CLAROTY
Clarity for OT Networks

Data Sheet

Secure Remote Access

Secure Remote Access

Secure Remote Access

SRA minimizes the risks remote users, including employees and 3rd party vendors, introduce to OT networks. It provides a single, manageable interface that all external users connect through, prior to performing software upgrades, periodic maintenance, and other support activities on assets within industrial control system networks.

The system enforces password management, authentication and access control policies for remote connections and monitors and records remote sessions. Network administrators employ SRA to proactively control which users are granted access to industrial control assets, for what purpose, and during what time windows.

Key Benefits

Secure Remote Access delivers organizations the following value:

- Isolate critical industrial systems from unmanaged and insecure VPN plus "jump box" scenarios
- Eliminate one of the most critical attack vectors that threat actors have used to gain access to industrial systems -- pathways that have been leveraged in multiple ICS attacks
- Remove the vulnerability presented by sharing passwords across internal teams or teams working for external contractors
- Enable granular auditing through video-based session recordings and detailed reporting with advanced filtering options

Use Cases

Network administrators have full visibility and control over 3rd party and employee accesses before, during and after a remote session takes place.

OT Plant/Operation can monitor and review remote sessions and validate that the user's stated purpose aligns with the actual session activity.

Security Teams and **Auditors** can validate that remote access control policies are being consistently implemented in industrial environments, watch active sessions, and review recorded sessions based on a risk assessment.

Capabilities

Secure and Isolate Remote Access

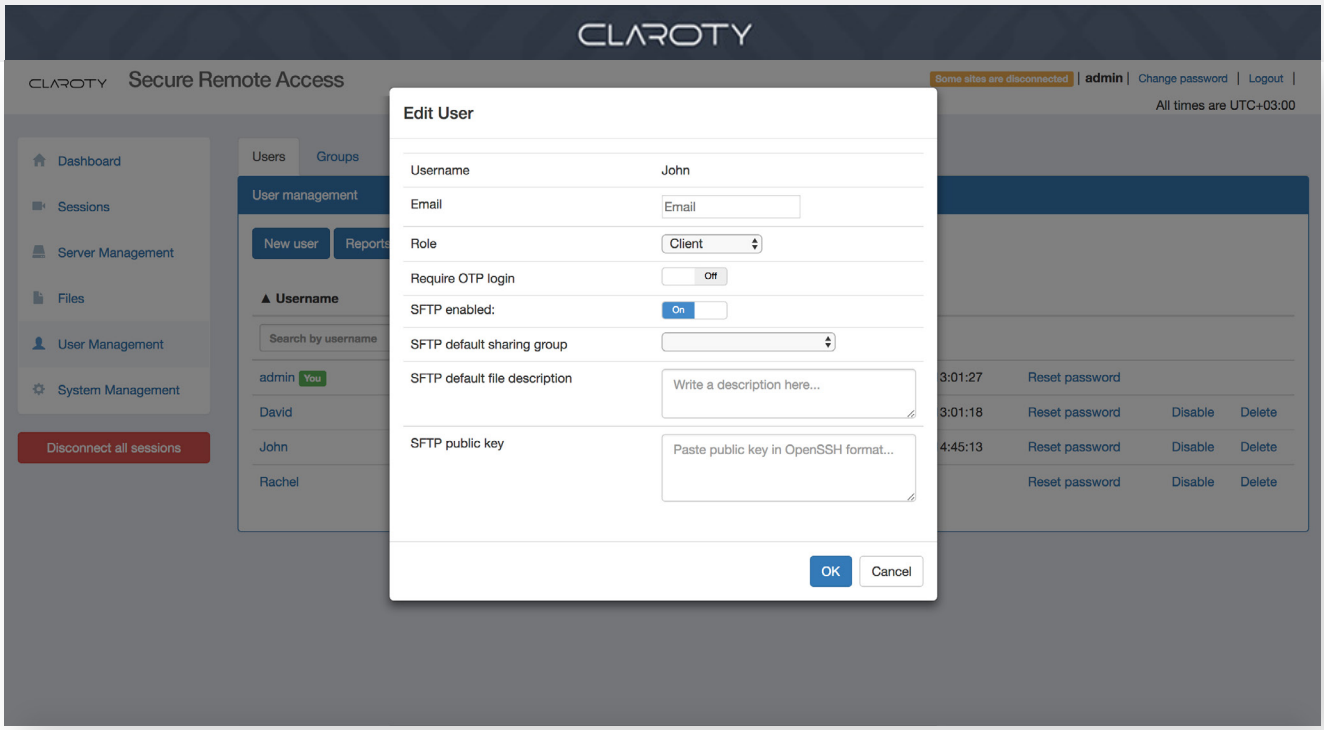
SRA acts as a security middleman between remote users and industrial network assets.
When a remote user logs into the web console, using two-factor authentication for example, the system fetches a replica of the requested asset's interface, accepts the user's input and forwards it only to the authorized asset.

