safous

SRA IN OPERATIONAL TECHNOLOGY

A Complete Guide to Secure Remote Access for OT Environments



Table of Contents

03 Executive Summary

04 The Evolving OT Landscape

05 What Is Secure Remote Access (SRA)?

06 Challenges of SRA Implementation

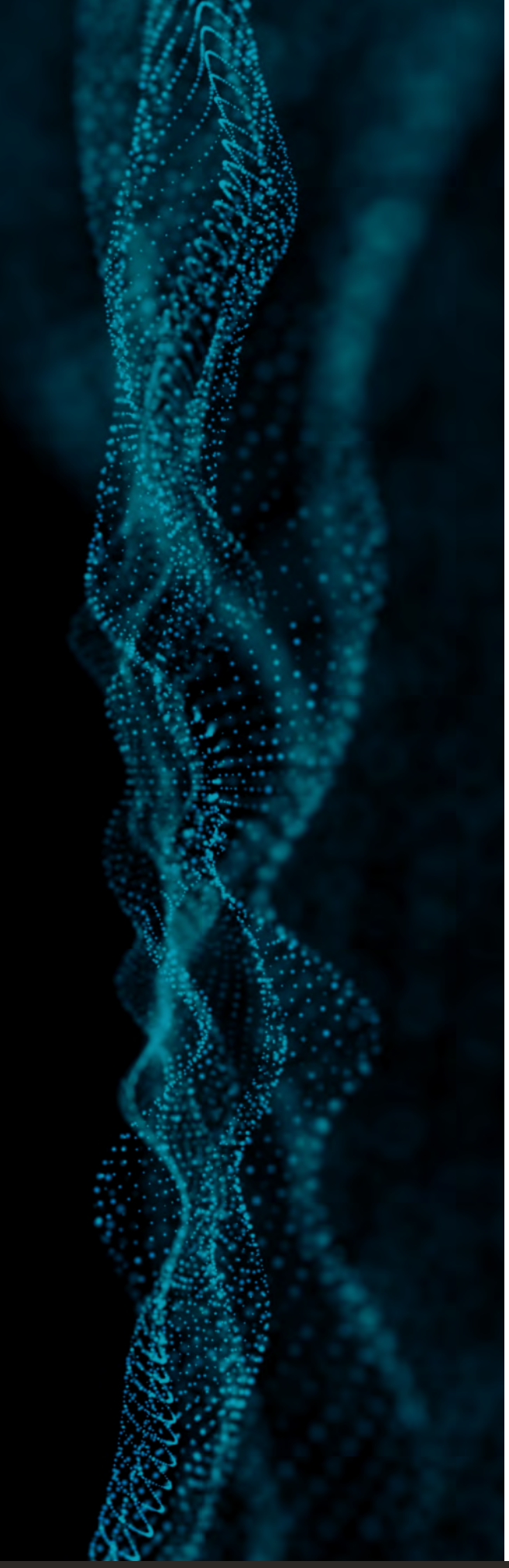
07 Best Practices for SRA in OT Environments

09 Real-World Applications of SRA in OT

10 Why Choose Safous for SRA?

11 Take the Next Step With Safous





Executive Summary

Operational technology (OT) environments are becoming increasingly connected, enabling advancements in efficiency, monitoring, and automation. However, this connectivity has also created heightened cybersecurity risks. **Nearly 70% of industrial organizations suffered an OT cyber attack in the past year,**[1] according to a 2024 report by Palo Alto Networks. As attackers exploit vulnerabilities in these expanding attack surfaces, securing OT environments has never been more critical.

Secure remote access (SRA) provides a framework for ensuring safe and controlled remote connectivity to OT systems. In this white paper, we'll explore the challenges and solutions associated with securing OT environments and how you can leverage SRA to safeguard your critical infrastructure.

1. https://www.paloaltonetworks.com/resources/research/state-of-ot-security-report

The Evolving OT Landscape

OT systems, once isolated from IT networks, are now integral to connected digital ecosystems. This integration introduces vulnerabilities like:

- **Increased Attack Surface:** Connectivity exposes OT systems to malware, ransomware, and other external threats.
- **Legacy Systems:** Many OT environments rely on outdated infrastructure that lacks modern security measures.
- **Infrastructure Disruptions:** Cyberattacks on OT systems can disrupt essential services like energy, transportation, and manufacturing.
- **Scalability Concerns:** If SRA solutions can't scale to accommodate new users, devices, and apps, it can lead to resource constraints and lower effectiveness.
- **Vendor Dependencies:** Dependence on third-party vendors for security updates and maintenance can delay responses to emerging threats.

Want to learn more about the risks modern OT environments face? Read our **guide to OT security.**



What Is Secure Remote Access (SRA)?

