proofpoint®

SOLUTION BRIEF

Proofpoint Core Email Protection API

Catch what reaches the inbox.
Protect everywhere the attack goes next.



Key benefits

- Catches the 27% of advanced email threats that Microsoft's native filtering misses
- 99.999% detection efficacy with an industry-leading false-positive rate of 1 in 19.7 million messages
- Independently benchmarked by Microsoft as the top-performing ICES vendor
- Multi-model Nexus® AI understands message intent, not just behavioral anomalies
- Live in as little as 48 hours with zero MX or mail flow changes and no migration project
- Protection extends beyond email to account takeover, supplier compromise, and messaging security
- One console—Threat Protection Workbench—for investigation and remediation across email and collaboration channels

Independently benchmarked by Microsoft as the top-performing ICES vendor measured.

The Gap: What Microsoft Defender Misses

Microsoft's native filtering misses an average of 27% of advanced email threats. That's because many of today's most effective attacks are novel and AI-generated, making them difficult to detect with techniques that rely on known indicators, signatures, or reputation.

Attackers now generate personalized lures at machine speed, send them from compromised accounts and trusted services, and move beyond email into collaboration tools and cloud accounts. Organizations need protection that catches threats after they reach the inbox—and continues protecting users wherever the attack goes next.

The numbers behind the gap

Email threats grew 46% year over year—from 4.4 billion in 2025 to 6.4 billion in 2026.

AI-generated phishing earns a 4.5x higher click-through rate than traditional phishing.

99%+ of organizations experienced an account takeover attempt in the past 12 months.

80% of organizations receive an attack from a compromised supplier every month.

Roughly **half of AI-related attacks** now extend beyond email into collaboration tools.

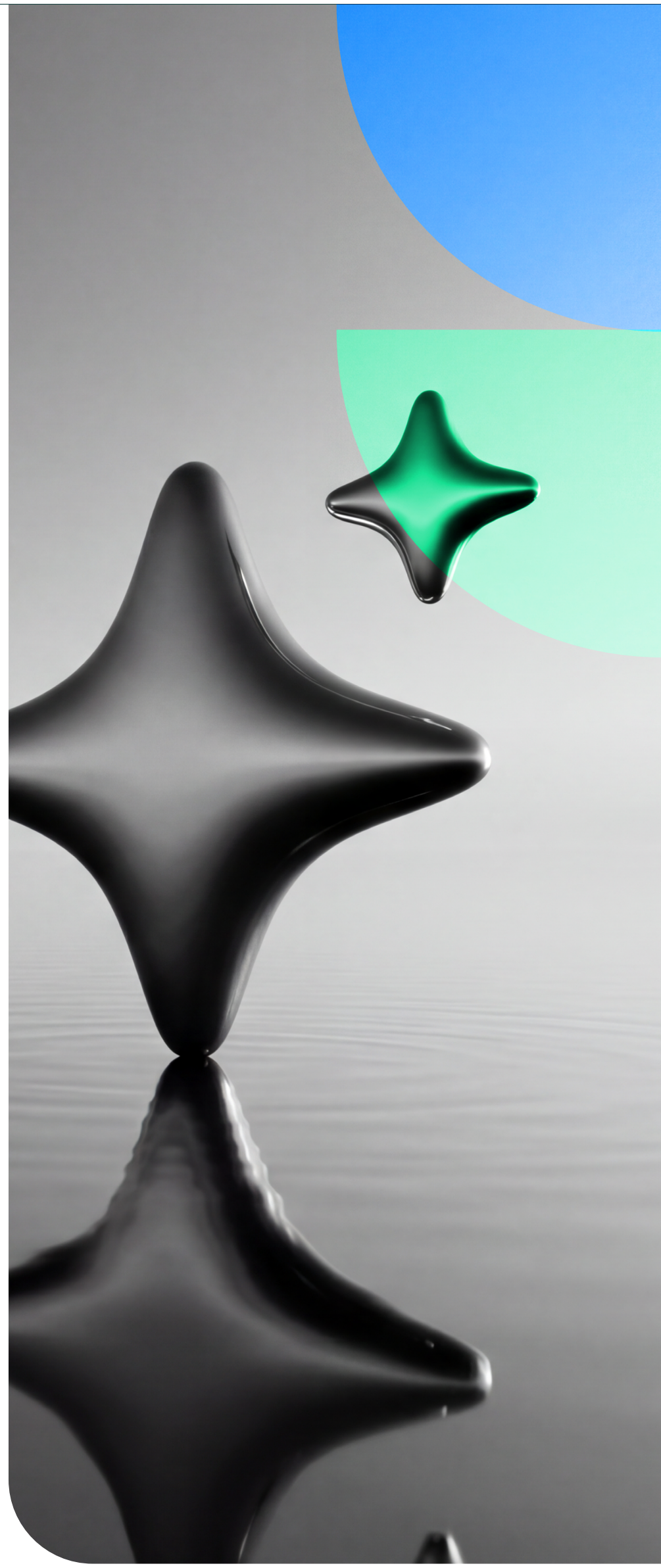
A security layer that only protects the inbox protects just one stage of a multistage attack.

