ARMIS®

SOLUTION BRIEF

Protecting Cyber Physical Environments with Secure Remote Access (SRA)

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

Landscape

Achieving proactive secure remote access begins with a holistic approach. Adopting a modern solution grounded in zero trust principles allows for granular, just-in-time access to individual assets. Armis understands the critical need for best-in-class Secure Remote Access capabilities in OT environments, as these systems are often complex, dispersed across different geos and in need of external access by authorized personnel. OT organizations are also increasingly targeted by cyber attacks, thus maintaining zero trust principles has never been more critical. Ensuring robust access controls in these settings is vital to prevent disruptions, data breaches, and unauthorized access (insider threats), all of which can have serious implications for safety and uptime. With Secure Remote Access powered by Xage, Armis delivers a comprehensive access control solution that enhances visibility, security and control for OT systems. This helps organizations maintain operational integrity and “least privilege access” that mitigates risks effectively.

The Limitations of the Current Approach

IT-centric remote access solutions

IT-centric remote access solutions often struggle to meet the complex demands of industrial environments, leading to a reliance on methods that can compromise security. Traditional VPNs, while commonly used, tend to offer all-or-nothing access, putting critical infrastructure at risk if a user’s credentials are compromised. This vulnerability allows attackers to gain unrestricted access to operational technology (OT) assets, which can have devastating consequences.

Cumbersome Firewall Rules

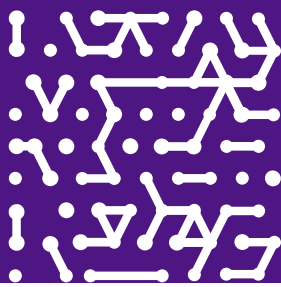
The management of firewall rules and network access control lists (ACLs) is often cumbersome, exposing systems to potential cyber threats such as ransomware and spoofing. These traditional security measures usually lack an understanding of OT protocols, making it challenging to implement fine-grained access policies.

PAM Tools Rarely Extend to all OT Assets

While jump servers and Privileged Access Management (PAM) tools are often necessary to enforce security, they often fail to extend protection to vulnerable OT assets like Programmable Logic Controllers (PLCs). This gap undermines the effectiveness of a least-privilege security model. Even the more advanced IT-centric solutions, though better than traditional VPNs, fall short in providing the necessary granular control over diverse OT devices, leaving industrial environments exposed to various threats. It is essential to select a remote access platform built to cater to cyber physical environments and the breadth of assets they house.

What If You Could?

- Enable external maintenance teams to access assets for ‘just-in-time’ windows?
- Block lateral movement and target discovery with machine-to-machine access control?
- Securely enable remote access to any device or service from anywhere?
- Protect against identity-based attacks with automatic credential rotation and elimination of default passwords?
- Unify access control across multiple cloud services and identity providers to minimize friction for administrators and end users?
- Stay operational even during service interruptions, with no dependence on internet/WAN connectivity?
- Simplify privilege management and revocation for all users, including authorized third parties?
- Enforce MFA, credential rotation, SSO for every resource?
- Align with the MITRE ATT&CK framework?
- Protect access to any application, workload, device, or data?
- Apply granular access controls, even when devices are offline?



Secure Remote Access based 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.

Key Use Cases

Identity-Driven Access

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. With SRA, Armis customers can seamlessly integrate sophisticated access controls, thereby improving overall security and operational efficiency.

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.

