles can also be configured to limit the actions a user can perform once connected to a device, as well as which protocols—such as HTTP/HTTPS versus RDP/VNC access, for example—a user can utilize.
Role-based Access Control (RBAC)	Due to the complex nature of OT environments, users often require access at multiple levels or geographic locations depending on the specific assets that require attention. The RBAC model supported by SRA helps to ensure enforcement of appropriate security policies accordingly.
Auditing, Forensics, & GDPR	All actions taken by users via SRA are logged at both the site-level and SAC. Logs include session information such as device, actions taken, session length, and correspondence with the administrator. In addition, all sessions are automatically recorded via full-length video for forensic purposes. This mechanism also supports GDPR requirements, which state that remote access recordings must be stored in the country/location where the asset is based.
Password Vaulting	When a user from a third-party vendor is granted access to a device, SRA embeds their credentials in the Claroty DB. The vendor does not retain direct access to them. These credentials are done at the user-level, providing varying levels of privileges on any one asset.
Safety-approved Access	For devices that pose a safety risk when accessed remotely, additional policies can be created to ensure the health and operability of the environment where the device is located. These additional policies also apply to users who retain regular access to the device.

Security Assurances

Penetration Testing & SSDLC	Claroty R&D upholds compliance to ISO9001 and ISO27001. As part of the Secure Software Development Lifecycle (SSDLC), Claroty follows Open Web Application Security Project (OWASP) and Top Ten Vulnerabilities to ensure code and design best-practices. In addition to these measures, Claroty employs penetration testing by third-parties, as well as encourages our customers and user base to conduct their own penetration testing.
CIFS/NEST/NERC CIP & Compliance	Claroty strives to help our customers adhere to a variety of regulatory requirements and supplemental compliance initiatives. We are also proud to be the first industrial cybersecurity provider to receive the U.S. Department of Homeland Security's SAFETY Act certification.
OS Hardening & Patches	Recognizing that SRA runs on an external OS, Claroty secures CentOS and Red Hat OS by default. All packages that are not in use by Claroty software are hardened and disabled as per the Center for Internet Security (CIS) benchmark.

About Claroty

Claroty is the industrial cybersecurity company. Trusted by the world's largest enterprises, Claroty helps customers reveal, protect, and manage their OT, IoT, and IIoT assets. The company's comprehensive platform connects seamlessly with customers' existing infrastructure and programs while providing a full range of industrial cybersecurity controls for visibility, threat detection, risk and vulnerability management, and secure remote access—all with a significantly reduced total cost of ownership. Claroty is backed and adopted by leading industrial automation vendors, with an expansive partner ecosystem and award-winning research team. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America, and deployments on all seven continents.

To learn more, visit **www.claroty.com**.

CONTACT US

contact@claroty.com