Cyber Resilience Pro Plan

Protection and Maximum Resilience

Protection against email-based threats is mandatory, but a more effective strategy requires a broader perspective. Mimecast Cyber Resilience Pro is designed to maximize your opportunities to break the attack chain at your perimeter and inside your network, and beyond.

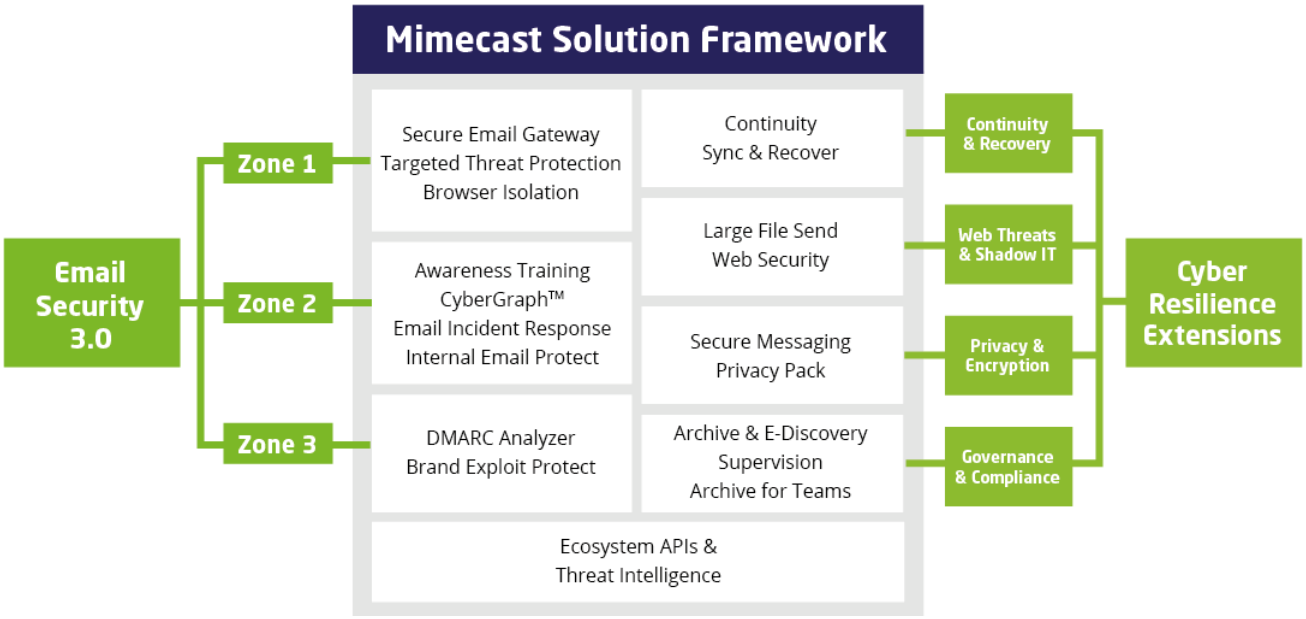
With solutions that keep employees connected during an email outage, protection against malicious web activity, encryption & data loss prevention, and archiving, Mimecast has you covered. It's the ideal solution for organizations that want the most sophisticated protection available and the resilience to keep business flowing, no matter what.

Key Benefits

- Safeguards your organization against threats from the number one attack channel
- Prevents the lateral and external spread of threats
- Integrates protection for web and email
- Reduces cyber risk with targeted training for the employees who need it most
- Reduces complexity and administrator time
- Makes end-users security assets, not liabilities
- Maintains productivity during cyber disruption
- Improves compliance and facilitates corporate governance

Security You Can Count On

- Neutralization of malicious URLs, attachments, spam and malware
- Prevention of account compromise to keep trusted senders from infecting others
- Quick remediation of threats from infected accounts
- Award-winning awareness training, proven to sharpen employee security reflexes so they can detect and avoid attacks
- Maintaining employee connectivity during planned or unplanned email outages
- Quick recovery of lost or stolen data



	Perimeter	Comprehensive	Pervasive	Foundations	Foundations +	Pro
At Your Email Perimeter						
Secure Email Gateway	•	•	•	•	•	•
Targeted Threat Protection	•	•	•	•	•	•
Browser Isolation						
Secure Inside Your Network And Organization						
Awareness Training		•	•	•	•	•
Internal Email Protect		•	•	•	•	•
CyberGraph™						
Mimecast Email Incident Response						
Defend Your Brand Beyond Your Perimeter						
DMARC Analyzer			•			
Brand Exploit Protect			•			
Improve Business Continuity And Recovery Time						
Email Continuity				•	•	•
Sync and Recover				•	•	•
Protect Against Web Threats And Shadow IT						
Web Security						•
Large File Send						•
Ensure Privacy And Communicate Securely						
Secure Messaging						•
Privacy Pack						•
Simplify Compliance And Accelerate E-Discovery						
Archive & E-Discovery					•	•
Supervision						
Archive for Teams						

