Cybersecurity INSIDERS RECOMMENDED

PRODUCT REVIEW: REDEFINING OT ACCESS SECURITY WITH SAFOUS INDUSTRIAL SRA

safous
THINK YOUR ACCESS

WHEN ISOLATION ENDS - THE ACCESS RISK RESHAPING OT SECURITY

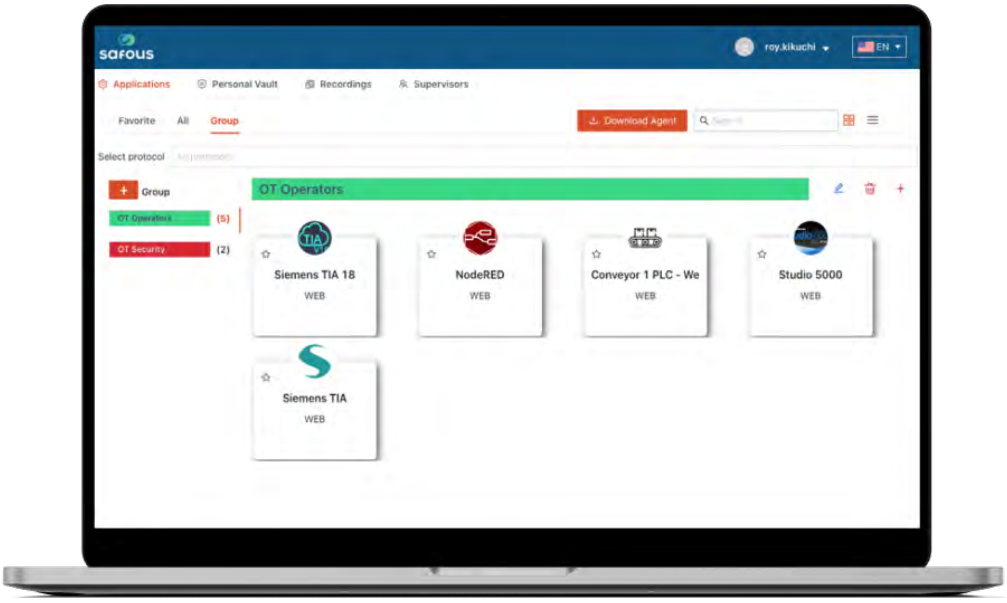
For decades, industrial environments relied on physical isolation to protect critical systems. Air-gapped networks, disconnected from the internet and often managed outside corporate IT, created a natural barrier against cyber threats. But as digital transformation accelerates, that barrier has all but disappeared.

Today, third-party vendors connect directly to production systems. Global dashboards aggregate real-time field data. Remote access enables diagnostics and analytics — increasing efficiency but also expanding the attack surface. These are not marginal enhancements; they mark a structural erosion of the divide between IT and OT.

Access-related risk has surged. Many organizations now permit external access via VPNs or RDP — often with minimal oversight. IBM reports that over 50% of organizations experienced a third-party-related security incident in 2022, with 70% affecting OT systems. These breaches rarely involve sophisticated exploits — they stem from compounding shortcuts: temporary VPNs, default credentials, and ad hoc firewall changes.

This risk is magnified by the use of IT-centric tools in OT environments. Enterprise solutions assume centralized management, regular patching, and modern identity governance — assumptions that rarely apply in OT. VPNs often flatten network segmentation, granting overly broad access to sensitive assets.

Mitigating this risk requires more than compensating controls. It calls for a purpose-built solution: one designed specifically for industrial realities. That's what Safous Industrial Secure Remote Access (SRA) delivers.



