proofpoint®

EBOOK

SEG + API

Continuous protection across the email attack lifecycle.

Email is the primary entry point for cyberattacks, responsible for 94% **of human-targeted threats**. Yet organizations still approach email security in fundamentally different ways. Some stop threats before they reach the inbox. Others focus on detecting and remediating them after delivery.

That inconsistency isn't accidental. It reflects how email security has evolved and why many organizations are now rethinking whether a single approach can keep up.

"It's a factor of history," said Andrew Goodman, director of product marketing at Proofpoint. For years, secure email gateways (SEGs) defined how organizations approached email security, sitting in front of email systems as the primary control point. As cloud platforms like Microsoft 365 became standard, API-based approaches introduced a faster, less disruptive way to deploy protection.

"The barrier to entry for email security was lowered dramatically when API deployment became a popular choice," Goodman explained. "Teams can get world-class protection without any sort of infrastructure change in as little as 15 minutes."

Both approaches persist because they solve different operational challenges. The question is whether either one, on its own, is enough.

The barrier to entry for email security was lowered dramatically when API deployment became a popular choice.

Choosing between SEG and API

Criteria	API-Based Email Security	Secure Email Gateway (SEG)
Time to value	Deploys in days; protection begins at launch	Deploys in weeks; requires deeper upfront investment
Microsoft alignment	Integrates directly into Microsoft Graph API	Deploys ahead of native Microsoft protections
Infrastructure fit	Ideal for simple, Microsoft-first environments	Ideal for advanced, high-security environments
Operational approach	Minimal disruption; no mail flow changes	Requires routing changes and policy configurations
Typical buyer	Lean teams prioritizing speed and simplicity	Security teams prioritizing control and risk reduction

Is a single layer enough?

Gartner made it clear in their Magic Quadrant for Email Security: “The use of overlapping, complementary solutions for email security may be preferable to relying on a single vendor.”

“Treating it as an either/or decision is dangerous,” Goodman said. “There’s a strong argument for defense in depth, just given the fact that organizations have a lot of emails coming through today. But even beyond that, the other definition of defense in depth, where there are certain types of attacks that only certain types of controls can address, is another reason why layered security is important.”

Attackers continuously refine their techniques against known defenses, making controls that operate at a single point in the email flow easier to study and bypass over time.

Some threats, like AI prompt injection, rely on reaching automated systems before any human interaction occurs. “You could have not checked your email in a month,” Goodman explained, “but if you have Copilot checking and responding, you better be careful.”

Others evade those controls entirely. “Threat actors really like to send clean links in email, and then after the email arrives, they add a redirect to a credential harvesting site,” he said.

These patterns highlight a broader shift: the email attack surface now spans before delivery, during user interaction and after the message is received. Effective protection requires visibility and control across that full threat lifecycle — something a single layer cannot provide on its own.

