Menlo Security

SECURING OFFICE 365 EMAIL WITH ISOLATION

WHITE PAPER

OVERVIEW

Introduction

Microsoft Office 365 is one of the fastest-growing cloud-based applications today. While many organizations were at first reluctant to embrace cloud-based applications, especially the Office 365 cloud-based Exchange Online email capabilities, recent adoption figures show that initial reluctance has quickly turned to acceptance. According to industry analyst reports, a majority of organizations have adopted and are actively using cloud-based secure email products. In addition, nearly all organizations interviewed that are newly adopting or transitioning existing services to the cloud are selecting cloud-based email delivery. Reports have estimated that by 2021, nearly three-quarters of business users will be substantially provisioned with cloud-based office productivity capabilities.

Why Office 365

Organizations are migrating from their on-premises–based Microsoft Office deployments to the cloud-based Office 365 for a number of reasons. One reason is ease of accessibility, and being able to work from anywhere, at any time, on virtually any device. Another is the cost savings that organizations can attain with Office 365, as they no longer have to administer, patch, or otherwise maintain on-site software or the hardware on which it is required to run. With Office 365, all ongoing maintenance is handled seamlessly by Microsoft, and deployment can be quick and simple. The ability to scale nearly at will is now also fast and easy with Office 365, requiring just a phone call and additional licenses, versus the previous procedure of purchasing and installing additional hardware and software.

Concerns about Office 365 still persist, however. While the ability to work virtually anytime, anywhere, and over any device sounds fabulous, there is the issue of user access being provided by the most advantageous and fastest route, as well as potential latency issues. Concerns have been voiced over potential bandwidth issues with Office 365, and possible inaccessibility as a result of those issues. But, far and away, the biggest concern for organizations and their users has been security.

CHALLENGES

Office 365 and Email Security

Office 365 security, particularly the security of its email capabilities, is a source of trepidation 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.

Microsoft has mentioned that phishing continues to be a top threat vector to email security for users of Office 365. In market reports, industry analysts have pointed out that the email security capabilities of Office 365 have lagged when compared with the email security available from other vendors. Those reports have indicated that many organizations migrating to or adopting Office 365 have begun to supplement its native email security capabilities with products from other vendors. While some Office 365 corporate customers believe the email security found in the cloud-based offering is "good enough," others feel that they need more effective security for email.

Microsoft Exchange Online Protection

Microsoft offers several different detection-based technologies, in two different add-on security offerings for Office 365. One is an email filtering service that provides real-time antispam and signature-based, multi-engine antimalware protection—including antivirus and antispyware protection—as part of Microsoft's Exchange Online Protection (EOP).

Microsoft EOP is a messaging protection solution that sifts received email through a variety of filters. For instance, once an email is received, it is passed through a connection filter, which checks the email sender's reputation. At the same time, a malware check is performed on the email. If the email passes those tests, it is then checked against messaging policies set by the organization; if the organization has licensed from Microsoft a separate data loss prevention (DLP) service, it is also applied to the email at this stage. If the email passes muster, it then proceeds to the antispam check, which reviews the email for wording and characteristics usually found in spam email. If successful in passing through all of these filters, the email is then delivered to the recipient's email inbox.

Microsoft Advanced Threat Protection (ATP)

Microsoft also offers Advanced Threat Protection as an add-on subscription service to its users who have EOP, and who have certain Exchange Online, Office 365 Business, Office 365 Enterprise, or Office 365 Education plans.

Microsoft ATP, like Microsoft EOP, is an email filtering service. It is cloud-based but can be used with on-premises Exchange Server and other on-premises SMTP email server environments, Exchange Online cloud-hosted mailboxes, and hybrid environments.

One of the key capabilities available in Microsoft ATP is named Safe Links. While email content is scanned, the URLs of any links within the email are rewritten to go through Office 365. The Safe Links feature is based on policies set by an organization's administrators, such as links that are whitelisted (a custom "Do Not Rewrite URLs" list) or blacklisted (a custom blocked URL list). Depending on the user policies and administrative policies that have been put in place, once a user opens an email that they have received in their Office 365 email inbox and clicks on a link in that email, Safe Links will allow the accessed website to open or will present the user with a warning page. The organization has the option of enabling a user, based on policy, to click through a warning page to the original website, or to disallow a user to click through. For Safe Links to work effectively, an organization's administrators must define default policies for the handling of certain links and websites. In the same way that Safe Links protects against users clicking on links in email, it also provides the same level of protection for links embedded in Office 365 documents, such as Word, Excel, and PowerPoint files. Safe Links also tracks the links that users have clicked on for further analysis and assessment.

