

Simple, Secure Access for Modern Manufacturers

Safous for Automotive Manufacturing

Automotive manufacturing is becoming more interconnected as organizations adopt automation, artificial intelligence, and manufacturing execution systems (MES) across global plants. This shift is already well underway, with **97% of automotive manufacturers and their suppliers either currently using or actively evaluating smart manufacturing technology.**¹

But while these advancements improve efficiency, they also expand the number of systems and identities that require secure access. IBM's 2025 Threat Intelligence Index revealed that **manufacturing was the most attacked industry for the fourth year in a row** – and with **identity-based attacks making up 30% of total intrusions,**² it's clear that securing access management in manufacturing environments has become a strategic imperative.

Safous Privileged Remote Access provides agentless, Zero Trust access for automotive IT and OT environments, enabling secure operations without introducing complexity or disrupting production.

Automotive Manufacturing Security Risks

Robotics, smart factory systems, and original equipment manufacturers (OEMs) across the supply chain are more vulnerable than ever before. And with disconnected security tools and manual approval processes slowing response times, manufacturers need centralized oversight that supports secure vendor access while protecting production systems.

Not convinced? Check out these industry realities:

Auto manufacturers ranked cyber risk as their top concern in 2024.¹

60%
of incidents affecting auto manufacturers in 2024 had a high or massive-scale impact.³

92%
of these incidents were executed remotely.³

- <https://www.rockwellautomation.com/en-us/capabilities/digital-transformation/state-of-smart-manufacturing.html>
- <https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/2025-threat-intelligence-index>
- <https://upstream.auto/reports/global-automotive-cybersecurity-report>

Case Study: Global Automotive Manufacturer



Scope:
100+ global production sites



Users:
2,000 remote maintenance and support engineers



The Need:
Secure third-party and remote access to factory floor systems

Challenges:

- ❌ Complex login workflows slowed maintenance and emergency response
- ❌ No secure method for transferring files into OT environments
- ❌ Required fast, auditable access for OEM and supplier support

Outcomes:

- ✅ Agentless remote access with MFA and credential vaulting
- ✅ Integrated ICAP file scanning with policy enforcement
- ✅ No changes to existing network topology
- ✅ Secure OEM access enabled in minutes
- ✅ Global rollout completed in days, not months

Manage Access in Connected Manufacturing Environments



Remote Vendor Access:

Enable OEMs and suppliers to access PLCs, HMIs, and diagnostic systems without VPNs or direct network exposure.



Granular Controls:

Enforce least-privilege access using identity, role, and session context to ensure users only access authorized data and systems.



OT Asset Monitoring:

Secure access to robotics controllers, sensors, and monitoring systems without installing agents on sensitive devices.



Global Plant Operations:

Manage access to production assets across APAC, North America, and EMEA from a single administrative console.



Flexible Deployment:

Deploy on-prem, in hybrid environments, or fully offline for high-security facilities, without redesigning existing networks.



