DATASHEET

Email Security Cloud Integrated

Protect your M365 investment with an AI-powered email security solution.

The Problem

Microsoft 365's native security features – including Exchange Online Protection (EOP) and Microsoft Defender for Office 365 – are increasingly challenged by today's sophisticated threat landscape. While these tools provide fundamental collaboration security, they struggle to detect and stop advanced attacks that exploit Microsoft's standardized security architecture. Threat actors are now bypassing Microsoft's traditional defenses through sophisticated social engineering, business email compromise, and AI-powered attacks that appear legitimate to rule-based detection systems. Recent security incidents highlight the limitations of relying solely on native Microsoft security. Organizations face additional challenges with Microsoft's complex security configuration requirements and the restriction of advanced protection features to premium licenses. This security gap demands a more sophisticated approach.

The Solution

Mimecast Email Security Cloud Integrated delivers comprehensive protection by augmenting Microsoft 365's native email security capabilities through an advanced, multi-layered approach. Powered by advanced AI, Cloud Integrated seamlessly integrates with Microsoft 365 to provide best-in-class detection capabilities that block even the most sophisticated email attacks. Advanced behavioral analysis capabilities continuously monitor communication patterns, leveraging social graphing to detect anomalies, combined with NLP-based threat- language detection to stop Business Email Compromise attempts before they reach user inboxes. Organizations benefit from a solution that's optimized out of the box, featuring simplified administration through an intuitive interface that can be deployed in under five minutes.

$2.9 BILLION IN LOSSES

due to BEC in 2023[1]

40% OF EMAIL ATTACKS

involve BEC and pretexting[2]

Mimecast Value

- **Get AI-powered, best-in-class email security**
  Protect your organization with AI-powered, industry-leading detection, trusted by 42K customers.
- **Close gaps in M365 email protection**
  Stop the threats that Microsoft misses – the equivalent of a malware, phishing, or untrustworthy email getting through to employees every seven hours.
- **Dramatically simplify email security administration**
  Spend less time managing email security with a solution that's optimized out of the box, highly intuitive, and fully deployed in less than five minutes.

1. www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report

2. www.verizon.com/business/resources/reports/dbir/

Feature	Details

BEC	• Analyze relationship strength between the sender and recipients
	• Detect threat-specific language within emails related to BEC threat categories, including:
	  • Requests for help with tasks
	  • Fake wire transfers
	  • Urgency indicators
	  • Communication channel switches
	  • Gift card scams
	  • Banking and finance scams
	• Interpret the context, nuances, and implications of messages to determine true intention
	• Update AI-driven email warning banners in real-time across all devices

Insider Threats	• Analysis of internal and outbound emails to protect against lateral spread of malware and phishing links
Malware	• Quarantine known bad files through automated detection • Scan password-protected attachments for potential threats • Inspection through multi-layered malware protection to defend against known threats and zero-day attacks • Perform static file analysis and execute sandbox testing for suspicious files
Phishing	• Rewrite all links in emails and subject lines to enable time-of-click scanning • Scan links through multi-stage analysis using machine learning-based threat detection • Protect against credential theft and malicious QR codes in emails and attachments • Isolate browsers when accessing unknown domains • Analyze direct download links through static file scanning and sandbox testing
Administration	• Manage administration centrally through a single, web-based console • Configure admin and end user notifications for detections • Access detailed information per detection for easy analysis • Create customizable policies to suit organizational requirements • Enable end user native reporting in Microsoft Outlook • Remediate malicious emails with one-click action • Restore Mimecast configuration in the event of setup errors • Integrate seamlessly with vendors including Splunk, Microsoft, and others

Feature	Details
Threat Scan	• Scan for threats without interrupting mail flow • 30-day look back scan
Available Add-Ons	• Collaboration Security • DMARC Analyzer • Mimecast Engage • Sync and Recover

Use Cases

Phishing and Business Email Compromise (BEC) Attacks

Mimecast's defense against sophisticated phishing and BEC attacks operates as an integrated platform. The process begins when threat feeds and email authentication protocols inspect incoming emails. Natural Language Processing (NLP) then extracts text and employs threat modeling to analyze contextual clues, identifying payloadless threats before they reach users' inboxes. Social graphing builds an identity graph based on sender-recipient relationships, enabling it to detect anomalous activities. When potential threats are identified, dynamic banners alert users to these risks. Attachment and link scanning features operate together, including Credential Theft Protection and Multi-stage Attack Detection, which examine all links to identify concealed phishing pages and malicious content.

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. For enhanced security, multiple antivirus engines are utilized to catch a wider range of 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.

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 the detection home page, admins 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 deletion of affected emails, minimizing potential damage and ensuring rapid response.