safous BY IIJ

DATASHEET:

Secure IT, OT, and IoT Environments With Safous

Discover how Safous secures corporate networks, industrial systems, and more through a platform that unifies Privileged Remote Access (PRA), Industrial Secure Remote Access (I-SRA), and Zero Trust Access (ZTA).

Most attacks targeting IT, OT, and IoT environments start with unsecured remote access or misused privileged accounts. However, traditional solutions like VPNs and legacy PAM platforms fall short – VPNs expose too much of the network, and PAM tools are too costly and complex to deploy. Organizations need a modern approach that delivers secure, compliant access without adding operational burden.

The Safous Platform

Safous offers a comprehensive cybersecurity platform purpose-built to provide end-to-end protection for every environment under a unified Zero Trust framework with integrated PAM. Its agentless, identity-based architecture enforces application-level access while simplifying compliance, so you can enable secure vendor and third-party sessions without exposing your network.

STRENGTHEN SECURITY AND REDUCE RISK

- **Limit Exposure With Application-Level Access:**
  Instead of giving users broad network access, Safous connects identities only to the specific apps they're authorized to use to minimize lateral movement risks.

- **Simplify Third-Party Vendor Onboarding:**
  External users can be provisioned without issuing credentials or granting full network access, reducing administrative burden and security risk.

- **Eliminate Standing Privileges:**
  Just-in-Time (JIT) access ensures users only gain temporary permissions when needed, preventing long-term credential abuse or leakage.

- **Enforce Real-Time Session Oversight and Controls:**
  Sessions are continuously monitored and recorded, and administrators can terminate connections or restrict actions if suspicious behavior is detected.

ENHANCE OPERATIONAL EFFICIENCY

- **Streamline Remote Access Across Environments:**
  Safous eliminates the complexity of jump servers and VPNs by enabling direct, audited access to IT, OT, and cloud systems through a unified platform.

- **Automate Provisioning Using Identity-Based Policies:**
  Grant access dynamically based on user identity, location, device posture, or other contextual signals to reduce manual overhead and human error.

IMPROVE USER EXPERIENCES

- **Offer Frictionless, Agentless Access:**
  Users can access applications securely through a web-based portal – no client installs, no VPN, and no added complexity.

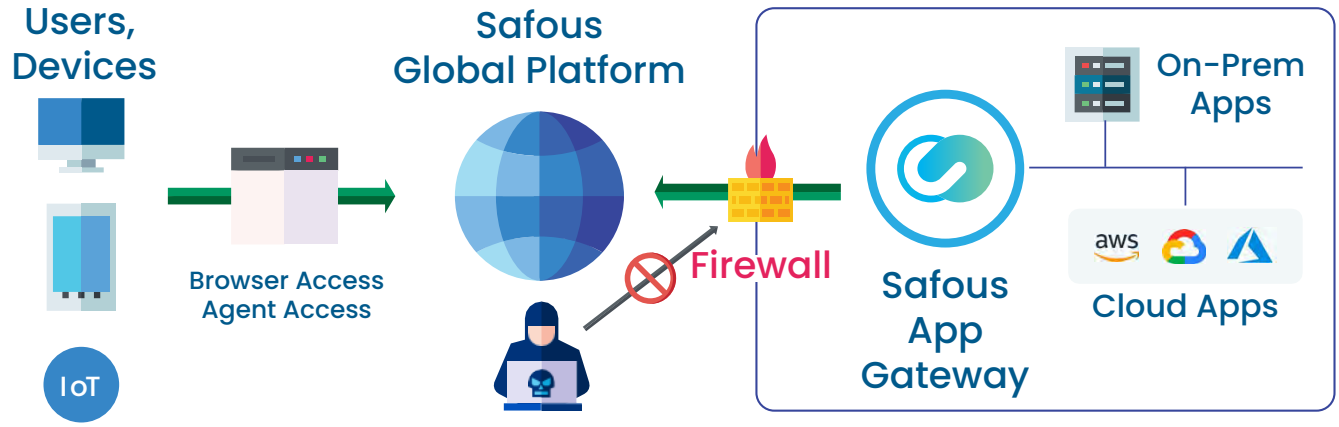
- **Support BYOD and Remote Work:**
  Safous doesn't rely on device management or endpoint agents, making it ideal for contractors, remote employees, and personal devices.

- **Simplify Authentication With Credential Injection:**
  Shared passwords and secrets are injected directly into sessions, improving usability while keeping sensitive data hidden from end users.