Working hand in hand with the Safe Links feature is Microsoft ATP's Safe Attachment capabilities. Safe Attachment scans the attachments of incoming email for known virus and malware signatures. Any email attachment that does not contain a known virus or malware is routed to an environment where real-time behavioral malware analysis using machine learning techniques evaluates the attachment's content to determine if there is anything that may be malicious or worrisome. If the attachment has been cleared and declared safe, it is released for access by the user. Email attachments that have been deemed unsafe are sandboxed, with any embedded malware detonated before the document is released to the user.

Microsoft ATP also includes spoofed email intelligence, which detects if a sender is sending email appearing to be from one of a subscribed organization's users. It allows an organization to review all senders who may be spoofing the organization's domain to determine if the sender should be allowed to continue sending the email, or should be blocked.

Microsoft ATP also provides machine learning–based antiphishing capabilities, in addition to reports and the ability to track links and trace URLs.

Office 365 Email Security Challenges

While Microsoft Exchange Online Protection (EOP) delivers basic email protections, which are enhanced with Advanced Threat Protection (ATP), the reality is that there are reasons to be concerned about Office 365 email security. Many organizations that are Office 365 clients that are deploying or have deployed cloud-based email are concerned enough to explore other options to augment their Office 365 email security capabilities.

While Microsoft EOP provides antimalware—both antivirus and antispyware—protection, it is only signature based. Signature-based protections have proven to be notoriously ineffective against the more sophisticated email attacks that have evolved and been launched. The reality is that in order for signature-based protections to work, the malware that they protect against must be known and must have had a signature created to uncover and stop the malware. Most modern attacks are obfuscated, easily circumventing signature-based malware protections.

Even Microsoft's Advanced Threat Protection (ATP) leaves gaps in email security support. For instance, while ATP includes the ability to detect malware embedded within attachments of received Office 365 email and to detonate the malware safely, it doesn't provide the same protection for malware embedded in email content. Also, ATP allows the original document to be accessible to and downloaded by the user after the document has been sandboxed and has been found not to include malware. However, most email-based attacks are moving toward fileless attacks. This means that there may be no executables or other signs that would indicate that the document is malware infected. Once the document is released to the user, and they open the document, the malware attack can be launched, even though the document had been sandboxed and determined to be safe. That is because a fileless attack doesn't include anything that may be detonated. A fileless attack typically leverages vulnerabilities or repurposes legitimate tools in a device's operating system, such as PowerShell in Windows, to expose the device to additional attacks. There are no signatures to detect, effectively negating the ATP detection capabilities.

In addition, the ability of ATP to rewrite URLs for Office 365 is only an "allow" or "block" decision, which is made at the time a user clicks on the link. However, any clicks before the URL is "convicted" and user access is disallowed can lead to a risk of infection. ATP also does not provide a solution for web-based malware attacks. For instance, when a user clicks on a link and the decision is made to allow the user to access the web page, ATP is no longer associated with the user's web session. So, if a web page included malware that was being delivered by malvertising, drive-by download, or watering-hole attack, the user and their device would be infected, potentially creating a waterfall of attacks for their organization.

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

SOLUTION

The New Approach: Isolation

An isolation platform can address many of the gaps in email and web security that are currently left unaddressed and assailable by attackers in Office 365. For one thing, isolation does not rely on signatures or detection. It doesn't make a "good vs. bad" or "allow vs. block" decision. An isolation platform simply assumes that all content —email, attachments, and web content—has the potential to be bad.

An isolation platform simply assumes that all content has the potential to be bad.

Therefore, an isolation platform completely contains and executes any content away from a user's device, rendering only safe visual elements for the user to view and work with.

For example, an isolation platform may rewrite the URLs for links embedded in email. It may open attachments in the isolation platform and provide user access only to safe, rewritten attachments, thereby negating the effectiveness and stealth of fileless malware attacks. An isolation platform may rewrite and re-render a web page to ensure that all content viewed by a user on their device is safe, while not interrupting or affecting user experience. It may strip away any active content, such as JavaScript and Adobe Flash, that might have served as a delivery mechanism for malevolent payloads, re-rendering their content safely and securely.

An isolation platform can ensure that an organization and its users—employees, contractors, and the like—are safe and protected from phishing, spear-phishing, credential theft, malware, drive-by exploits, watering-hole attacks, and more.

But not all isolation platforms are built alike.

Why Menlo Security

Menlo Security's Isolation Platform enables a greater number of enhanced email and web security options for Office 365 users and their organizations.

