mimecast®

SOLUTION BRIEF

Mimecast Services for Microsoft Office 365™

Office 365 is Microsoft's fastest growing business ever but don't sleep walk into the Cloud

The trend towards moving from Exchange on-premise to Exchange Online and Office 365 continues to pick up speed with more migrations across all sizes of organizations. Office 365 has been called Microsoft's fastest growing business ever, a statement that is particularly meaningful given the past success of the technology giant. A look at the adoption numbers adds considerable credence to this statement. Over 50,000 organizations are moving to Office 365 each month, taking advantage of the shared infrastructure and technology services that make up the cloud collaboration service. While Office 365 encompasses a broad suite of capabilities, the number-one driver for organizations moving to Office 365 is email.

Economics of the Cloud make sense

For most organizations, the move to Office 365 and the cloud is largely an economic decision. With cloud services, including Office 365, organizations can leverage service infrastructure rather than investing in expensive dedicated infrastructure and personnel. In addition, cloud service providers assume responsibility for the technical expertise required to keep the platform running and available. This is a real benefit as organizations can move precious resources to projects that provide true competitive differentiation. But many organizations moving to the cloud mistakenly assume that IT no longer has responsibility for mitigating risk and strategically responding to events such as security threats, data loss and service downtime. Let's look at some of these misconceptions in more detail.

Common Misconceptions When Moving to Office 365

Email Threats like whaling, spear-phishing and ransomware are covered

Email continues to be the number-one threat vector for business. Over 90% of data breaches start with an email, underscoring the need for organizations to invest in security best practices and capabilities. Robust email security requires defense in depth, combining multiple solutions to best protect against constantly evolving threats that exploit the tendency of humans to place too much trust in email.

Top threats in email include:

- Business Email Compromise or Whaling
  A well-researched, social engineering attack where a cyber-criminal, disguised as the CEO, CFO or other senior executive, sends an email message to a recipient and convinces this person to initiate a wire or data transfer.
- Malicious URLs
  URLs embedded in email are designed to trick an unsuspecting employee into providing credentials or by infecting the PC for a delayed exploit. All links in email should be checked in real-time by examining the destination site for suspicious code and blocking access if appropriate.
- Malware-Laden Attachments
  Macro-enabled Office documents and other file types present a clear danger to the organization. Traditional defenses against malicious attachments have used sandboxing, which introduces latency and can still miss exploits that are programmed to lie dormant until launched from a "real" inbox.
- Ransomware
  With ransomware, the files on the infected computer and network are encrypted to lock out access until a specified amount is paid. Organized crime groups are increasingly using ransomware to target businesses because it's easy to monetize and difficult to fight once encrypted. Email is the primary vector with malicious URLs and attachments delivering the ransomware.

Best practices in the cloud are different from on-premise

For many years organizations have made investments in hardware and software to manage the risks that threaten or exploit email communications. With the emergence of email as the dominant form of business communication, surrounding the mail environment with additional capabilities helped drive down risk to a manageable level. Some examples include redundant systems, high availability, multiple layers of security and encryption capabilities. The risks of email don't change whether you are running in the cloud or on-premise. All organizations need to assess and plan for additional risk management services around Office 365.

There isn't a need for an archive or backup

Regardless of whether the email environment is on-premise or in the cloud, the risks of human error, technical failure and malicious intent still exist. Every organization has employees and administrators that are prone to making mistakes. This extends to the Office 365 engineers responsible for keeping the service running as smoothly as possible. The Office 365 cloud is created using real data centers and staffed with real people. While mistakes can be minimized, with technology something always can (and usually will) go wrong. Having the ability to restore Office 365 data to a known good point in time is important in the event something is mistakenly deleted or possibly lost. It's critical to recognize that Service Level Agreements (SLAs) apply to service availability, not to data recovery or resilience.

