mimecast®

DATASHEET

Mimecast Targeted Threat Protection: Internal Email Protect

AN INSIDE LOOK AT THREATS ON THE INSIDE

For many years the use of email in cyberattacks has proven to be very effective for attackers. The goal of most cybercriminals is to get in and around your organization as quickly and quietly as possible, with the ultimate goal of stealing your sensitive information or locking your systems or data and ransoming access back to you.

And email has proven to be a very effective system for them to accomplish this. The ubiquity and speed of email works against the defenders. In the vast majority of cases, mostly without their knowledge or understanding, your staff plays an integral role in these attacks. According to Forrester, insiders accounted for 39 percent of data breaches in 2015 through accidental or misuse of data. Think a threat cannot spread via email once it is inside your organization's four walls? Think again.

To combat this threat Mimecast provides Internal Email Protect, a threat monitoring and remediation service for internally generated email, delivered as a purely cloud-based security service. Internal Email Protect expands the capabilities of the Mimecast Targeted Threat Protection solution, enabling organizations to monitor, detect and remediate email-borne security threats that originate from within their email systems, whether the emails are destined for other internal users or out to users in external email domains.

Internal Email Protect includes the scanning of attachments and URLs for malware and malicious links as well as content filtering enforced by Data Leak Prevention services. In addition, Internal Email Protect includes the ability to automatically delete infected emails and attachments from employees' inboxes.

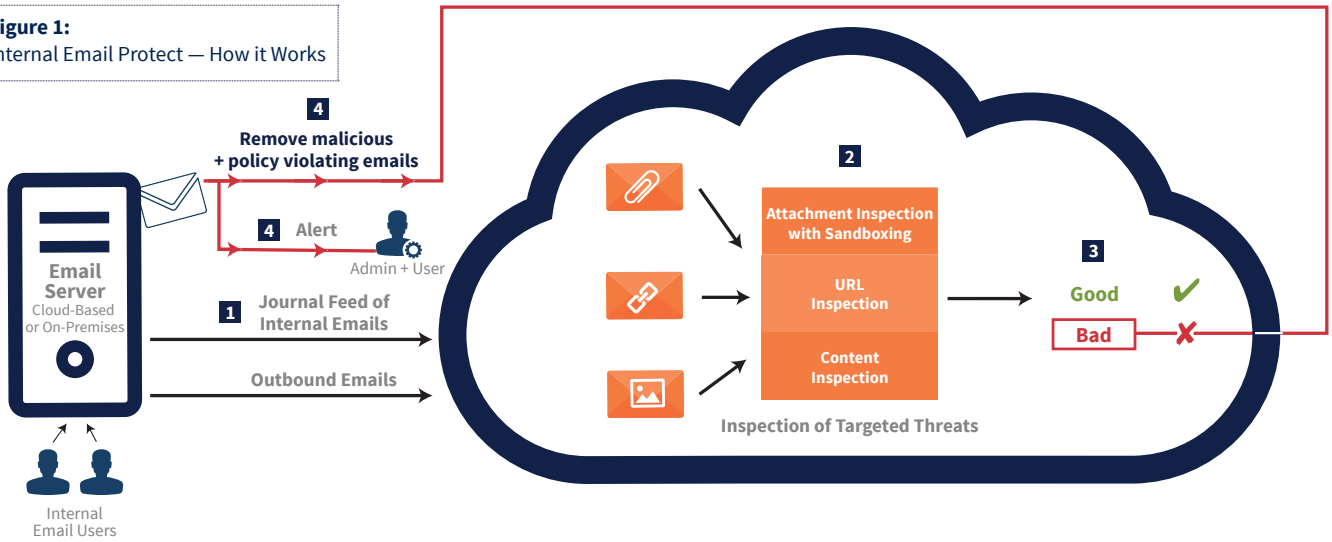
To round out your email security defenses you need to consider – and plan to combat – three types of internal threat profiles:

1. **The Compromised Insider -** External attackers often take over the accounts or systems of unsuspecting users through credential harvesting, social engineering, phishing emails, and the installation of various forms of malware – like ransomware, remote-access Trojans or key loggers. While many of these takeovers are initiated via email, Web drive-bys and botnets can also be the cause of compromise. In a recent survey conducted by Forrester, 63% of respondents reported that Compromised Insiders have been involved in security incidents in the past 24 months.*
2. **The Careless Insider -** There are employees at every organization who ignore or simply don't fully understand the organization's security policies and rules. While ignoring these policies is not done with malicious intent, the actions – such as sending sensitive information insecurely - puts the organization at greater risk of sensitive data leakage and malware infections. In the same survey conducted by Forrester, 61% of respondents reported to be very concerned or concerned about the threat posed by Careless Insiders inside their organizations.*
3. **The Malicious Insider -** Though not common, malicious insiders do exist. And when they strike, they can cause