Safous Industrial (SRA) - Zero Trust Network Access for OT

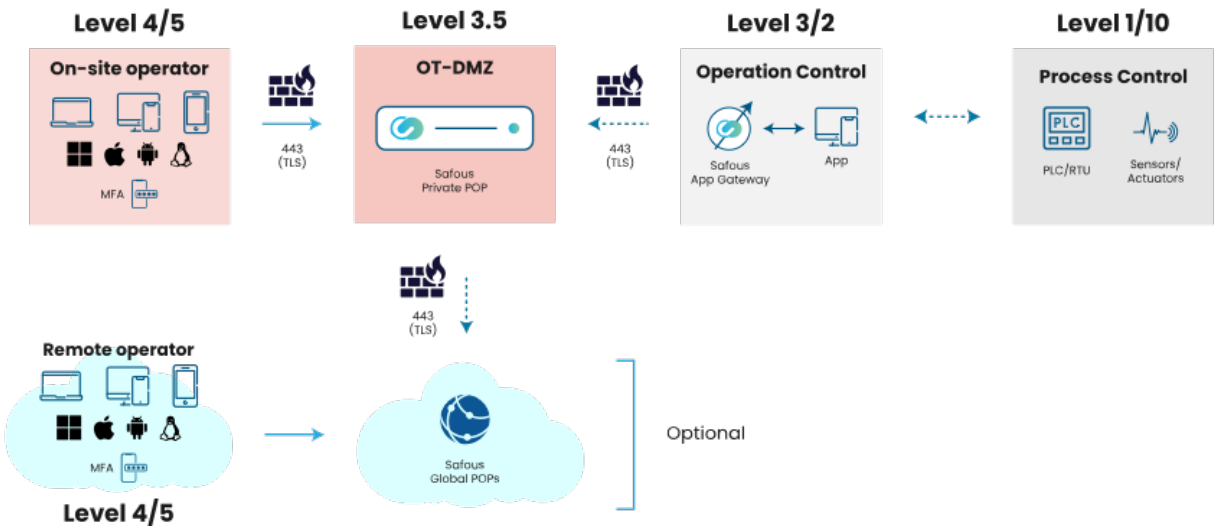
 Copyright © 2025 Cybersecurity Insiders. All Rights Reserved

A SECURE ARCHITECTURE BUILT FOR INDUSTRIAL CONSTRAINTS

Safous Industrial SRA is engineered from the ground up to respect OT boundaries. Its architecture adheres to the Purdue Model and enforces security without disrupting operations.

Each component is designed to solve a distinct OT challenge. Identity verification is handled through federated authentication and MFA, ensuring every access request is deliberate and verifiable. Sessions are routed through Private POPs — customer-dedicated points of presence that offer geographic flexibility and policy control.
At the heart of the model is the Safous App Gateway, positioned in the OT-DMZ. It brokers access at Level 3.5, abstracting connections to prevent users from ever touching Levels 3 or below. All traffic is outbound-only and encrypted via TLS, preserving segmentation and protecting air-gapped environments.

With this secure foundation in place, Safous enables a wide range of operational scenarios — from remote diagnostics to multi-site support — without exposing critical systems to undue risk.



Safely Connect Remote Operators While Keeping Air Gap Security Level

To meet operational needs, Safous includes:

- Just-in-time (JIT) access provisioning
- Full session recording (screen, keystrokes, metadata)
- Supervised access workflows for high-risk tasks
- Agentless compatibility with legacy and validated systems
- Support for both isolated environments and connected factory

 Copyright © 2025 Cybersecurity Insiders. All Rights Reserved

ENABLING SECURE ACCESS WITHOUT SACRIFICING UPTIME

In industrial operations, uptime isn't negotiable. Maintenance must be fast. Diagnostics must be remote. And access must be granted without compromising the predictability or safety of control systems.

Safous supports these realities across key OT workflows. Vendors can securely troubleshoot PLCs or SCADA systems without relying on VPNs. Internal engineers can support multiple sites without traversing fragile, region-specific infrastructures. Even unpatched or identity-lacking systems can be accessed safely through browser-based portals — scoped, recorded, and policy-bound.

This replaces shared credentials and one-off firewall changes with identity-aware, role-based access to defined applications. Sessions are ephemeral and logged automatically. The result is faster resolution, reduced risk, and greater operational confidence.

Real-world deployments show this at scale. A global manufacturer eliminated VPN chaos across 100+ sites by centralizing all third-party access through Safous. A regional water authority enforced disciplined access without altering its legacy SCADA environment or increasing IT overhead.

DESIGNED FOR OPERATIONAL REALITIES

Safous isn't a generalized ZTNA product repurposed for OT. It was built to fit industrial environments where downtime is unacceptable and change must be minimal. It assumes legacy systems, segmented networks, and regulatory oversight — and it works within those constraints.

