CLAROTY

# Security Principles of Secure Remote Access

## Secure-by-Design

Claroty Secure Remote Access (SRA) is purpose-built for operational technology (OT) remote access, providing a simple to use, OT-aware solution that supports distributed deployments. SRA is secure-by-design, boasting a wide array of capabilities and features that provide the highest security measures with efficiency and operability in mind.

Remote access poses a unique challenge for OT environments and places an emphasis on the security of remote access technology. OT networks often comprise critical infrastructure and core industries that span wide geographic areas, rendering them extra sensitive to unscheduled downtime and making them a high-value target for malicious actors. These conditions highlight the need for a remote access solution that supports OT workflows, benefits operational efficiency, and implements and enforces comprehensive security controls. The below table illustrates the principles that drive SRA's secure-by-design nature:

### Security Infrastructure

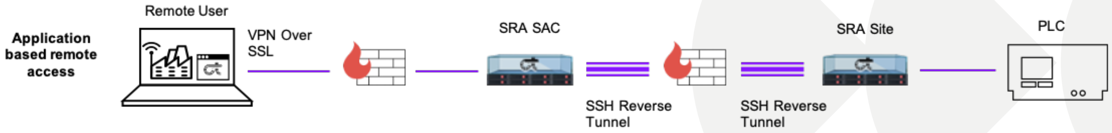
**Data at Rest**

Password vault data for user access and asset data is stored and encrypted in the Claroty DB using AES-256 and hashed as SHA 256-bit. When information is pulled for use credentials are not cached or stored in any decrypted form. In addition to this, disk encryption for details surrounding remote sessions (who logged in, for how long, etc) can be encrypted if the user requires this as part of their security policies.

**Data in Transit**

SRA splits all data in transit between two encrypted tunnels:

- One tunnel is between the user and the 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 of only interacting one layer up or down and complies with ISA/IEC 62443.

**Authentication**

SRA supports app authentication with advanced security policies such as password length, complexity, and history. For users requiring further integration Claroty has developed SAML support for third-party Identity and Access Management (IAM) providers as well as integrations with user directories like Microsoft Azure AD.

| | |
|---|---|
| **Principle of Least Privilege (PoLP) Support** | SRA administrators can limit user profiles to have access only to devices that they need access to as well as limiting what actions they can take with that device once inside. Users can also be limited by protocols that they require access to, for example, HTTP/HTTPS vs RDP/VNC access. |
| **Role-based Access Control (RBAC) & User Management** | 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 security policies. |
| **Autiditing & Forensics and GDPR** | Every action taken in SRA by remote users is logged at both the site-level and SAC including session information such as the device actions, length of session, and correspondence with the administrator. In addition, all sessions are recorded for forensic purposes by default. This mechanism also supports GDPR requirements that state that remote access recordings should be stored in the country/location where the asset is based. |
| **Password Vaulting** | Once a vendor is granted access to a device SRA embeds those credentials in the Claroty DB, the vendor does not retain direct access to their own credentials. 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/NIST/NERC CIP & Compliance** | Claroty strives to meet and comply with a variety of regulatory requirements and supplemental compliance initiatives. We are also proud to be the first OT security 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 bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015.

CONTACT US

**contact@claroty.com**