The elimination of any direct interaction between remote users and network assets materially reduces the exploitability of 3rd party and other remote connections by threat actors.

Strict Access Control

With full visibility, network administrators have control over 3rd party and employee access before, during and after a remote session takes place. Leveraging a granular permission mechanism, administrators can define a policy of authentication requirements, allowed assets and sites, privilege and access times for each user or group. Additionally, they can view live remote session activity, review logs, and disconnect users using a "big red button" capability.

Following the initial definition of users/user groups, individuals access the web interface to gain access to specific assets (using RDP, VNC or SSH), request a remote session, or perform file transfers. The system includes capabilities to authenticate, process, securely send/retrieve files and document the session in a log file in addition to a live video recording for future audits.



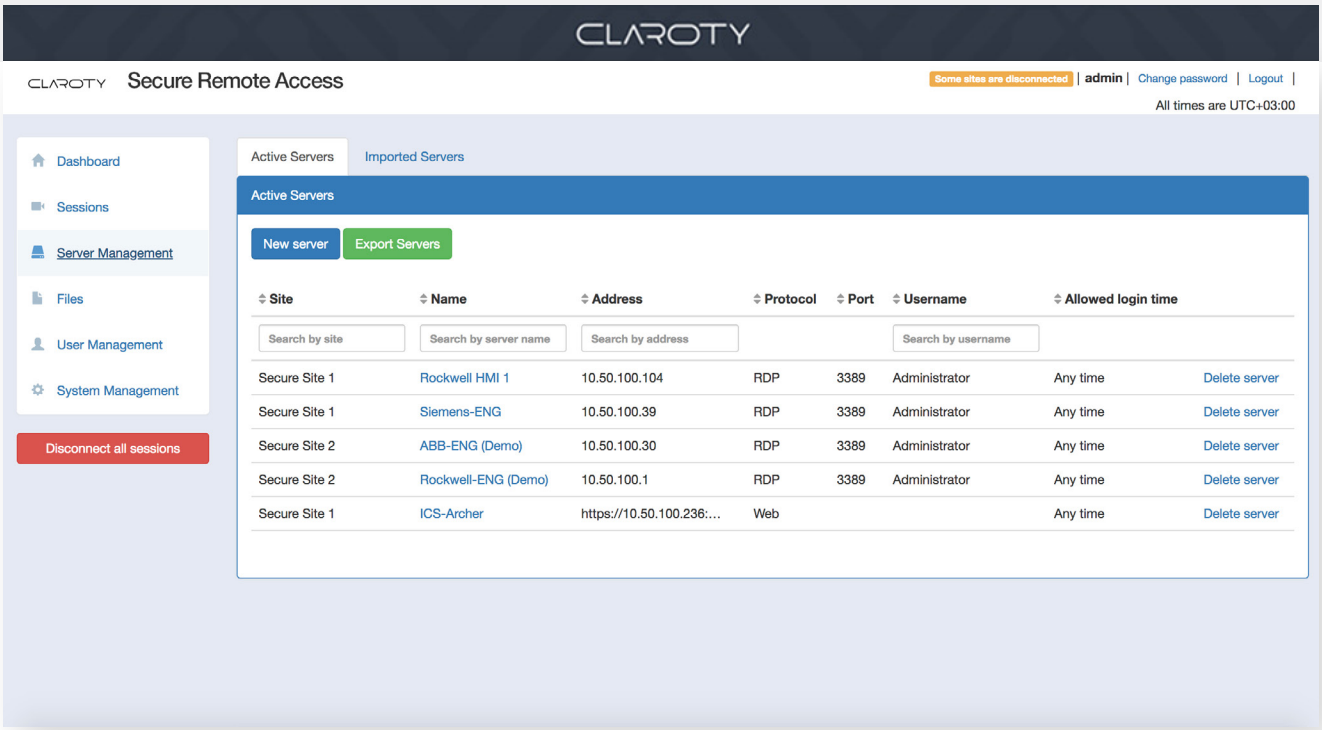
Granular Auditing

SRA allows system administrators to easily and effectively audit remote access sessions leveraging video recording of each session including detailed reporting capabilities:

