Strengthen the Security of Office 365

McAfee® Email Protection solutions provide advanced defenses against phishing attacks.

Organizations of all sizes are adopting cloud-based Microsoft Office 365 as a way to give users greater flexibility and access to core business applications anytime, anywhere, and on virtually any device. While Office 365 includes built-in security capabilities, additional protection is needed when it comes to spear-phishing exploits that use social engineering methods and other tactics to find and exfiltrate vital corporate data. McAfee® Email Protection solutions provide enterprise-grade security for Microsoft Office 365, defending against phishing attacks faster, offering greater reliability, and improving email continuity. Enterprise-grade email protection is available for most popular email form factors, along with the flexibility and scalability to support changing customer environments in any sector.

Why You Need Additional Security for Office 365

Office 365 is an indispensable business tool—and a key attack vector for email phishing. With 95% of all attacks originating from spear-phishing attempts, more robust email security is a top priority. It's easy to see why spear phishing has become a popular mode of attack. According to the 2014 Verizon Data Breach Investigations Report, one in five people will click on a URL in a phishing message—and human resources and finance, departments where most sensitive data resides, are the biggest offenders. In a recent phishing quiz conducted by McAfee, a part of Intel Security, 80% of 60,000 users across 49 countries failed to identify at least one phishing email.1

“When we moved our customers over to Office 365, we found the email filtering was simply not up to par. Adding McAfee brought us better filtering, plus reporting and message tracking not available from Microsoft.”

—Michael Patrick, Solutions Architect, The Mirazon Group (McAfee Partner)
Tactics that go beyond social engineering

Aside from exploiting human vulnerability, cybercriminals have also developed new techniques that make it more difficult to detect malicious links and malware:

- **One-time URLs**: These can be difficult to detect, as they barely register a blip on the radar. Forensics prove to be nearly impossible because once the infection has occurred, the URL no longer exists, so it's difficult to do any type of investigation.

- **Delayed infection**: At times, the malicious payload is dropped into the target website after an email is scanned and delivered to corporate inboxes—trusting recipients often end up believing the email is legitimate and will click on the bad links.

- **Multistage attacks**: These consist of a series of emails. The first email is designed to learn about targeted endpoints or gather details about the network of an organization in order to craft a more lucrative, pinpointed spear-phishing email.

Built-in security is not enough

Relying solely on security features in Office 365 can be risky. Time and again, spam and phishing attempts continue to surface—and clean-up is both costly and time consuming. Also, organizations find that email outages associated with Office 365 are disruptive to productivity and the conduct of business.

Lack of flexibility

Migration of mailboxes to the cloud is a big undertaking that requires a great deal of planning and testing in multiple environments. Your existing email security solution may not be flexible to accommodate this change, which means you'll probably need more licenses or multiple solutions for this complex process to be secure.

McAfee Email Protection for Office 365

When layered over Office 365, McAfee Email Protection can provide the advanced threat protection businesses need to prevent attacks and stop advanced malware.

Advanced phishing protection

With McAfee Email Protection, you get phishing protection from the number-one-rated² zero-day McAfee Gateway Anti-Malware Engine—a technology that's part of McAfee Web Protection—built into email security as a core feature. We help you defend against advanced phishing tactics with ClickProtect, powered by this engine and available at no extra cost. ClickProtect, a feature of McAfee Email Protection, works in real time—at the time when a URL is clicked—and asks the all-important question: “Is this URL safe?” URLs are inspected by the McAfee Gateway Anti-Malware Engine, which uses emulation to detect malicious web content, without the need for a signature. It also provides users with customizable warning pages and secure previews of the destination web page to reinforce their phishing detection skills. And no matter what device users access or to whom they forward the email, ClickProtect security follows the message.

McAfee Email Protection also prevents sensitive data from escaping via email because it leverages McAfee Data Loss Prevention (DLP) and McAfee SaaS Email Encryption technologies—there's no need to integrate separate solutions. Built-in compliance templates are more extensive and more accurate than Office 365 when it comes to identifying confidential data. These DLP capabilities are fully compatible with Office 365 and Google Apps for Work.

Email attachments may also be scanned for stealthy, advanced malware. Through signatureless detection technology, including file emulation, static code analysis, and sandboxing, these threats can be uncovered and blocked with McAfee Advanced Threat Defense for Email Protection.

"McAfee Email Protection integrates seamlessly with Microsoft Office 365, and allows me to provide a reliable, enterprise-grade solution for my small business."

—Justin Lasley, CIO
Brown Metals Company

McAfee Email Protection

McAfee Email Protection

Provides advanced attack protection, hosted mailbox security, and the flexibility to deploy in your form factor of choice.
Faster, more reliable protection
McAfee Email Protection solutions offer faster and more reliable security through McAfee Global Threat Intelligence, which provides real-time cloud threat intelligence from multiple sources. Emails that originate from suspicious sources or contain links to suspicious websites are automatically blocked, keeping users and networks more secure, while reducing risk, data loss, and remediation costs. With our ability to apply threat protection faster, time to protection is significantly shortened. With failover email continuity, users will have access to email, even in the event of planned or unplanned Office 365 outages.

Ultimate flexibility
As you move your mailbox infrastructure to Exchange Online or a Hybrid Exchange, McAfee Email Protection follows, providing advanced, enterprise-grade security during testing, migration, and post-migration. Regardless of when and where mailboxes are deployed, email security can migrate with them. Flexible, hybrid deployment options with a single management and reporting console enable you to take advantage of the cloud without sacrificing privacy.

Learn More
For more information or to start an evaluation of McAfee Email Protection Solutions, contact your McAfee representative or channel partner, or visit www.mcafee.com/emailsecurity and www.mcafee.com/o365.

“39% of business users are concerned they will not be able to access cloud applications.”

1. Phishing Deceives the Masses: Lessons Learned from a Global Assessment
2. AV-TEST: McAfee Web Gateway Security Appliance Test