

# Protect Against Risky Attachments in Microsoft Office 365

Office 365 continues to use a detect-and-respond approach to cybersecurity. Menlo Security's Internet Isolation Gateway can make sure your users are safe from malicious email attachments.

## Benefits:

- Prevent malware from being delivered to users' devices through email attachments
- Render risky email attachments as read only
- Isolate web traffic, protecting users from embedded malicious links in an attachment
- Integrate directly into Office 365 platform and workflows
- Maintain native email and web-browsing experience
- Gain powerful insights into phishing attempts and users posing the most risk to the organization

## Office 365 Is a Tempting Target

Microsoft Office 365 is one of the fastest-growing cloud applications ever, with more than 135 million monthly active users at the end of 2018, according to the company. And this growth makes sense. Any organization already using Word, Excel, PowerPoint, and Exchange should want to take advantage of the power, accessibility, and scale of the cloud.

However the success of, Office 365 is a blessing and a curse. Those 135 million users are also 135 million potential targets for phishing attacks. Malicious actors can easily spin up an authentic-looking email branded with a fake Microsoft logo and send it to targets, knowing that there's a good chance they are Office 365 users. These phishing emails often include malicious attachments that include code that infects the user's device when downloaded. Once a device is infected, an attacker knows that it's fairly easy to infiltrate the corporate network and other critical business systems. According to Microsoft, 100 million malicious emails targeted Office 365 users in 2017.

## Security Issues with Office 365 Email

The problem is that Office 365 uses traditional email security solutions that haven't evolved to meet today's cybersecurity demands. The two plug-ins that enterprises can add to their Office 365 subscriptions—Exchange Online Protection (EOP) and Advanced Threat Protection (ATP)—continue to rely on a detect-and-respond approach, using sandboxing to detect and quarantine malicious attachments before they have a chance to infect an endpoint.

## Menlo Security Internet Isolation Gateway

Enterprises can harden their Office 365 email security posture by adding isolation capabilities on top of existing cybersecurity solutions and techniques. Menlo



---

**100 million malicious emails** targeted Office 365 users in 2017.

Security's Internet Isolation Gateway can be deployed within an existing Office 365 or Exchange Online email workflow. If a user tries to download a risky attachment, the document is opened within the Menlo Security Isolation Cloud and a safe, read-only version is delivered to the user's local client. Menlo also isolates all web traffic, so users are even safe from malicious links embedded in attachments.

## Policy-Based Control

In some instances, you may not want to isolate every attachment for certain users. Policies can be set up by group or individual that allow specified users to download original documents, but only after the files have been fully inspected by advanced anti-malware and quarantined in a sandbox for further inspection.

## Better Reporting and Insight

Menlo also offers better reporting and insight into malicious activity encountered by users. A company's security team can see repeat offenders who pose the most risk to the enterprise and can customize time-of-click messages that are helpful for continuing anti-phishing education. Information can be forwarded to advanced threat detection solutions for further analysis and threat intelligence.

## How Secure Is Secure?

Many organizations feel that Microsoft's add-on detection-based security offerings for Office 365 are "good enough." But is "good enough" really enough when your use of the Office 365 platform makes you susceptible to more sophisticated phishing attempts? Adding Internet isolation capabilities on top of existing cybersecurity solutions and techniques provides comprehensive protection from weaponized documents.

To find out how Menlo Security solutions can protect your organization, contact us at [ask@menlosecurity.com](mailto:ask@menlosecurity.com).

---

## About Menlo Security

Menlo Security protects organizations from cyberattacks by seeking to eliminate the threat of malware from the web, documents, and email. Our 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.

© 2019 Menlo Security, All Rights Reserved.

### Contact us

[menlosecurity.com](https://menlosecurity.com)

(650) 614-1705

[ask@menlosecurity.com](mailto:ask@menlosecurity.com)