- **Session:** detailing the sessions that have taken place and any comments that were made during those sessions.
  - Session documentation: video and reports (per either user/asset/sessions)
  - 'Red-button' to immediately terminate live connection for security concerns.
  - Real time visibility of ongoing session activities: logged in users, video view and user comments

- **User:** reports detailing users and user groups, the specific assets to which users/groups have access to, and when a last logged in occurred.
  - Email notification of pending requests.
  - Define for each user the authorized assets, time and authentication method, group association and file transfer permissions.
  - Optional two-factor authentication for increased security.
  - Password Vault: encryption and full control and management of all the actual asset passwords.

- **Asset:** reports detailing each asset in the system, who has access to them, and the total number of users who have access to each specific asset.



Capabilities

Secure File Transfer

A direction-agnostic security layer, coupled with its DMZ location, makes SRA the ideal gatekeeper for file transfer between two networks. As such, predefined endpoints within the OT network are configured to securely connect to the SRA server (similar process for remote users). Following the configuration, these endpoints are only allowed to interface between the two networks for inbound files such as firmware upgrades and AV updates, or outbound files that typically include raw operational data for analysis or log files.

This applies equally to both manual file transfers by human operators within the OT network and machine-to-machine (M2M) data sent by OT endpoints (often found in manufacturing sites).

Password Vaulting

Remote users wishing to access network assets authenticate directly with the SRA server and not with the assets themselves. This allows for full isolation where the asset's actual credentials are never exposed to end users or shared across teams. The SRA server stores and manages all remote users and industrial system passwords:

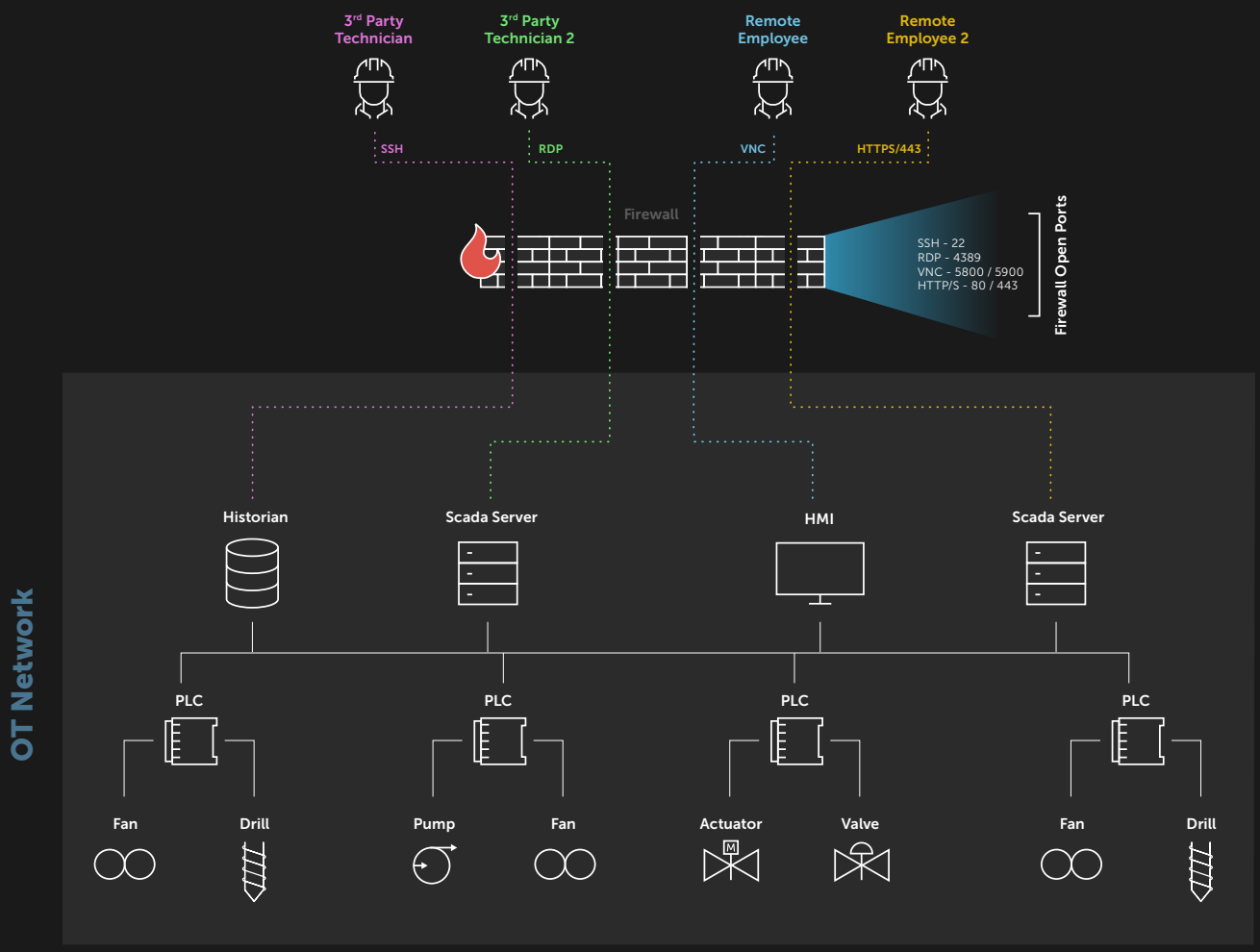
- **Eliminate shared passwords:** Removes the need to share passwords with multiple individuals or across 3rd party organizations.

