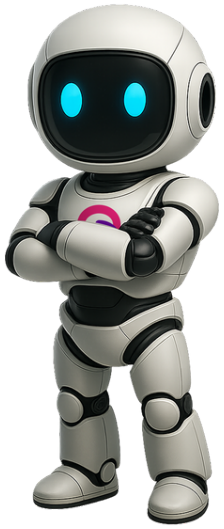
StrongestLayer

AI Native Email Protection and Human Risk



As AI transforms the threat landscape, email attacks have exponentially evolved, with Harvard research showing AI-generated phishing now fooling over 50% of humans while reducing attack costs by 95%. First-generation email security relies on static rules and pattern matching, but these approaches fail catastrophically when AI-enabled threat actors generate personalized attacks designed to evade known signatures—creating infinite attack variants with zero historical patterns to match.

StrongestLayer TRACE represents true third-generation email security, combining LLM native threat reasoning with AI-driven employee coaching to eliminate false positive investigations while achieving the highest detection rates across attack vectors that legacy platforms miss, delivering 400-500% ROI within 12 months.

Detecting Advanced AI-Generated Attacks

- LLM-native reasoning engine analyzes intent, context, and threat indicators to detect attacks that are tailored and unique.
- Dual evidence architecture simultaneously investigates business Legitimacy (normal) and threat indicators (anomalous), enabling very advanced detection while lowering false positives.
- Real-time behavioral analysis understands organizational communication patterns to spot AI-generated attacks that are multi-channel and that span multiple communications.

Reducing Operational Costs

- Transparent reasoning allows analysts to rapidly triage an alert - in 1 to 2 minutes - versus the 15 minutes it takes with “black-box” platforms that use rules / patterns.
- Reduces false user submissions from 60-70% to <1% of user submission with our AI advisor, Which provides real-time coaching on both good and bad emails Catches and prevents several advanced attacks that are evading current technologies, shifting left many potential incidents before they become costly to address.

Employee Empowerment & Productivity

- Provide real-time coaching with AI Advisor to employees on when and how to trust emails. The tool allows them to instantly analyze both legitimate and suspicious emails, and takes out the stress of having to be always vigilant throughout their workday.
- Provide employees with personalized, nano-sized training tailored to their roles and threat landscape delivered contextually to their mailbox
- Build strong security instincts with phishing simulations that actually work with scenarios specific to the organization's supply chain, vendor relationships, and threat environment.

Key Features And Benefits

For CISOs

- CISO-level dashboard with deep insights and trends
- Sophisticated ROI calculator based on the FAIR Institute methodology
- Improved detection around the sophisticated threats that account for +90% of breach costs

For Security Operations

- Self-service quarantine digest that saves email administrators time by allowing users to self-release
- Time-saving automations that rapidly triage similar malicious emails when threats are detected
- Customizable email warning banners that align security nudges to company culture
- Full detection explainability providing all evidence, good and bad, alongside reasoning and all contextual investigation data.

For Human Risk Managers

- LLM-generated phishing simulations with high premise-alignment
- LLM-generated nano-training delivered contextually within inbox workflow, tailored to the company threat environment
- AI advisor allows employees to assess risk of good and bad emails, improving productivity, callibrating trust and reducing risk
- Customizable email warning banners provide teachable moments and/or nudges for employees

Customer Insights

StrongestLayer's detection and threat intelligence capabilities are outstanding. Their advanced AI driven phishing campaigns are both highly effective and realistic!

Information Security Analyst
Banking & Financial Services

Phishing attacks aren't just evolving — they're mutating. With generative AI, attackers can craft highly convincing, targeted messages at scale, making traditional defenses obsolete. The real risk isn't just in the inbox — it's in every human decision that follows

CISO
Legal Services

Zero-Memory architecture
Your data never trains a model

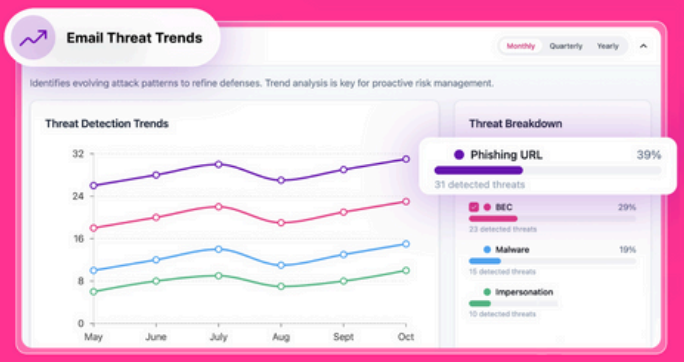
Multi-Lingual Detection
Same detection efficacy in 15 languages

Deploys in less than Five minutes
Api-based. No MX changes. No learning.

Ready for a Demo?

Visit the Strongestlayer website for more details, or email demo@strongestlayer.com

Strongestlayer.com



As seen in Industry publications

SC Media
A CRA Resource

Article explains how legacy email security platforms built on pattern-matching and machine learning cannot detect novel AI-generated phishing attacks, requiring a fundamental shift to LLM native "third-generation" systems

DARK READING

Attackers are abusing Microsoft 365's Direct Send feature to spoof internal emails and bypass traditional email defenses, with the campaign successfully detected by StrongestLayer through advanced AI-native correlation & analysis.

UNITE.AI

The article details StrongestLayer's "third-generation" email security platform that replaces static rules with LLM-powered reasoning engines capable of detecting AI-generated threats through business context analysis.

About StrongestLayer

StrongestLayer is the world's first AI-native platform combining advanced email threat detection with AI-powered human risk management. The StrongestLayer TRACE™ Platform uses contextual threat reasoning to stop sophisticated phishing attacks while delivering personalized nano-training and real-time AI advisory to employees, empowering organizations to defend against AI-generated threats through both technological intelligence and human resilience. Leading organizations across government, manufacturing, banking, legal, and insurance trust StrongestLayer to transform email security and employee awareness for the AI era.

Strongestlayer.com
sales@strongestlayer.com