Mimecast Plans & Services

Mimecast's flexible and scalable suite of cyber resilience services help protect organizations from malicious activity, human error and technology failure. Supporting multiple email platforms including Office 365™, Exchange, and Google® G Suite, Mimecast services help organizations be more resilient.

			Email Security 3.0 Programs			Cyber Resilience Programs	
			Perimeter Defense Plan (Zone 1)	Comprehensive Defense Plan (Zone 1+2)	Pervasive Defense Plan (Zone 1+2+3)	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
EMAIL SECURITY 3.0	ZONE 1	SEG	•	•	•	•	•
		URL PROTECT	•	•	•	•	•
		ATTACHMENT PROTECT	•	•	•	•	•
		IMPERSONATION PROTECT	•	•	•	•	•
	ZONE 2	INTERNAL EMAIL PROTECT		•	•	•	•
		AWARENESS TRAINING		•	•	•	•
	ZONE 3	DMARC ANALYZER			•		
		BRAND EXPLOIT PROTECT			•		
RESILIENCE EXTENSIONS		EMAIL CONTINUITY				•	•
		SYNC & RECOVER				•	•
		WEB SECURITY					•
		LARGE FILE SEND					•
		SECURE MESSAGING					•
		PRIVACY PACK					•
		99 YEAR ARCHIVE					•

Mimecast Service Description

● – Standard ○ – Available at an additional fee

For more detail on add-on services, see footnotes as referenced in the table below.