- **Simplify substitutes:** Reduces the overhead associated with management of temporary or permanent user changes. Vaulting of the asset credentials in the server obviates the need for users to hand endpoint credentials over to a substitute. System administrators can quickly and easily delete former users while adding new ones.

- **Comply with password rotation policies:** Rotating passwords on a regular basis is an important security best practice. However, when rotating passwords in a shared password scenario, changes need to be coordinated across multiple individuals. In practice, password changes rarely happen or not at all, leaving systems exposed. SRA dramatically reduces this risk by eliminating the need to share passwords or to coordinate password changes by enabling strict rotation policies.

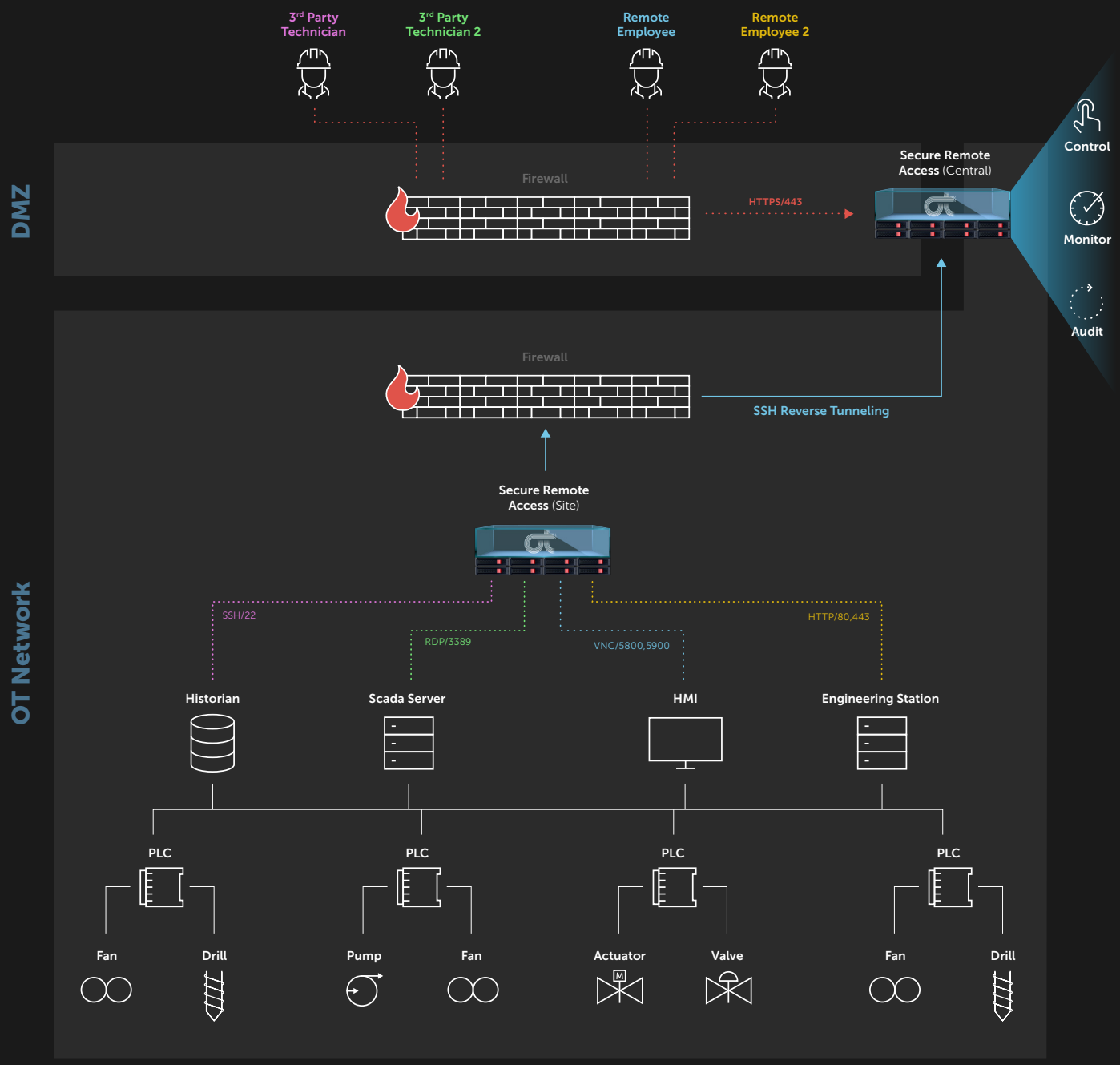
Secure Remote Access

Reference Architecture - Before



Secure Remote Access

Reference Architecture - After



This unique visibility provides a number of advantages including:

- **Monitoring:** While SRA enables system administrators to watch the entire remote session, CTD simplifies the monitoring process by generating an alert on the action that is taken. If, for example, a technician logged into SRA with the stated purpose of updating the firmware on a controller, system administrators can use CTD to proactively validate that a firmware upgrade was indeed performed.
- **Security:** If a contradiction between the stated remote access purpose and the actual activity occurs, system administrators can immediately terminate the remote session, preventing network disruption, and improving overall cyber resiliency.
- **Auditing:** Following the remote session, system administrators and auditors can playback a full video recording of each session, as well correlate specific reports filtered by user, asset or session to facilitate retrospective auditing.

