

Email Security: API-Based Proof of Value

*Surface dormant threats. Monitor live mail.
Make an informed decision.*

The Challenge

Email-based threats are growing in volume and sophistication, and phishing is leading the charge. AI has made it faster, more personal, and harder to catch - the 2026 Verizon DBIR ⁽¹⁾ found phishing accounted for 44% of all AI-assisted initial access vectors. As attackers grow adept at bypassing built-in protection, Mimecast finds that 28% of emails reaching mailboxes are still malicious or unwanted, pushing organizations toward API-based email security that remediates threats from mailboxes in seconds. The method hasn't changed; the scale and sophistication have.

Yet evaluating security posture against this shifting landscape has historically come with real limitations:

- No visibility into threats already sitting in inboxes before live evaluation begins
- Evaluations often require changing existing security Microsoft policies
- Evaluation tools often demand MX record changes, disrupting live operations

The Solution

Mimecast's API-based protection for email connects directly to Microsoft 365 via the Microsoft Graph API - no gateway infrastructure, no MX record changes, no disruption to existing mail flow or security policies. The evaluation runs in two phases: an optional retrospective scan of historical inbox mail, followed by

continuous real-time monitoring. Both are powered by Mimecast's complete threat detection engine.

Unlike evaluations that only observe future mail, this proof of value can give prospects immediate, evidence-based answers to the two questions that matter most: what has your current security already let through, and how does the tool perform in live daily operations? Detections are fully visible throughout, while monitor policies can keep mail flow completely uninterrupted. The proof of value is optimized to give security teams the confidence to make an informed commercial decision

28% of emails reaching mailboxes is found either malicious or unwanted by Mimecast ⁽²⁾

- **Uncover threats already hiding in your inboxes**, before live scanning even starts
- **Zero infrastructure changes, no deliverability risk.** Connects via Microsoft Graph API
- **Automated threat reports.** Ready to share with stakeholders straight out of the box
- **Evaluation to full production, no reconfiguration.** What you test is what you deploy

Verizon DBIR 2026: <https://www.verizon.com/business/resources/reports/dbir/>

Mimecast Threat Intelligence, Mailbox-Level Scanning Analysis (n=13,453,544 emails, 60-day period)

Gartner MQ for Email Security 2025: <https://www.mimecast.com/resources/analyst-reports/mimecast-leader-gartner-email-security/>

Key Capabilities

Threat Scan - Optional	<ul style="list-style-type: none">• 30-day retrospective scan after completing configuration - real emails, real users, real environment. Detects phishing, BEC, credential harvesting, malware, ransomware, and impersonation attacks already present your inboxes• Prospect-initiated with explicit consent - runs once, results are clean and auditable• Generates a dedicated Threat Scan Report on completion, downloadable and share-ready in PDF format
Live Mail Scanning	<ul style="list-style-type: none">• 30 Days of live threat detection via Graph API - zero mail flow disruption during POV• Completely non-intrusive: no rerouting, no modifications, no changes to existing security policies• Threats surface instantly in Mimecast's Analysis & Response ready for review• One click to move policies from monitor to protection when you are ready to act
Threat Coverage	<ul style="list-style-type: none">• Surfaces AI-assisted phishing, business email compromise, credential harvesting, zero-day malware, impersonation, spam, and graymail• Backed by 40+ intercorrelated detection layers and Mimecast AI, processing over 18 billion security events every day
Reporting & Evaluation Management	<ul style="list-style-type: none">• Threat Scan Report reveals dormant threats already hiding in mailboxes - categorized by threat type, top targeted users, volume trends, and industry benchmarks. Downloadable as a PDF for easy stakeholder sharing• On-demand and scheduled reporting, accessible to both the Mimecast solution engineer and prospect throughout the evaluation• Seamless conversion to production: all configurations and report history carry over automatically

42,000 +

Organizations trust
Mimecast globally

LEADER

Gartner MQ for
Email Security 2025

18 BILLION +

Security events analyzed
daily by Mimecast AI

Understand the value of Mimecast email security and request an API-based Proof of Value via: <https://www.mimecast.com/proof-of-value/>