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Mimecast Service Platform					
ISO 27001:2013 Information Security Management Systems (ISMS) certified	●	●	●	●	●
ISO 27018:2014 Information Security Management Systems (ISMS) certified	●	●	●	●	●
ISO 22301:2012 Business Continuity Certification	●	●	●	●	●
Secure, scalable, jurisdictionally segregated geographically-dispersed data centers	●	●	●	●	●
Multi-network data centers with load balanced Internet connectivity	●	●	●	●	●
100% service availability punitive SLA	●	●	●	●	●
No additional on-premises hardware or appliance required during and after implementation	●	●	●	●	●
Single web-based Administration Console for all service administration requirements	●	●	●	●	●
Microsoft Active Directory (incl. Azure) synchronization and administrator-controlled metadata retention for policy configuration	●	●	●	●	●
Authentication					
Secure login for administrators and end users using pre-defined cloud password	●	●	●	●	●
Secure login for administrators and end users using Active Directory or Office 365 credentials	●	●	●	●	●
Secure end user login using Integrated Authentication (with Mimecast for Outlook)	●	●	●	●	●
Complexity and expiration rules of cloud password configurable by administrator	●	●	●	●	●
Authentication options configurable by administrator	●	●	●	●	●
SAML 2.0 (SSO and 2FA) and 2-step authentication support for Administration Console	●	●	●	●	●
SAML 2.0 (SSO and 2FA) and 2-step authentication support for Mimecast Personal Portal, Mimecast for Outlook, Mimecast Mobile and Mimecast for Mac.	●	●	●	●	●
Granular policy application to all users or specific senders, recipients or groups	●	●	●	●	●
Policies applied based on Directory attributes or group membership	●	●	●	●	●
Policy and Authorization					
Multiple admin levels with flexible permission settings	●	●	●	●	●
Assignment of administrators to pre-defined or customizable roles with associated permissions	●	●	●	●	●
Flexible management of end user permissions using group application settings	●	●	●	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Audit log of access, events, policy creation, changes	●	●	●	●	●
Monitoring and Reporting					
Scheduled and defined reports of corporate email system usage patterns	●	●	●	●	●
Download historical email usage patterns in PDF format	●	●	●	●	●
Download of connection, rejection and bandwidth details in CSV format	●	●	●	●	●
Custom report generation showing communication views by both message and byte count	●	●	●	●	●
Detailed email activity report filtering down to the top communication pair levels	●	●	●	●	●
Online Service Monitor dashboard for inbound and outbound email queues	●	●	●	●	●
Online Service Monitor dashboard for journal queues	●	●	●	●	●
Online Service Monitor dashboard for monitoring of synchronization services	●	●	●	●	●
SMS and email alerting of potential service issues	●	●	●	●	●
Inbound and outbound email continuity event monitoring				●	●
Email Gateway					
Scalable, proprietary Message Transfer Agent (MTA)	●	●	●	●	●
Advanced inbound traffic splitting for customers with multiple sites and email servers	●	●	●	●	●
Maximum message throughput supported by grid-wide intelligent processing and routing	●	●	●	●	●
Full online queue management with manual retry, bounce, reject and extended spool options	●	●	●	●	●
Real-time view of all SMTP connections and rejections	●	●	●	●	●
Hold for Review policy and workflow	●	●	●	●	●
Policies and routing applied based on Microsoft Active Directory attributes or group membership	●	●	●	●	●
Full or partial email address rewrite capabilities	●	●	●	●	●
Online real-time rerouting of queued items to remote DR site during local outages	●	●	●	●	●
Administrator-defined Auto Response functionality	●	●	●	●	●
Email Security					
Connection-based spam filtering using Mimecast Global Reputation Service	●	●	●	●	●
Real-time threat protection with Mimecast proprietary Advanced Reputation Management (ARMed SMTP™)	●	●	●	●	●
Commercial anti-malware engines for multi-layer protection	●	●	●	●	●
Anti-virus SLA - 100% virus protection with rescan ability upon release of items	●	●	●	●	●
Anti-spam SLA – 99.5% spam protection, 0.0001% spam false positive rate	●	●	●	●	●
Outbound email signing with Domain Keys Identified Mail (DKIM)	●	●	●	●	●
Sender Policy Framework (SPF) checks on inbound mail	●	●	●	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Automatic spam test bypass for known good correspondents with real-time learning algorithm	●	●	●	●	●
Zero-day threat protection with Mimecast Zero-Hour Adaptive Risk Assessor™ (ZHARA™)	●	●	●	●	●
Mimecast Dark Traffic Analysis Group (DTAG™) provides protection against evolving threats	●	●	●	●	●
Threat Dashboard consolidates data about threats targeting your organization into actionable insights and analysis	●	●	●	●	●
Thread Feed enables integration of threat data into third party security applications via API	●	●	●	●	●
Encrypted email transmission with best-effort Transport Layer Security (TLS)	●	●	●	●	●
Encrypted email transmission with policy-based Transport Layer Security (TLS)	●	●	●	●	●
Administrator-managed account-wide permit and block policies and lists	●	●	●	●	●
End-user personal block/allow to tune spam preferences	●	●	●	●	●
End-user email digests for quarantine management	●	●	●	●	●
Real-time image scanning to enforce attachment policy	●	●	●	●	●
Optional Graymail Control – detect and action Newsletter and Bulk mail independently to spam configuration	●	●	●	●	●
