Introducing Salpa

An AI-driven email security solution

WHY YOUR EMAIL SECURITY STACK STILL HAS A BLIND SPOT — AND HOW SALPA FIXES IT

Phishing remains the number one initial access vector in breaches worldwide. Despite billions spent on secure email gateways, AI filters, and user awareness training, attackers continue to reach inboxes because most defenses rely on reputation lists and sender scoring that sophisticated campaigns easily bypass.

The signals are in the email itself — in the headers, the URLs, the language, the structure — but most tools never look closely enough.

That is the problem Salpa was built to solve.

Salpa is a phishing email analysis engine that protects your enterprise with multiple features to produce a transparent, weighted phishing score. No black boxes. No opaque threat labels. Every score comes with a full breakdown of what was detected and why it matters.

The engine evaluates ten independent signals, including:

- Sender integrity — spoofed Return-Path and Reply-To headers
- Authentication failures — SPF, DKIM, and DMARC verification
- Suspicious URLs — IP hosts, deceptive anchors, suspicious TLDs, URL shorteners, and hacked CMS paths
- Brand impersonation — display name, body text, and URL mimicry across 26 monitored brands
- Header anomalies — missing fields, suspicious mailers, and HELO spoofing

Each feature contributes a weighted score. The final result is a single 0-to-1 phishing score with a clear verdict: not suspicious, suspicious, or phishing/spam. Security teams get the "what" and the "why" in one report.

Why CISOs should care

Most email security products sit inline and make a binary allow-or-block decision in milliseconds. Salpa operates differently. It is a forensic analysis layer — designed for the emails that have already landed, the ones users reported, the ones your threat hunting team pulled from quarantine. It answers the question your SOC analysts ask dozens of times a day: is this actually phishing, and how confident are we?

Because every verdict is explainable down to the individual feature, Salpa reports double as training material for junior analysts and audit evidence for compliance reviews. There is no ambiguity about why an email scored the way it did.

Salpa runs on the Python standard library with zero external dependencies. It can be deployed on air-gapped networks, embedded in automated triage pipelines, or run from a laptop during an incident response. No API keys, no cloud connectivity, no vendor lock-in.

In its latest production run, Salpa analyzed over 6,000 real-world samples sourced from public threat intelligence repositories. Every file was processed with zero errors, producing structured JSON reports that identified over 5,200 emails as suspicious or phishing — all with full per-feature transparency. That is the kind

of signal-to-noise ratio SOC teams need when they are triaging hundreds of reported emails a day.

What's next for Salpa

The team is actively developing the next wave of Salpa capabilities:

- Personalized protection that learns from your employee's patterns to mitigate risk of falling to BEC
- QR code extraction and analysis for quishing attacks that evade traditional URL scanners
- Natural language scoring powered by lightweight local models to detect social engineering beyond keyword matching

Phishing is not a solved problem. Attackers evolve faster than static rule sets, and security teams deserve tools that show their work. Salpa is built on the principle that detection without explanation is not detection — it is guessing.