KEY CAPABILITIES:

- Provides comprehensive protection from targeted threats as a complement to Mimecast Attachment Protect, URL Protect, and Impersonation Protect
- Single cloud solution to inspect email coming into, going out of and staying within an organization.
- Detection of lateral movement of attacks via email from one internal user, to another.
- Identification of threats or sensitive data leaving an organization that can result in reputational damage.
- Automated removal of internal emails which are determined to contain threats.
- Reduced risk of a breach or damaging security incident spreading throughout the organization.
- Single administration console for reporting, configuration and management across entire email security solution.
- 100% cloud-based solution

Figure 1:
Internal Email Protect — How it Works



significant damage. These employees either intend to profit personally from, or do damage to the organization by stealing, leaking or compromising confidential data and systems. In the same Forrester survey it was found that 64% of organizations had significant or moderate financial losses in the past 24 months from incidents that were traced to Malicious Insiders.*

How it Works For Internal Emails

- Email is sent from one internal user account to another internal user account. This email does not pass through the Mimecast Email Security Gateway as it does not exit the organization's email environment.
- The email server sends a regular journal feed to the Mimecast service.
- The Mimecast Internal Email Protect service analyzes the emails in the journal feed for malware attachments, malicious URLs, and sensitive content.
- At the option of the customer, for all "bad" emails, Internal Email Protect can either automatically reach into the inboxes of the recipient and remove the malicious or policy violating emails or attachments or alert the administrator and user to the existence of these emails.

How it Works for Internal Emails Going to External Users

- Email is sent from an internal user account to an external email address. This email passes through the Mimecast Email Security Gateway on exit.
- The Mimecast Internal Email Protect service analyzes the emails for malware attachments and malicious URLs when passed through the gateway.
- Emails with malware attachments or containing malicious URL are blocked by the Mimecast service. At the option of the organization and based on configurable policies, outbound emails containing sensitive content can either be blocked or forced to use Mimecast's Secure Messaging Service, if available.

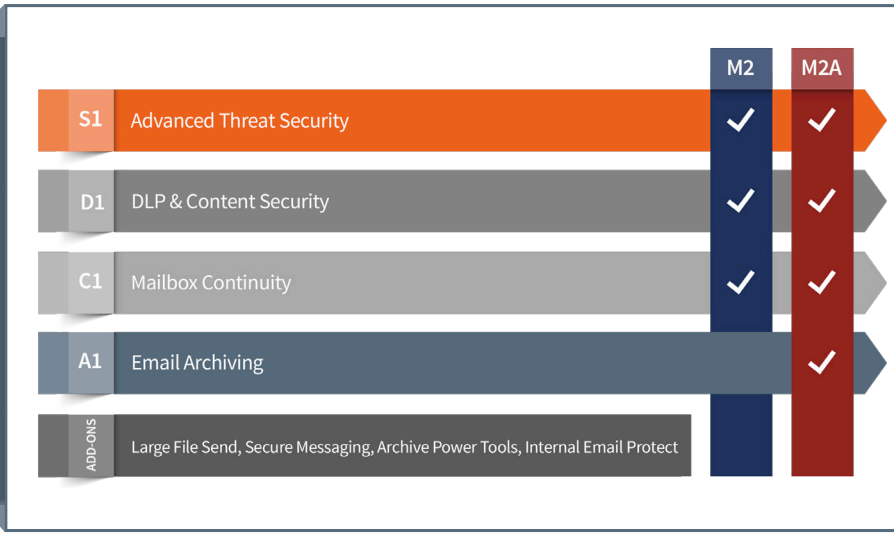
*Forrester, Mimecast Technology Adoption Profile, February 2017.

Make Email Safer for Business

Mimecast integrated service bundles deliver the ultimate in cyber security, resiliency and archiving. Get comprehensive risk management or address specific requirements - all in a single platform.

LEARN MORE

mimecast.com/products/email-management-bundles/



Mimecast (NASDAQ: MIME) makes business email and data safer for thousands of customers with millions of employees worldwide. Founded in 2003, the company's next-generation cloud-based security, archiving and continuity services protect email and deliver comprehensive email risk management.