mimecast | Data Sheet

Mimecast Advanced Security

Cloud-based protection against advanced email-borne threats

Mimecast Advanced Security is a collection of cloud services designed to protect your organization and your employees from the threats that lurk within business email communications. Whether the email be inbound, outbound, or internal, Mimecast Advanced Security defends against malicious URLs, weaponized attachments, impersonation attacks, internal compromise, as well as spam and viruses. Combined with the ability to automatically remediate threats and see the what, when, how, where, and why with threat intelligence specific to your tenant and broader trend data on attacks occurring in your region, Mimecast helps strengthen your cybersecurity and resilience.

The Mimecast Security Suite includes:

1. MIMECAST TARGETED THREAT PROTECTION (TTP): A suite of services delivering inspection of inbound, outbound and internal emails to help detect and fight phishing, ransomware, impersonation attempts, malicious URLs, weaponized attachments, and internal compromise.
2. CONTENT CONTROL & DATA LEAK PREVENTION (DLP): Protection against the loss of intellectual property, customer data and other sensitive information. Content 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 employee productivity. Mimecast offers 100 percent anti-virus and 99.5 percent anti-spam SLA's removing threats in the cloud before they reach your network.
4. MIMECAST THREAT REMEDIATION: Automatic or manual removal of unsafe, undesirable, or malicious content post-delivery, based on the latest intelligence and analysis. Customers with Internal Email Protect (IEP) can leverage Threat Feed (the threat intelligence API) to search for, remove or restore emails through a SIEM or SOAR.
5. MIMECAST THREAT INTELLIGENCE: Provides actionable insight into the cyberthreats your organization faces with expert analysis of the attacks our services detect. The Threat Dashboard provides information on users who are most at-risk, malware origin by geo-location, and recently observed threats with the ability to search by message ID and file hash to determine what Mimecast knows about specific threats. Use the Threat Feed API to surface this information in your tool of choice.

Key Capabilities:

- Mitigate the risk of spear-phishing and advanced threats in email
- Removes the graymail burden for employees
- Protects employees against social engineering and impersonation attacks
- Detects and blocks attacks from both external and internal threat actors / compromised users
- All customers are instantly protected based on blocking a threat for just one
- Multi-tenant cloud delivers always up-to-date defenses
- Remediates potential threats/undesirable emails post-delivery, automatically or manually
- Delivers deep insights on malware attacks targeting your organization and, through Threat Feed, Mimecast's Threat Intelligence API, other Mimecast customers in your geographical region
- Enables automated TLS email encryption

How it Works

SIMPLE TO DEPLOY, SIMPLE TO MANAGE

- Switch MX records to point to the Mimecast cloud platform.
- Inbound, internal, and outbound traffic inspected by the Mimecast service.
- Messages found to be spam or containing malware are automatically rejected or deleted.
- Policy-based email content, attachment, and image filtering performed.
- Inbound URLs are analyzed at the gateway and re-written for on-click destination site examination.
- Internal and outbound URLs, and those in attachments, are analyzed at the gateway.
- Static-file analysis, sandboxing, and/or instant safe-file conversion to protect against weaponized attachments.
- Blocks or flags email-borne impersonation attacks.
- DLP dictionaries with content scanning to prevent the loss of sensitive company information.
- Continuous rechecking of delivered emails, with automatic or manual remediation if found to be malicious.
- A Threat Dashboard delivers easily consumable, actionable information on malware sent to your account. Additional insight into attack patterns in your region is available through Threat Feed, Mimecast's threat intelligence API.

ALWAYS-ON SECURITY

Anti-spam and anti-virus protection, data leak prevention, URL inspection, safe-file conversion, impersonation protection, malware blocking, internal monitoring with threat intelligence, and graymail control for email are all delivered as part of a single unified solution. Mimecast's global threat researchers and Security Operations Center analysts and advanced email security technology help to ensure that you remain protected against the latest threats, while delivering deeper insight on those targeting your organization. Once in place, Mimecast will secure your users' inboxes, protecting them from cyberthreats, leaving you to focus on delivering core business services.

ADVANCED THREAT PROTECTION

Mimecast's massively scalable email security services are built on the Mime|OS cloud platform. Email related threats such as malware, spam, spear-phishing, 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 Targeted Threat Protection addresses the risk of spear-phishing and targeted attacks in email. Every URL in all inbound email is re-written to point to Mimecast's cloud, protecting users from accessing phishing sites and those containing malware.

Email attachments undergo static file analysis and can also be pre-emptively scanned in a secure, full-system emulation sandbox, as well as converted to safe file formats, to protect against weaponized attachments. Administrators can determine what Mimecast knows about specific threats by searching for specific files or messages, either directly through Mimecast's Administration Console, or using the tools available in their SIEM, TIP or SOAR.*

Employees are equally protected from social engineering and email impersonation attacks, with a sophisticated set of security checks designed to detect and stop spoofing, supply chain impersonation, homoglyph/homograph impersonation and fraudulent requests. Employees can also 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 customers and partners. With the continuous rechecking of emails that exist in your environment, remediation of unsafe, unwanted, or malicious content can be enforced automatically, or manually by the administrator.

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, minimizing help desk calls. Self-learning technology and personal block and permit lists ensure that similar messages are handled appropriately in the future.

* requires integration with Threat Feed, Mimecast's threat intelligence API.

Key Features:

MIME|OS CLOUD SECURITY PLATFORM

- Centrally administered via a single, web-based administration console
- Scalable, multi-tenant cloud infrastructure backed by 100% availability 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
- Full suite of end user tools

ADVANCED THREAT PROTECTION

- Multi-layered malware protection against known and zero-day threats
- URL re-writing of all links in emails, with on-click scans to protect employees from malicious sites
- Scans for and blocks malicious URLs in email attachments
- Static file analysis and pre-emptive attachment sandboxing to protect against weaponized attachments, with safe-file conversion of attachments to remove any threats and deliver instantly to users
- Sophisticated protection against social engineering, homoglyph/homograph deception and impersonation attacks
- Analysis of internal and outbound emails to protect against compromised, careless, and malicious insiders
- Remediation of unsafe, unwanted, or malicious emails, automatically or manually based on preference
- SLAs: 100% virus protection; 99.5% spam protection; 0.0001% spam false positives
- Threat Feed, Mimecast's threat intelligence API, enables you to view Mimecast information about threats to your specific tenant and threat trends in your region in the SIEM, TIP or SOAR of your choice.
- For customers with Internal Email Protect (IEP), Threat Feed also facilitates remediation or restoration of files from third party platforms
- Easily consumable and actionable threat intelligence specific to your organization