DATA SHEET

CLAROTY SECURE REMOTE ACCESS (SRA)

Frictionless, Reliable, and Highly Secure Remote Access for Industrial Networks

The Industrial Network Remote Access Challenge

We created Claroty SRA to tackle the operational technology (OT) remote access challenge. More specifically, while OT remote access is a critical necessity for industrial enterprises, it has long been risky and difficult for three key reasons:

1. End-User Complexity: Increases MTTR

Since most traditional remote access tools are designed for IT networks, they often have cumbersome access mechanisms and interfaces that are unsuitable for OT needs.

Not only do end-users typically need to undergo lengthy onboarding and training before using these tools—but the tools' complexity and inefficiency mean that regardless of how much training users receive, they may still struggle to repair industrial assets as quickly as necessary.

These conditions increase users' mean time to repair (MTTR), which can be problematic in situations where emergency repairs must be made immediately to avoid or reduce downtime or other serious consequences.

2. Administrator Complexity: Increases TCO

Internal and third-party users must be able to remotely access industrial assets when needed for maintenance or other purposes.

However, managing this access requires administrators to maintain costly, complex infrastructure while addressing users' onboarding and troubleshooting needs.

Third-party users can be especially difficult to support because they typically cannot share jump servers or other infrastructure with those from other vendors, further complicating matters for administrators.

This process is expensive and timeconsuming, making the total cost of ownership (TCO) of traditional remote access tools high for OT environments.

3. Poor Visibility and Security Controls: Increase Exposure to Risk

OT remote users could make unauthorized changes that pose risks to operations. These risks are compounded by using traditional remote access tools that give cybersecurity staff poor visibility into users' activities and do not enable such staff to implement role-and policy-based access controls for users.

Another concern is that such tools are often inherently insecure because they commonly use vulnerable RDP protocols and go against industrial cybersecurity best practices by breaking the Purdue Model. As a result, cybersecurity staff cannot identify or control who logs in from where, when, or why. They also cannot identify or respond to incidents related to these users' activities, all of which expose the OT environment to greater risk.

About Claroty SRA

Claroty SRA tackles the OT remote access challenge by delivering frictionless, reliable, and highly secure remote access to OT environments for internal and third-party users. Unlike traditional remote access solutions—most of which are designed solely for IT networks—Claroty 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 configuring and administering access for your OT remote users, and diminishes your OT environment's exposure to the risks posed by unmanaged, uncontrolled, and unsecured access.

SRA Features & Capabilities

A User Experience that Reduces MTTR

By reducing the end-user complexity of OT remote access, SRA enables users to access, troubleshoot, and repair industrial assets more quickly and easily whenever necessary. Highlights include:

- **Just-in-Time (JIT) User Provisioning:** SRA integrates with a variety of identity providers (IdPs) via SAML and OpenID Connect (OIDC), enabling administrators to automate and streamline creation of SRA user accounts as part of the single sign on process. This means new users can be automatically added to and start working with SRA right away – all without requiring any additional steps from the administrator.
- **Efficient Authentication & Access:** SRA also offers native multi-factor authentication and does not employ jump servers. As a result, authorized SRA users can authenticate and gain access rapidly and securely when they need it most.
- **An Intuitive Interface:** The SRA interface mirrors each user's on-premises technology experience, providing unmatched usability with no learning curve or need for extensive training.
- **High Availability:** SRA includes a High Availability mechanism that ensures users maintain access no matter the circumstances.

Key Features & Benefits

- SRA reduces MTTR & boosts up-time by making it faster and easier to connect to and repair OT, IoT, and IIoT assets at any time, anywhere.
- SRA decreases the complexity & cost of safe, secure, reliable OT remote access by providing flexible configuration options, centralized management, and everything your internal and third-party users need.
- SRA minimizes the risks of OT remote access by empowering you to control, secure, and gain visibility into all remote connections and activities in your network.