Mimecast Secure Messaging for email communication via a secure web-based channel	o[3]	o[3]	o[3]	o[3]	●
Targeted Threat Protection					
Extend phishing and spear-phishing protection to all inboxes	●	●	●	●	●
Automatically rewrite URLs in inbound emails allowing for on-click scanning in real-time	●	●	●	●	●
URLs scanned on every click protecting against safe URLs being compromised subsequently	●	●	●	●	●
Security check of URLs inside attachments	●	●	●	●	●
Block or warn on URLs that point to file downloads	●	●	●	●	●
Block, warn and sandbox attachments accessed via URL link	●	●	●	●	●
Ability to permit and block individual URLs and/or base domains	●	●	●	●	●
Configurable scanning levels and actions	●	●	●	●	●
Comprehensive log of all scanned URLs including a dedicated monitoring dashboard	●	●	●	●	●
Dynamic user awareness drives employee caution and learning – includes the option for customized alerts and security tips	●	●	●	●	●
Administrator notification / alerting options	●	●	●	●	●
Extend phishing and spear-phishing protection to zero-hour attachment threats	●	●	●	●	●
Pre-emptive sandboxing to automatically security check email attachments before delivery, incl. static file analysis	●	●	●	●	●
File conversion to safe formats & on-demand sandboxing to mitigate threats without introducing latency	●	●	●	●	●
Choice of file conversion formats	●	●	●	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Comprehensive log of all safe / unsafe sandboxed attachments including a dedicated monitoring dashboard	●	●	●	●	●
Dynamic attachment protection for automated safe file on-demand for trusted senders	●	●	●	●	●
Automated threat remediation using threat intelligence to detect and remove attachments deemed malicious post-delivery		●	●	●	●
Real-time protection against malware-less social engineering attacks like impersonation, CEO fraud, business email compromise or W-2 fraud	●	●	●	●	●
Protection against unknown or newly observed domain names used as part of an attack	●	●	●	●	●
Protection against lookalike domain names incl. use of non-western character sets	●	●	●	●	●
Popular internet domain brand impersonation protection	●	●	●	●	●
Protection against display name or friendly name spoofing	●	●	●	●	●
Protection against supply chain impersonation – incl. custom list creation	●	●	●	●	●
Visibly mark suspicious emails and those originating from an external source to enhance end user protection	●	●	●	●	●
Inspection of all internal and outbound mail alongside inbound messages to identify and remediate or block advanced threats – remediation / removal also available through the Threat Feed API		●	●	●	●
Backed by comprehensive protection from Mimecast's threat intelligence infrastructure and SOC teams	●	●	●	●	●
Complete administrative control over security of message; quarantine, bounce or mark emails based on security posture	●	●	●	●	●
Email Attachment Management					
Flexible attachment management rules applied via administrator-defined policies to allow, block, strip or hold	●	●	●	●	●
Policy-based inbound gateway strip and link keeping large email attachments away from the local mail store	●	●	●	●	●
Policy-based outbound gateway strip and link to assist with deliverability of large email attachments	●	●	●	●	●
End-user-invocation of strip and link functionality (via Outlook)	●	●	●	●	●
Administrator configurable email or attachment size limit policies	●	●	●	●	●
Mimecast Large File Send					
Ability to send and receive large files securely via email. Available as an add-on for the indicated services	o[2]	o[2]	o[2]	o[2]	●
Email Stationery and Marketing Tools					
Flexible corporate branding and image management	●	●	●	●	●
Microsoft Active Directory attribute or variable population	●	●	●	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Recipient click tracking to record interaction with email marketing messages	●	●	●	●	●
Microsite creation functionality for rapid publication of temporary web landing pages	●	●	●	●	●
Recording of click activity to a microsite or Internet URL	●	●	●	●	●
Predefined layouts and ability to upload custom templates	●	●	●	●	●
User-invoked email stationery application at email composition from administrator-defined selection	●	●	●	●	●
Data Leak Prevention					
Real-time protection against leaks of confidential or sensitive information	●	●	●	●	●
Identify confidential files using cryptographic checksums	●	●	●	●	●
Analysis of content within email body, HTML, subject lines, headers and attachments	●	●	●	●	●
Intelligent identifiers for the recognition of structured data such as credit card numbers	●	●	●	●	●
Integrated Mimecast-managed Reference Dictionaries	●	●	●	●	●
Weighted dictionaries for threshold policy triggering to reduce false positives	●	●	●	●	●
Document fingerprinting to help prevent drip feed data loss	●	●	●	●	●
Stripping of confidential metadata from MS Office files to avoid unintentional data leakage	●	●	●	●	●
Addition of a configurable watermark for MS Word files	●	●	●	●	●
Conversion of MS Office files to PDF before delivery	●	●	●	●	●
User invocation of document transformation policy from administrator-defined selection	●	●	●	●	●
Mimecast Secure Messaging for email communication via a secure web-based channel	O[3]	O[3]	O[3]	O[3]	●
Secure Messaging enforcement using key phrases in any email content	O[3]	O[3]	O[3]	O[3]	●
End-user invocation of Secure Messaging in Outlook	O[3]	O[3]	O[3]	O[3]	●
