DATASHEET

Email Security, MX-Based Protection

Your AI-powered email security & resilience companion

The Problem

Advanced phishing attacks, business email compromise (BEC) scams, and malicious tactics are just some of the email threats your organization must combat. E-mail security solutions struggle to keep pace, frequently missing advanced social engineering attempts, zero-day malware, and domain spoofing attacks—leaving your business communications exposed to compromise. And as attackers increase focus on platforms like M365 and Google Workspace, a layered email security approach has become essential.

The Solution

As a cloud-based Secure Email Gateway, Mimecast's MX-Based Protection is designed to keep even the most complex email environments secure through its multi-layered inspection capabilities, powered by traditional defenses, threat intelligence, and advanced AI. Our comprehensive solution inspects every element of an email in real-time, stopping threats before they reach your inbox. With customizable policies, granular controls, and a broad range of complementary solutions, this solution seamlessly integrates with your existing security stack while providing automated remediation capabilities. This enables IT and security teams to effectively control risk while taming complexity, empowering your organization to defend against sophisticated email attacks without compromising business continuity.

$6.3 BILLION
in losses due to BEC in 2024[1]

40%
of email attacks involve BEC and pretexting[1]

Mimecast Value

- **Get The Best Protection**
  Block all email-based threats with AI-powered, industry-leading detection, trusted by 42K customers.
- **Tame Complexity**
  Easily manage complex email environments; consolidate and simplify security services.
- **Simplify Security Operations**
  Reduce the burden, keep people informed & empowered.

1 https://www.verizon.com/business/resources/reports/dbir/

Feature	Details
BEC	• Protection against social engineering, homoglyph/homograph deception, and impersonation attacks • Relationship strength analysis between the sender and recipients within the organization* • Detection of threat-specific language within emails related to BEC threat categories, such as requests for help with a task, fake wire transfers, urgency, communication channel switches, gift card, banking, and finance scams* • Focus on understanding the context, nuances, and implications of the message to accurately interpret the true intention* • AI-driven email warning banners that are surfaced and updated in real-time across devices based on risk level*
Insider Threats	• Detection of potentially misaddressed emails to defend against data leaks • Analysis of internal and outbound emails to protect against compromised, careless, and malicious insiders
Malware	• Multi-layered malware protection against known and zero-day threats • Static file analysis and full emulation sandboxing • Safe-file conversion of attachments into benign PDF documents • Decryption portal enables password-protected malware and URL scanning
Phishing	• URL rewriting of all links in emails, with time-of-click scanning • Multi-stage deep URL scanning with machine learning-based threat detection and credential protection • QR codes protection in emails and attachments with deep URL scanning • Direct download links are scanned through static file analysis and sandboxing
Administration	• Central administration through a single, web-based console • Support for M365, Google Workspace, on-premises, hybrid, and others • Advanced and federated account administration supporting frequent M&A activities • Intelligent email routing based on indicators, recipients or policies • Automated synchronization with IAM for policy and access control • Centralized threat intelligence and streamlined administrative workflows • Automated or manual remediation of unsafe, unwanted, or malicious emails • Ingest threat feeds specific to your tenant and regional threat trends into your SIEM, SOAR, or TIP • Easy integration with vendors including Splunk, CrowdStrike, Netskope, and others
Available Add-Ons	• Cloud Archive • Continuity • DMARC Analyzer • Large File Send • Mimecast Engage • Mimecast Email Incident Response • Secure Messaging

Email Security Use Cases

Phishing and Business Email Compromise (BEC) Attacks

Mimecast's defense against sophisticated phishing and BEC attacks is tightly integrated. Threat feeds and email authentication protocols inspect emails, followed by Natural Language Processing (NLP) for text extraction and threat modeling to analyze contextual clues and identify payloadless threats, stopping them before they reach users' inboxes. The social graph technology creates an identity graph of sender-recipient relationships, enabling the detection of anomalous activities with dynamic banners that alert users to potential threats. The platform's attachment and URL scanning capabilities, including Credential Theft Protection and Multi-stage Attack Detection, scan all links to detect phishing pages.

Malware and Ransomware Threats

Mimecast's comprehensive malware detection system employs multiple layers of protection to ensure maximum security. Files are checked against Mimecast's proprietary database, which maintains a record of previously scanned files and can integrate with customer-specific threat intelligence data. For enhanced security, multiple antivirus engines are utilized to catch a wider range of malware threats. Rapid static analysis of files is performed, checking for suspicious characteristics such as hidden code, unusual structures, or connections to known malicious sites. Finally, files undergo detailed analysis in a full emulation sandbox environment, which simulates a complete computer system. Optionally, through safe file conversion, potentially dangerous executables can be stripped away before file delivery.

Mitigating a Phishing Attack

In the event of a phishing attack, native remediation tools within the Mimecast can be used to efficiently manage and mitigate threats without relying on external systems. Through Analysis and Response, analysts can quickly identify the scope of the threat and search for further indicators of compromise, simplifying the process of threat categorization and response. Threat Remediation allows for the streamlined removal of affected emails directly from user inboxes, minimizing potential damage and ensuring rapid response. Additionally, these remediation capabilities can be utilized through integrated tools like SOAR or XDR platforms.