The Menlo Security Isolation Platform (MSIP) eliminates malware infections from two primary attack vectors: web and email. MSIP stops the risk of infection by web-borne and email-delivered malware. It eliminates the possibility of malware reaching user devices via compromised or malicious websites or documents. A user's web session and all active content—including JavaScript and Flash—are completely executed and contained within the Isolation Platform. There is no "good vs. bad" or "allow vs. block" decision to be made. Only safe, malware-free rendering information is delivered to a user's device. No web page component or active content, including any potential malware, leaves the Menlo Security Isolation Platform. There's no path for isolated malware or other malicious content to reach a user's device, and legitimate content is not unnecessarily blocked in the interest of security.

Two of the most common attack vectors today are phishing and targeted spear-phishing email. Phishing and spear-phishing attacks are launched by malicious email, typically crafted to resemble an email from a familiar, trusted brand or contact. Attackers try to fool users by employing a number of psychological means and taking advantage of human nature—such as by conveying a false sense of urgency, importance, or criticality; promising money or threatening the loss of money; offering free food, drink, or fabulous social opportunities; or making claims that generally pique curiosity. Users then click on a link in an email, opening a web page to a phishing website that either downloads malware to their device or entices them to fill out a fake web form that steals their user credentials.

Menlo Security's Phishing Isolation solution is deployed within an existing Office 365 or Exchange Online email workflow. Menlo's Phishing Isolation solution rewrites all web links a user receives in Office 365 email messages so that, if the user does click on a malicious web link in an email, their web browser is forced to open the questionable website within the cloud-based Menlo Security Isolation Platform. There is no detection or decision necessary about whether the link is good or bad. There is no need for the organization to define whitelists or blacklists of URLs. Menlo's Phishing Isolation platform not only provides the protection of isolation, but it can also be configured to prevent a user from uploading or typing in any information in untrusted web forms, including corporate or personal credentials such as usernames and passwords.

Another common attack method is to "weaponize" documents, and either post them on a website or attach them to a phishing email. A weaponized document can be an Office 365 document—such as a Word document, an Excel spreadsheet, or a PowerPoint presentation—as well as a PDF file or other files, embedded with malicious code that runs when a user opens the document, compromising a user's device. A weaponized document may also be an attachment that launches a fileless attack, undetectable by most signature- or detection-based antimalware offerings. Many times, the attack will inject a dropper onto the user's device, open a backdoor, and steal information from the user's device. The Menlo Security Isolation Platform blocks attacks using weaponized documents by safely rendering an isolated version of a document being downloaded. It also wraps email attachments, allowing for safe handling options. For instance, Menlo's Isolation Platform enables a safe document view, where the user can view the document online,

safely, without fear of malware infecting their device. MSIP can also convert the attachment to a safe PDF file, downloadable by the user, if they require a hard copy. Based on administrative policies as set for a group or for individual users, the original document may be downloaded by an approved user—but only after the document has been fully inspected by advanced antimalware and has been quarantined in a sandbox for further inspection. Only after it has been deemed safe and malware-free will the document be released to the user.

The Menlo Isolation Platform remains active with the user throughout their web session, protecting them from web-borne malware attacks via drive-by downloads, watering-hole attacks, malvertising, or other means.

MSIP is able to track how Office 365 users interact with web links contained within the email they receive. It also enables enhanced investigative abilities for forensics, tracking what a user may have accessed that was infected with malware, whether the malware infection came through an email and, if so, whether the email was accessed from their work inbox or personal email, and more. With this information, the point of access that infected the user's device can be identified and located quickly, allowing access to be stopped and preventing it from happening again. The Menlo solution delivers auditing and reporting that is not available with Office 365 solutions. The Menlo Security Isolation Platform also delivers real-time, customizable phishing training, via on-screen messages.

It is simple to deploy MSIP with Office 365. Since Office 365 email is already cloud based, integration and conversion are easy, with no interruption in email service or change in user experience. There is no additional bump in the chain, since deployment requires only a connector, a few new roles, and a user Active Directory —even Active Directory Federation Service (ADFS) can be leveraged to simplify user authentication.

Conclusion

While Office 365 is fast becoming the de facto standard for cloud-based application services, securing its email capabilities requires additional services. While Office 365 email security and Microsoft's add-on subscription services may be "good enough," is "good enough" security really good enough? Does legacy detection- and signature-based security protect users and organizations from new, sophisticated advances in malware and its delivery mechanisms, when all that's needed is one misstep in security to create a headline and ruin a long-standing, time-built reputation?

Office 365 may be the bellwether for cloud-based application services. But a new approach is necessary to address email and web security.

That new approach is isolation. And Menlo Security is the isolation leader.

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