Solution Brief

mimecast

Email Security 3.0

Web Threats & Shadow IT

Expand Protection While Minimizing Cost and Complexity

Simplify Security Across Email and Web

End users are focused on getting their jobs done, and systems or policies that are viewed as added work can lead to risky behavior. Insecure websites, unsecured file sharing services, public Wi-Fi. "What harm could they do?", employees often think.

IT and security teams know the answer is a lot.Credentials can be compromised, data can be stolen, and your organization can be exposed to legal and compliance risks. Visibility and control are essential, whether users are on your network or off and regardless of the device they're using.

Enter Mimecast Web Threats and Shadow IT. Easy to deploy and fully integrated, it allows you to protect users online, anytime and anywhere; get visibility into which websites and cloud apps are being used; and provide a convenient, secure alternative to one of the most commonly used unsanctioned IT applications – cloud file sharing services.

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.

Keep Users Safe Online

Mimecast Web Security allows your users to safely surf the web by stopping malware and other web threats before they can reach your network or endpoints, a key advantage over more traditional defenses like firewalls and endpoint protection. The solution protects users both on and off your network, while also securing guest Wi-Fi connections and allowing you to block website categories that are risky or inappropriate. In addition, it's fully integrated with Mimecast's Email Security with Targeted Threat Protection service, so you can protect the top two attack vectors with a single, easy to deploy, easy to manage solution.

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

Mitigate Shadow IT

Mimecast Web Security includes Application Visibility and Control to help you see into the blind spots of uncontrolled cloud app use in your environment. You get full visibility into which apps are being used, by whom, and how often, along with the ability block or monitor apps as needed.

Share Large Files Quickly, Easily, and Securely

Email server file limits and security controls often cause users to take the path of least resistance and send files using unsanctioned applications. Fully integrated with Email Security, Large File Send lets users securely send and receive large files without ever leaving Outlook or your Mimecast mobile or web apps. Data loss prevention policies and additional security controls, including setting an expiry and requiring an access key, can also be applied to prevent information from ending up in the wrong hands.

Real-World Scenario

Justin was panicking. A huge deal was on the line; but try as he might, his company's email system kept rejecting his attempts to email the final 25-page contract to the client. Then he remembered a Dropbox promotion sent to his personal email. He set up an account and logged in, uploaded the contract, and sent the link to his client. Easy as that, the deal was done.

Three weeks later, however, he couldn't find any files on his computer. After days of troubleshooting, IT discovered his credentials had been stolen. Justin had used his corporate credentials to create a Dropbox account on what turned out to be a spoofed website. All his new client's information was now exposed, along with details from all his other accounts.

How Mimecast Could Have Helped

- Mimecast Web Security would have blocked access to the spoofed Dropbox site, preventing Justin from handing over his credentials
- Mimecast Large File Send would have allowed Justin to send/receive his contract without leaving Outlook
- Mimecast Large File Send would have applied expiry, no print/forward, and an optional password on the file
- Mimecast Large File Send would apply content controls to the file to ensure compliance