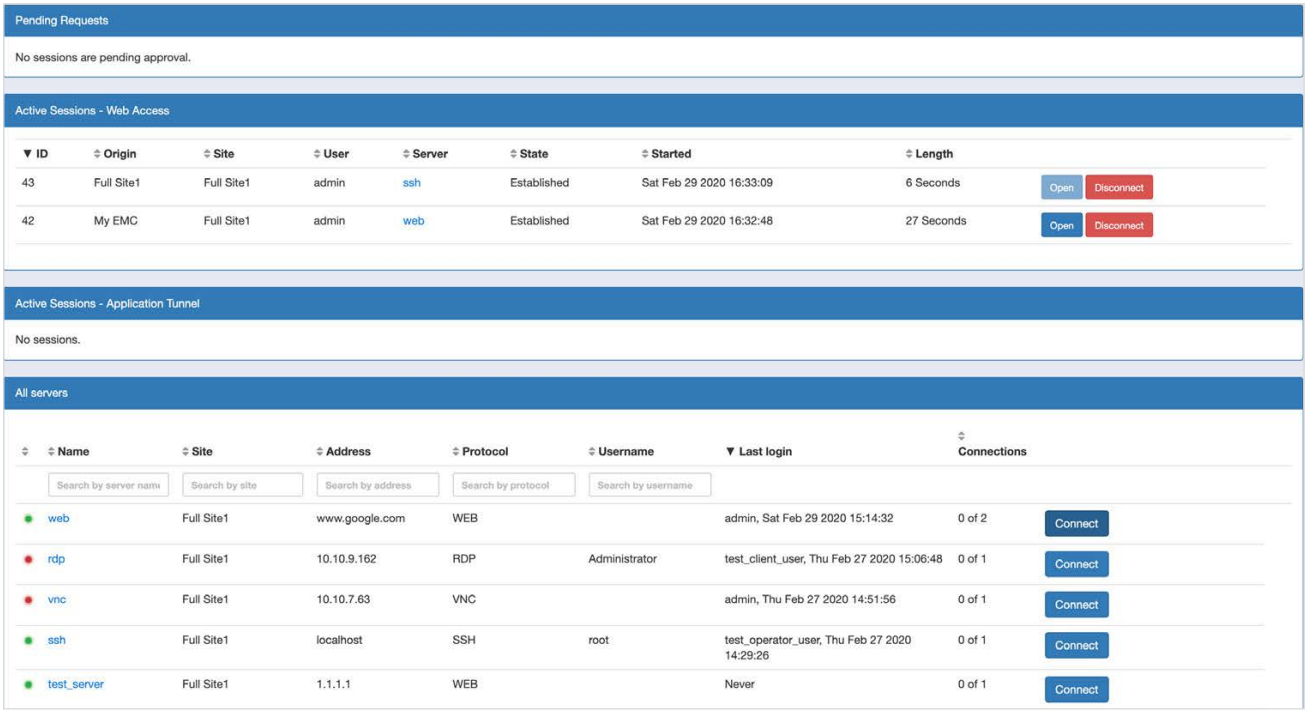

Fig 1: SRA Home Page view with active remote connections

Administrative Features that Decrease the TCO of Managing OT Remote Access

SRA decreases the typically high total cost of ownership (TCO) of OT remote access for administrators by providing flexible configuration options, centralized management, and everything internal and third-party users need to support their OT remote access use cases. Highlights include:

- **JIT User Provisioning:** In addition to benefitting SRA users, JIT user provisioning also enables SRA administrators to save considerable time and resources by automating the otherwise-largely manual and time-consuming process of provisioning and securing access for, as well as onboarding, new SRA users.
- **Flexible Deployment & Configuration Options:** Neither deploying nor configuring SRA requires the use of jump servers, complex firewall rules, or other often-costly and complicated architectural components common to traditional remoteaccess solutions. As a result, SRA administrators get to spend less time and money deploying and managing their users' remote access infrastructure, thereby decreasing its TCO.
- **Comprehensive Support for all OT Remote-Access Use Cases:** SRA is truly a one-stop-shop solution for OT remote access because it includes the full spectrum of features and capabilities needed to support all OT remote-access use cases. These include an OT purposebuilt user interface, multiple options for multi-factor authentication, password vaulting, secure file management, high availability, over-the-shoulder monitoring, and more. This means you can satisfy the OT remote-access needs of both your internal and third-party users without having to procure, deploy, and maintain multiple solutions.