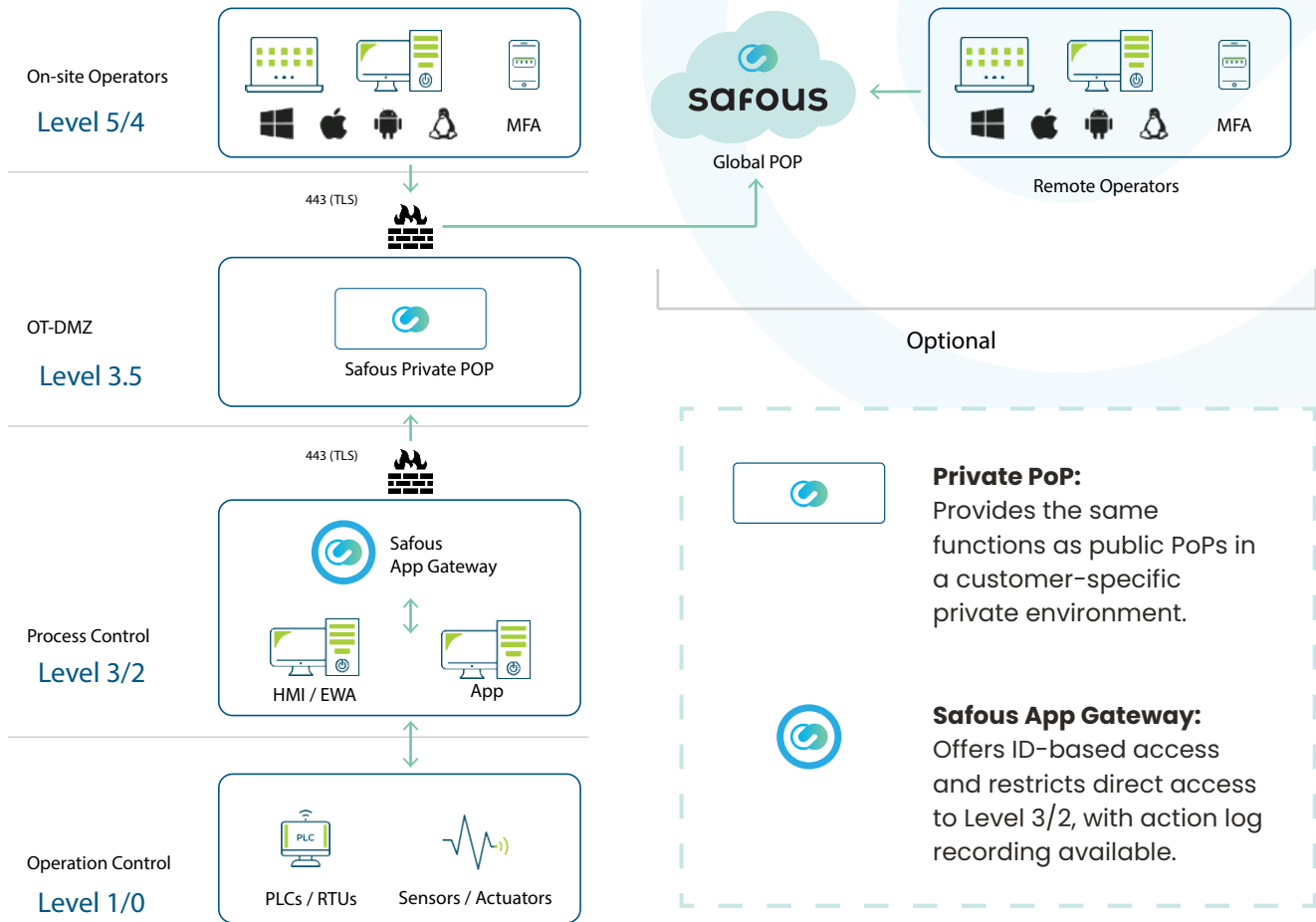
Simplified Compliance:

Enforce segmentation, supervision, and audit trails to support automotive industry security and compliance requirements. For detailed alignment with frameworks such as IEC 62443 and regional automotive guidelines (e.g., JAMA/JAPIA), please refer to the relevant checklists.

Industrial Outcomes

- ✅ Stronger OT security
- ✅ Centralized access control
- ✅ Safer factory operations
- ✅ Improved user experience
- ✅ Support for compliance requirements
- ✅ Fast deployment

How Safous Secures Manufacturing Environments



Safous Benefits

- Keep Data Within Trusted Boundaries:** Privileged access is brokered through Safous without exposing production networks or OT assets directly to users, vendors, or the internet.
- Low Impact Deployment:** Safous requires no software on PLCs, HMIs, or legacy OT systems, reducing operational risk and eliminating downtime during rollout.
- Centralized Governance Across Sites:** Manage all access policies, approvals, and oversight across global plants and suppliers from a single administrative console.
- Fast and Simple Operations:** Browser-based access, unified policies, and a single outbound App Gateway allow teams to go live in 3-5 business days with minimal operational overhead.

Secure Access for Automotive Manufacturers – Without Adding Complexity

Safous secures remote access for automotive manufacturing environments with a unified Zero Trust platform built to support IT and OT operations.

GET STARTED TODAY.