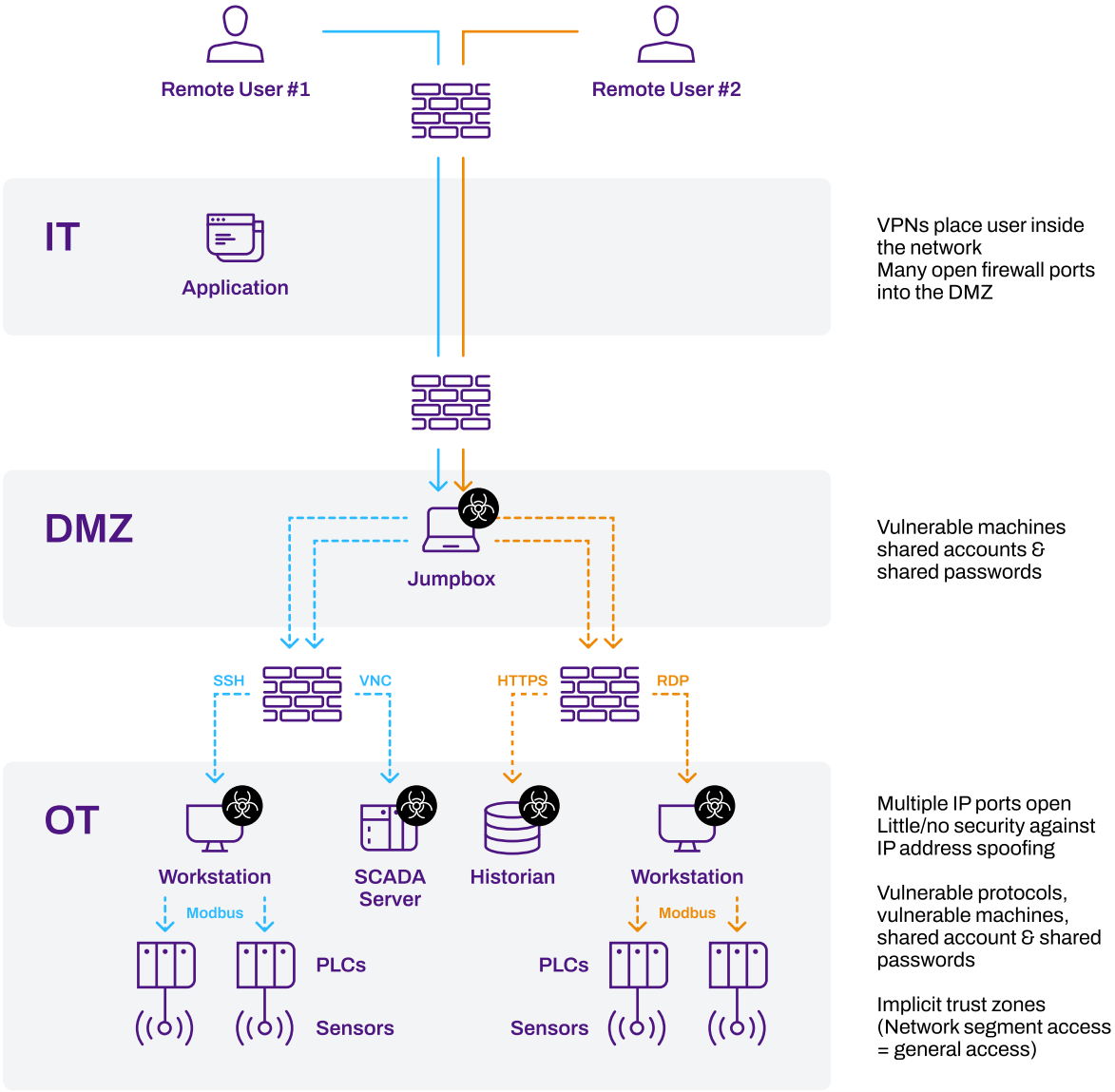
Protected Remote Access with Policy driven Access, Audit Trails and Session Recording

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. This single pane of glass improves incident response capabilities and helps demonstrate regulatory compliance and aligns with security frameworks, thereby providing Armis customers with unparalleled visibility, security and control over their remote access activities.

