Excalibur SAM vs. WALLIX

Streamed Access Management Battle Card

Key Competitive	Excalibur (Modern)	WALLIX (Traditional)
Platform	✅ Unified Platform, Passwordless-first, visual streaming isolation Integrated MFA + PAM + Remote Access in one easy-to-manage platform with true air-gap isolation via DOM streaming. No complex integrations, multiple agents, or modules needed.	⚠️ Proxy-based gateway, traditional credential vaulting Proxies secure connections but allows potential direct interaction between endpoint and resource. Appliance-based architecture with less flexibility for modern cloud environments.
Deployment	✅ Low: Cloud-native, deploys in hours Kubernetes-based cloud-native deployment with secure tunnels — eliminates VPN complexity. Quick time-to-value with minimal operational burden.	⚠️ Medium: Appliance-based, longer deployment Appliance-based architecture requires more infrastructure planning and setup time. Less dynamic scaling compared to modern cloud-native approaches.
Total Cost (TCO)	✅ Lower, streamlined licensing Cost-efficient licensing structure with everything included — no hidden fees for MFA, RBI, or session recording. Cloud-native architecture reduces infrastructure and operational costs.	⚠️ Moderate, add-ons increase cost Competitive base pricing but additional modules and external MFA solutions add to total cost. Appliance-based model requires more infrastructure investment.
NIS2 Readiness	✅ Full coverage out of the box, single platform Covers NIS2 requirements for access control, MFA, session monitoring, and incident response — in a single platform. Compliance is the reason organisations buy — we make it simple to achieve.	⚠️ Good coverage but requires add-ons Covers core PAM requirements but may need additional modules for complete NIS2 compliance. No built-in passwordless MFA — requires external integration.
Data Sovereignty	✅ 100% EU owned & operated, zero US footprint Fully European company with zero US presence — not subject to the US CLOUD Act in any way. No foreign government can compel access to your data or demand secret backdoors.	⚠️ French HQ but international presence raises questions Headquartered in France (EU), but having presence in the US which may create jurisdictional exposure. Companies with any US employees, offices, or subsidiaries can be subject to US CLOUD Act.
Architecture	✅ Isolation by Design, resilient to Zero-Day Threats Architecture inherently protects against zero-day threats through isolation and air-gap design. Reduce attack surfaces, no lateral movements, no reliance on signatures or known threat databases — unknown attacks are neutralised by default.	⚠️ Proxy-Based, Limited Zero-Day Resilience Proxy-based architecture relies on filtering and policy enforcement rather than true isolation. Less inherent protection against novel zero-day attacks compared to air-gap approaches.
AI & Governance Model	✅ Pre-Execution (Pre-Emptive) Pre-emptive governance reduces risk exposure and eliminates reactive firefighting. Real-time AI analyzes user intent and behavior for threat detection before actions are executed.	⚠️ Post-Execution (Reactive) Reactive model means damage may already be done before intervention. Security controls primarily detect and respond after actions have already occurred.
Web Access & RBI	✅ Native DOM-streaming RBI with WAF, bi-directional protection Innovative DOM-streaming Remote Browser Isolation (RBI) with visually lossless, lag-free sessions. Zero-trust, bi-directional protection — guards users from malicious web apps AND web apps from user threats.	❌ No inherent RBI-WAF, resource protection only, no user-side protection Primarily protects resources; no inherent user-side RBI-WAF capabilities. Limited protection against sophisticated web-based threats targeting users.
MFA Integration	✅ Built-in, Passwordless Built from the ground-up on passwordless authentication (biometric phone MFA, passkeys) Users never handle passwords directly — credentials are transparently managed.	⚠️ External MFA providers, password-based Relies primarily on external MFA providers, password rotation, and credential vaulting. More complex to manage, not future-proofed for passwordless authentication.
Audit Security	✅ Cryptographically Signed Audits Actions cryptographically signed and tied directly to authenticated identity. Enhanced compliance, forensic strength, internal accountability.	⚠️ Standard Audit Logging Detailed session logs and keystroke capture but without inherent cryptographic non-repudiation. Less robust for compliance and forensic requirements.
Endpoint Agents	✅ Fully agentless, HTML5 browser only Completely agentless — no endpoint agents required. Access via standard HTML5 browser. Easy rollout and support with zero client installation.	⚠️ Requires plugins for advanced features Typically agentless for basic access but can require endpoint agents/plugins for certain advanced features. Higher deployment complexity and management overhead for full capability.

