All Competitors

Excalibur SAM vs. WALLIX

EU Sovereignty & Compliance

EU SOVEREIGNTY & 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	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.