Excalibur SAM vs. CyberArk PAM

Streamed Access Management Battle Card

Key Competitive	Excalibur (Modern)	CyberArk (Legacy)
Platform	✅ Unified & Simple Platform Integrated MFA + PAM + Remote Access in one easy-to-manage platform. No complex integrations, multiple agents, or modules.	⚠️ Complexity & Resource Intensity Complex setup, lengthy deployment, significant admin overhead. Requires dedicated security teams capable of managing complexity.
Deployment	✅ Fast & Simple Deployment Deploys in hours with minimal configuration. No dedicated security team needed. Quick time-to-value with minimal operational burden.	❌ Complexity & Resource Intensity Complex deployment requiring lengthy professional services engagements. Months-long rollouts with significant admin overhead.
Pricing	✅ Low, Transparent, Per-User Pricing Simple per-user pricing — no add-ons, no hidden fees, no surprise costs. All-inclusive licensing that scales predictably with your team size.	❌ High, Infrastructure-Heavy, Per-Device Pricing Requires spinning up 6–8 VMs just to run the platform, driving significant infrastructure costs. Extra expenses in professional services, add-on modules, and ongoing maintenance.
Total Cost (TCO)	✅ Significant Cost Savings, More Accessible Cost-efficient licensing structure — ideal for SMEs & mid-market with minimal infrastructure overhead. No costly add-ons or hidden fees.	❌ Very High Cost, Premium Pricing Premium pricing model with large enterprise focus. Excessive costs for organizations with limited security budgets.
NIS2 Readiness	✅ NIS2-Ready Out of the Box Covers NIS2 requirements in a single platform that deploys fast, simple to achieve.	❌ Non-Compliant with EU Sovereignty Direction Having major headquarters in the US, increasing regulatory risk for customers.
Data Sovereignty	✅ 100% EU Owned & Operated, No US CLOUD Act Fully European company — not subject to the US CLOUD Act. No foreign government can compel access to your data or demand secret backdoors. Critical for NIS2 compliance and upcoming EU digital sovereignty regulations.	❌ US CLOUD Act Exposure Having major headquarters in the US, fully subject to the US CLOUD Act. US authorities can compel access to any customer data stored anywhere in the world. Forced data disclosure, secret backdoors, and gag orders are legally mandated. Upcoming EU digital sovereignty regulations could ban the use of non-EU vendors for high-risk organizations.
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.	⚠️ Limited, Signature-Based, Vulnerable to Zero-Day Threats Protection relies heavily on signature-based detection and known threat patterns. Novel zero-day attacks can bypass defences until signatures are updated.
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	✅ VITRO Technology with Native DOM-Streaming RBI & WAF Innovative DOM-streaming Remote Browser Isolation (RBI) with visually lossless, log-free sessions. Zero-trust, bi-directional protection with built-in WAF functionality.	⚠️ Limited Isolation, Basic Web Access No true RBI/WAF capabilities for comprehensive protection. Vulnerable to sophisticated web-based threats.
MFA Integration	✅ Truly Passwordless and Built-in MFA Built from the ground-up on passwordless authentication (biometric phone MFA, passkeys). Users never handle passwords directly — credentials are transparently managed.	⚠️ Vault-centric, Traditional Credential Checkout Traditional password-based approach with complex authentication flows. Potential productivity loss and user resistance.
Endpoint Agents	✅ Agentless Completely agentless — no endpoint agents required. Access via standard HTML5 browser. Easy rollout and support with zero client installation.	⚠️ Often Required (Agents/Add-Ons) Often requires installation of endpoint applications or add-ons. Less adaptable to modern cloud environments.

WHY EXCALIBUR SAM WINS

- **Unified platform** — MFA + PAM + Remote Access in one (**Simplicity**)
- **Fast Deployment** — no lengthy professional services (**Speed**)
- **Transparent per-user pricing** — no hidden fees (**Value**)
- **NIS2-ready** out of the box in one platform (**Compliance**)
- **100% EU sovereignty** — no US CLOUD Act exposure (**Trust**)
- **Pre-emptive model** — stops threats before execution (**Pre-emptive**)
- **Isolation by design** — resilient to zero-day threats (**Architecture**)
- **VITRO RBI-WAF** — bi-directional browser isolation (**Protection**)
- **Passwordless MFA** — eliminates credential theft (**Security**)
- **Fully agentless** — zero endpoint software needed (**Simplicity**)

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	CyberArk
Company Ownership	✅ 100% EU owned, zero US footprint	❌ Major HQ: Newton, Massachusetts, USA
US CLOUD Act	✅ Not subject — zero US presence	❌ Fully subject — compellable backdoors & gag orders
NIS2 Coverage	✅ Full coverage in a single platform	❌ Non-compliant with EU sovereignty direction
EU Vendor Qualification	✅ Qualifies for upcoming EU vendor-preference regulations	❌ Cannot qualify as EU vendor

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 ADVANTAGES

COST EFFICIENCY

- **Single-Platform Pricing** — One license covers PAM + MFA + RBI-WAF + session recording. CyberArk charges separately for Vault, PTA, Identity, and Alero.

SIMPLICITY

- **Cloud-Native (K8s)** — Deploy via Helm in hours with auto-scaling; CyberArk requires on-prem Vault servers + weeks of professional services.

EU COMPLIANCE

- **100 % EU Sovereignty** — EU-owned, EU-hosted, zero US footprint. Immune to the US CLOUD Act — a structural gap CyberArk (NASDAQ: CYBR; Newton MA) can never close.

SECURITY

- **Zero-Trust Isolation** — Air-gap architecture physically separates endpoints from resources; CyberArk's proxy model leaves the attack path open.
- **Built-in RBI + WAF** — Bi-directional web protection (browser-to-app and app-to-browser) out of the box; CyberArk has no equivalent.

- **Passwordless MFA** – Native FIDO2 / biometric auth ships in the platform; CyberArk relies on third-party MFA add-ons.