

Secure Remote Access for the Mining Sector – Simplified

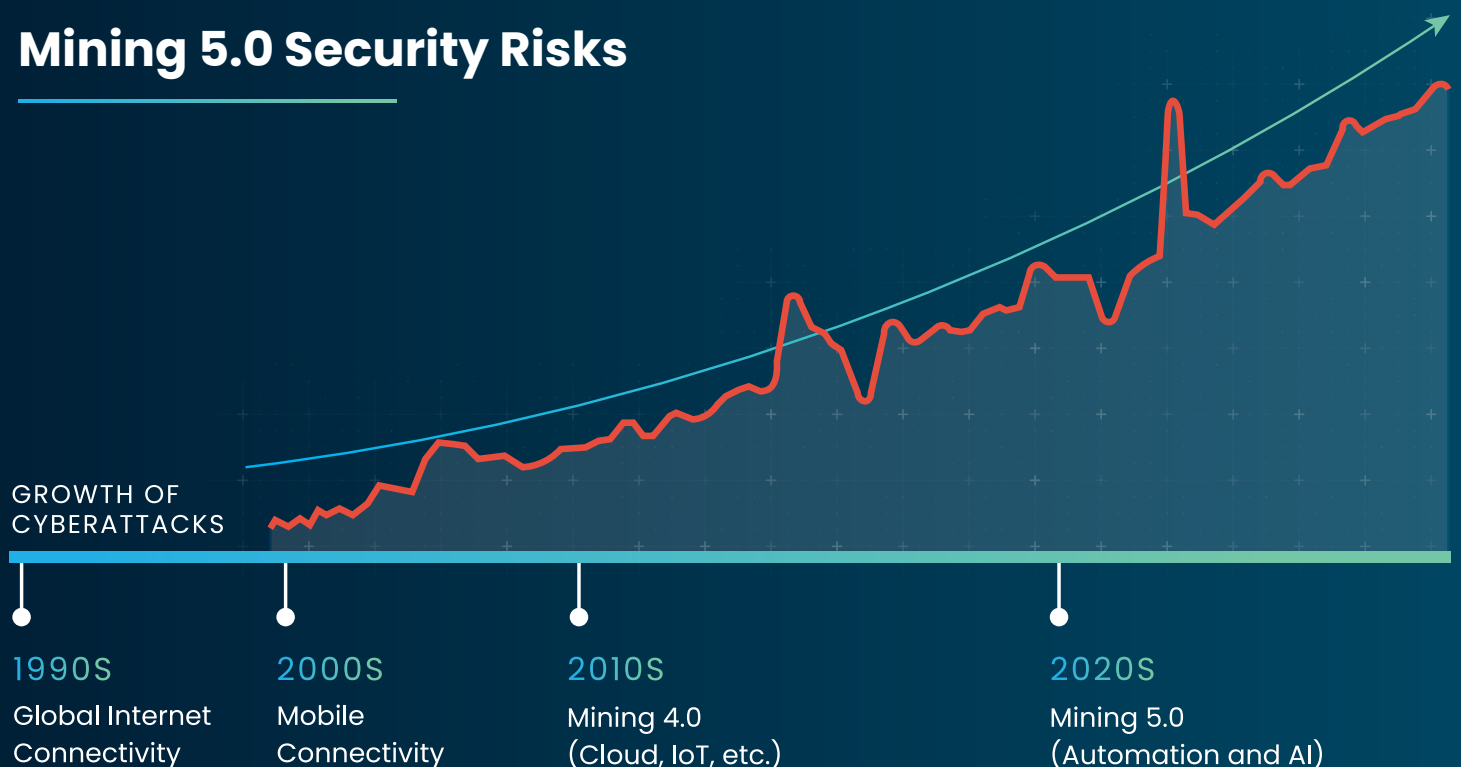
Safous Privileged Remote Access for Mining 5.0

Mining 5.0 – the next phase of mining transformation – combines automation and AI with sustainability and human-centered operations. But while this shift makes mining operations smarter, it also creates more digital entry points for attackers to exploit.