Secure Email Gateway

- **Anti-Virus and Anti-Spam** – Comprehensive protection delivered via multi-layered engines with an optimum mix of proprietary and best of breed third-party technology
- **Data Loss Prevention** – Protect your sensitive and confidential information from accidental or intentional exposure with fine grained policy controls
- **Signature Disclaimer & Management** – Achieve consistency in all email communications with email signature and disclaimer management based on Active Directory credentials
- **End User Productivity Applications** – Boost your employee productivity with self-service security, email and archive access features with apps built for Outlook, mobile, Mac and Web
- **Intelligent Email Routing** – Support complex on-premises, cloud, or hybrid email environments and achieve rapid email system integration or separation associated with a merger, acquisition, or divestiture
- **Threat Intelligence** – Gain insight into threats targeting your tenant with the Threat Intelligence Dashboard or use our Threat Intelligence API to feed threat data into a third-party tool of your choice
- **API (Application Programming Interface)** – Create an extensible architecture for complete visibility and efficiency by integrating Mimecast with your current or planned IT solutions

Targeted Threat Protection

- **URL Protect** – Protect your organization and employees against malicious websites containing malware, phishing and other threats through URL rewriting and on-click deep site inspection
- **Attachment Protect** – Defend against infection from weaponized attachments often used in ransomware, keylogger, trojan and spyware attacks with multi-layered inspection including advanced static and dynamic analysis
- **Impersonation Protect** – Comprehensive protection against social engineering attacks like Business Email Compromise, CEO fraud and phishing targeting your employees

Internal Email Protect

- **Protection from Threats Inside your Email Perimeter** – Detect and prevent security threats that originate internally as a result of account compromise, human error or malicious action with comprehensive file and URLs checks on internal and outbound email
- **Threat Remediation** – Continuous monitoring of lateral and outbound email using the latest intelligence with automatic or manual remediation of files or emails post-delivery

Awareness Training

- **Core Infosecurity** – Change behavior and lower organizational risk with persistent, engaging security awareness training. Help make employees part of your defense against web and email attacks, data loss, and other security threats
- **Phishing Simulation** – Test employee susceptibility with realistic phish tests. Phishing simulations are integrated with core training, making it easy to deploy reinforcement of training concepts based on test response
- **Risk Scoring** – Identify your riskiest employees so you can focus precious time and budget supporting the employees who need it most. Benchmark aggregate company score against other organizations in your industry to gauge your overall risk posture
- **Custom Content** – Enhance existing modules with supplemental training material or create your own module for training needs unique to your organization
- **Targeted Training** – Deploy additional training to employees who need it most. Create custom lists based on training performance, phishing simulation response or risk score so you can assign and send additional modules or conduct other types of training or remediation
- **HIPAA Modules (Optional)** – Supplement core information security training with modules covering issues specific to the Health Insurance Portability and Accountability Act (HIPAA)

Web Threats and Shadow IT

- **Malicious Site Defense** – Protect your employees and guests from accessing malicious sites with comprehensive category and security policy controls
- **Acceptable Use Enforcement** – Control what content is accessible by your employees and guests by enforcing acceptable use policies through 80+ granular category filters
- **Application Visibility and Control** – Help mitigate shadow IT risks with full visibility of what cloud applications are being used. Then monitor, sanction or block access to all or groups of employees
- **Intelligent Proxy** – Ensures deeper inspection of suspicious sites, including file downloads, by inspecting this traffic via a proxy and applying additional checks including anti-virus and static file analysis
- **On Network Protection** – Protection is automatically applied for all web requests originating from employees or guests on your network
- **Protect Guest Wi-Fi** – Network-level controls help reduce legal and compliance risks by preventing access to malicious sites and blocking inappropriate content for visitors, customers and anyone else using your guest Wi-Fi networks
- **User Reporting** – The ability to report on web access down to a user level when the Mimecast Security Agent is deployed to employees' devices
- **Large File Send** – Ensure employees can easily and securely share large files up to 2GB via email whilst maintaining corporate security, compliance and data retention policies

Continuity and Recovery

- **Email Continuity** – Allows you to continue to communicate internally and externally during any planned or unplanned email service downtime with a 100% SLA on email availability
- **Sync and Recover** – Continuous synchronization of email that ensures an email or entire inbox can be recovered following an attack, breach or user error

Privacy and Encryption

- **Secure Messaging** – Enable your employees to securely send confidential and sensitive information via email with administrator defined and user selectable controls and policies
- **Privacy Pack** – Dedicated lexicons designed for those needing to identify personally identifiable information (PII), financial or healthcare related data

Governance and Compliance

- **99-Year Retention** – Long term data retention with a multipurpose cloud archive for compliance, e-Discovery, case review, restoration of email and increased user productivity
- **E-Discovery** – Comprehensive search, e-Discovery, and compliance support capabilities to provide retrieval of corporate data