Date-specific or indefinite content protection policies	●	●	●	●	●
Automated DLP policy application according to sender / recipient / user group membership	●	●	●	●	●
Analysis of outbound file content against DLP rules when sent via Mimecast Large File Send (LFS)	O[2]	O[2]	O[2]	O[2]	●
Block, hold pending review, bcc a group, add content, add to shared smart folder	●	●	●	●	●
Analysis of internal mail against DLP rules	O[1]	●	●	●	●
Email Continuity					
Failover routing of email to remote DR site during local outages	O	O	O	●	●
Automatic email queuing / spooling for 4 days plus the option to pause inbound delivery	O	O	O	●	●
Administrator or end user invocation of continuity service	O	O	O	●	●
Continuity Event Management features provide detection, administrator alerting and easy invocation of continuity service	O	O	O	●	●
Always-on access to live email and calendar information via the Mimecast Personal Portal	O	O	O	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
No action required for cached Outlook clients to invoke continuity service via Mimecast for Outlook	○	○	○	●	●
Customizable administrator-controlled mailbox continuity SMS alerts to users	○	○	○	●	●
Administrator-controlled and customizable continuity service notifications for BlackBerry users	○	○	○	●	●
Access to live email via BlackBerry smartphone during BES unavailability, RIM NOC or Exchange outages	○	○	○	●	●
Administrator-controlled iPhone and Android apps enable email access during ActiveSync unavailability	○	○	○	●	●
Administrator-controlled native Mac application that enables email access during Exchange outages	○	○	○	●	●
Awareness Training					
Engaging training modules, risk scoring, and phishing simulations help drive positive change in security behavior	○[7]	●	●	●	●
Web Security					
Extend protection to all web browsing on and off the network – incl. malicious sites, inappropriate web use and shadow IT risks associated with uncontrolled cloud app use	○[8]	○[8]	○[8]	○[8]	●
DMARC Visibility & Reporting					
360-degree visibility, reporting and workflows to help reduce the time and complexity of enforcing DMARC authentication	○[9]	○[9]	●	○[9]	○[9]
Brand Exploit Protection					
Find and stop online brand impersonation, including blocking and taking down suspicious and active scams	○[10]	○[10]	●	○[10]	○[10]
Email Retention & Archiving					
Maximum message throughput supported by grid-wide intelligent processing and routing	●	●	●	●	●
All retained email is encrypted and held in triplicate to ensure tamper proof, secure data storage	●	●	●	●	●
All data is held in jurisdictionally defined locations	●	●	●	●	●
Retention of all inbound, outbound and internal email according to centrally-managed retention policy	30 days	30 days	30 days	1 year	99 years
POP3 or SMTP journal-based live archiving of internal email				●	●
Detailed receipt and/or delivery log held for every stored email	●	●	●	●	●
Every iteration of every message is stored with an audit trail of all policies it was evaluated against	●	●	●	●	●
Ability to grant and revoke Administrator content viewing rights	●	●	●	●	●
Delegated content view permissions via smart tags			●	●	●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Categorize / group messages in smart tags based on message content, or via policy			●	●	●
Categorize / group messages in smart tags based on e-discovery functionality				●	●
User can move messages to personal retention folders in Outlook				●	●
Staggered deletion schedules from Exchange, Mimecast personal and Mimecast administrative archive				●	●
Personal Exchange folder structure preserved in Mimecast archive				●	●
Policy defined message stubbing of full messages or attachments only on Exchange				●	●
User invoked message stubbing via Outlook				●	●
Self-service recovery of deleted or lost end user messages				●	●
Inbuilt sensitivity filter for exclusion of personal and private messages from Delegated Mailboxes	●	●	●	●	●
Access to Retained / Archived Data					
Near real-time administrative search of entire Mimecast archive with or without content viewing rights				●	●
Comprehensive log of all Administrator searches				●	●
Log of all messages accessed by an Administrator (including metadata and content views)				●	●
End-user access to Mimecast Inbox and Sent Items via Outlook, Apple Mac, smartphone, tablet or web				●	●
End-user personal archive search via Outlook, Apple Mac, smartphone, tablet, or web				●	●
End-user search of personal and delegated archive including Smart Tags directly from Outlook and Apple Mac				●	●
'Export and Save' facility between Mimecast personal archive and Outlook mailbox for easy message recovery				●	●
Sync & Recover for Exchange and Office 365™					
Automated data recovery and advanced email management tools including mailbox and folder sync & recover, granular retention and mailbox storage (stubbing) management	○[4]	○[4]	○[4]	●	●
Supervision					
Monitoring of users with a supervisory rule and queue to address supervisory compliance requirements covering illegal activity					○
Compliance Protect					
Meet regulatory compliance requirements by adding a minimum retention and removing deletion capabilities to the archive					○
Instant Messenger Archiving					
Archive, index and search Lync/Skype for Business messages					○[6]
E-discovery and Litigation Hold					
Near real-time, organization-wide e-discovery search capability across all data					●

