Email Security 3.0

Protecting You Inside Your Network & Organization

Zone 2

Protection From the Inside Out

Threats that exist inside an organization are often underestimated, which means they also carry a lot of risk. Attacks can spread silently and rapidly from user-to-user or even worse, from employees to customers and partners. And without adequate security awareness, end-users are highly susceptible to making an innocent but devastating mistake.

When You Consider That...

- 60% of most organizations' email traffic is internal (user to user) and outbound*
- Human error is a factor in the vast majority of successful attacks
- 71% of organizations report having malicious activity spread from user to user in the last 12 months**

...applying a best-practice security approach inside your organization becomes an imperative, rather than a nice to have.

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.

*Based on aggregate data of Mimecast customers

** 2019 State of Email Security Report

Preventing attackers from breaching your internal email systems, while also making employees aware of common tactics and best security practices, is the focus of Mimecast's email security strategy in Zone 2 – inside your network and organization.

Strengthen Your Last Line Of Defense

Even with a robust email security perimeter in place, attackers can bypass the perimeter and operate inside your email network, using compromised employee accounts, social networks, file sharing sites, and other techniques to gain access and send bad things inside and out. Mimecast's integrated approach and award-winning technology come together to help you address internal risks, including:

- **User-to-user and user to third-party compromise –** When internal email traffic is left exposed, attacks can easily spread within your organization or to customers, partners, and suppliers. With Mimecast, the same robust stack of email security technologies used at the perimeter can be applied to internal and outbound traffic as well, ensuring that ALL email is protected.
- **Latent malware –** Not all malicious content is detected at the gateway – some is designed to activate after delivery. To mitigate the associated risks, Mimecast's technology continuously checks previously delivered files for malicious content, so you can take action when needed.
- **Threat remediation –** When internal email is left unprotected, finding the source of an attack can take weeks or months, not to mention the time spent on remediation. With Mimecast, you can quickly identify and remediate threats with technology that allows you to search for files by hash, from and to, or message ID and then automatically or manually remove them from users' inboxes post-delivery.
- **Strengthening employees' security reflexes –** Approximately $1.5 billion is spent annually on security awareness training, yet the vast majority of security breaches involve employee error. Clearly, something isn't working. Mimecast Awareness Training turns the traditional training model on its head, helping you reduce the risk of human error by creating a virtuous learning cycle through fast,

Real-World Scenario

Thousands of users at a major healthcare company received a malicious attachment titled "Employee Notice". Hundreds of employees opened it within a matter of hours, infecting their computers and creating havoc. IT scrambled to stop the attack, then started cleaning all affected systems and looking for the source of the problem.

After days of manual 24x7 work, they discovered the attack had originated with one of their financial controllers. He'd been compromised six months prior when he entered his credentials on a fake Office365 login page.

How Mimecast would have helped…

- Best-practice inspections of internal email, including URLs and attachments
- Rapid remediation of threats
- Awareness training designed to make employees a security asset

high-impact training videos. The approach realizes serious results by (very intentionally) not taking itself too seriously, providing laugh out loud training that your employees approach with excitement instead of dread. And to keep things real, the solution also provides easy to deploy phish testing capabilities.

- **Identifying and supporting most at-risk users –** Most training programs treat everyone the same, but different end-users represent different degrees of risk. Mimecast Awareness Training lets you measure employee awareness and risk at an individual level, accounting for both knowledge and sentiment. Risk scores then allow you to easily track awareness over time and prescribe targeted training and support when needed.

By pairing proven training techniques with best-practice internal email inspections, you can close gaps in Zone 2 defenses and enhance your overall security posture.

Build Trust On The Inside

Make internal security a strength, not a weakness with technology that allows you to:

- Apply best-practice security inspections to ALL email
- Protect against latent malware with continuous re-checking of previously delivered content
- Automatically or manually remediate unwanted emails post-delivery
- Prevent user-to-user and user to third party compromise
- Provide training that engages employees and changes behavior
- Measure security awareness risk at the employee and organizational level