Cyolo

Safely Connecting to Operational Technology

Cyolo vs. Claroty SRA

Industrial enterprises rely on Secure Remote Access (SRA) because it brings valuable benefits to the whole organization. While the methodology has evolved over time, the goal is to enable remote maintenance and troubleshooting of critical assets while reducing downtime and minimizing onsite visits. SRA enforces granular access controls, enhances security, and improves operational efficiency through streamlined processes. Since it strengthens the overall cybersecurity posture of industrial enterprises as well, it is not surprising that many are looking for next-generation ways to safely enable Secure Remote Access.

Claroty's SRA is designed for OT environments and offers role-based access control, session recording, and just-in-time access. However, it has some notable deficiencies.

- **Integration complexity:** Customers face challenges during the integration of Claroty SRA with existing infrastructure, requiring careful planning and coordination.
- **Virtual Private Networks (VPN) Dependency:** Reliance on VPN connectivity introduces complexity and lowers overall security.
- **Training and adoption:** Users must adapt to a new interface and workflows, necessitating training efforts for effective platform utilization.
- **Ongoing maintenance and support:** Sustaining and addressing technical issues with Claroty SRA may require dedicated resources and expertise.

The implementation of Claroty SRA presents several challenges. It demands a burdensome and time-consuming amount of installation and set-up which involves staging software components and network changes. Additionally, it requires external connections and the use of a VPN. The system requires integration with Identity and Access Management (IAM) systems, which can further complicate the implementation process and imposes limitations on enforcing least privilege access. The user interface, although somewhat intuitive, proves to be difficult to operate, demanding considerable attention and maintenance. Claroty's SRA relies on multiple technologies, such as tunneling protocols, network firewalls, and software components deployed on virtual machines or in the cloud, further adding to the complexity and potential points of failure.

In contrast, Cyolo's Zero Trust Access (ZTA) platform brings significant value to OT/ICS environments by providing secure and efficient remote access. It offers a range of features tailored specifically for OT, ensuring the protection of critical assets. The platform enables authorized personnel to securely access and manage OT systems from anywhere, reducing the need for on-site visits and minimizing downtime. It enforces strong access controls, ensuring that only authorized individuals can interact with sensitive OT systems. Cyolo ZTA enhances operational efficiency, streamlines maintenance processes, and strengthens the overall cybersecurity posture of OT/ICS organizations.

	Cyolo Zero Trust Access	Claroty SRA
Purpose Built for OT	✓	✓
Ease of Deployment	✓	
Offline Deployments	✓	
Zero Trust Traffic Routing	✓	
No VPN Required	✓	
Native Identity & Access Management	✓	
Agentless Deployment	✓	✓
Actual User Experience	✓	
No Network Changes	✓	
Just-in-Time Access	✓	✓
Supervisor Approval	✓	✓
Session Recording	✓	✓
Realtime Monitoring	✓	✓
Complete Analytics	✓	
Enforces Least Privilege Access	✓	
Connection Isolation	✓	✓
Granular Connection Control	✓	
Application Specific Access	✓	
Overall Ease of Use	✓	

OT/ICS organizations are increasingly adopting Secure Remote Access (SRA) solutions to address the evolving security challenges in their environments. One key driver is the need for remote maintenance and troubleshooting of critical OT assets located in remote or inaccessible locations. SRA enables authorized personnel to securely access and manage these assets from anywhere, minimizing downtime and reducing the need for on-site visits. Additionally, SRA helps organizations enforce granular access controls, ensuring that only authorized individuals can interact with sensitive OT systems. By implementing SRA, OT/ICS organizations can enhance operational efficiency, streamline maintenance processes, and strengthen their overall cybersecurity posture.

When looking at Claroty and their SRA (Secure Remote Access) solution, it is clear it was specifically designed for Operational Technology (OT) environments. It aims to provide secure access to OT assets while minimizing risks and ensuring operational continuity. Claroty SRA offers a range of features tailored for OT, including role-based access control, session recording, and support for various OT protocols. It provides a user-friendly interface that mirrors the on-premises experience, enabling easy navigation and minimal training requirements. The solution emphasizes protocol isolation, ensuring that interactions between users and OT assets are secure and protected from potential threats.

However, the offering has certain deficiencies that need to be considered.

- **It requires significant setup and configuration. Often, the initial work involves complex integrations with existing network infrastructure. This can lead to challenges during deployment, potential misconfigurations, and increased dependency on IT teams for implementation and maintenance.**
- **It lacks data stream protection. Claroty SRA does not provide video streaming or similar mechanisms to protect direct access to live data streams. This can be a concern, as it leaves a potential vulnerability where threat actors could insert malicious commands into conversations between users and OT assets.**
- **Dependency on the cloud. While introducing additional complexity and potential points of failure, Claroty SRA relies on cloud connectivity for many advanced funcitons. Organizations relying on the cloud-based version may experience disruptions in access if there are outages with the cloud service provider.**

Overall, while Claroty SRA offers valuable OT-focused features, organizations considering the adoption of Claroty SRA should carefully evaluate these limitations and assess whether the solution aligns with their specific OT security requirements.

Cyolo