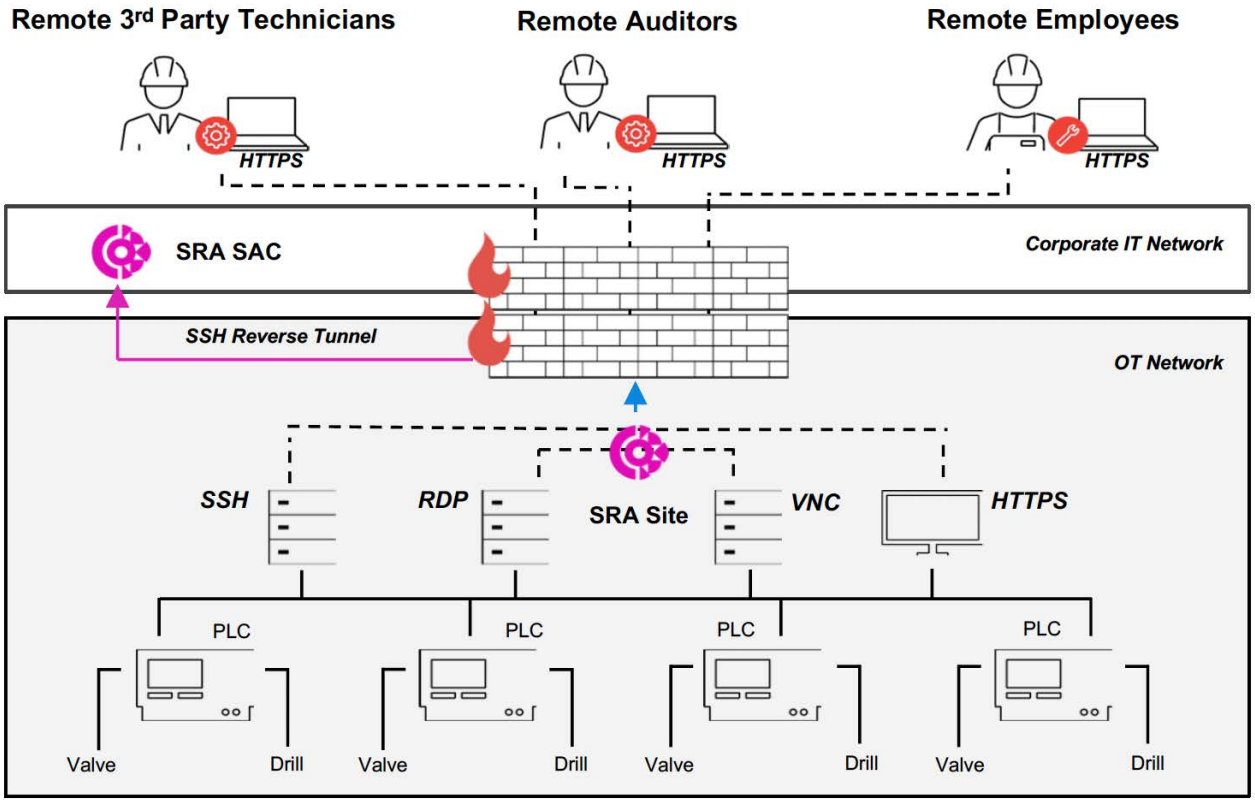

Fig 2: Example deployment architecture of SRA showing its simple configuration for multiple types of remote users

Access & Authentication Controls that Minimize Risks Posed by Remote Users

SRA administrators can control access to their industrial network across multiple tiers with the specificity to determine who can access which assets, how, when, for what purpose, and with which protocols. Highlights include:

- **Secure Authentication:** SRA includes native multi-factor authentication and credential management options, supports enforcement of password hygiene requirements, and offers the ability to integrate with SAML- and OIDC-based identity providers.
- **Integration with Identity Providers:** SRA administrators who opt to integrate the system with their existing identity provider can automatically extend enforcement of SAML- or OIDC-based authentication policies and password requirements already in place at their organization to their SRA user accounts, ensuring strong user authentication for OT employees and third parties alike. This capability also enables the SRA credentials of former employees to be automatically invalidated, thereby eliminating high-risk attack vectors commonly used in privilege escalation and password-reuse attacks.

- **Role- & Policy-based Access:** SRA administrators can define and enforce extremely granular access controls for industrial assets at multiple levels and geographic locations, ultimately streamlining user workflows while shielding critical functionalities from unnecessary access. Such controls support Zero Trust and Least Privilege security principles.
- **Safety-Approved & Emergency Access:** For assets that pose a safety risk when accessed remotely, additional policies can be created to ensure the health and operability of each asset's environment.