Secure Remote Access Before and After:

Without Armis

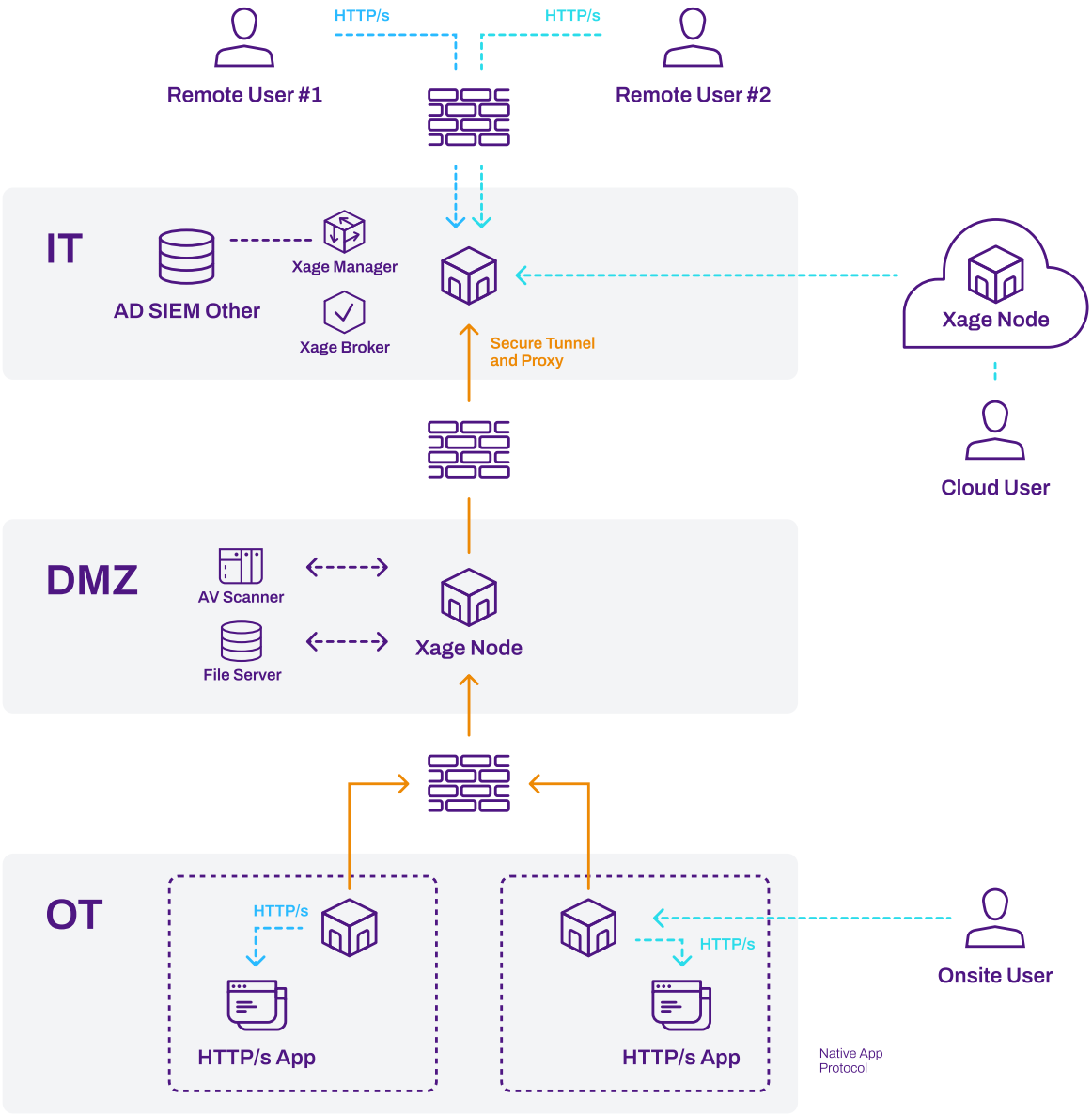
The contemporary operational landscape encompasses field/plant, control center, datacenter, and cloud deployments, facilitating intricate interactions among personnel, machines, applications, and data across these environments and external entities. Current methodologies must evolve to ensure that when a user or application seeks access to a resource, it can be granted without creating vulnerabilities that expose systems to potential attackers. The outdated tools currently in use fail to deliver the necessary level of granularity required to maintain security integrity. It is imperative that we advance our approaches to safeguard against emerging threats effectively.



