Cybersecurity
INSIDERS

SOLUTION REVIEW

Safous Privileged Remote Access

Turning High-Risk Remote Access into Governed Privileged Operations

WHY REMOTE ACCESS HAS BECOME A PRIVILEGED OPERATIONS PROBLEM

The most consequential users of remote access today aren't employees. They're the OEMs, contractors, MSSPs, and OT engineers who carry privileged access to critical systems while sitting outside the corporate identity perimeter. Attackers are getting in through them.

Verizon's 2025 DBIR put third-party involvement in breaches at 30%, double the year before. Edge and VPN exploitation grew nearly eightfold.

VPN connected users to networks. Traditional PAM was designed around administrators inside the firewall. ZTNA narrows access decisions but leaves credentials, sessions, and audit trails to other tools. None governs privileged remote operations end-to-end.

Remote Privileged Access Management is the response: one operating model for governing privileged remote operations across employees, third parties, and OT environments. Safous PRA is built for this model.

OLD REMOTE ACCESS MODEL	PRIVILEGED REMOTE OPERATIONS MODEL
User connects to network	Verified identity connects to authorized application
Broad access after login	Least-privilege access by role, context, and policy
User handles credentials	Credentials vaulted, injected, rotated
Limited visibility after access	Sessions recorded, supervised, audit-ready
Persistent access paths	JIT, approval-based, time-bound access
Hard to govern third parties	Vendor access brokered, monitored, revocable

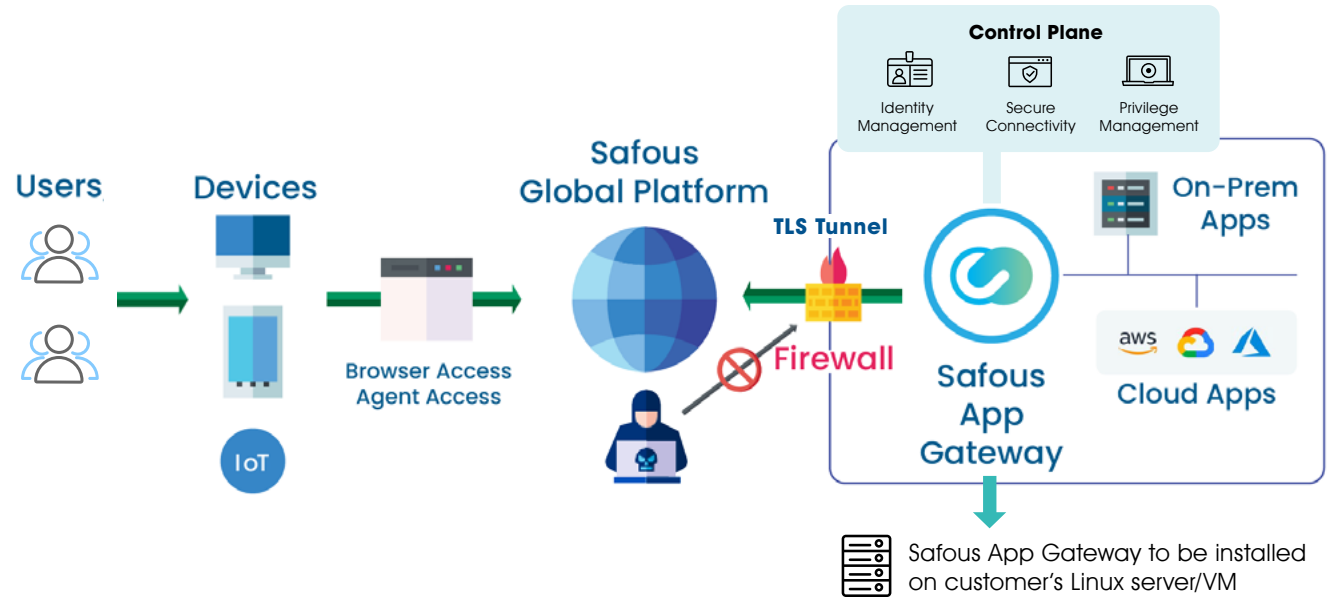
Remote PAM / RPAM in Context

Remote PAM is an emerging category for governing privileged remote operations. It combines PAM, ZTNA, vendor access management, credential protection, and session governance. It controls who can access what, when, with which credentials, and what evidence remains afterward.