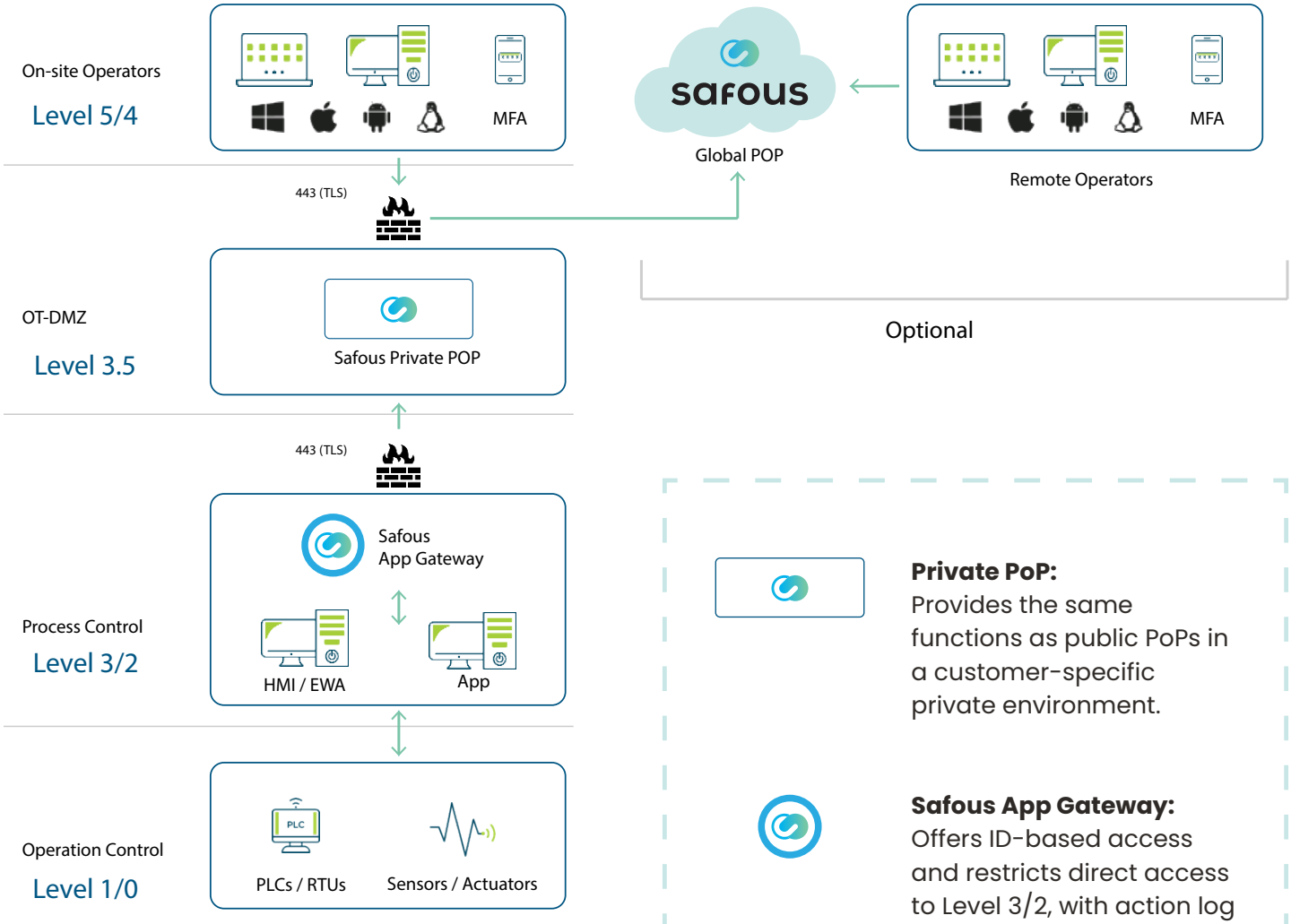
Safous Architecture

By combining Zero Trust principles like continuous verification and JIT access with Remote Privileged Access Management tools, Safous helps organizations minimize the attack surface and obscure critical applications from public exposure while providing seamless, policy-based access at the application level.

SAFOUS PRA AND ZTA



SAFOUS I-SRA



Private PoP:
Provides the same functions as public PoPs in a customer-specific private environment.

Safous App Gateway:
Offers ID-based access and restricts direct access to Level 3/2, with action log recording available.

Safous Features & Capabilities

Safous ensures secure access at every step – all while simplifying compliance and streamlining the user experience.

