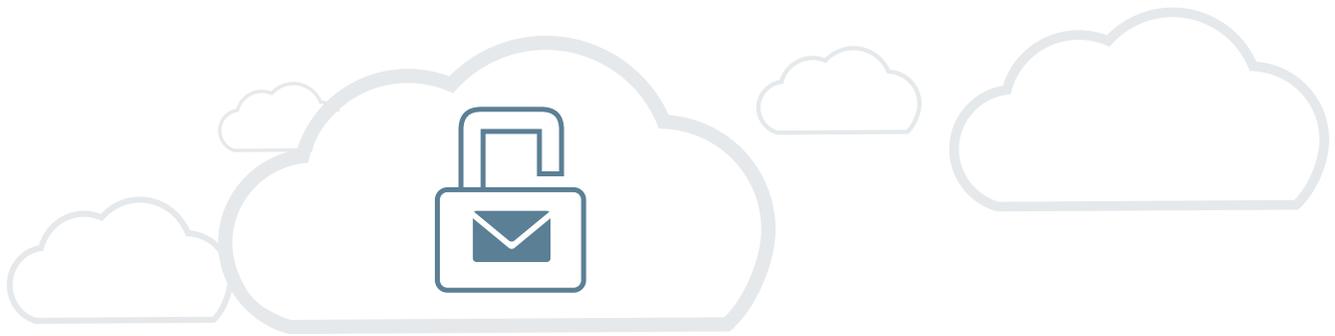# Mimecast Email Security

An always-on, cloud-based email security solution that reduces the complexity of protecting your organization from malware, spam and data leakage.

Mimecast Email Security is the most comprehensive cloud-based email security and compliance solution on the market today. Mimecast's massively scalable mail transfer agent (MTA) with its multiple layers of malware and spam protection acts as your email bridgehead in the cloud, stopping known and emerging email borne threats before they reach your network.

Granular and flexible email content and secure communication policies can be created and applied to outbound traffic in real-time, enabling you to take responsive data leak prevention (DLP) measures.

Key Features

- Always-on cloud-based security service
- Real-time online queue management
- Stops spam and malware in the cloud
- DLP policy setting with immediate enforcement
- AD synchronization enables group policy setting
- Document metadata stripping
- Secure message delivery
- Disclaimer and legal notice management
- Email stationery management and marketing tools

Benefits at a Glance

- No more unwanted email
- Interactive digests from Outlook
- Self-service quarantine
- Personal block and permit lists reflect user preferences
- User invoked secure communication

Mimecast is a leading provider of essential cloud services for Microsoft Exchange. Mimecast delivers enterprise email management services that include security, continuity, and archiving.

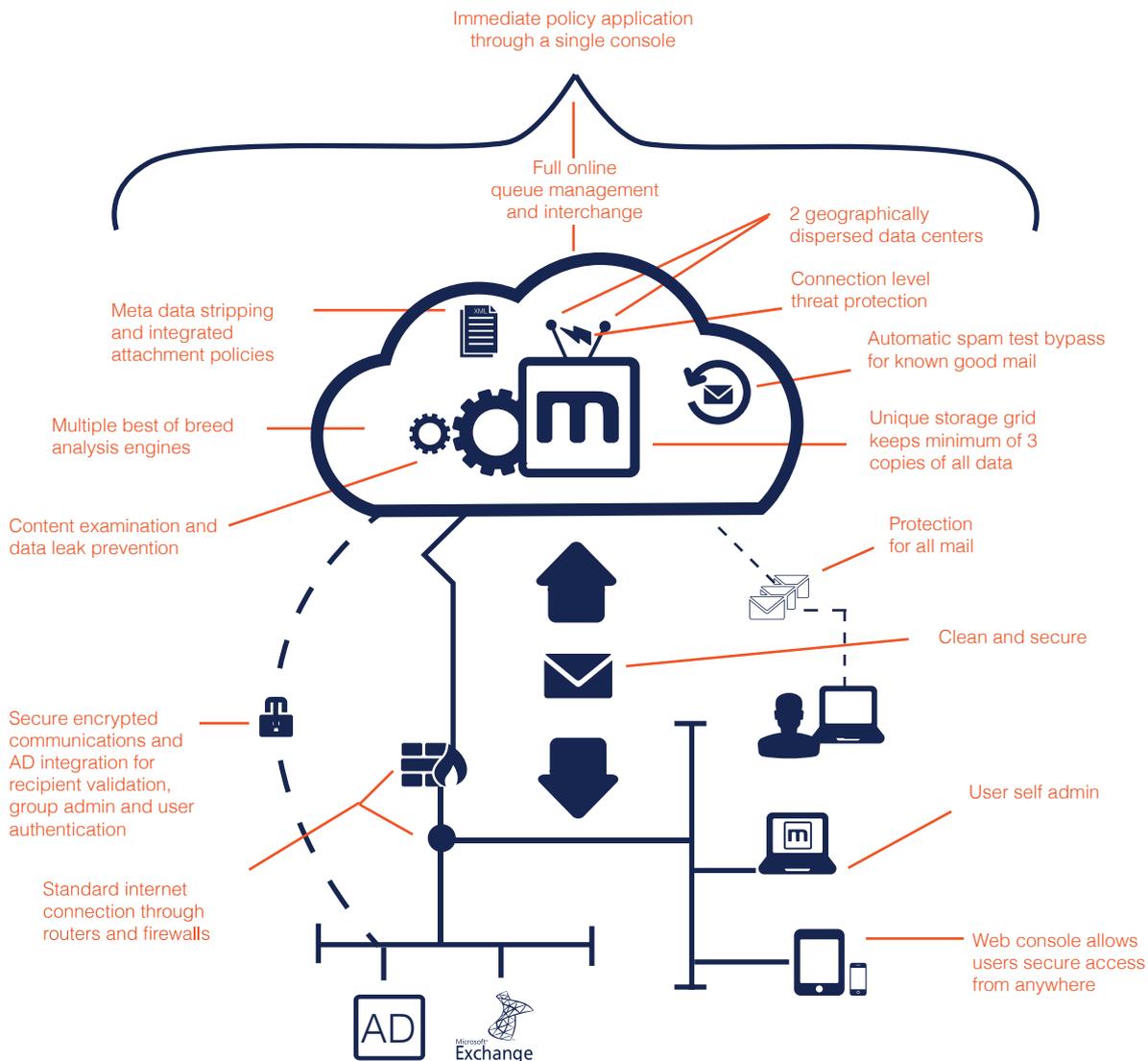Mimecast Email Security includes Mimecast Secure Email Gateway and Content Power Tools.