HOW SAFOUS PRA WORKS

Safous PRA solves the problem most remote access tooling pretends doesn't exist: how to give a contractor enough access to do real work, without giving them enough access to do real damage. The product comes from Safous by IIJ, a foundational Japanese network operator with global infrastructure and top tier customers across the industry.

The platform puts three control planes in one place: Identity Modernization (who is the user), Zero Trust (what they can reach), Privileged Access (what they can do once there). Buy these separately and spend two years integrating them.



A user authenticates through Safous Global Access Points. Verified traffic crosses a TLS tunnel to a Safous App Gateway running inside the customer's network. The App Gateway is the only Safous component that ever touches privileged systems.

Four design choices that matter operationally

1

Identity to application, not user to network

The user never touches the network, so an attacker who hijacks a session has nowhere to pivot.

2

Cloud routes, customer hosts

Credentials, recordings, and logs stay on the customer-deployed App Gateway. The cloud handles transit and policy only.

3

Browser for vendors, agent for employees

External users connect from a browser with no install. Managed users get the agent where deeper posture matters.

4

Overlay, not replacement

PAM projects fail at the integration estimate, not the security model. Safous skips that pattern — App Gateway as overlay, first use case live in weeks.

CAPABILITIES ACROSS IDENTITY, ZERO TRUST, AND PRIVILEGED ACCESS

Privileged remote work raises three questions. Safous answers each with a dedicated control plane.

Identity Modernization — Who is the user?

The vendor population driving Remote PAM adoption doesn't sit in the corporate directory. Safous covers the practical bases: MFA across TOTP, SMS, WhatsApp, and email; identity federation and IdP proxy for legacy systems; device posture checks; and self-registration that compresses contractor onboarding from days to minutes.

Zero Trust Access — What can the user reach?

Role and attribute-based controls scope access to specific applications. Just-in-time controls bound access by time, date, location, and source IP. Policy-level threat intelligence blocks connections from VPN exit nodes, Tor, and risky hosting. RDP, SSH, and RemoteApp delivery happens through the browser — no client install, no exposed RDP port. The platform also protects what's behind the gateway: WAF and DDoS at the edge, real-time malware scanning on file uploads and downloads, and a Secure Web Gateway with URL filtering. Operational usability is itself a security control: vendors who can't use the platform route around it.

Privileged Access — What can they do once there?

This is where most ZTNA solutions thin out. Safous covers the privileged layer end-to-end: password vaulting with credential injection (superuser accounts used without ever being exposed), automated rotation, session recording with SSH text search and command control, granular session controls covering clipboard, file uploads and downloads, and ICAP-based file scanning, multi-level approval workflows including N-out-of-M thresholds, real-time supervision, and instant collaboration links for external specialists.

GARTNER RPAM CAPABILITY AREA	SAFOUS PRA COVERAGE
Authentication & Authorization	MFA (TOTP, SMS, WhatsApp, Email); least privilege; granular access policy
Identity Administration & Federation	Self-registration; identity federation; IdP proxy mode
Credentials Management	Password vaulting with credential injection; automated rotation
Session Management	Access and action controls; session termination; JIT access; multi-level and N-out-of-M approval
Session Monitoring & Auditing	Real-time supervision; session recording; SSH text search and command control; audit trails

WHERE SAFOUS PRA STANDS OUT

Four things separate Safous from typical Remote PAM platforms: how it handles third-party and vendor populations, how much it consolidates the stack, where data physically sits, and how cleanly it extends into OT.

1

Built for third-party and vendor access governance

OEMs, contractors, suppliers, and MSSPs are now the fastest-growing population needing privileged access — and none of them appear in the corporate directory. The Snowflake, MOVEit, and Change Healthcare breaches all involved that exact pattern: external parties with privileged access through pathways built for employees. Safous addresses this population directly: browser-based access, instant collaboration links, credential injection, multi-level approvals.

CASE STUDY: A global food and manufacturing company replaced a seven-login RDP workflow with a single sign-on across 150 sites, deployed in under 90 days, no network topology change.

2

Lower operational overhead

Safous puts identity verification, application access, credentials, session governance, and audit evidence on one platform — without major network redesign, infrastructure replacement, or multi-module integration projects. Existing IdPs integrate through federation or proxy. Deploy against one use case, prove value, expand.