Mimecast Services	Perimeter Defense Plan	Comprehensive Defense Plan	Pervasive Defense Plan	Cyber Resilience Foundations Plan	Cyber Resilience Pro Plan
Creation of e-discovery cases to allow relevant archive searches to be stored as a group					●
Case review app provides effective early case assessment					●
Granular litigation hold features to support legal requirements					●
Permanent removal of messages from the archive by coordinated action of multiple admins					●
E-discovery cases and litigation holds to include archived IM chats					○[6]
API for 3rd party e-discovery tool support					●
Support					
Bronze package – including Knowledge Base access, business hours email support, and telephone support during implementation	●	●	●	●	●
Choose from Silver, Gold or Platinum packages to best suite your requirements – see details at end of this document.	○	○	○	○	○

Mimecast Add-Ons Service Description

● – Standard

1. Internal Email Protect (Included in Comprehensive and Pervasive Defense Plans, Cyber Resilience Foundations and Pro Plans)	
Inspection of all internal and outbound mail alongside inbound messages to identify and remediate or block advanced threats	●
Full attachment sandboxing to identify hidden malware in outbound and internal email	●
URL inspection uncovers malicious links in outbound and internal email	●
Detects lateral movement of attacks via email from one internal system or user, to another	●
Automated removal of internal emails containing identified threats	●
Ability to alert administrators and / or end users about remediation taken	●
Single console consolidated reporting, configuration and management	●
Automated threat remediation using threat intelligence to detect and remove attachments deemed malicious post-delivery	●

2. Mimecast Large File Send (included in Cyber Resilience Pro Plan)	
Maximum file upload size	2GB
Annual total storage allowance for large file sending	30GB/user
Number of users	Min. of 100 users or total users within an organization, whichever is greater.
Link expiry	Flexible
Notification when files are first accessed by the recipient	●
Ability for originator to receive large files in return	●
Configurable / optional password protected exchange of large attachments with controlled download link extension and expiration	●
Administrator-controlled invocation of Large File Send capabilities	●
Automatic bypass of local email infrastructure for large outbound messages reducing operational overhead	●
Analysis of all inbound and outbound large files against DLP policies	●
Virus scanning of all inbound and outbound large files	●
Files automatically archived and indexed for search and e-discovery	●
Files archived in line with customer retention policy	●
User-invoked Large File Send capabilities	●
Administrator reporting and management of users and usage. Control of all Large File Send interactions	●

3. Secure Messaging (included in Cyber Resilience Pro Plan)	
Send and receive sensitive and confidential information via email – with recipient access via a secure web portal	●
Granular sender controls including restrict print, reply and reply all	●
Ability to set the expiration of secure messages including revocation	●
Optional request of read receipts for secure messages	●