Continuous Threat Detection

About Claroty

The Industry's Leading Industrial Cybersecurity Company

Claroty was conceived and is actively supported by the world famous Team8 foundry. With substantial funding from an unrivaled syndicate of global investors, including some of the most important industrial automation companies on earth, Claroty has built the leading company in industrial cyber today.

Claroty's technology has been tested, selected and adopted by the most influential industrial automation control vendors and networking companies in the world. Our strategic partnerships also include prominent system integration and managed security services firms worldwide.

Claroty has assembled an unprecedented executive team and attracted a premier interdisciplinary team of cybersecurity and industrial control system experts. We leveraged deep ICS knowledge and experience gained from industry and elite cyber units of the Israeli Defense Forces to design and build a platform for protecting your plants, processes and operations from cyber threats.

Claroty has very large-scale production deployments across six continents and nine industrial segments. With offices around the globe and an unmatched team, technology and partnerships, Claroty is the company that will be there to protect your critical industrial processes over the long-haul.

CLAROTY

Claroty was conceived to secure the safety and reliability of industrial control networks that run the world from cyber-attacks. The Claroty Platform is an integrated set of cyber security products that provides extreme visibility, unmatched cyber threat detection, secure remote access, and risk assessments for industrial control networks (ICS/OT).

www.claroty.com | **contact@claroty.com** |