3

Data sovereignty by design

Regulators asking where contractor session recordings physically live want a defensible answer mapping to data residency requirements. Safous keeps credentials, recordings, and logs inside the customer trust boundary while routing access through global infrastructure. Easier to defend than full-SaaS PAM.

CASE STUDY: A national banking institution replaced VPN access across 300-400 servers with granular application-level control. Password sharing disappeared. Full session monitoring and recording now produce audit-ready evidence as sessions happen.

4

OT support, without OT-only positioning

Safous Industrial SRA extends the same model into OT through Private POPs, Purdue-aligned App Gateway placement, and agentless architectures. It pairs with OsecT (NTT DOCOMO BUSINESS) for combined discovery, detection, and governed access, mapping directly to SANS ICS Critical Controls #3 (network visibility monitoring) and #4 (secure remote access). The same architecture handles IT and cloud admin access — OT proves the model under the hardest operational constraints.

CASE STUDY: A maritime infrastructure operator in Southeast Asia governs remote maintenance across 200 lighthouses, 250 offshore plants, and 1,000 port operation facilities. Connectivity over Starlink. Access governed by Safous.

WHAT BUYERS SHOULD KNOW

Seven moments determine how a Remote PAM platform performs in production: how it onboards external parties, what it takes to deploy, how credentials and sessions are governed, how collaboration is scoped, how it extends into OT, and how deep it integrates with existing tooling.

Evaluation considerations

EVALUATION AREA	BUYER QUESTION	HOW SAFOUS ANSWERS
Third-party governance	*How does the platform onboard, approve, supervise, and revoke access for external teams outside the corporate directory?*	Self-registration; multi-level and N-out-of-M approval workflows; real-time supervision with takeover; revocation through Safous-managed identity, no AD changes required.
Vendor usability	*Can external users connect via browser without agents or complex identity workflows?*	Yes. Agentless browser access for RDP, SSH, and RemoteApp. MFA via TOTP, SMS, WhatsApp, or email; no corporate directory join required.
Deployment overhead	*What network, infrastructure, identity, and workflow changes precede the first use case going live?*	Overlay App Gateway, no network topology change. IdP federation or proxy. First use case typically live in weeks.
Credential and session lifecycle	*How are credentials and sessions vaulted, recorded, searched, and stored?*	Credential injection (passwords never exposed); automated rotation; recordings and logs inside customer trust boundary; SSH text search and command logging.
Collaboration controls	*How are instant collaboration links scoped, approved, time-bound, recorded, and revoked?*	Scoped to specific apps; identity-bound, time-bound; recorded with host session; revoked at session end or admin discretion.
OT deployment	*How does the platform handle OT, DMZ, and air-gap architectures?*	Industrial SRA: Purdue-aligned App Gateway, customer-DMZ Private POPs, air-gap topology supported; pairs with OsecT for OT visibility.
Integration depth	*Which IdPs, SIEMs, ITSM tools, and asset inventories are supported?*	Federates with Entra ID, Okta, Ping, Google Workspace, LDAP. SIEM and syslog integration available. ITSM and asset inventory depth varies; validate during proof-of-concept.

Best fit for Safous PRA

- Organizations governing access for vendors, OEMs, contractors, and external support teams
- Organizations reducing VPN exposure for privileged users
- Manufacturers and industrial operators with distributed maintenance access
- Critical infrastructure operators with OT remote operations needs
- Regulated industries with audit pressure (banks, payments, healthcare, public sector)
- Organizations modernizing access controls on legacy systems that can't natively support MFA, federated identity, or agent-based posture checks
- Buyers wanting Remote PAM without a full PAM-suite rollout as the first step

The verdict

Safous PRA is strongest with the access populations traditional PAM was not designed for: third-party vendors, OEMs, contractors, OT engineers, distributed administrators. Three architectural choices distinguish Safous: cloud routes, customer hosts; one platform instead of three; agentless for vendors who won't install agents. That combination makes the platform deployable where traditional PAM stalls. Delivered as a managed service from IIJ's global infrastructure, with forward-looking capabilities like post-quantum encryption and instant collaboration links.

For organizations reducing VPN exposure, governing vendor access, or extending it into OT, Safous PRA earns serious evaluation.

ABOUT SAFOUS

Safous is a global cybersecurity team and product suite within the Internet Initiative Japan Inc. (IIJ) Group. Our Zero Trust security platform protects key entry points from ransomware and other cyberattacks while ensuring secure, seamless access for remote teams.

www.safous.com