Key design advantages include:

- Agentless operation for fragile or validated systems
- Outbound-only connectivity that maintains perimeter integrity
- Application-layer access that eliminates lateral movement

Safous also integrates into enterprise governance workflows:

- Logs can be forwarded to SIEM platforms like Splunk or QRadar
- Access policies can align with IEC 62443, NIST 800-82, and CMMC
- Authentication ties into existing identity providers via SSO, AD, or LDAP

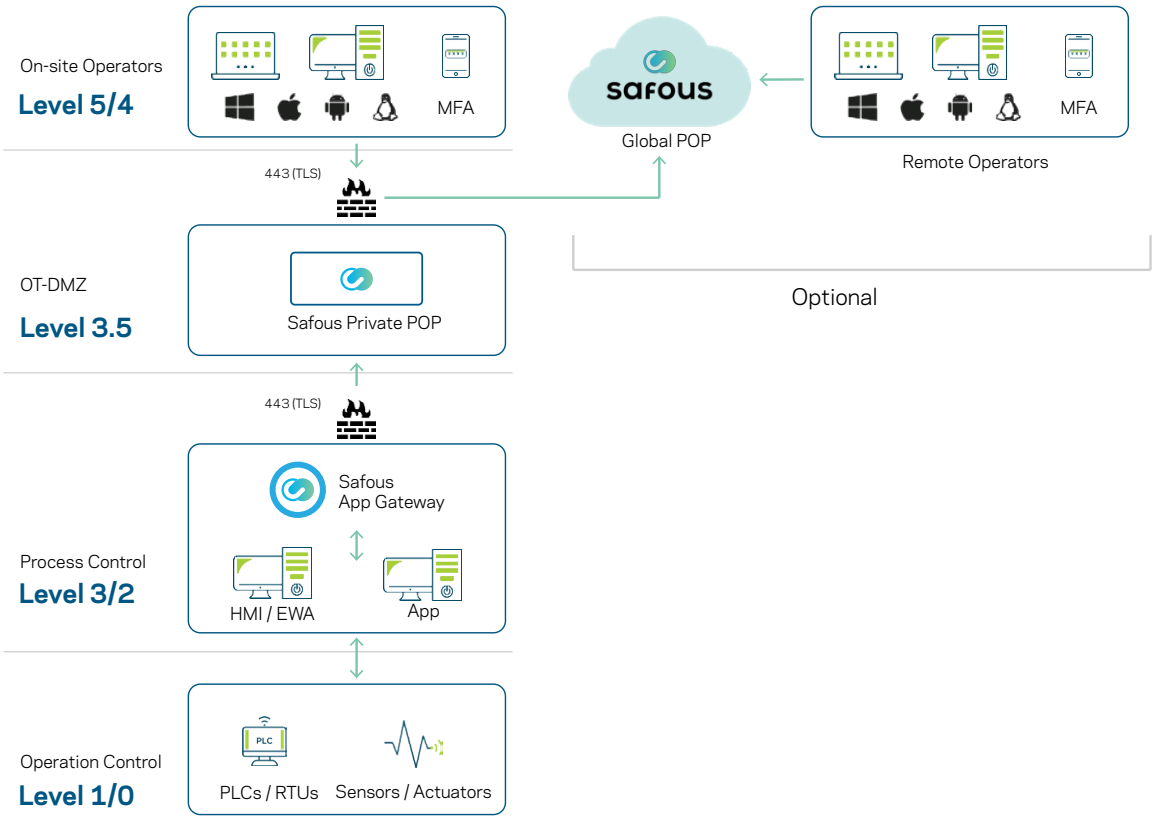
Whether deployed in a single plant or across hundreds of sites, Safous respects the unique operational context of OT environments while delivering enterprise-grade security controls.

 Copyright © 2025 Cybersecurity Insiders. All Rights Reserved

A MODERN BLUEPRINT FOR SECURE OT ACCESS

Safous Industrial SRA isn't simply a tool — it's a strategic control layer that modernizes how industrial organizations manage remote access. It replaces brittle, overprivileged pathways with granular, identity-driven workflows.

It delivers visibility for security teams, speed for operations, and governance for compliance. By design, it turns one of the most dangerous exposure points in OT — remote access — into a scalable strength. For organizations modernizing without margin for error, Safous Industrial SRA isn't just a better way to manage access. It's an operational imperative.



Safous SRA Architecture

To explore deployment options or schedule a technical consultation, visit:

www.safous.com/services/industrial-secure-remote-access

 Copyright © 2025 Cybersecurity Insiders. All Rights Reserved