Mimecast Advanced Security

Cloud-Based email security services that help to protect your organization from advanced email-borne threats

Mimecast Advanced Security is a set of cloud services that help organizations defend against advanced email-borne threats. The Mimecast services defend against email-borne impersonation attempts, malicious URLs and malware attachments, threats that are internal to the organization, as well as spam and viruses.

The Mimecast services include:

1. MIMECAST TARGETED THREAT PROTECTION (TTP)
   Inspection of inbound, outbound and internal emails to help detect and fight phishing, ransomware, impersonation attempts, malicious URLs and attachments. TTP includes URL Protect, Attachment Protect, Impersonation Protect and Internal Email Protect.
2. CONTENT CONTROL & DATA LEAK PREVENTION (DLP)
   Protection against the loss of intellectual property, customer data and other sensitive information. Email content and secure communication policies can be created and applied to inbound, outbound and internal traffic in real-time.
3. SPAM AND VIRUS PROTECTION
   Stops infected email from reaching the network and impacting user productivity. Mimecast offers 100 percent anti-virus and 99 percent anti-spam service levels – removing threats in the cloud before they reach your network.

KEY CAPABILITIES:

- Defends against the risk of spear-phishing and advanced threats in email.
- Blocks spam & viruses.
- Protects employees against social engineering and impersonation attacks.
- Neutralizes threats from malware attachments and malicious URLs.
- Removes the graymail burden for end users.
- Enables automated email encryption and secure message deliver.
- Various end user applications enhance user experience.
- Helps to improve users' security awareness.
- Eliminates need to manage on-premises email security software and hardware.
- Detects and blocks attacks from both external and internal threat actors.
- Leveraging the cloud, provides immediate availability of the most current email security protections.

HOW IT WORKS

SIMPLE TO DEPLOY, SIMPLE TO MANAGE

- Switch organization's MX records to point to the Mimecast cloud platform.
- Inspect all inbound, internal, and outbound traffic through the Mimecast service.
- Multiple proprietary and commercially licensed signature-based malware and anti-spam inspections are performed.
- Messages found to be spam or contain malware are automatically rejected or deleted.
- Policy-based email content, attachment, and image filtering performed.
- All inbound URLs are analysed at the gateway, re-written, and scanned in real-time on click.
- Applies static-file analysis, sandboxing, and/or instant safe-file conversion to protect against weaponized attachments.
- Blocks or flags email-borne impersonation attacks.

ALWAYS-ON SECURITY

Anti-spam and anti-virus protection, data leak prevention, URL inspection, safe-file conversion, impersonation protection, malware blocking, internal monitoring, and graymail control for email are all delivered as part of a single unified solution. Mimecast's team of skilled threat intelligence experts that are part of the Mimecast SOC and advanced email security technology helps to ensure that you remain protected against the latest threats. Once in place, Mimecast will secure your users' inboxes, protecting them from spear-phishing, leaving you to focus on delivering core business services.

ADVANCED THREAT PROTECTION

Mimecast's massively scalable email security services are built on the proprietary Mime|OS cloud platform. Email related threats such as malware, spam, spear-phishing

attacks, and other attacks are stopped before they reach your email system. This reduces risk to your employees and improves the performance of your email system.

Mimecast's Targeted Threat Protection addresses the risk of spear-phishing and targeted attacks in email. Every URL in all inbound emails are re-written to point to Mimecast's cloud, so users clicking on malicious sites are prevented from accessing damaging content or malware delivery sites.

Email attachments undergo static file analysis and can also be pre-emptively scanned in a secure sandbox, as well as converted to safe file formats, in order to protect against weaponized attachments, macro threats and malicious content.

End users are equally protected from social engineering and email impersonation attacks, with a sophisticated set of security checks that protect against spoofing and fraudulent requests. End users can be alerted to suspicious emails to prevent data loss.

Internal and outbound mail is analyzed for malicious URLs, attachments, as well as content (DLP) to prevent compromised, careless, or malicious users from spreading attacks within an organization or to its external contacts.

END-USER SELF-SERVICE

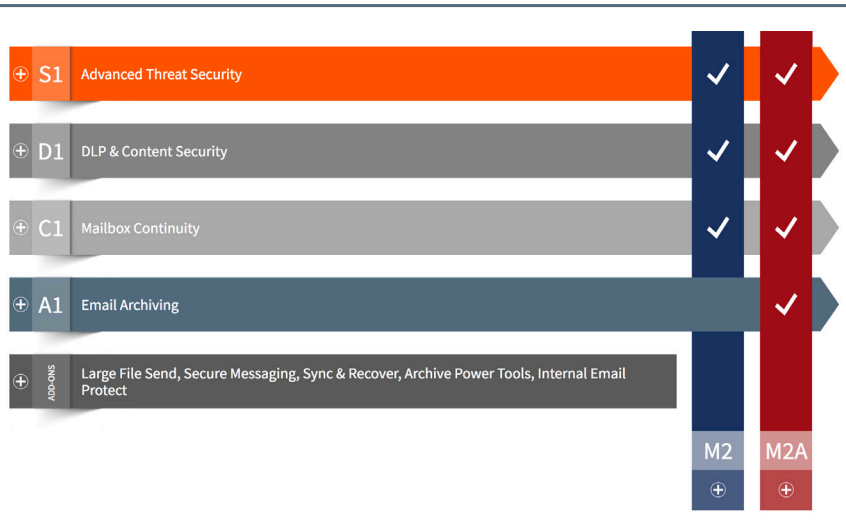
Should the occasional good message be quarantined, end user self-service is facilitated from within Outlook, web, and mobile applications. These end user applications make retrieving messages simple, thus minimizing help desk calls. Self-learning technology and personal block and permit lists ensure that similar messages are handled appropriately in the future.

MIMECAST EMAIL SECURITY - KEY FEATURES

Mime|OS cloud security platform
Centrally administered via single, web-based administration console
Various End User tools for users
Scalable, multi-tenant cloud infrastructure backed by 100% SLA
Automated synchronization with Active Directory for policy and access control
Monitoring dashboard for email queues and services, with SMS and email alerting
Advanced routing capability supporting real-time view of all SMTP connections and rejections
Detailed transmission data for every email that is processed by Mimecast
Advanced threat protection
Multi-layered malware protection against known and new threats
URL re-writing of all links in emails, with on-click scans to protect end users from malicious URLs
Scans for and blocks malicious URLs in email attachments
Pre-emptive attachment sandboxing to protect against weaponized attachments
Instant safe-file conversion of attachments strips out active code to remove macro threats
Sophisticated protection against social engineering and impersonation attacks
Provides security inspections for inbound, outbound, and internal emails
Comprehensive connection-based and content-based spam and phishing protection
Personal permit and block lists to fine tune spam preferences and end user email digests for personal quarantine
SLAs: 100% virus protection; 99% spam protection; 0.0001% spam false positives

Make Email Safer for Business

Mimecast integrated service bundles deliver the ultimate in cyber resilience. Get comprehensive risk management or address specific requirements - all in a single platform.



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.

SCHEDULE A MEETING

CHAT WITH SALES

GET A QUOTE