Every new connected device, from PLCs to autonomous vehicles to sensor networks, represents a potential target for cyber attacks designed to disrupt critical infrastructure – and many mining and metals are already experiencing a sharp rise in external threats.

Combating these increased risks and complexity requires mining companies to adopt a security strategy that doesn't slow performance. Safous Privileged Remote Access is purpose-built to provide this protection, combining privileged access management, identity and access management, and zero-trust network access into a unified platform that secures IT and OT environments without adding complexity.

Mining 5.0 Security Risks



As Mining 5.0 introduces new efficiencies, it also heightens risk. Increased reliance on remote connectivity to OT systems creates exposure that cybercriminals can exploit, and leveraging cloud and automation technologies increases this vulnerability.

Not convinced? A 2024 survey of mining and metals executives found that:¹

74%
said integrating
emerging technology is
their top cybersecurity
challenge.

61%
believe there are
too many potential
attack surfaces.

48%
are very concerned
about technology
infrastructure risks.

22%
said budgets are lower
than needed to address
cyber-related challenges.

1. <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/energy-resources/documents/ey-top-10-business-risks-and-opportunities-for-mining-and-metals-in-2024-final.pdf>

Case Study: Global Mining Operations Company



Scope:

50+ mining sites
across North America
and APAC



Users:

1,200 remote
maintenance
engineers and
third-party vendors



The Need:

Secure remote
access to SCADA
and PLC systems

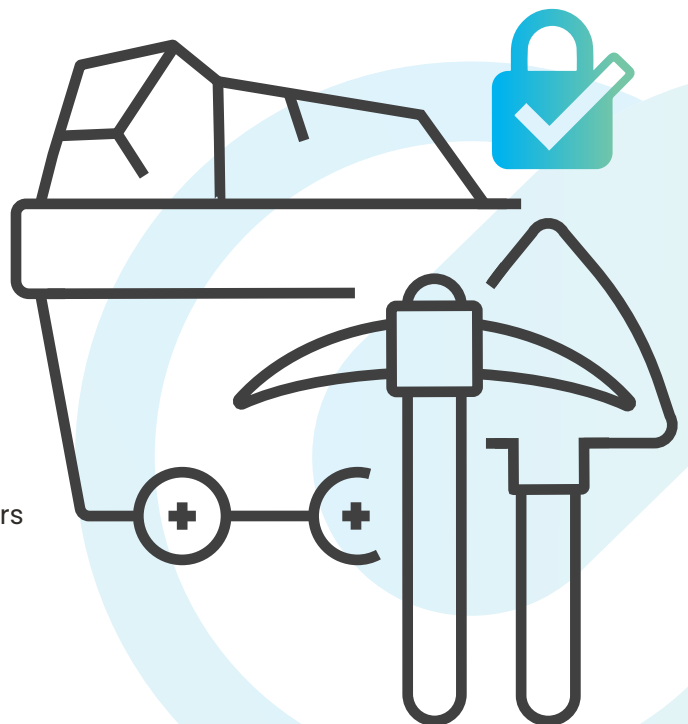
Challenges:

- ✗ Needed fast, auditable access for emergency OEM support
- ✗ Lacked secure file transfers for OT environment updates
- ✗ Inconsistent access management across geographically dispersed sites

Outcomes:

- ✔ Agentless remote access with MFA and credential vaulting
- ✔ Integrated ICAP file scanning with granular access controls
- ✔ No network topology changes required
- ✔ Secure OEM support enabled in minutes vs. hours
- ✔ Deployed globally across all sites in days

Safous' identity-based, agentless architecture enabled these outcomes – all without requiring changes to network topology.



Purpose-Built to Protect Critical Operations



Secure Remote Access:

Allow operators and third-party technicians to access SCADA systems for maintenance without a VPN or direct network access.



OT Asset Monitoring:

Securely access smart sensors and monitoring devices without deploying agents in sensitive environments.



