Excalibur SAM vs. Segura

Streamed Access Management Battle Card

Key Competitive	Excalibur (Modern)	Segura (Traditional)
Approach	✅ Unified Platform, Passwordless-first, visual streaming isolation Integrated MFA + PAM + Remote Access in one platform with true air-gap isolation via DOM streaming. No complex integrations or separate modules needed.	⚠️ Traditional PAM with credential vaulting
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
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 RBI-WAF capability
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.
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.	⚠️ Partial — needs additional modules Covers core PAM requirements but may need additional modules for complete NIS2 compliance. No built-in passwordless MFA — requires external integration, increasing regulatory risk.
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.	⚠️ Verify company jurisdiction and US footprint Verify Segura's company ownership and whether any US employees, offices, or subsidiaries create exposure to the US CLOUD Act — which can compel access to customer data stored anywhere in the world. Upcoming EU digital sovereignty regulations could restrict the use of non-EU vendors for high-risk organisations.

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**)
- **Cryptographic audits** — tamper-proof logs (**Compliance**)
- **100% EU sovereignty** — no CLOUD Act risk (**Trust**)
- **NIS2-ready** — out of the box (**Compliance**)

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	Segura
Company Ownership	✅ 100% EU owned, zero US footprint	⚠️ Verify jurisdiction
US CLOUD Act	✅ Not subject — zero US presence	⚠️ Verify US footprint
NIS2 Coverage	✅ Full coverage — single platform	⚠️ Verify — may need additional vendors for MFA & monitoring
EU Vendor Qualification	✅ Qualifies for upcoming EU vendor-preference regulations	⚠️ Verify jurisdiction & US footprint

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