Secure Remote Access from Armis Centrix™

Zero trust granular access from anywhere, with the security you need everywhere.

Protecting Cyber Physical Environments with Secure Remote Access (SRA)

Armis provides a comprehensive Secure Remote Access solution for OT environments, utilizing zero trust principles to ensure granular, just-in-time access. With OT systems often complex and dispersed, and increasingly targeted by cyberattacks, maintaining robust access controls is crucial to prevent disruptions, data breaches, and insider threats. Powered by Xage, this solution enhances visibility, security, and control while ensuring “least privilege access” to mitigate risks and protect operational integrity.

Grounded in Zero Trust Principles

Identity-Driven Access
Transition from a network-centric to an identity-centric remote access model, where each identity establishes its own security perimeter.

Continuous Verification
Enhance your cybersecurity by eliminating all-or-nothing access, irrespective of the maturity of native device controls.

Least Privilege
Minimize your vulnerable attack surfaces, granting just enough access for just enough time to bolster cyber-hardening without disruption.

Secure Remote Access **Use Cases:**

Granular Policy based access designed to operate on a person by person basis

Armis’s SRA enhances comprehensive OT security by enabling the creation and enforcement of granular, identity-driven access policies between operational assets and remote users and applications. This advanced capability ensures that digital interactions are securely managed without the need for disruptive changes to existing infrastructure.

Secure Across Zones

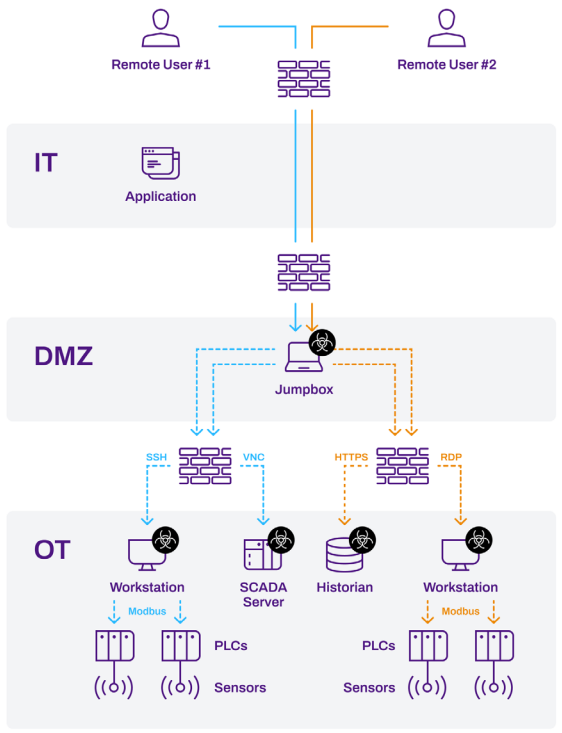
SRA bolsters Armis Centrix™ for OT/IoT Security by simplifying and securing connectivity through OT-IT DMZs. This eliminates the need to open multiple firewall ports for commonly used protocols like SSH, VNC, RDP, HTTPS, PROFINET, and Modbus. By doing so, it safeguards at-risk assets while maintaining productivity. Armis customers benefit from streamlined, secure access management that aligns with their operational requirements and enhances their security posture.

Protected Remote Access with Policy driven Access, Audit Trails and Session Recording.

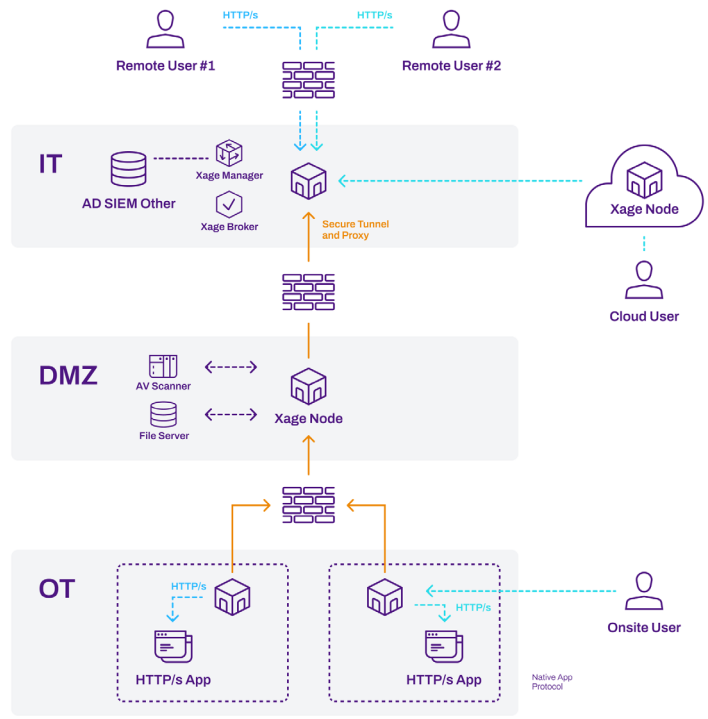
SRA strengthens Armis’s OT security offering by cyber-hardening virtually any cyber-physical system. It provides robust security controls including point-in-time access approval workflows, and role-based access policy controls, regardless of the native device capabilities. Additionally, it offers a unified interface for managing, monitoring and auditing all remote activities.

Armis Centrix™ for Secure Remote Access Features Key Benefits:

- **Built for OT Users:** Seamlessly integrates with complex production environments.
- **Meets Regulatory Pressures:** Helps organizations exceed compliance requirements like NERC-CIP, IEC 62443, and TSA Cybersecurity Directives, with minimal disruption.
- **Prevents Lateral Movement:** Controls machine-to-machine access, limiting threat spread and maintaining security across different infrastructure segments.
- **Unified Access:** Centralized, policy-driven access control for all assets and remote users, enabling granular, identity-based remote access.
- **Simplified and Secure:** Provides controlled, "just-in-time" access for remote operators, vendors, and partners.
- **Modernizes Security Controls:** Adds layers of security, such as Multi-Factor Authentication, Single Sign-On, and advanced secrets management, to virtually any device.
- **Session Collaboration:** Enables secure collaboration across remote access protocols (RDP, VNC, SSH), allowing users to invite others to active sessions.
- **Full Insight and Control:** Offers context-rich monitoring, identity-based logging, auditing, and session recording for complete visibility of remote access activity.
- **Mitigates Cyber Risks:** Blocks threats like malware and anomalous behaviors with dynamic access policies.



Before: Remote Access without Armis



After: Armis for Secure Remote Access