mimecast | Datasheet

Mimecast Internal Email Protect

Build trust on the inside

When evaluating and building cybersecurity strategies, most organizations focus primarily on inbound emails, treating their operations essentially like castles. They build high walls, dig deep moats, and put sentries in every tower to ensure their perimeters are secure, all the while assuming there's little to no risk from those who reside within their four walls.

The reality is that there is significant danger inside the perimeter as well. Emails sent between users or to third parties like customers and suppliers typically represent 60% of an organization's email traffic[1]; however, they are often left under protected. Employees frequently become unwitting participants in attacks as a result.

When organizations lack inside-the-perimeter defenses, they also typically lack visibility of internal and outbound email traffic, making it difficult to identify the source of attacks and opening the door to significant and lasting damage. They are also unable to effectively guard against the inadvertent or intentional distribution of sensitive information, minimize the damage when leaks or attacks do occur, and meet a growing need to monitor communications for inappropriate or policy-prohibited content.

The problem is not one to be taken lightly. In Mimecast's **2018 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:

- 80% of surveyed companies had experienced threats caused by attackers infiltrating and compromising users' email accounts.
- 88% were exposed to attacks by the actions of careless users.
- 61% had malicious activity spread from one infected user to other employees via email.

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 internally generated email traffic. The conclusion: It's time to take inside-the-perimeter threats seriously.

Protection from the inside out

Mimecast Internal Email Protect applies best-practice security protocols to the inspection of internal and outbound email, delivering:

1. **Advanced threat remediation,** including continuous rechecking of emails and automatic or manual remediation of malicious or undesirable emails post-delivery.
2. **Rapid threat detection,** to prevent the lateral movement of attacks and minimize damage.
3. **Reputational protection,** by preventing the spread of attacks to third parties and protecting against the exposure of sensitive information.
4. **Full visibility** into internal and outbound email, which typically represents 60% or more of an organization's email traffic.
5. **Seamless connection** to the Mimecast security eco-system.

Understanding the Risk

Your organization faces a wide variety of risks when internal email traffic is left unprotected, many of which you've likely experienced first-hand. There's the infected email attachment sent from user to user, the email containing confidential information (e.g., a salary spreadsheet) that was sent accidentally, or the compromised account that's used to send infected emails internally or outbound.

Internal email attacks originate in a number of ways, but human error nearly always plays a supporting role. When the anatomy of these attacks is analyzed, most can be attributed to two general categories of users.

The first is the **compromised insider.** 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 then easily be spread internally via email and even worse, externally to customers, partners, and suppliers.

The second is **careless insiders.** These are employees who don't fully understand or simply ignore security policies and rules or who make innocent – even well-intentioned – mistakes. While these users' actions aren't undertaken with malicious intent, they do increase risk.

And although less common, organizations also face risks from malicious and/or abusive insiders who are disgruntled, behaving inappropriately, or who intentionally seek to do damage. While unusual, the acts perpetrated by these individuals can be particularly damaging, as employees' insider status uniquely positions them to cause significant harm.

Mimecast Internal Email Protect

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. A 100% cloud-based service, it includes scanning of attachments and URLs, as well as 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 scans 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.

3. **Threat Remediation Dashboard.** Administrators may want to monitor, search, and manually remediate specific emails. Mimecast provides a dashboard within the administrative 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.

The Internal Email Protect Time Machine

Ever wish you could turn back time and prevent an employee from sending “that” email? If only there were a better way of addressing the problem than sending a recall notice that only draws more attention to the email you fervently wish hadn’t gone out in the first place. Thanks to Internal Email Protect from Mimecast, now there is. Just as no email security system is infallible, no organization has employees who will never make mistakes, so the key is being able to minimize damage when attacks, breaches, and missteps do occur. 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 infected emails or those sent by mistake or with malicious intent. It may not be as if the event never happened, but it’s about as close as you can get.

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 applies world-class security protocols to ALL organizational email, reducing both cost and complexity while expanding your ability to safeguard employees, intellectual property, customer data, and your organization’s brand reputation.

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 or manual remediation of emails determined to be malicious or undesirable post-delivery.
- Provides a Threat Remediation Dashboard that allows for search and remediation based on administrator and/or organizational requirements.
- Reduces the risk of a breach or damaging security incident spreading throughout the organization.
- 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.
- Provides flexibility, scalability, high performance, and continuous innovation thanks to the solution’s multi-tenant cloud architecture.

[1] Based on aggregated data from Mimecast Internal Email Protect customers

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.