- **Internal IDP/MFA/SSO:** Functions as an IdP or IdP proxy, enabling centralized identity management, MFA enforcement, and SSO across all applications.
- **End-User Self-Operation Tools:** Offers self-registration, password reset, and lifecycle management features so users can manage their identities without IT intervention.
- **Remote Access Gateway:** Provides agentless HTTP/HTTPS, RDP, SSH, Telnet, VNC, SMB, and Browser Isolation connections, and agent-based access to any TCP/UDP protocols.
- **Access & Action Management:** Allows administrators to define conditions and actions for any access, user, and device, and manage all sessions, including controls for clipboard, file downloads & uploads, and session termination.
- **Session Audit & Recording:** Enables session recording and logging at the command level, with keyword search and audit trail capabilities to support investigations and compliance audits.
- **Zero Trust for Devices:** Supports device posture checks, managed device control, and browser isolation to ensure only trusted endpoints can initiate access.
- **Zero Trust for Users:** Supports identity federation, allowing secure logins via external IdPs and JIT authorization by time, IP, or location, or policy-based approvals.
- **Application Security:** Enforces malware, WAF, and DDoS protections at the cloud level to safeguard applications against OWASP Top 10 Threats.
- **Vault:** Stores and rotates credentials securely in a personal or shared vault, with password injection that prevents users from viewing sensitive login details.
- **JIT & Supervised Access:** Requires supervisor approval to access certain applications, and enhances security with live session oversight and the ability for supervisors to assist or take control.

IDENTITY

Feature	Technical Description	PRA	I-SRA	ZTA
Multi-Factor Authentication	Strengthens authentication with MFA for TOTP, email, and SMS.	✓	✓	✓
RBAC/ABAC	Enforces role-based and attribute-based access controls.	✓	✓	✓
IdP Integrations	Supports multiple IdP standards, including SAML 2.0, OpenID Connect (OIDC), and LDAP/AD.	✓	✓	✓
Dynamic Group Mapping	Automatically map users to groups based on SAML/OIDC attributes.	✓	✓	✓
Just-in-Time (JIT) Access	Grants time-limited access only when needed to reduce exposure.	✓	✓	✗
Zero Standing Privileges (ZSP)	Enforces least privilege by removing default access.	✓	✓	✓
Credential Injection	Securely injects credentials for RDP, SSH, TELNET, VNC, and SMB.	✓	✓	✓
Personal/Shared Vaults	Personal and shared vaults for passwords, API keys, private keys, and certs.	✓	✓	✓
Web Authentication	Supports web authentication with HTTP basic auth and web form login injection.	✓	✓	✓

APPLICATION

Feature	Technical Description	PRA	I-SRA	ZTA
Application-Level Isolation	Blocks lateral movement by isolating access to specific apps.	✓	✓	✓
Agentless/Agent-Based Access	Enable secure access to any resource without VPN or firewall changes.	✓	✓	✓
Live Session Monitoring & Control	Administrators can view and terminate active sessions in real-time.	✓	✓	⊗
Session Recording	Full session recording for RDP, SSH, VNC, and TELNET.	✓	✓	⊗
Command-Level Logging	Records CLI commands for audit and security purposes.	✓	✓	⊗
Clipboard/File/Session Controls	Restricts file transfer, clipboard usage, and session behavior.	✓	✓	✓
App Gateway Status Monitoring	Provides real-time visibility into App Gateway and system status.	✓	✓	✓
Application Health Checks	Ensures endpoint availability and security with health checks.	✓	✓	✓

COMPLIANCE

Feature	Technical Description	PRA	I-SRA	ZTA
Session Logs	Creates session logs with timestamps, commands, and actions.	✓	✓	✓
Activity Reports	Generates reports on access history and user activity.	✓	✓	✓
SIEM Integration	Compatible with Splunk, ELK, and other platforms.	✓	✓	✓
SMTP Configuration	Supports default and custom SMTP servers.	✓	✓	✓
Compliance Support	Aligns with compliance standards like SOC 2, ISO 27001, NIST, and HIPAA.	✓	✓	✓

ADMINISTRATION

Feature	Technical Description	PRA	I-SRA	ZTA
User Portal	Personalizable user portal with branding support for logo, colors, and portal name.	✓	✓	✓
Admin Portal	Centralized portal to manage users, sessions, and policies.	✓	✓	✓
Private PoP	Ensures data sovereignty with private PoP deployment option.	✓	✓	✓
Isolated App Gateway	Offline deployment model for air-gapped environments.	✗	✓	✗

