Data Sheet

mimecast

Insider Risk Protection

Get advanced protection against threats in internal and outbound email with Internal Email Protect

It’s a common misconception that email-borne attacks come only from the outside. While most attacks do start there, attackers typically look to land and expand once they are inside an organization. Despite this risk and the fact that the majority of email volume is internal, many organizations lack the protections – like data leak prevention, remediation, URL inspection, and sophisticated malware detection – required to keep attacks from spreading internally or outbound to customers and partners. Compromised and careless insiders, along with the rare but extremely dangerous malicious insider, pose outsized risk.

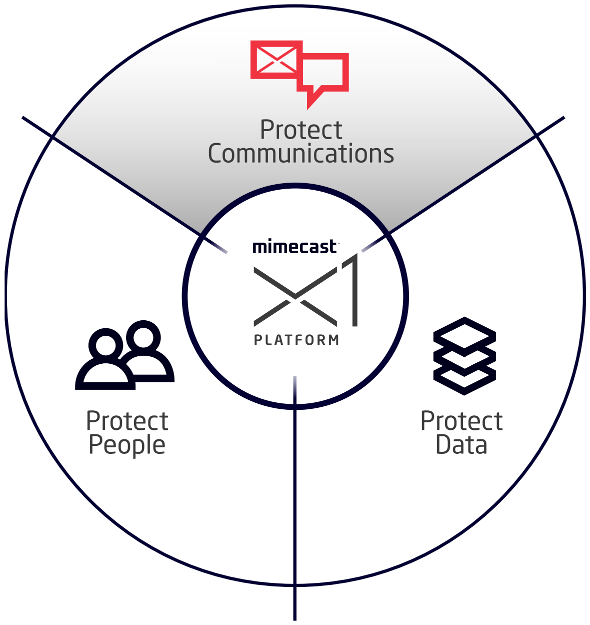
Build trust on the inside

Mimecast’s Internal Email Protect solution applies best-practice security inspections to internal and outbound email traffic, allowing you to monitor, detect, and remediate security threats that originate from within your email systems. From compromised users whose accounts are being exploited by attackers to employees who engage with malicious links or simply make mistakes, this solution provides an additional layer of protection designed to keep you secure. A 100% cloud-based service, Internal Email Protect includes scanning of attachments and URLs, as well as content inspections for violations of data leak prevention policies.

Key Benefits

Internal Email Protect

- Provides comprehensive protection from threats originating in 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
- Enables removal of saved attachments when used in conjunction with Mimecast’s Web Security solution and Security Agent



Quickly and easily remove dangerous emails from employees' inboxes

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 activities.

Block internal and outbound email threats

Internal Email Protect applies best-practice email inspections to internal and outbound email, including deep analysis of attachments and URLs, as well as content inspections for violations of data leak prevention policies. A 100% cloud-based service, it supports all types of email environments – from Microsoft 365 and Google Workspace to on-premise Exchange and hybrid.

Get full visibility of email traffic and threats enterprise-wide

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.

> "Our email security added the same static warnings to all emails, and our users became numb to them. Mimecast's banners convey engaging contextual information about the threat and are automatically updated as the artificial intelligence learns more about it."
>
> **IT Director, Chicago-based PE firm**