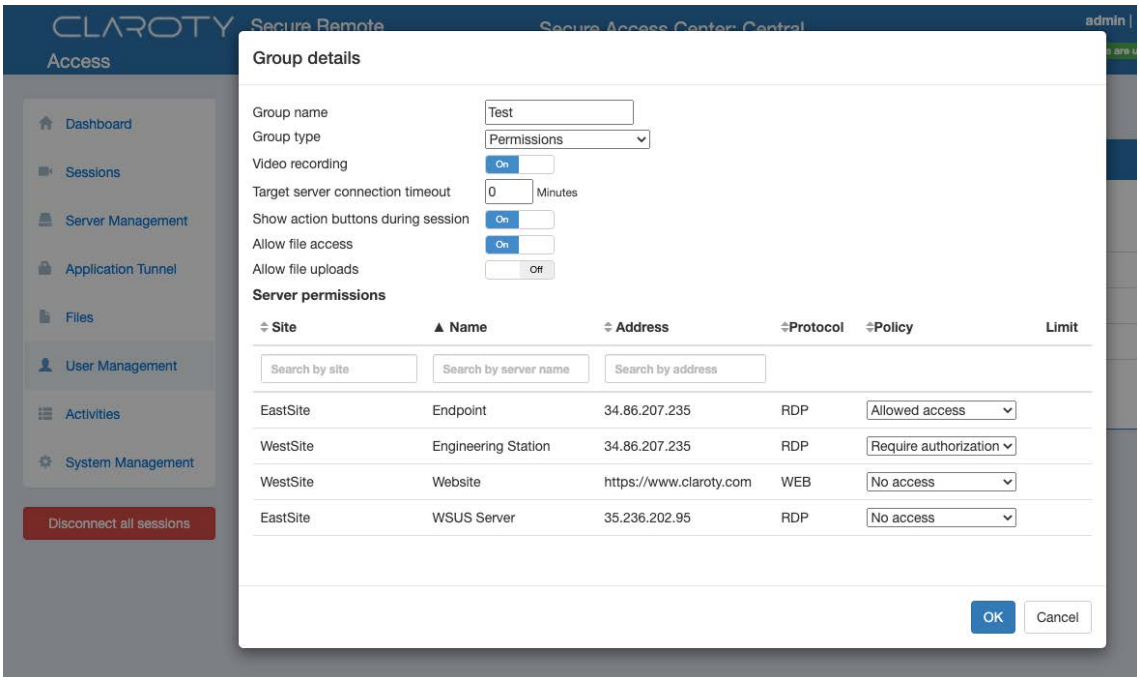

Fig 3: Group details witihin SRA

Inherently Secure Architecture & Features that Reduce the Attack Surface

Isolating the critical assets in your industrial network from external connectivity and proactively protecting against malware are crucial for reducing the attack surface and thus the risks posed by remote users. SRA provides these capabilities by:

- **Using Encrypted Tunneling for Data-in-transit:** SRA splits data in-transit between two encrypted tunnels to reduce the number of devices connected to the network, the number of open ports in the firewall, and, thus, the attack surface.
- **Preserving the Purdue Model:** All SRA deployment options adhere to the industrial cybersecurity best practice of preserving the Purdue Model, helping to ensure that one connection point does not provide broad network access.
- **Integrating with Antivirus Solutions:** SRA integrates with all ICAP-based antivirus solutions. This capability helps protect your industrial network from malware by increasing the safety of uploaded files necessary for carrying out remote maintenance and related tasks on industrial assets. In the event that such a file is malicious, SRA users will be immediately notified and prevented from uploading it to the respective asset.

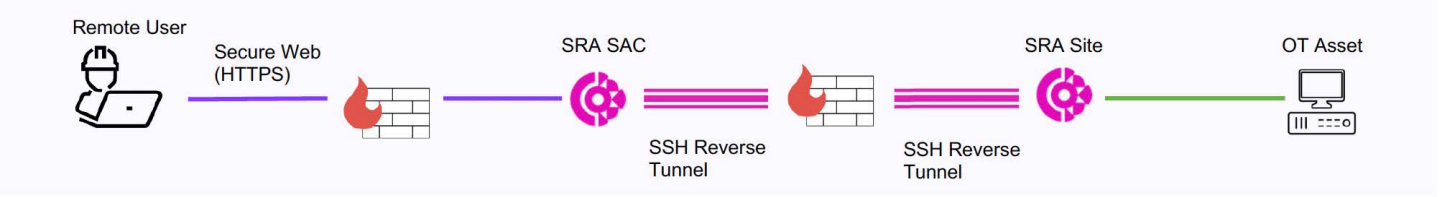

Fig 4: Diagram of SRA's encrypted tunneling

Monitoring Capabilities that Streamline Audits and Optimize Investigations

By offering comprehensive monitoring capabilities that far surpass the basic logging functionality and limited audit trails provided by most traditional remote access technologies, SRA enables you to gain full, real-time visibility into SRA users' activity, streamline audits, and optimize incident investigations. Highlights include:

- **Live, Over-the-shoulder Monitoring:** SRA administrators have the option to monitor active SRA sessions in-real time, allowing for easy troubleshooting, user supervision, and emergency termination of risky sessions whenever deemed necessary.
- **Full-length Video Recordings:** In addition to keeping detailed logs of all remote sessions, SRA automatically records a full-length length video of each session to support response actions, investigations, and audits.