With Armis

Armis provides secure remote access to cyber physical environments with granular, identity-based access control for field and plant assets. By simplifying access management and replacing traditional security measures like firewalls, VPNs, and jump boxes, Armis reduces complexity and lowers operational costs.

Previously, remote access to OT assets was granted on a per-site or per-zone basis, often allowing unrestricted access with no logging or accountability. With Armis, every access event is authorized and authenticated, with multi-factor authentication (MFA) available down to individual assets, ensuring a higher level of security and control.



Feature Benefits

Built Specifically for OT Users

SRA considers the unique needs of both first and third-party users, our solution is designed to seamlessly integrate into the complex production environments in which they operate. It ensures compatibility and efficiency across various operational setups. Achieve robust identity and access management solutions for every device, including legacy assets, PLCs, and other critical infrastructure components, thereby enhancing overall security and ensuring that even the oldest equipment remains protected against modern threats.

Meet the Increase in Regulatory Pressures

Governments are acting to protect environments that underpin national security and public safety, these regulations mandate stricter compliance measures and necessitate advanced protective solutions to safeguard critical infrastructure and ensure the continued safety of essential services. Rapidly meet and exceed compliance requirements and industry standards, such as NERC-CIP, IEC 62443 (the only secure remote access solution to comply with IEC 62443), and TSA Cybersecurity Directives. With SRA pragmatic controls to improve your industrial cybersecurity posture immediately without adding risk or requiring disruptive changes.

Prevent Lateral Movement

Stop lateral creep within your network with machine-to-machine access control, limiting the potential spread of threats and maintaining compartmentalized security across different segments of your infrastructure.

Unified Access

Managing access on a policy basis enables you to centrally create and enforce unified, granular identity-driven remote access control policies across all your operational assets and remote users.

Simplified and Secure

Whether you are a remote operator, a third-party maintenance vendor, or a supply chain partner, you'll have the same experience and only have the access required for the job function at hand. Set 'just-in-time' access windows to allow external teams to access your environment and provide essential maintenance. This controlled access minimizes the risk of unauthorized entry while ensuring that necessary updates and repairs can be conducted efficiently.

Seamlessly Modernize and Elevate Security Controls

Embrace cybersecurity best practices by adding new layers of security controls to virtually any device. Enact Multi-Factor Authentication (MFA), enable Single Sign-On (SSO), implement advanced secrets management, and more – regardless of the maturity of the native device capabilities.

Enable Session Collaboration Across Any Remote Access Protocol

Boost user productivity, maintain separation of duties, or speed up technical support with session collaboration across any remote connectivity protocol, including RDP, VNC, and SSH. SRA makes it easy to securely invite other users to active remote sessions with full or view-only control seamlessly – even for air-gapped and private on-premises networks.

Full Insight and Control of Remote Sessions

Gain peace of mind with unmatched monitoring of all remote access activity. SRA unlocks context-rich insights, including identity-based logging, auditing, traceability, and session recording. You'll always know who is accessing which assets, even if the devices lack unique user accounts, without additional agents or software installed throughout your OT environment.

Mitigate the Risks of Malware and Uncover Anomalous Behaviors

Proactively block cyber risks before they can wreak havoc across your industrial environment. Reduce vulnerable attack surface area with dynamic, granular access policies, as well as detecting and blocking a wide range of threats – insecure network protocols, unusual interactions between assets, malicious software, and more.

Summary

Armis is enhancing its OT security offerings with tailored solutions that significantly improve the daily operations of plant managers and personnel in remote cyber-physical environments. Our industry-leading zero trust remote access solution, powered by Xage's advanced technology, delivers a secure, unified approach to managing remote access across operational landscapes.

This initiative addresses the urgent need for stronger security measures in OT environments that are increasingly susceptible to cyber threats. By implementing identity-driven remote access that is continuously verified and governed by least privilege principles, we support our clients in maintaining operational integrity, mitigating risks, and complying with rigorous regulatory standards.

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial