Menlo Security

SECURING OFFICE 365 EMAIL WITH ISOLATION

SOLUTION BRIEF

THE PROBLEM

Microsoft Office 365 is one of the fastest-growing cloud-based applications today. Many organizations that were initially resistant to cloud-based applications, especially Office 365's cloud-based Exchange Online email capabilities, have reconsidered and are quickly migrating to cloud-based email. There are many reasons for the shift from on-premises to cloud-based email, including ease of accessibility, lower cost, and resource savings—as a result of no longer having to administer and maintain on-site email software and hardware, and the ability to scale nearly at will.

However, some organizations have lingering concerns when it comes to cloud-based email, and specifically Office 365. Some of the apprehension that organizations have with Office 365 are about the prospect of latency and its effect on the user experience, as well as possible bandwidth issues, leading to inaccessibility. But, the most persistent hesitation is with the security of Office 365, Exchange Online, and user email.

Office 365 security, particularly the security of its email capabilities, has been and continues to be a source of concern for users of the cloud-based service.

The apprehension is not only felt by organizations migrating to or adopting Office 365, but it has also been covered by industry analysts and has even been analyzed and publicized by Microsoft.

Phishing continues to be a top threat to email security for users of Office 365. Microsoft does offer several different detection-based technologies found in two different add-on security offerings for Office 365—Microsoft's Exchange Online Protection (EOP) and Advanced Threat Protection (ATP). However, while some organizations that have adopted Office 365 feel that Microsoft's add-on detection-based security offerings are "good enough," many organizations and some industry analysts believe Microsoft's "good enough" email protection is not good enough.

THE SOLUTION

Microsoft Office 365 users realize that they need a better, more effective approach for securing their email, attachments, and web access. Isolation is that approach.

Menlo Security's Isolation Platform enhances email and web security for Office 365 users and their organizations. The Menlo Security Isolation Platform (MSIP) eliminates malware infections from the two most leveraged attack vectors: web and email. MSIP stops the risk of infection by web-borne and email-delivered malware. All web page components and all active content—including JavaScript and Flash—are executed and contained within MSIP. There is no detection, and there are no "good vs. bad" or "allow vs. block" decisions. Only safe, malware-free rendering information is delivered to a user's web browser.

Menlo Security's Phishing Isolation solution is quickly deployed within an existing Office 365 or Exchange Online email workflow. The solution rewrites all web links a user receives in Office 365 email messages so that if the user clicks on a suspicious web link in an email, the questionable website is opened within the cloud-based Menlo Security Isolation Platform. Menlo's Phishing Isolation platform can also be configured to prevent users from uploading or typing any information in untrusted web forms.

The "weaponization" of documents, such as Office 365 documents, and posting them on a website or attaching them to a phishing email is another popular attack method. The Menlo Security Isolation Platform blocks these attacks by safely rendering an isolated version of a downloaded document. It also wraps email attachments, allowing for safe handling options. Policies can also be set by group or by individuals, allowing them to download an original document, but only after it has been fully inspected by advanced antimalware and has been quarantined in a sandbox for further inspection.

Menlo's Isolation Platform also tracks how Office 365 users interact with web links within received email, enhancing forensics. MSIP also delivers real-time, customizable phishing training via on-screen messages.

Menlo Security

About Menlo Security

Menlo Security protects organizations from cyber-attacks by seeking to eliminate the threat of malware from the web, documents, and email. Menlo Security's cloud-based Isolation Platform scales to provide comprehensive protection across enterprises of any size, without requiring endpoint software or impacting the end-user experience. Menlo Security is trusted by major global businesses, including Fortune 500 companies and financial services institutions, and backed by General Catalyst, Sutter Hill Ventures, Engineering Capital, Osage University Partners, American Express Ventures, Ericsson Ventures, HSBC, and JP Morgan Chase. Menlo Security is headquartered in Palo Alto, California.

2300 Geng Rd., Ste. 200

Palo Alto, CA 94303

Tel: 650 614 1705

info@menlosecurity.com

menlosecurity.com