Bridging the gap with integrated protection

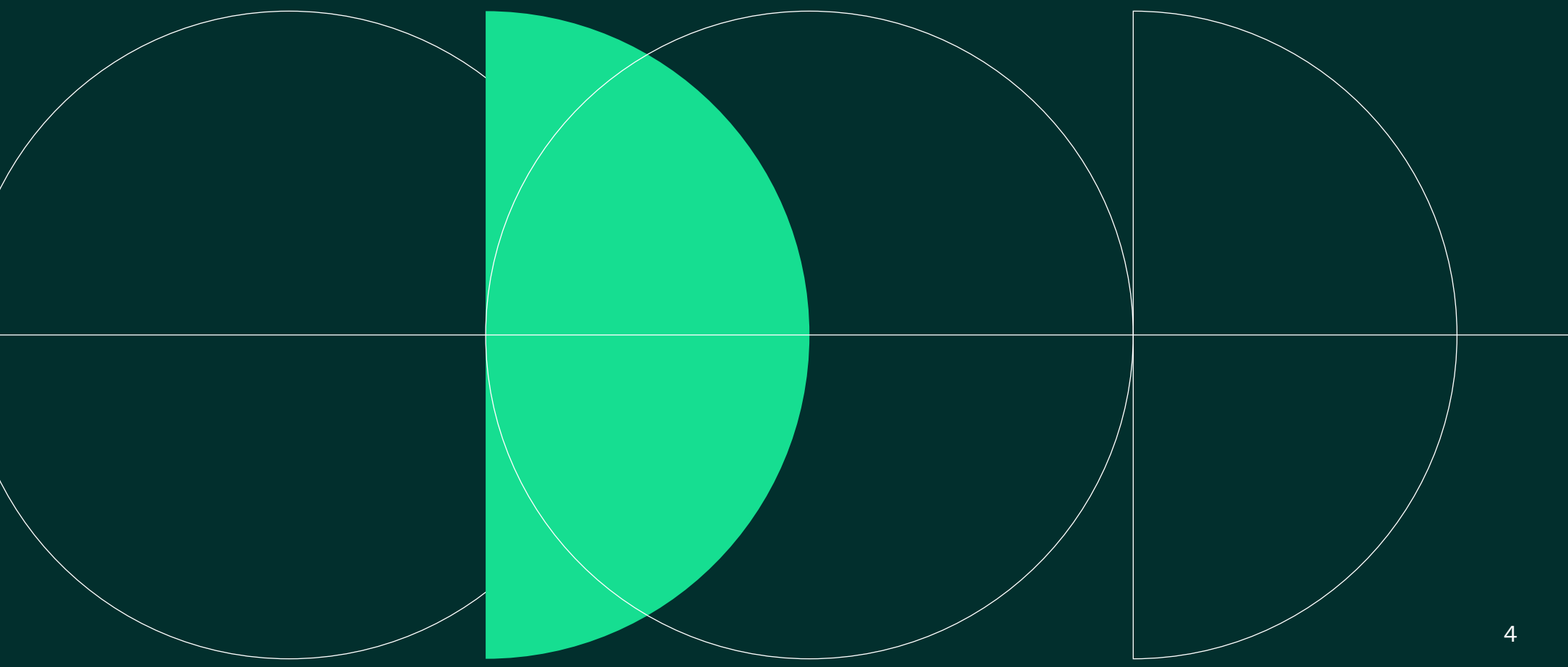
Proofpoint's approach is built for a threat landscape that continues to evolve in both scale and sophistication, without requiring organizations to choose a single security model upfront.

Core Email Protection supports both SEG and API-based deployments within a single platform, allowing organizations to apply protection where it's most effective while maintaining flexibility as their needs change. That flexibility extends directly to day-to-day operations.

"You don't even have to move workflows when switching from one to the other," Goodman said. "It's the same panel, same button, same list of threats. We're just changing where the control happens."

Advantages of SEG + API

- **Continuous Protection:** Prevention, continuous detection, remediation, and click-time control, not a post-delivery-only approach.
- **Broader Coverage:** Stop internal-internal malicious mail and close direct send coverage gaps with protection in the mailbox
- **Intelligence Convergence:** Threat intelligence flows between gateway and API layers, with findings from one informing detection in the other, improving accuracy and eliminating blind spots
- **Rapid Incident Response:** Unified investigation and automated remediation across gateway and API accelerates threat containment without switching between separate systems or tools
- **Reduced Complexity & Cost:** One security team, one platform, one console replaces fragmented gateway and API solutions—cutting management overhead, training burden, and total cost of ownership



Building resilience for what's next

Looking ahead, the biggest challenge for organizations may not be any single threat, but rather the pace at which the threat landscape is changing.

Email itself isn't going away. If anything, its role is expanding. New use cases, from machine-generated messages to automated agents, are increasing both the volume and the number of ways it's used across organizations. At the same time, email remains a primary threat vector.

What is changing is how those attacks are executed. So far, advances in AI have driven scale more than novelty. The result is a surge in highly targeted attacks delivered at volume—messages that reflect real relationships, business processes and context. Campaigns that once took time to develop are now generated, tested and refined automatically.

"This is not a Nigerian prince scam," Goodman warned. "They will try to compromise you however they can."

This is where architectural decisions made today become critical. By combining flexible deployment options with shared intelligence, automation and full-lifecycle coverage, Proofpoint allows organizations to evolve their defenses without rebuilding them. As the scale and sophistication of attacks continue to increase, organizations that can adapt their defenses will be better positioned to maintain security, continuity and trust in the years ahead.

About Proofpoint

People protection

3.4 T
Emails scanned per year

>1.4 T
SMS/MMS scanned per year

124 M
BEC attacks stopped per month

>183 M
Phishing simulations per year

0.8 T
Attachments scanned per year

21 T
URLs scanned per year

177 M
Telephone-oriented attacks stopped per year

Market adoption

2.7 M+
Customers

150 +
Global ISP and mobile operators

80 %
F100 protected by Proofpoint

57 %
F100 using Proofpoint DLP

>63 %
F1000 protected by Proofpoint

proofpoint®

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

DISCOVER THE PROOFPOINT PLATFORM →

7/26