Safous App Gateway Server Requirements

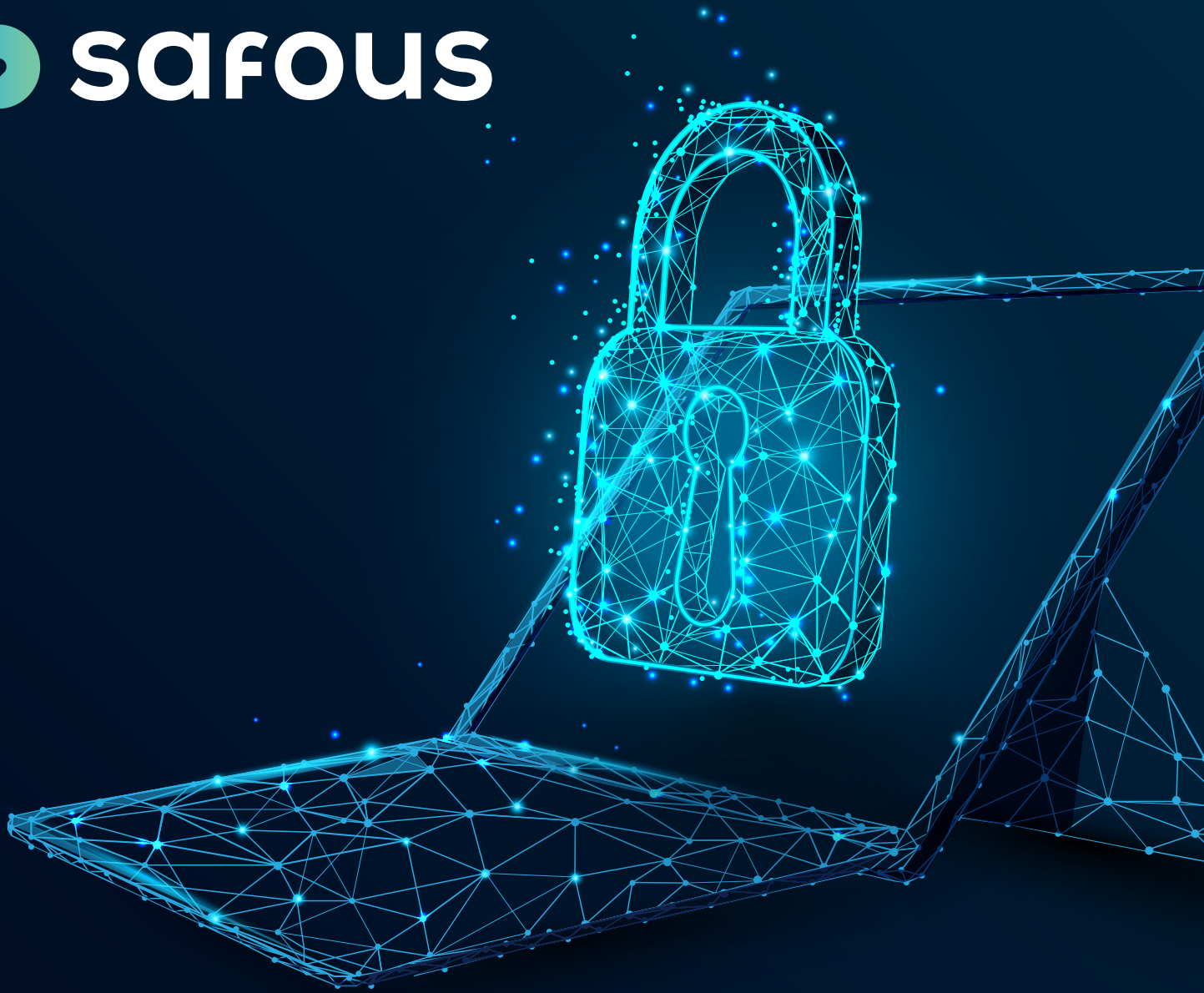
The Safous App Gateway can be installed on an on-premise server, virtual machine, or cloud environment. Here are the minimum requirements for server specifications:

No.	Server Specifications	System Requirements	Notes
1	Operating System	• Ubuntu Server 22.04 • Ubuntu Server 24.04 • RHEL 8.x (Server Package Required) • RHEL 9.x (Server Package Required) • Rocky Linux 9.x	
2	CPU Cores	4 cores minimum, 6 cores recommended	For larger deployments, we recommend adding more App Gateways over calling CPU cores.
3	RAM	8 GB +512 KB/user	
4	Disk	150 GB	Allocate additional disk space if you intend to store recordings. For high recording volumes, consider mounting an external drive. Please ensure you have sufficient Disk IOPS for optimal performance; 3000 IOPS is the baseline.
5	Network Bandwidth	32 Kbps/users	

About Safous

Safous offers a comprehensive suite of cybersecurity tools built to secure corporate networks, industrial systems, and more through a single, user-friendly platform. We make it easy to securely connect employees and third-party vendors to your critical assets – without replacing existing systems.

Trusted by 11,000+ global enterprises and MSPs alike, Safous empowers organizations to modernize with confidence.

Visit safous.com to learn more.

safous