Cloud outages won't impact the organization

Every system has downtime. Especially a multi-tenant cloud platform that encompasses multiple software applications and needs to scale to meet the needs of over 70 million commercial users. Multiple infrastructure components must work in tight coordination to authenticate users, apply security policies, permit access to archives and allow administrators to control the service. If one component is offline, employee productivity can grind to a halt. Cloud outages put IT administrators in a difficult position. With on-premise environments, admins can take the necessary steps to restore the environment and bring users back online. In the cloud, frustrated employees are told they must wait for an update from the service provider. Without proper planning, administrators have few options for restoring service or providing a short-term solution.

Mimecast for Office 365

Mimecast is a centrally-managed cloud solution that perfectly complements Office 365. Architected and built 100% for the cloud, Mimecast helps thousands of organizations manage the risks of email. Mimecast provides:

- An additional layer of security for Office 365 against constantly evolving threats.
- Enhanced Whaling, URL and Attachment protection for employees and the organization.
- An independent, bottomless archive offering a true archive with access for employees and admins that need powerful e-discovery.
- Continuity for sending and receiving email, even when Office 365 goes down.
- A single administrative console for all email risk management capabilities.

Mime|OS

Mimecast developed Mime|OS as a proprietary operating system for native cloud services. Mime|OS enables secure multi-tenancy and takes advantage of the cost and performance benefits of using industry-standard hardware and resource-sharing specifically for the secure management of email and data. This enables Mimecast to provision efficiently and securely across our customer base, minimizing the impact of spare or overprovisioned processing and storage capacity and reducing the cost of providing our services.

Mime|OS utilizes a common code base to control the hardware, and the storage, indexing, processing, services, administrator and user interface layers of our cloud environment. It has been specifically designed to enable us to scale our storage, processing and services to meet SMB and large enterprise-level email and data demands, while retaining the cost and performance benefits of a native cloud environment.

As a foundation, Mime|OS enables tightly integrated solutions and a single administration console to control the services. The central web-based console provides policy management, dashboards, rich reporting and workflow for handling suspect and malicious email.

> "The Bay Club relies on Mimecast's cloud archiving solution not only to complement its Microsoft Office 365 email environment, but because Mimecast can scale alongside its growth."
> **— Bay Club**

> "Because of the Lagan Group's reliance on email, I needed the additional insurance that Mimecast was able to offer. Adding Mimecast to our Office 365 environment enabled us to provide the company with as close to a risk-free approach to email management as you can get."
> **—Lagan Construction Group**

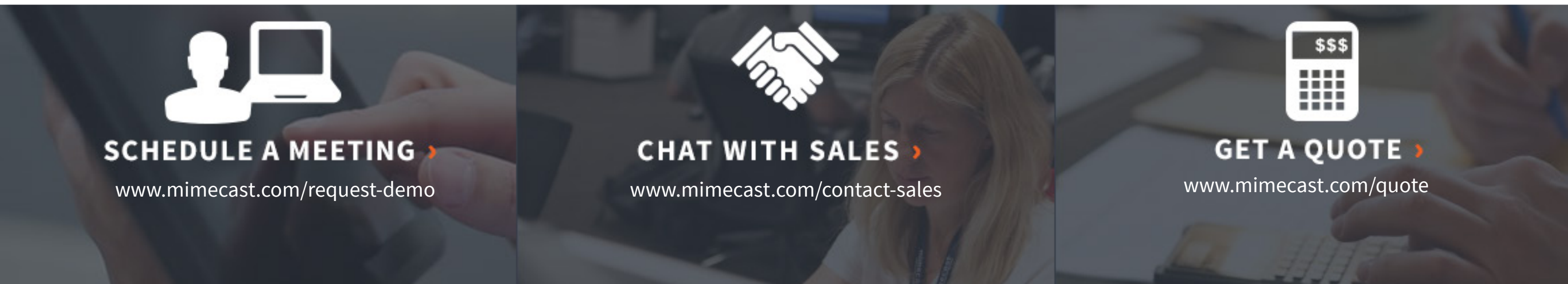
Mimecast Service Bundles

Most Mimecast customers prefer a bundled service over purchasing individual security, archiving and continuity cloud offerings. All built on top of Mime|OS, the services can be rolled out quickly and enhanced easily with additional capabilities when necessary.