The Solution: Proofpoint Core Email Protection API

Proofpoint Core Email Protection API catches the advanced email threats that get past Microsoft's native filtering. Powered by multi-model Nexus® AI, it understands attacker intent—not just patterns or behavioral signals—to detect novel, AI-generated attacks with high precision.

Protection doesn't stop at the inbox. Automated remediation removes malicious messages after delivery, while integrated protection extends to account takeover, supplier compromise, and messaging security. For organizations that also require pre-delivery protection, Core Email Protection API pairs seamlessly with Proofpoint SEG.

Independently benchmarked by Microsoft as the top-performing integrated cloud email security (ICES) vendor.



Critical Capabilities

1. Multi-model Nexus AI

Traditional email security often relies on a single detection technique, asking, "Does this look different from normal?" Proofpoint asks a different question: "What is this message trying to do?" Multi-model Nexus AI evaluates attacker intent alongside behavioral signals, language, relationships, threat intelligence, and message content to identify novel attacks with greater precision.

- **Understands attacker intent** alongside behavioral signals to detect novel, AI-generated attacks.
- **Inspects URLs and attachments dynamically** using sandboxing to uncover malicious payloads.
- **Learns from unmatched scale**—3.4 million+ customers, 2.37 trillion emails, and 19.5 trillion URLs analyzed annually.
- **Continuously improves protection** as intelligence from one customer strengthens detections for all customers within 18 minutes.

2. One console for every investigation

Modern email attacks rarely stop with a single message. Analysts need complete visibility across the attack chain, not separate tools for separate threats. Threat Protection Workbench brings investigations, evidence, and remediation together in a single workspace.

- **Visualize the entire attack** with the Threat Interaction Map, showing what was detected, who was targeted, how the attack unfolded, and the potential impact.
- **Understand every verdict** with explainable detections, including sender behavior, sandbox results, and confidence scores.
- **Investigate from one console** across API, SEG, account takeover, and supplier compromise without switching tools.

