Quantifying the Failure of "Good Enough" Cloud Email Security

Reliance on bundled cloud email security platforms or legacy Secure Email Gateways (SEGs) has created a measurable "detection despair" gap.

Inbound email security tools that could once do the job are struggling in the face of evolving threats born from AI-powered bad actor innovation. Consider that small-to-midsize enterprises (SMEs) spent 27% more on cyber incident response in 2025 due to AI-specific threats. Additionally, the average cost per AI-related breach reached $5.7 million in 2025, a 13% increase from the prior year.

KnowBe4's data has found that some **14.1 million threats bypassed traditional filters** and were only identified via end-user reporting.

58,000 per day

Bundled technology packages often reek of unprioritized innovation, making them easy targets and lacking sufficient outbound protection. This bundled "Good Enough" model has fallen from cost-saving measure to high-interest debt that eventually comes due through reputational damage, regulatory penalties and security operations center (SOC) burnout.

This guide breaks down the numbers you and your team need to make the case for an integrated cloud email security approach that teams AI-backed detection capabilities and human smarts.

The Inbound Miss Rate

Standard filters are effectively "marking their own homework," leading to a false sense of perimeter integrity. Data shows significant failure rates in high-stakes attack vectors:

- **Business Email Compromise (BEC):**
  The big name players in the email security space miss **between 51% and 60% of BEC attacks**
- **Link-Based Attacks:**
  Legacy SEGs allow **58%** of malicious links to reach the inbox
- **The Hidden Threat Delta:**
  Best-of-breed behavioral AI from KnowBe4 identifies **10x more hidden threats** than static, rule-based systems by analyzing 1,500+ identity and context signals in real-time

KnowBe4 identifies

10x

more hidden threats than static, rule-based systems

The Outbound Blind Spot

Outbound security is the most neglected pillar of "Good Enough" suites, making especially highly regulated industries vulnerable to fines and other regulatory violations:

- **Undetected Exfiltration:**
  In 2025, KnowBe4 stopped 1.2 million potential breaches. Legacy SEGs are capped at roughly 62% of those events, leaving nearly 38% high-risk events undetected. Legacy incumbents leave customers stuck with hard-coded, static DLP rules that can't keep up with evolving compliance mandates or detect malicious insider exfiltration.
- **Regulatory Liability**
  With average breach settlements exceeding **$4.5 million**, the inability to prevent PII exfiltration via accidental or malicious outbound mail is an unacceptable risk.
- **Insider Threats**
  AI-aided insider threats caused over $2.4 billion in damages in 2025, largely due to machine learning systems identifying exploitable access roles.
- **95% Behavioral Change in End Users**
  Stop users from proceeding with risky actions through high-visibility, real-time teachable moments.

Operational ROI and the "SOC Burnout" Metric

The surge in manual labor required to fix filter failures can often eat up any savings realized by "bundling:"

- **Manual Containment**
  Traditional "Good Enough" setups require significant manual work due to the inability to customize
- **The Efficiency Gain**
  Transitioning to an automated, AI-driven ICES suite reduces threat containment time by **95%**

ICES suite reduces threat containment time by

95%

CISO Audit Checklist: Is Your Defense Beyond "Good Enough?"

1. **Explainability**
   - [ ] Can your AI explain why it flagged a message for audit purposes?
2. **Self-Grading**
   - [ ] Is your primary filter the same vendor that provides your inbox?
3. **Outbound Parity**
   - [ ] Can your admins independently deploy bespoke DLP rules and custom pattern matching in minutes with AI, or are you locked behind a professional services/ high license cost paywalls?
4. **Manual Triage**
   - [ ] Is your SOC spending more than 10 hours a week on manual phish reporting?

Avoiding Detection Despair

A packaged deal when it comes to email security may be too good to be true. Middle-of-the-road platforms or tools bundled together are not saving anyone money if they're missing the threats you're depending on them to detect.

KnowBe4's inbound and outbound email security finds the threats that have made it past traditional filters. We scale human intuition with adaptive AI to secure the inbox where the danger is the highest, allowing you to scale operations without increasing the burden on your SOC.

Learn More About KnowBe4's Approach to Cloud Email Security

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
855-KNOWBE4 (566-9234) | www.KnowBe4.com | Sales@KnowBe4.com

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

Copyright © 2026 KnowBe4 All Rights Reserved.