Session Oversight:

Real-time alerts, supervised access, and time-bound permissions help prevent misuse and ensure every session is traceable.



Compliance Support:

Capture privileged sessions in real time to align with control requirements for ISA/IEC 62443, ISO/IEC 27001, and other standards.



Agentless Architecture:

No software to install on legacy OT devices keeps critical systems stable and reduces operational risk.



All-in-One Licensing:

A single subscription fee includes all privileged access management, identity management, and zero-trust network access features.



Global Plant Operations:

Centrally manage critical infrastructure across sites in APAC, North America, and EMEA from a single admin console.



Fast Time to Value:

With only one outbound App Gateway to deploy, you can go live in 3–5 business days without disrupting operations.



Business Outcomes

- Secure global connectivity
- Centralized management
- Safer mining operations
- Increased production
- Reduced costs & complexity
- Simplified compliance

Use Cases Across the Mining Sector



Facilitate Third-Party Access

Safely connect contractors and vendors to your OT environments for maintenance and support without exposing your production networks.



Provide OEM Access

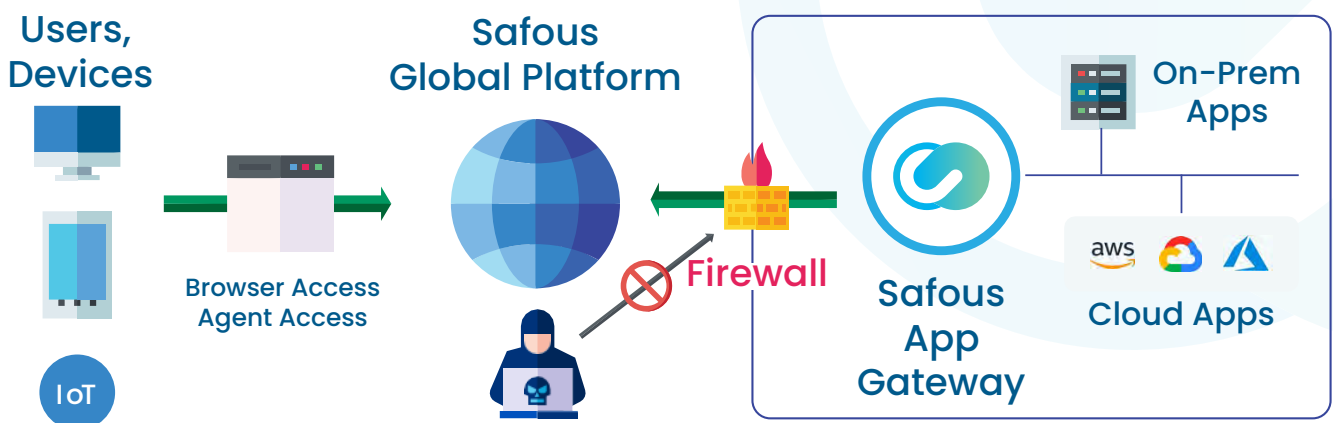
Enable rapid equipment support and emergency fixes while maintaining full audit trails and preventing unauthorized access to adjacent systems.