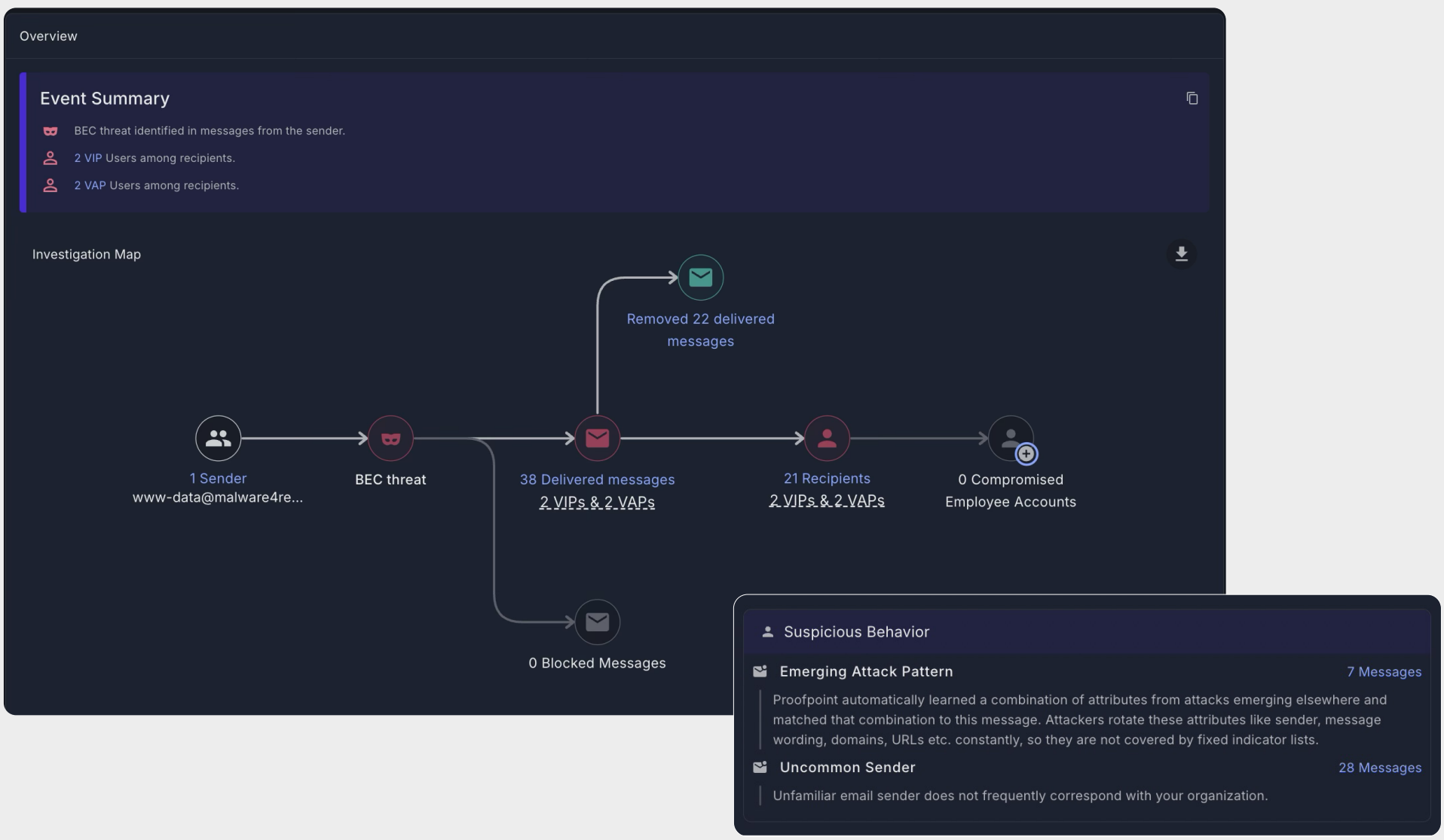


Figure 1. Ensure secure, clean, and HIPAA-aligned transactional patient email.

3. Continuous protection beyond the inbox

Modern attacks don't end when a message reaches the inbox. Protection shouldn't either. Core Email Protection API continues detecting, remediating, and containing attacks as they spread across accounts, collaboration tools, and cloud services.

- **Contain account compromise automatically** by terminating sessions, removing malicious mailbox rules, revoking risky OAuth applications, and reversing unauthorized file sharing.
- **Turn real attacks into better user defenses** by feeding live phishing campaigns directly into AI ThreatFlip Workflow for realistic security awareness training.
- **Extend protection to collaboration tools** with Collaboration Protection, correlating attacks across email, chat, and SaaS applications in a single investigation.
- **Add pre-delivery protection when needed** by pairing seamlessly with Proofpoint SEG for unified pre-delivery, post-delivery, and click-time protection on the same detection engine.

4. Independently validated

Independent testing and real-world threat intelligence demonstrate that Proofpoint consistently catches the attacks Microsoft misses. Combined with industry-leading threat research and global telemetry, Core Email Protection API delivers protection that's continuously validated against today's evolving threats.

- **Ranked the top-performing ICES vendor by Microsoft**, detecting 6.57% of the residual malicious email that Microsoft's native filtering missed—the highest rate among all ICES vendors evaluated and approximately 30% higher than the nearest competitor.
- **Backed by world-class threat intelligence**, with Proofpoint Threat Research tracking approximately 200 threat actors and more than 9,000 active threat campaigns by name.
- **Proven at global scale**, stopping approximately 2.2 billion phishing, 369 million malware, 138 million BEC, and 395 million TOAD attacks every year.
- **Continuously strengthened by global intelligence**, as detections from across the Proofpoint customer base improve protection against emerging threats.

Get Started

Proofpoint Core Email Protection API deploys in as little as 48 hours—no mail-flow changes, no migration project—and closes the gap Microsoft's own data shows is still open.

Learn more at **proofpoint.com**.

About Proofpoint, Inc. Proofpoint, Inc. is a global leader in human- and agent-centric cybersecurity, securing how people, data and AI agents connect across email, cloud and collaboration tools. Proofpoint is a trusted partner to over 80 of the Fortune 100, over 10,000 large enterprises, and millions of smaller organizations in stopping threats, preventing data loss, and building resilience across people and AI workflows. Proofpoint's collaboration and data security platform helps organizations of all sizes protect and empower their people while embracing AI securely and confidently.
Learn more at www.proofpoint.com.

Connect with Proofpoint: LinkedIn

Proofpoint is a registered trademark or tradename of Proofpoint, Inc. in the U.S. and/or other countries. All other trademarks contained herein are the property of their respective owners.