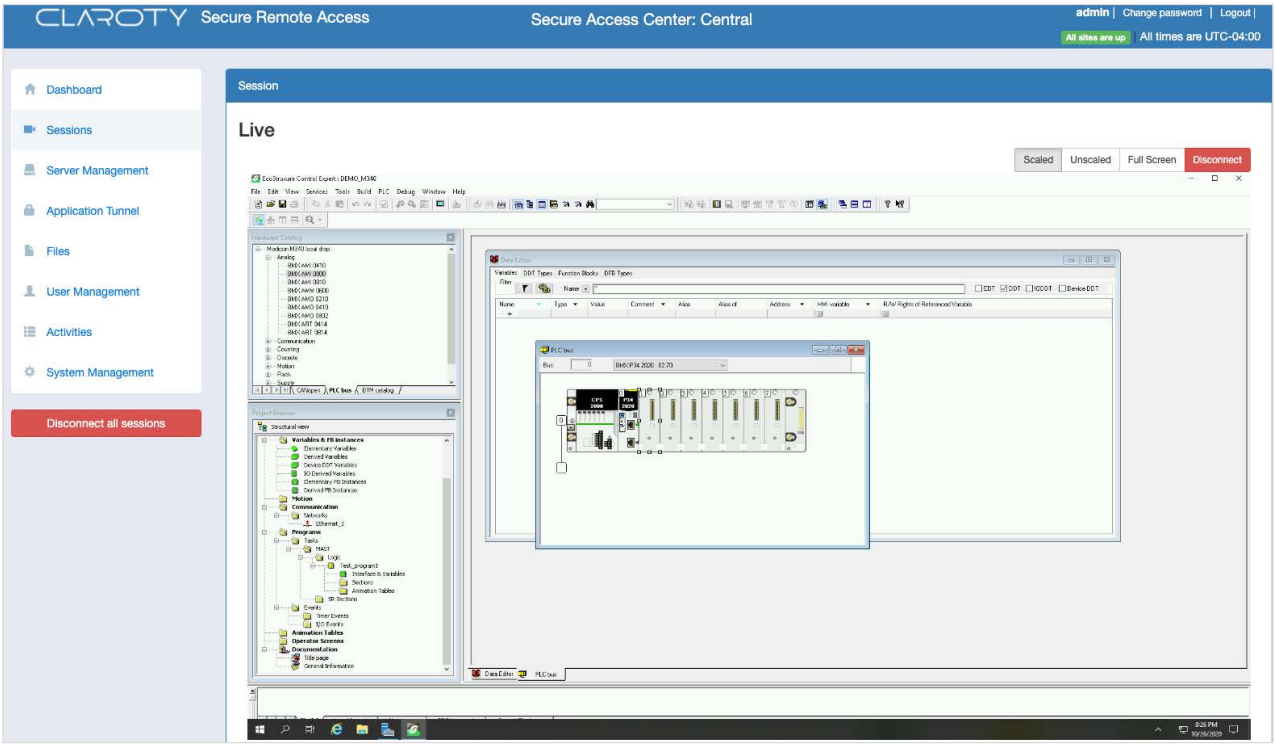

Fig 5: An SRA Administrator's live, over-the-shoulder view of a user's SRA remote connection

Extensive Support for Remote Incident Management

SRA integrates seamlessly with Claroty Continuous Threat Detection (CTD) to distinguish The Claroty Platform as the industry's first industrial cybersecurity solution to offer fully integrated remote incident management capabilities.

These capabilities span the entire incident lifecycle, enabling you to detect, investigate, and respond to industrial cybersecurity incidents across the broadest possible attack surface from any location. As a result, you can easily evolve and adapt your organization's overall security posture and workflows for a remote, distributed, and/or highly variable work environment. Highlights include:

- **Receive Alerts Related to OT Remote User Activity:** CTD triggers alerts when users partake in unauthorized or abnormal activities—such as configuration downloads or servicing assets outside of predetermined maintenance windows—while connected to the industrial network via SRA These alerts include details such as the SRA user, session intent, associated indicators, assets involved, and a root-cause analysis to support prioritization and triage efforts.
- **Investigate OT Remote User Activity:** All CTD alerts related to OT remote user activity include a direct link to the associated SRA session and the ability to monitor that session live. If the session is no longer active, the alert will link directly to a full-length video recording that can be viewed for investigation purposes.
- **Respond to OT Remote User Activity:** All CTD alerts related to OT remote user activity also enable administrators to immediately disconnect the associated SRA session if deemed necessary as a response action in order to prevent, contain, and/or remediate any damages caused by unauthorized changes or other activities conducted by OT remote users.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access.

Backed by the world's largest investment firms and industrial automation vendors, 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.

For more information, visit claroty.com or email contact@claroty.com.