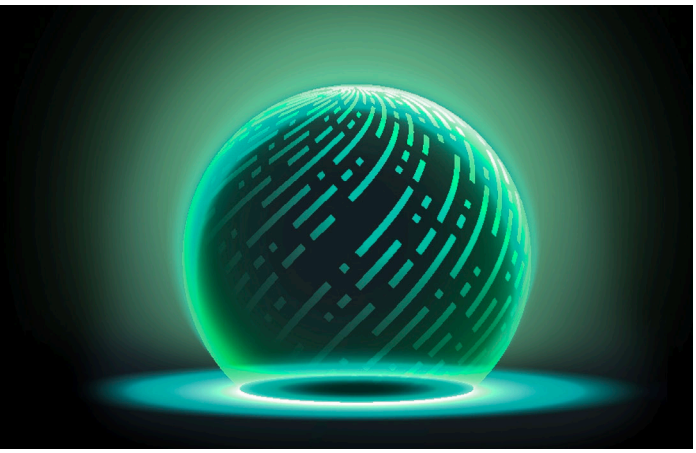
Exceptional Email Security

/LIBRAESVA

Semantic AI: Privacy-first email defense

Because today's email threats no longer look like threats.



Today's email threats are so sophisticated that they no longer look like threats. Attackers increasingly use well-written, well-formatted emails, often crafted by AI, to bypass traditional filters. These messages rarely contain known malicious signatures or obvious red flags that trigger rules-based defenses.

Semantic AI solves this problem by going beyond keywords, links, and sender history. It analyzes the actual meaning and logic within messages to detect inconsistencies and intent-based anomalies — even when everything else appears legitimate.

Semantic AI is Libraesva's next-generation Small Language Model (SLM)-based engine, offering deep, context-aware email threat detection without compromising privacy. It runs locally on your existing hardware — no cloud, no data offshoring, no third-party AI APIs.

- ☑ **Detects what others miss** Flags unexpected vendor names, mismatched tone, or illogical requests —in otherwise flawless emails.
- ☑ **Day-zero detection** Catches sophisticated threats before signatures or heuristics are updated.
- ☑ **Enhances decision confidence** Deterministic outputs ensure consistent results — the same message always produces the same outcome.
- ☑ **Protects without compromise** Privacy-first by design — no cloud, no offloading, no third-party data sharing.
- ☑ **Works where it matters** Only activates on messages flagged by Adaptive Trust Engine, delivering depth without drain.

PRIVACY BY DESIGN

- No cloud processing or data offloading
- No model training on customer data
- No third-party AI APIs or dependencies
- Full on-prem execution and data control
- 100% compliant with local data protection policies

CORE TECHNOLOGY HIGHLIGHTS

- Discriminative AI: Deterministic outputs, zero entropy, consistent results
- Contextual Analysis: Detects anomalies in meaning, logic, and intent
- Lightweight SLM: 100M-parameter model trained on curated email threats
- CPU-Optimized: Runs on standard hardware with <1s delay
- Complements existing protections (ATE, rules, sandboxing, AV)
- Works in parallel with Adaptive Trust Engine (ATE) to reduce alert fatigue

Give your security stack the ability to understand intent — not just structure.
You'll get safer inboxes, smarter detection, and protection that adapts to how threats really behave.

Ready to get started?

sales@libraesva.com

www.libraesva.com

Libraesva is an award-winning email security company, named as Category Leader in Email Security by GetApp, a Gartner company, and Innovation Leader on the Frost Radar. Libraesva is consistently certified by Virus Bulletin as one of the best email security systems, and is trusted by leading brands around the world.

/LIBRAESVA
EmailSecurity