Secure remote access (SRA) is a framework designed to enable secure remote connectivity to OT environments. SRA ensures authorized personnel – employees, contractors, or vendors – can access critical systems without compromising network security.

Core features of SRA include:



Data Encryption:
Protects data during transmission for secure communications.



Role-Based Access Control (RBAC):
Limits access to specific resources based on user roles.



Multi-Factor Authentication (MFA):
Adds layers of verification to strengthen access control.



Network Segmentation:
Prevents threats from moving laterally within the network.

Challenges of SRA Implementation

While SRA strengthens OT security, businesses implementing these solutions may face challenges like:



Legacy Systems:
Integrating modern SRA tools with older infrastructure often requires customized approaches.

Compliance Requirements:
Industries like energy and healthcare face regulatory demands, such as NIST, ISO 27001, and sector-specific guidelines.

Operational Downtime:
Transitioning to SRA must be carefully managed to avoid impacting critical operations.

Limited Visibility:
Only 5% of organizations report having complete visibility of OT systems,[2] which can hinder real-time threat detection and response.

2. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Best Practices for SRA in OT Environments

Here are a few steps you can take to implement SRA into your OT environment effectively:

01 **Adopt Zero Trust Principles:**
Implement the "never trust, always verify" model to secure every access request.

02 **Monitor Continuously:**
Deploy tools that provide real-time visibility into user activities and detect anomalies promptly.

03 **Set Granular Access Controls:**
Apply the principle of least privilege to minimize potential damage from compromised accounts.

04 **Encrypt Communications:**
Encrypt all remote sessions to prevent hackers from intercepting your data.

05 **Segment Your Network:**
Divide OT systems into smaller, isolated segments to limit the spread of potential threats and protect your assets.



Best Practices for SRA in OT Environments (cont.)

06 **Leverage MFA:**
Require multiple forms of verification for all remote access attempts to ensure only authorized users gain entry.

07 **Secure Vendor Access:**
Use SRA to manage third-party vendor access carefully and reduce risks to your OT systems.

08 **Review Security Policies:**
Stay ahead of new threats by updating your SRA policies and configurations.

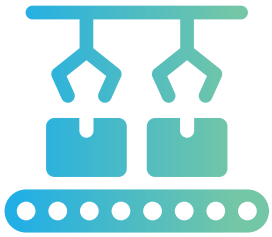
09 **Conduct Security Assessments:**
Regularly evaluate your OT environments to keep your defenses strong and aligned with the latest risks.

By following these best practices, you can secure your OT environments without disrupting operations – and gain peace of mind that your systems are protected.



Real-World Applications of SRA in OT

Still not sure how secure remote access can benefit your OT systems?
These scenarios showcase how organizations leverage SRA:



Manufacturing Plant:

A manufacturing company might use SRA to secure remote access for supply chain vendors that manage inventory levels or coordinate deliveries. Implementing MFA and RBAC would let them restrict vendors' access to only the systems they need, minimizing risks while maintaining operations.



Energy Provider:

An energy provider that faces frequent ransomware threats can use SRA to secure their operational systems. Enhancing data protection would contribute to reduced ransom payment risks and improved regulatory compliance.



Utility Provider:

A utility company could use SRA to support remote access for maintenance teams working on city-wide infrastructure. Implementing features like session monitoring would help them maintain uptime by responding to security incidents faster.

Why Choose Safous for SRA?

As IT/OT convergence continues, scalable SRA solutions will be essential for organizations to secure their digital ecosystems. Safous Industrial SRA (I-SRA) extends zero trust security to OT/ICS environments, enabling users to securely access and manage critical assets remotely – whether they're responding to urgent alerts from home, performing routine maintenance from regional offices, or managing facilities across different time zone.

Safous I-SRA is purpose-built for industrial operations. It supports fast connections, provides a single-pane-of-glass view into segmented networks, and maintains end-user agility without disrupting workflows. Combined with our integrated Safous remote privileged access management (RPAM) features, which deliver complete control over remote access to privileged user activities, Safous I-SRA enables you to safeguard your entire industrial environment while maintaining efficient remote operations.





Safous Industrial SRA Features

Safous I-SRA minimizes your industrial network's attack surface by giving users asset access only.

Here's how:

- Identity-based, application-level access
- Continuous authentication and monitoring
- Ability to block risky actions in real-time
- Access request feature to grant access approval for critical operations
- Audit trail with session recordings, access logs, and user history
- Credential vaulting and retention
- Fast deployment, no change management

For more information about our solutions, explore our **OT security blog** to see how we can support your organization's journey toward comprehensive security.

Take the Next Step With Safous

Ready to secure your OT environment with cutting-edge **industrial SRA solutions?**

Contact us today to learn how Safous SRA can protect your industrial assets and simplify remote access management. Together, we'll create a more secure and resilient future for your business.



safous

www.safous.com