How it works

Simple to deploy, simple to manage

- Switch corporate MX records to point to the Mimecast platform
- Route all outbound traffic through the Mimecast platform
- Suspicious connections are dropped
- Multiple signature-based malware inspection is performed
- Zero-hour threat analysis performed to identify emerging threats
- Messages found to contain malware are automatically rejected prior to receipt
- Message content filtering is applied to further reduce unwanted emails
- Policy-based email content, attachment and image filtering performed
- Messages that trigger a policy are held in a queue for optional review and release
- Secure delivery methods invoked based on message content, sender, or recipient rules
- Online traffic analysis available for managing live messages

Immediate policy application through a single console

Full online queue management and interchange

2 geographically dispersed data centers

Meta data stripping and integrated attachment policies

Connection level threat protection

Automatic spam test bypass for known good mail

Multiple best of breed analysis engines

Unique storage grid keeps minimum of 3 copies of all data

Content examination and data leak prevention

Protection for all mail

Clean and secure

Secure encrypted communications and AD integration for recipient validation, group admin and user authentication

User self admin

Standard internet connection through routers and firewalls

Web console allows users secure access from anywhere

AD

Microsoft Exchange

mimecast®

Mimecast Email Security

Always-on security

Anti-spam and anti-virus protection, data leak prevention, secure communication and email routing are all delivered as part of a single unified solution. Mimecast's team of skilled threat experts, and auto-learning technology, ensures that you remain protected against the latest threats. Once in place, Mimecast will keep on delivering the same high-level of protection, leaving you free to focus on core business activity.

Increased protection

Mimecast's massively scalable MTA becomes your email bridgehead in the cloud. Email related threats such as malware, spam, phishing attacks, denial of service and directory harvest attacks are all stopped before they reach your network. This not only reduces risk to your network but also improves the performance of your Exchange server.

Enhanced visibility and control

Organization-wide email security policies are managed from a single interface and can be applied with immediate effect, enabling you to respond rapidly to evolving situations. Advanced monitoring functionality gives you real-time views of your SMTP traffic and offers online queue management and advanced routing capability, to ensure that you stay in control.

End user self-service

Should the occasional message be accidentally quarantined, end user self-service facilities from within Outlook makes retrieving messages simple, and minimizes help desk calls. Self-learning technology and personal block and permit lists ensure that similar messages are handled appropriately in the future.

Unified Email Management

Mimecast Email Security is just one component of Mimecast's unified email management suite of services. This means that you have the flexibility to easily add email continuity and archiving services either now or in the future, all managed from a single administration console.

Combining these services also brings additional security benefits. Email policies are continuously enforced during local email outages and important data is stored offsite in a secure, tamper proof archive.

Mimecast Email Security is also included in the following Mimecast unified email management services:

- Mimecast UEM Express
- Mimecast UEM Enterprise

Mimecast Email Security - Features

Secure Email Gateway

Mimecast service platform

Centrally administered via single, web-based administration console

Mimecast Webmail portal for user access to held messages

Backed by 100% service availability SLA

Automated synchronization with company directory

Monitoring dashboard for email queues and synchronisation services

Customizable SMS and email alerting of potential email service problems

Assignment of administrators to pre-defined or customizable roles with associated permissions

Advanced MTA capability

Advanced routing capability

Real-time view of all SMTP connections and rejections

Online queue management

Detailed transmission data for every email that is processed by Mimecast

Reports of email usage patterns

Protection from email-based attacks e.g. denial of service (DoS), directory harvest attacks (DHA)

Large attachment management with strip and link capability

Email threat protection

Multi-layered malware protection against known and zero-day threats

Comprehensive connection-based and content-based spam and phishing protection

Personal permit and block lists to fine tune spam preferences

End user email digests for personal quarantine management

Image scanning for policy enforcement

Policy-based attachment management rules

SLAs: 100% virus protection; 98% spam protection; 0.0001% spam false positives

Content Power Tools

Data leak prevention capability

Granular email policy setting with secure Active Directory (AD) synchronization

Content examination of email body text, attachments, HTML, headers and subject

Weighted dictionaries for threshold policy triggering

Intelligent identifiers for the recognition of structured data (e.g. credit card numbers)

Recognition of known confidential files

Immediate enforcement of email security and DLP policies

Risk management options; block, hold pending review, bcc a group, add content

Metadata stripping and PDF conversion

Secure message delivery

Email encryption with best-effort and policy-enforced TLS

Closed Circuit Messaging (CCM)

Email stationery management and marketing tools

Flexible, policy-based signature and legal notice creation and application

Corporate branding and imagery management

Recipient click tracking capability

Microsite creation and publishing