4. Sync & Recover for Exchange and Office 365 (Included in Cyber Resilience Foundations and Pro Plans)	
Sync and recovery of mailbox folders, mail (metadata), calendars and contacts across Exchange, Office 365 and hybrid environments	●
Organizational view (for admins) of all synced mailboxes	●
Admin initiated export of all mailbox data, including folders, to PST	●
Admin initiated export of all mailbox data, including folders, to native format (EML, ICS, VCF)	●
Admin initiated restore of mailbox data, including folders, directly to Exchange	●
User 'drag and drop' access to personal retention folders in Outlook	●
Staggered deletion schedules from Exchange, Mimecast personal and administrative archive	●
Personal Exchange folder structure preserved in Mimecast archive	●
Policy defined message stubbing of full messages or attachments only on Exchange	●
User invoked message stubbing via Outlook	●
'Export and Save' facility between Mimecast personal archive and Outlook mailbox for easy message recovery	●

5. Archive Power Tools	
User 'drag and drop' access to personal retention folders in Outlook	●
Staggered deletion schedules from Exchange, Mimecast personal and administrative archive	●
Personal Exchange folder structure preserved in Mimecast archive	●
Policy defined message stubbing of full messages or attachments only on Exchange	●
User invoked message stubbing via Outlook	●
'Export and Save' facility between Mimecast personal archive and Outlook mailbox for easy message recovery	●

6. Cloud Archive for IM	
Connector to archive Microsoft Lync 2010 and 2013, and Skype for Business 2015 Server peer-to-peer and conference instant messages	●
Archiving of conference content like uploaded handouts and event-related details such as joining / leaving	●
Archive conference whiteboards and polls for Microsoft Lync 2013 and Skype for Business 2015	●
All content retained and held in triplicate to ensure tamper-proof, secure data	●
All data is held in jurisdictionally defined locations	●
IM conversations retained in accordance with corporate email retention policy	●
IM archive accessible to administrators via Administration Console	●
Archived IM conversations can be included in e-discovery cases	●
Archived IM conversations can be referenced in litigation holds	●

Mimecast Awareness Training Service Description

● – Standard ○ – Available at an additional fee

7. Mimecast Awareness Training (Included in Comprehensive and Pervasive Defense Plans, Cyber Resilience Foundations and Pro Plans)	AT1
Monthly deployment of core cyber security awareness video-based training modules - covering phishing, data, information and password protection, data in motion and office hygiene	●
PCI module	●
GDPR module	●
HIPAA modules	○
Custom content: Ability to include PDF, PPT or DOCX with each module	●
Employee risk scores	●
Company risk score	●
Sentiment tracking	●
Industry comparison rates for module test questions	●
Performance metrics including completion rates and correct responses	●
Watchlists for those who haven't watched or had incorrect responses	●
Module deployment controls - ability to set timing, order and cadence	●
One-click summary reports (downloadable as PDF)	●
User-enabled multi-language support & closed captioning	●
Phishing campaigns and reporting	●
Outlook add-in and Gmail extension for reporting phishing emails	●
Single page and multipage phish test templates	●
Phishing campaign builder	●
Learning Management System (LMS) integration	○
SSO and user provisioning	●
Compliance: International Organization for Standardization (ISO 27001 v 2013 - 9.1 | ISO 31000 v2009 - 5.6)	●
Compliance: National Institute for Standards and Technology (NIST 800-53 rev 4 | PM-6, AT-2[1], AT-4)	●
Compliance: National Institute for Standards and Technology (NIST 800-53 rev 5 | AT-2[3], AT-3[3], AT-3[4], AT-4)	●
Compliance: National Institute for Standards and Technology (NIST 800-160 | 3.3.7 and 3.3.8)	●
Compliance: National Institute for Standards and Technology (NIST 800-171 rev 1| NFO)	●
Compliance: National Institute for Standards and Technology (NIST CSF v1.1 | PR.IP-8)	●
Compliance: Payment Card Industry Data Security Standards (PCIDSS) PCI-DSS v3.2 - 12.6.2	●
Compliance: General Data Protection Regulation (GDPR) - EU GDPR Art. 32.1, 32.4 and 57	●
Compliance: US Health Insurance Portability and Accountability Act (HIPAA) - 164.308(a)(1)(i), 164.316, 164.308(A)(5)(ii)(ii)(A), 164.312(c)(2), 164.308(a)(7)(ii)(D), 164.308(a)(8), 164.316(b)(2)(iii), 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii), 164.308(a)(2), 164.308(a)(3)(i), 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(5)(ii)(D), 164.530(b)(1)	●