S1 – Advanced Threat Security Comprehensive protection from the latest email-borne threats including whaling (CEO fraud), ransomware, spear-phishing and other sophisticated attacks.	● Defense against malware-less, social engineering attacks. ● Protection against ransomware and other evolving threats. ● On-click protection from malicious URLs in email. ● Attachment sandboxing and innovative safe file conversion. ● SLA-backed spam and malware protection and defense against zero-day threats. ● Email encryption, flexible attachment management and stationery. ● Dashboards and reporting to help administrators stay ahead of potential risks. ● Employee desktop and mobile apps for spam and quarantine management.
D1 – DLP & Content Security Compliance-led security to prevent sensitive and confidential information from leaving the organization.	● Real-time protection against outbound data leaks (DLP) with automated policy application. ● Pre-built intelligent identifiers of structured data like credit card numbers, social security numbers and healthcare information. ● Integrated Mimecast managed reference dictionaries. ● Watermark and convert Microsoft Office documents to PDF on send, strip attachment metadata. ● SLA-backed spam and malware protection and defense against zero-day threats. ● Email encryption, flexible attachment management and stationery. ● Employee desktop and mobile apps for spam and quarantine management.
C1 – Mailbox Continuity Protect employee productivity and business operations with uninterrupted access to email during on-premise or cloud email outages.	● Full email access during outages – read, send, reply, forward live and historic mail from any device. ● Outlook integration means employees can carry on working as normal during downtime. ● Complete administrator control of continuity events, including scheduled events. ● Mimecast apps included as standard - Outlook for Windows, native app for Mac users, iPhone, iPad, Android, BlackBerry and Windows Phone. ● Security policies maintained during continuity events. ● Always-on archive access (requires Mimecast Email Archive).

A1 – Email Archiving A highly secure, scalable and easily-accessible cloud archive to meet data retention, compliance and legal requirements.	● Support compliance with all inbound, outbound and internal email held perpetually in a tamper-proof archive with auditable chains of custody. ● A complete archive using journal, gateway, LAN/cloud sync and ingestion data inputs. ● Comprehensive e-discovery and rapid archive search powered by Mimecast’s grid architecture. ● Rapid employee archive access from any device – backed by a 7-second search SLA. ● Replicated Exchange folders in the archive help employees find information faster (requires Archive Power Tools add-on). ● Option to add file and IM archiving.
M2 – Cyber Security and Resiliency Comprehensive security and cyber resilience in a single integrated service.	● S1 - Advanced Threat Security Comprehensive protection from the latest email-borne threats including spear-phishing, ransomware, whaling (CEO fraud) and other sophisticated attacks. ● D1 - DLP & Content Security Compliance-led security to prevent sensitive and confidential information moving outside the organization. ● C1 - Mailbox Continuity Protect employee productivity and business operations with uninterrupted access to email during on-premise or cloud email outages.
M2A – Cyber Security and Resiliency with Archiving M2A is the most complete email risk management service bundle from Mimecast.	● S1 - Advanced Threat Security Comprehensive protection from the latest email-borne threats including spear-phishing, ransomware, whaling (CEO fraud) and other sophisticated attacks. ● D1 - DLP & Content Security Compliance-led security to prevent sensitive and confidential information moving outside the organization. ● C1 - Mailbox Continuity Protect employee productivity and business operations with uninterrupted access to email during on-premise or cloud email outages. ● A1 – Email Archiving Email Archiving with 99-year retention, comprehensive e-discovery and rapid employee archive access from any device – backed by a 7 second search SLA.

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 ›
www.mimecast.com/request-demo

CHAT WITH SALES ›
www.mimecast.com/contact-sales

GET A QUOTE ›
www.mimecast.com/quote