mimecast™

Pervasive Defense Plan
Protection at Your Perimeter, Inside Your Network, and Beyond

Brand impersonation is a growing challenge with potentially devastating consequences. It's easy for attackers to spoof your website, a trusted supplier's website, or a Microsoft log in page. Threat actors will even use legitimate domains to send fake emails designed to trick unsuspecting customers and partners.
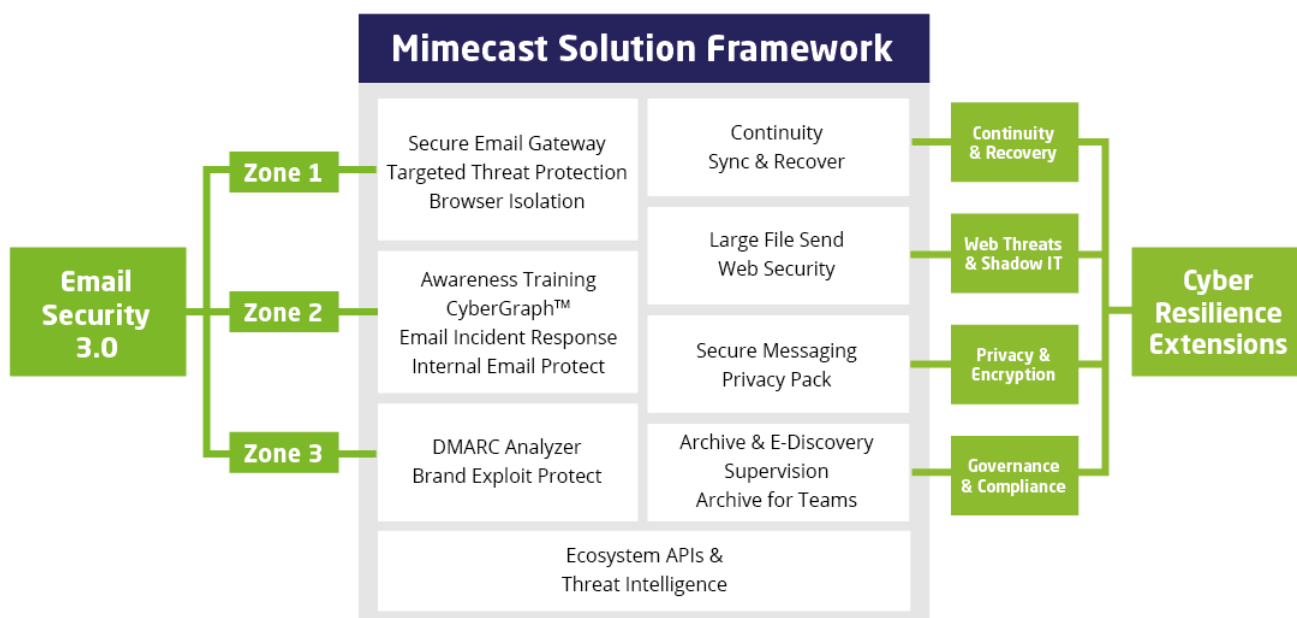
Stop attackers from destroying your brand with Pervasive Defense from Mimecast. This plan extends protection beyond your perimeter, allowing you to proactively gain intelligence and shutdown attacks or quickly remediate them if they go live. With at the perimeter and inside your network protection built in, Mimecast's Pervasive Defense is a security game changer.

Key Benefits

- Safeguards your organization against threats from the number one attack channel

- Prevents the lateral and external spread of threats

- Reduces cyber risk with targeted training for the employees who need it most

- Reduces complexity and administrator time

- Stops attackers from destroying your brand

- Rapidly takes down web sites mimicking your brand

- Leverages DMARC standard to safeguard emails

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

- Prevention of fraudulent use of your owned domains

- Protection for customers and partners from phishing attacks impersonating your brand

Mimecast Solution Framework

Email Security 3.0

Zone 1
- Secure Email Gateway
- Targeted Threat Protection
- Browser Isolation

Zone 2
- Awareness Training
- CyberGraph™
- Email Incident Response
- Internal Email Protect

Zone 3
- DMARC Analyzer
- Brand Exploit Protect

- Continuity Sync & Recover
- Large File Send / Web Security
- Secure Messaging / Privacy Pack
- Archive & E-Discovery / Supervision / Archive for Teams

Ecosystem APIs & Threat Intelligence

Cyber Resilience Extensions
- Continuity & Recovery
- Web Threats & Shadow IT
- Privacy & Encryption
- Governance & Compliance

	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)

DMARC Analyzer

- **360 Degree Visibility & Governance** – Easy to use reporting and forensics that let you see and analyze who is sending email on your behalf to identify legitimate versus fraudulent senders

- **Assisted DMARC Enforcement** – Self-service email intelligence tools, guided workflows and wizards designed to reduce the time, effort and cost of enforcing a DMARC policy to stop domain abuse

Brand Exploit Protect

- **Proactive Threat Hunting** – Harness artificial intelligence and machine learning to scan quadrillions of web addresses to find websites spoofing your brand, even before they become live attacks

- **Web Detection Agent** – Discover if your website has been scraped and cloned anywhere on the internet

- **Remediation** – Initiate a rapid takedown of suspicious or active sites while protecting your employees by blocking URLs and domains across both Mimecast's Email and Web Security services