

They've never seen these attacks before.

No one has.

AI-generated email attacks are unique every time. Your security stack was built to match patterns. That model is now mathematically broken.

✓ No Malware ✓ No Payload ✓ EDR Clean ✓ Trusted brand →

CREDENTIALS GONE.

THE PROBLEM

✗ **RULES & SIGNATURES**
Require known indicators

✗ **MACHINE LEARNING (ML) MODELS**
Trained on yesterday's attacks

✗ **PATTERN MATCHING**
Fails when every email is unique

THE PATTERN-MATCHING CLIFF

Traditional detection requires 85–95% similarity across attack variants. AI-generated phishing shares only 12–18% common features – each email is effectively unique. Below the 30% threshold, pattern-matching becomes statistically ineffective. This is an architectural limit, not a tuning problem.

OUR RESEARCH

2,042+ advanced threats studied — every one bypassed Microsoft E3/E5 & leading SEGs before we found it.

77%

TRUSTED BRANDS
Exploited platforms too critical to block

281

DOCUSIGN ATTACKS
#1 impersonated brand for credential theft

5.9%

CALENDAR ATTACKS
A growing channel your email security never inspects

45%

AI-GENERATED
Projected to reach 95% by 2027

See links to our 4 threat research papers on back →

OUR SOLUTION: **AI-Native Reasoning** > Rules & Signatures

INTENT ANALYSIS

ANOMALY DETECTION

DECEPTION SCORING

HARM PREDICTION

RISK-ADJUSTED TRIAGE

Instead of asking “does this look like a known attack?” we ask “does this email make sense for this business?” That shift eliminates the blind spot where AI-generated threats live.

CUSTOMER RESULTS

95%

FEWER FALSE POSITIVES
Dramatically reduce SOC noise

< 2 min

ALERT RESOLUTION
From 20+ minutes to under two

15 min

TO PROTECTION
API-based — no rip & replace

strongestlayer.com/resources

15-minute POC · See what your current stack misses

Flip for our published threat research →

Thought Leadership Library

Original research from the StrongestLayer Threat Intelligence team. Scan any QR code to read the full paper.

THREAT INTELLIGENCE

01

What Your Email Security Can't See

Analysis of **2,042 advanced threats** that bypassed Microsoft E3/E5 and leading SEGs. 77% exploited brands too critical to block.

SCAN TO
READ

02

The Architecture of Evasion: QR Code Phishing

92 attacks across 19 campaigns that defeated every major email gateway. The mobile device gap is an architectural constraint.

SCAN TO
READ

03

The DocuSign Detection Gap

281 credential harvesting attacks in Q4 2025. DocuSign's legitimate behavior mirrors every phishing red flag — a business logic vulnerability.

SCAN TO
READ

04

Calendar Invitation Attacks

3,839 confirmed attacks analyzed. Calendar + QR delivery now account for ~10% of bypass attacks. Includes APT41 using Google Calendar for C2.

SCAN TO
READ

SECURITY OPERATIONS

05

The Collapse Of Traditional Threat Detection In The AI Era

How AI-generated attacks expose the limitations of pattern-matching security and the rise of reasoning-based detection.

SCAN TO
READ

06

The Training Paradox

How security awareness training became your biggest security risk. Examining the unintended consequences of traditional awareness programs.

SCAN TO
READ

07

The Zero Trust Paradox

Organizations invest millions in Zero Trust — then deploy email tools that force permanent exceptions. False positives dismantle the architecture.

SCAN TO
READ

08

Email Security Gap Analysis: Law Firm Case Study

Major law firm with E5 + leading SEG discovered **347 threats in 10 days** bypassing existing controls. >99% novel detection, ~1% false positive rate.

SCAN TO
READ

8

RESEARCH PAPERS

8,500+

THREATS ANALYZED

Q3–Q4

2025 DATA

Ready to see what you're missing?

15-minute POC · strongestlayer.com/demo