WHY EXCALIBUR SAM WINS

- **True air-gap isolation** — no proxy gateway (**Zero trust**)
- **Endpoint threats isolated** — ransomware-proof (**Protection**)
- **Passwordless MFA** — built-in, no add-ons (**Security**)
- **RBI-WAF** — bi-directional browser isolation (**Protection**)
- **Fully agentless** — zero endpoint software (**Simplicity**)
- **Cloud-native K8s** — scales dynamically (**Scaling**)
- **Cryptographic audits** — tamper-proof logs (**Compliance**)
- **100% EU sovereignty** — no CLOUD Act risk (**Trust**)
- **NIS2-ready** — out of the box (**Compliance**)
- **Lower TCO** — all-inclusive licensing (**Value**)

THE COMPLIANCE BUYING LOGIC

Nobody buys security because they want to — only because they have to

Regulations like **NIS2**, **DORA**, and the **EU Cyber Resilience Act** are what drive purchasing decisions. The winning vendor is the one that covers all requirements, deploys easily, and costs less. With upcoming EU digital sovereignty rules, being a truly European vendor with **zero US footprint** is no longer optional — it's a decisive advantage.

- **Regulation creates the need** — NIS2, DORA, CRA force organisations to act
- **We cover all requirements** — MFA, PAM, session control, monitoring in one platform
- **We make it easy** — cloud-native tunnels, agentless, deploys in hours
- **Then it's about price** — same coverage, significantly lower cost
- **Pure EU sovereignty wins** — zero US footprint eliminates all doubt

Sovereignty Dimension	Excalibur SAM	WALLIX
Company Ownership	✅ 100% EU owned, zero US footprint	⚠️ French HQ, but international operations
US CLOUD Act	✅ Not subject — zero US presence	⚠️ Verify US footprint — potential exposure
NIS2 Coverage	✅ Full coverage — single platform	⚠️ Partial — lacks built-in passwordless MFA
EU Vendor Qualification	✅ Qualifies for upcoming EU vendor-preference regulations	⚠️ International presence may create jurisdictional risk

Understanding the US CLOUD Act and "European" vendors

Not All "EU" Vendors Are Equal
— A company headquartered in the EU but with US offices, employees, or subsidiaries can still be subject to US CLOUD Act jurisdiction. The test is whether there is any US "presence" that creates legal nexus.

WALLIX's International Footprint
— WALLIX has international operations beyond France. Customers should verify the exact US footprint to assess CLOUD Act exposure.

Excalibur's Position
— Zero US presence of any kind — no US employees, no US offices, no US subsidiary. This makes Excalibur categorically immune to US CLOUD Act demands.

The Decisive Question
— Ask any vendor: 'Do you have any employees, offices, subsidiaries, or legal entities in the United States?' If the answer is anything other than 'No', they may be subject to forced data disclosure.

What is NIS2?

- EU cybersecurity law (effective October 2024) covering **18 sectors**
- Mandates **access control, MFA, session management, monitoring & incident response**
- Requires **supply-chain security** — you must vet your vendors
- **Personal liability** for executives; fines up to **€10M / 2% global turnover**

What is the US CLOUD Act?

- US law (2018) that lets the government **demand any data** from any company with US presence — regardless of where data is stored — without EU court approval
- Can **compel backdoors** and impose **gag orders** — disclosure means imprisonment / extradition
- Applies to **any US nexus** — offices, subsidiaries, or even employees in the US is enough

Upcoming EU Regulation

The EU is advancing **digital sovereignty** rules that will prefer — or require — EU-owned vendors for critical infrastructure. The proposed regulation means choosing a non-EU vendor today risks a costly forced migration tomorrow.

HANDLING OBJECTIONS

KEY DISCOVERY QUESTIONS

KEY COMPETITIVE ADVANTAGES