Mimecast Web Security Service Description

● – Standard ○ – Available at an additional fee

8. Mimecast Web Security (included in Cyber Resilience Pro Plan)	W1	W1N
Granular policy application to specific sites / networks, everyone, specific users or groups	●	Wi-Fi network policy-based protection
Web content filtering based on 80+ website categories	●	●
Custom allow/block lists	●	●
Customizable block page including ability to co-brand	●	●
Mimecast root certificate authority for SSL inspection	●	●
SafeSearch enforcement policy for Google, Yahoo and Bing	●	●
Dynamic DNS Proxy for inspection of unknown or risky websites	●	●
Ability to block newly observed domains	●	●
URL classification testing	●	●
Report potentially misclassified URLs	●	●
Integration with Mimecast Targeted Threat Protection URL Protect for consistent web security controls no matter the source of the web access	●	●
Support for advanced similarity detection	●	●
Inspection of file downloads from suspicious sites via a Mimecast web proxy service with static file analysis and multiple AV engines	●	●
Ability to configure service bypass exceptions	●	●
Mimecast security agent for Windows and Mac protects roaming users on or off the network	●	
Single administration console supporting both email and web security	●	●
Dedicated administration dashboard for high visibility into traffic and threats	●	●
DNS activity report with 90 days of activity	●	●
Security Report that shows all security risks detected over the last 7 days	●	●
Top 10 domains, categories, blocked domains and blocked categories dashboard widgets	●	●
Ability to export report data from the system via .csv	●	●
Full audit log of system access, events, policy creation and changes	●	●
Configurable logging policy to exclude retention of personally identifiable information (PII) for specific users, groups or locations	●	
Integration with core Mimecast role-based access control, including custom roles	●	●
Globally distributed datacenters providing minimal latency and high performance and reliability	●	●

Mimecast DMARC Analyzer Service Description

● – Standard ○ – Available at an additional fee

9. Mimecast DMARC Analyzer (Included in Pervasive Defense Plan)	DMA
360-degree visibility and governance across all email channels	●
Real-time domain monitoring	●
Unlimited monthly DMARC compliant email volume	●
Automated sub-domain detection	●
Unlimited active, in-active domains and sub-domains	●
DMARC aggregate (RUA) and encrypted forensic (RUF) report overviews	●
Built-in project management tools, including DMARC deployment workflow, setup wizards and recommendation engine for simple self-service	●
SPF delegation to manage SPF records and overcome lookup limits	●
DMARC record generator	●
DMARC, DKIM and SPF record checkers	●
Alerts and reporting by email (incl. compliance monitor, DMARC summary, DNS monitor)	●
DNS timeline to show and track changes to DNS record over time	●
Domain export capability provides the ability to export (CSV) all data as shown within the “domains dashboard”;	●
Language support for NL/EN/DE/FR/ES/PT	●
Fully managed service, incl. assigned deployment specialist, onboarding, training, project plan, bi-weekly project meeting, recommendations, alerting and advice following an attack, monitoring by assigned specialist	○
Service implementation to support onboarding and setup	○