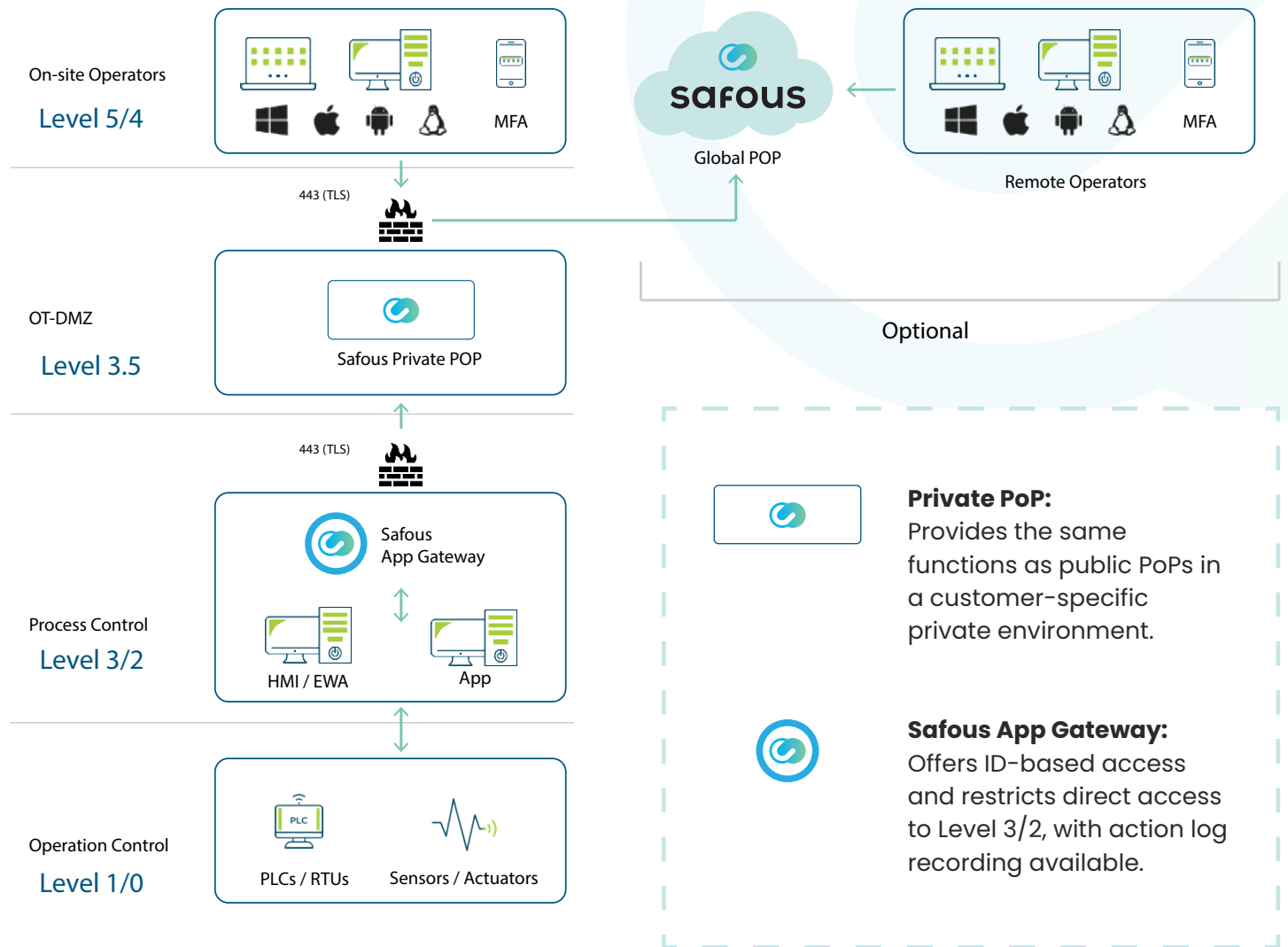
Manage Critical and Risky Access

Secure all access points to your mission-critical assets, whether on-prem or remote, with centralized governance and real-time supervision.

Safous Architecture



How Safous Secures Industrial Environments



Safous Privileged Remote Access Benefits

- Truly agentless – no software to install on target hosts
- Extends identity authentication and security to legacy applications
- SaaS + one outbound App Gateway deploys in 3–5 business days
- Flat subscription covers all privileged access, PAM, and IAM services
- Centralized governance and site-based administration
- On-prem & air-gapped with Industrial Secure Remote Access

Secure Mining 5.0 Operations With Safous Privileged Remote Access

Safous provides secure, compliant remote access for IT and OT environments with a globally proven Zero Trust platform, making it particularly well-suited for large, multi-site mining operations in APAC.

GET STARTED TODAY. →