Email Security 3.0

Keeping You Safe At Your Perimeter

Zone 1

The Email Security Imperative

Keeping email safe continues to be among the biggest challenges IT and security teams face. From business email compromise and spear phishing to weaponized attachments and malicious URLs, there are so many ways for attackers to get in – and those tactics change and get more sophisticated all the time. The simple fact remains that securing email is one of the most important steps organizations can take to safeguard against business disruption, data loss, and financial damage.

Applying the most effective controls possible to keep email secure is the focus of Mimecast's protections in Zone 1 – At Your Email Perimeter. Our email security service with targeted threat protection offers best-in-class defenses against even the most sophisticated attacks.

World-Class Security, Simply Delivered

Mimecast Email Security is a cloud-based service with all functions fully integrated and engineered to work together. Built to keep pace with a rapidly changing threat landscape, it combines a secure email gateway with data loss prevention, content controls, and targeted threat protection.

Email Security 3.0

Mimecast Email Security 3.0 helps you evolve from a perimeter-based security strategy to one that is comprehensive and pervasive, providing protection across three zones. These protections are enhanced by a wide range of complementary solutions, actionable threat intelligence, and a growing library of APIs.

Zone Defense

- *Zone 1* **At Your Perimeter**
- *Zone 2* **Inside Your Network & Organization**
- *Zone 3* **Beyond Your Perimeter**

Extensions

- **Continuity & Recovery**
- **Web Threats & Shadow IT**
- **Privacy & Encryption**
- **Governance & Compliance**

Ecosystem & Threat Intelligence

This fully cloud-based services helps you defend against:

- **Business email compromise, phishing, and spear-phishing –** Impersonation attacks are on the rise, with attackers increasingly using social engineering and other sophisticated techniques. Get comprehensive protection with real-time examination of the inbound email's display name, reply-to information, and body content, as well as detection of character switching, advanced similarity checks, and the use of long URL strings.
- **Weaponized attachments –** It's all too easy for attackers to infect attachments with scripts that download malicious content like ransomware, trojans, and botnets. Protect your end-users with multiple layers of defense, including safe file conversion, static file analysis, and sandboxing when needed.
- **Signature-less malware and zero-day attacks –** The use of malware with algorithms designed to evade signature-based detection methods is a dangerous attack type. Shut down these threats with Mimecast technology that can quickly detect the algorithm's structure, allowing us to rapidly deploy protections and defend you against zero-day, polymorphic malware.
- **Malicious URLs –** URLs that point to phishing sites or that are designed to install malware, viruses, or trojans are a major security challenge. With Mimecast, you get multi-step detection and blocking of malicious URLs, including pre-click URL discovery, protection on and off the enterprise network from any device, rewriting of all URLs in inbound email, and real-time scanning on every click.
- **Loss of sensitive or proprietary information –** Data loss is a high-profile issue that can quickly erode trust. Keep sensitive data and intellectual property secure with Mimecast data loss prevention, which allows you to use both pre-built and custom libraries and apply automated controls to keep employees from accidentally or intentionally sending information to people who shouldn't have it. Policies can also be triggered to require the use of Secure Messaging.

Real-World Scenario

Paul finally got his organization moved to Office 365. Soon after, his CFO, Mark Towns, barged into his office to ask why his team kept getting emails from a "Mark Townes" requesting wire transfers. Paul opened a ticket with Microsoft and waited for a response. A short time later, Microsoft had Active Directory issues that slowed down all Office 365 applications, including Exchange Online. Mark came back to Paul's office, this time wondering why he couldn't send or receive email. Again, Paul opened a ticket with Microsoft. As the influx of spam and targeted attacks continued, it became clear to Paul that he needed a solution capable of blocking unwanted mail before it hit Office 365.

How Mimecast would have helped...

- Multi-layered email inspections
- Protection against sophisticated attacks, like phishing and spear phishing
- Flexible support plans designed to meet varying levels of need

- **Lean IT** – Lean IT is becoming standard operating procedure for more and more organizations, resulting in smaller staffs, limited bandwidth, and expertise gaps that are hard to fill. Ease the burden on staff and reduce both cost and complexity with a comprehensive set of email security services delivered in a single, cloud-based, easy-to-use platform.
- **Gaps in Office 365 security –** There's no question that Office 365 is a great email service, but you need email security technology that's equally as effective. Organizations that rely on O365 security alone often discover that what seemed like an easy solution creates a lot of challenges instead – lower efficacy, more spam, and limited support. Mimecast's Email Security service complements O365, adding multiple layers of protection and resilience so you can reap the benefits of moving to the cloud without increasing risk.

Trust Your Email Again

Secure your most critical communications channel with email security that allows you to:

- Defend against spear-phishing and advanced email threats
- Protect employees against impersonation attacks that spoof a trusted sender
- Neutralize threats from malware attachments and malicious URLs
- Take advantage of the cost and performance benefits of multi-tenant cloud
- Simplify administration and reduce the burden on IT and security
- Reduce cost and complexity
- Get a forever-modern service with the latest protections automatically applied
- Empower end users with self-service capabilities accessed from within Outlook, web, and mobile applications.