Datasheet

mimecast

Internal Email Protect

Advanced protection against threats in internal and outbound email

Mimecast Internal Email Protect applies best-practice security inspections to internal and outbound email traffic, allowing organizations to monitor, detect, and remediate security threats that originate from within their email systems. Threats like these include compromised users whose accounts are being taken advantage of, un-compromised users who engage with malicious, credential harvesting links, and simple employee mistakes.

A 100% cloud-based service, it includes scanning of attachments and URLs, as well as content inspections for violations of data leak prevention policies. Internal Email Protect is a component of Mimecast's Targeted Threat Protection service and integrates seamlessly with Mimecast's full suite of security solutions. It provides the following core capabilities:

1. **Journaling of internal email for the inspection of threats:** Internal Email Protect allows you to integrate a journal feed from your email server to Mimecast to conduct security checks on internal traffic. This inspection process monitors internal and outbound email, conducts data leak prevention inspections of the content, and performs deep analysis of attachments and URLs.

2. **Content remediation:**
When Internal Email Protect detects unsafe, undesirable, or malicious content, you have the option to remediate this content from end-user mailboxes either automatically (i.e., the infected email will disappear from the inbox with an optional notification to the end user), or through the manual intervention of the administrator. This reduces the exposure time to malicious emails/content and also identifies all instances of the malicious content (e.g. forwarded emails, distribution list recipients) to be removed from the mailbox(es) and archive.

   Content remediation includes the ability to be triggered via API by orchestration and response tools, and delivers a full log of remediation activity.

Key Capabilities

- Provides comprehensive protection from threats originating from internal and outbound email.
- Detects lateral movement of attacks via email from one internal user to another.
- Identifies and prevents threats or sensitive data from leaving an organization.
- Automates the detection and removal of internal emails that are determined to contain threats.
- Continuously rechecks delivered files to identify previously unidentified malware.
- Supports automatic and manual remediation of emails determined to be malicious or undesirable post-delivery.
- When used with the Mimecast Security Agent, supports manually triggered removal of saved attachments.
- Provides a Threat Remediation Dashboard that allows for search and remediation based on administrator and/or organizational requirements.
- Simplifies administration with a single console across Mimecast's entire email security solution.
- Increases employees' security awareness by notifying them when malicious emails are found.

3. **Threat Remediation Dashboard:**
Administrators may want to monitor, search, and manually remediate specific emails. Mimecast provides a dashboard within the administration console that gives you full visibility of email traffic and threats enterprise-wide, and allows search based on message ID and attachment file hash, as well as from and/or to address.

Understanding the Risk

In Mimecast's **2019 State of Email Security Report,** data from Vanson Bourne showed that many firms have experienced some form of insider-aided security incident within the last year:

- 41% of respondents saw internal threats or data leaks increase over the previous 12 months.
- 71% saw an attack where malicious activity was spread from one infected user to other employees (up from 64% last year).
- 61% believe it's likely or inevitable they'll suffer a negative business impact from an email-borne attack.

However, most organizations don't have the advanced inside-the-perimeter defenses – like data leak prevention, remediation, URL inspection, and sophisticated malware detection – required to effectively protect against:

- **Compromised insiders:** External attackers take over the accounts, credentials, or systems of unsuspecting users through credential harvesting, impersonation attacks, phishing emails, or the installation of various forms of malware. These attacks can spread when the attacker uses compromised accounts to distribute malware or send phishing emails. Accounts can also be used to exfiltrate data.
- **Careless insiders:** These are employees who don't fully understand or simply ignore security policies and rules or who make innocent mistakes.
- **Malicious and/or abusive insiders:** Whether the damage be done with malicious intent or the behavior via email is particularly inappropriate, employees' insider status uniquely positions them to cause significant harm.

Build Trust from the Inside

As email-borne cyberattacks grow in both volume and sophistication, you need comprehensive, proven email security strategies that are as agile, smart, and adaptable as the methods used by those who seek to cause harm. Mimecast Internal Email Protect both continuously rechecks previously delivered inbound files to identify malware that wasn't initially detected and allows you to automatically or manually reach back in to users' inboxes to remove unsafe or undesirable emails. By applying world-class security protocols to ALL organizational email, you will reduce both cost and complexity while expanding your ability to safeguard employees, intellectual property, customer data, and your organization's brand reputation.