Mimecast Brand Exploit Protect Service Description

● – Standard ○ – Available at an additional fee

10. Mimecast Brand Exploit Protect (Included in Pervasive Defense Plan)	BEP
Proactive intelligence to identify online brand-related manipulation and fraud	●
Multi-tier domain monitoring	●
Targeted scans using machine learning and key indicator analysis incl. new domain registrations and security certificate issuance	●
Threat detection agent to detect website cloning	●
Dashboard showing all suspicious sites and active attacks	●
Unlimited users access to the dashboard	●
Zero integration or onboarding	●
Data on historical URL detections and TLD distribution	●
Rendering of the site content and its history inside the dashboard for visual identification	●
HTML data and history for every URL detected	●
DNS and WHOIS information and history on each domain detected	●
Rapid site takedown initiated directly from the dashboard – average 3-hour takedown	●
Malicious social media account and mobile app takedown capabilities	●
Phishing site blocking in different browsers, web-extensions and across AV engines through intelligence sharing	●
Block suspicious and active attack domains and URLs instantly across Mimecast Email Security and Web Security services	●
Fully managed service	●
24/7/365 support	●
Data theft countermeasures	○

Select a Success Package

Mimecast's Customer Success Packages offer several support tiers available to all customers, regardless of their size.

- **Bronze Package**: Included with all Mimecast services as standard. This package includes unlimited access to the Mimecast Knowledge Base, online support during business hours and telephone support during the implementation phase.
- **Silver Package**: Bronze package plus local business hours telephone support and access to a Customer Success service desk
- **Gold Package**: Silver package plus 24x7x365 telephone support, named Customer Success Manager, prioritized telephone support for P1 issues, proactive customer success planning and optimization, annual service reviews and an online cyber resilience training session.
- **Platinum Package**: Gold package plus follow the sun support for P1 issues, named senior Customer Success Manager, bi-annual service reviews, annual immersion day onsite for end users, named Mimecast Executive sponsor, bi-annual strategic roadmap session and access to beta and early adopter programs.

Select an Implementation Package

Mimecast offers four levels of implementation packages to suit customers of all sizes and requirements. The relevant implementation package will be suggested during the pre-sales phase to ensure that you are implemented with the correct level of support.

- **Core Connect:** Unlimited access to the Mimecast Knowledge Base, account provisioning, Mimecast's Connect Application and telephone support, as needed.
- **Guided Implementation**: Core Connect plus a named Implementation Engineer, hosted scoping kick-off call, best practice documentation and a final validation call to wrap-up the implementation.
- **Managed Implementation**: Guided Implementation plus regular scheduled calls and remote sessions, named implementation engineer to guide you through all changes, knowledge transfer at key milestones, legacy policies review and migration guidance, weekly status updates, system administrator training and kick-off and completion calls.
- **Advanced Implementation**: Managed Implementation plus named Professional Services Consultant, online consultation (onsite available), multi-site or multi-country account configuration, eDiscovery sessions, production of a Statement of Work and end-user app set-up. Access to a dedicated team of implementation engineers to assist with any questions or problems. Creation of Mimecast account and assistance with each step of the process ensuring a smooth transition to Mimecast. On completion, all documentation and key information is passed to the Mimecast Support team, who have access to the original implementation engineer if required.

Add Archive Data Migration

For customers with a plan that includes archiving, Mimecast Simply Migrate can accelerate the process of migrating to the Mimecast Cloud Archive and beginning realizing the benefits of risk mitigation, pro-active e-discovery and integrated backup and archive.

Mimecast Education

All Mimecast training courses are run by experienced trainers and each is designed to help your administrators get the most from your chosen Mimecast service/s. Each course includes a mixture of instruction, demonstrations and exercises and is designed to enable you to maximize the benefit of your Mimecast service.

- Get access to unrestricted self-paced training content, unlimited instructor led training courses, and eligibility for role-based product certifications with Mimecast's new Education program. Visit our website: https://www.mimecast.com/customer-success/education/
- From end user to Super Administrator and everyone in between, Mimecast's new Education program with training videos, technical guides, and live instructor-led training courses ensure you master the Mimecast skills you need. Experienced instructors will help you gain the best return on your Mimecast investment.
- Maximize your security investment - Mimecast now offers the lowest cost training in the industry, with the best value for money and return on investment for customers. With Mimecast Education, you get access to unrestricted self-paced training content, unlimited instructor led training courses, and eligibility or role-based product certifications".