StrongestLayer

Email Security Gap Analysis

Major Law Firm Case Study: 347 Threats Bypassed Microsoft E5 + Leading SEG in 10 Days

Company Profile: Major Law Firm | 2,500-5,000 mailboxes
Assessment Period: 10 business days (October 2025)
Existing Security: Microsoft 365 E5 + Leading SEG

The Detection Gap: Premium Security Missing Modern Threats

A law firm with Microsoft E5 + leading SEG discovered a critical blind spot: AI-powered social engineering attacks bypassing traditional signature-based detection. In 10 days, 347 sophisticated threats reached user mailboxes undetected by existing controls.

10-Day Assessment Results

Threat Category	Volume (10d)	Annual Threats	Success Rate	Successful Attacks/Year	Per Day
Business Email Compromise	156	5,694	5.4%	307	1.2
Credential Harvesting	124	4,526	3.2%	145	0.6
Internal/HR Phishing	67	2,446	4.1%	100	0.4
TOTAL	**347**	**12,666**	**4.36%**	**552**	**2.1**

Real Attack Example: CFO Wire Transfer Scam

Attack Profile: Professional executive impersonation targeting finance team. $847K wire transfer request with "confidential acquisition" urgency. Sent from legitimate third-party email service.

Why Traditional Security Missed It
- ✓ Passed SPF/DKIM
- ✓ No malicious links
- ✓ Professional language
- ✓ Legitimate financial term
- ✓ Clean reputation

How Enhanced Analysis Caught It
- ✓ Unusual request pattern
- ✓ Domain/identity inconsistency
- ✓ Deviation from workflows
- ✓ Financial req + external
- ✓ Authority exploitation

Measured Business Impact

Metric	Result	Business Value
Threat Detection	> 99% novel attacks caught	Enhanced security posture
False Positives	~1% FP on AI-authored malicious detections (vs 25-40% for SEGs)	Eliminated business disruption
Security Team Efficiency	80% reduction in investigation time	Operational cost savings

Key Differentiators

Contextual Understanding: Analyzes organizational patterns, communication styles, and business workflows—not just content

Multi-Factor Risk Scoring: Combines dozens of signals into comprehensive risk assessment vs. single threat score

Human-Readable Explanations: Every detection includes detailed reasoning for security teams and audit documentation

The Solution: Complementary Architecture

StrongestLayer is API-based (Google/MS) and deploys easily alongside Microsoft E5 + SEG (non-disruptive) in 15 min with no MX record changes needed. Traditional controls handle signature-based threats. AI-native analysis adds behavioral reasoning for sophisticated attacks.

Traditional Security Checks
- Sender domain blacklisted?
- Known malware sigs?
- Suspicious links?
- Reputation score?

AI-Native Behavioral Analysis
- Request pattern?
- Comm style?
- Org context?
- Multi-factor risk?

Ready for a Demo?

Visit the StrongestLayer website for more details, or email sales@strongestlayer.ai

StrongestLayer.com