McAfee Email Protection

Advanced protection for mailboxes anywhere, anytime

Enterprises need advanced email protection now more than ever. According to the SANS Institute, 95% of network attacks are the direct result of successful spear phishing.[1] Users continue to fall for social engineering techniques, and cybercriminals have expanded their repertoire to include other clever tactics that can catch even security-conscious organizations off guard. Advanced malware and loss of corporate intellectual property are growing problems that can have a dramatic negative impact on any organization. Enterprises are also beginning to migrate email to hosted mailboxes, which can increase the level of risk. Finally, lack of flexibility in legacy email protection solutions may force companies to seek a better alternative. McAfee® Email Protection is the answer. This powerful solution provides enterprise-grade protection against targeted phishing threats, complete with integrated data loss prevention (DLP) technology and email continuity. With flexible deployment options—as a cloud-based, on-premises, or integrated hybrid solution—you can implement email security the way you want, when you want.

Key Advantages

Protection against targeted phishing attacks

- Detect malicious URL threats in real time with ClickProtect.
- Integrates with McAfee Advanced Threat Defense to defend against stealthy malware.
- Built-in data loss prevention technology.

Security for hosted mailboxes

- Targeted attack protection no matter where the email goes.
- Graymail end-user controls.
- Email continuity.
- Granular data loss protection and encryption capabilities.

Flexible deployment options

- Deploy any way you want, when you want.
- Hybrid deployment option with a single management and reporting console.

Beyond Social Engineering: New Spear-Phishing Tactics

When it comes to phishing attacks, the user is the weakest link. *The Verizon Data Breach Investigation Report, 2014*[2] notes that nearly one in five users will click on a link within a phishing email. Cybercriminals continue to take advantage of user vulnerability with social engineering techniques, but they have taken it a step further with other sophisticated tactics that make email threats difficult to trace. Here are a few examples:

- **One-time URLs:** Cybercriminals are taking down malicious URLs after users fall victim to phishing scams and infection occurs. This makes detection and forensics difficult, if not impossible.
- **Delayed infection:** In some cases, attackers wait until *after* an email is scanned, approved, and delivered to corporate inboxes before dropping the payload onto the target website. Employees tend to trust emails they receive at work and may end up clicking on a bad link.
- **Sandbox-aware malware:** This type of malicious code evades detection by remaining latent, only to wreak havoc later on.

Advanced Layered Defenses

Click-time protection

McAfee Email Protection offers multiple layers of protection to help you fend off sophisticated spear-phishing attacks and the stealthy malware associated with them. Leveraging the number-one rated McAfee Gateway Anti-Malware Engine[3] from McAfee Web Gateway, McAfee Email Protection includes scan-time and click-time URL protection known as ClickProtect,

intel Security

which works from any device anywhere to thwart spear-phishing attempts. ClickProtect detects and eliminates threats from embedded URLs within an email message. It checks for changes in URL intent that occurs between the time the message is scanned—regardless of how harmless it may appear—and at the time a user clicks on it.

Let's look at a delayed malware scenario where an attacker crafts an email with a seemingly non-malicious URL that targets the financial controller within your organization. Your email security solution receives the email, interrogates it, finds that it's safe, and delivers it to the targeted inbox. But now that the email is in the financial controller's inbox, the attacker drops malware on the destination web page. If the controller clicks on the link, your network gets infected.

With ClickProtect, at the time a URL in an email is clicked, it asks the question: "Is the URL still safe?" All delivered URLs are rewritten and inspected by the McAfee Gateway Anti-Malware Engine, using behavioral emulation to detect malicious web content without the need to rely on a signature.

A safe preview allows users to view malicious websites safely and learn best practices, adding another layer of security and reducing overall risk. Messages can be safely forwarded, and, even if recipients don't have ClickProtect, the protection follows the email everywhere it goes.

Stealthy malware detection and blocking

Thanks to integration with McAfee Advanced Threat Defense, McAfee Email Protection can detect and block stealthy, zero-day malware in suspicious file attachments before they ever reach your inbox. This innovative, layered approach combines in-depth static code (reverse engineering) and dynamic analysis (sandboxing) to analyze the actual behavior of malware. Full static code analysis provides detailed malware classification information, broadens protection against highly camouflaged, evasive threats, and allows identification of associated malware leveraging code re-use. Delayed or contingent execution paths, often not executed in a dynamic sandbox environment, can be detected through unpacking and full static code analysis.

Built-in data loss prevention

Targeted spear-phishing attacks ultimately have one goal in mind: appropriating valuable and sensitive data. Integrated into McAfee Email Protection is industry-leading technology from our DLP solutions. Included are built-in content dictionaries for PCI DSS, healthcare, financial information, regional privacy regulations, and more to help you develop compliance policies for identification, storage, and transmission of sensitive data.

By creating and storing digital fingerprints of selected documents, McAfee Email Protection learns about the kind of content that needs to be controlled and protected by policies. The regular expression tool, customizable dictionaries, threshold counters, deep content scanning in more than 300 document types, and whitelists enable you to create and enforce attachment and content policies for different user groups within your organization.

McAfee Email Protection includes on-box push, pull, or TLS, S/MIME, PGP email encryption for deployment as a virtual appliance, hardware appliance, or blade server at no additional cost.

Email continuity for business continuity

Business doesn't stop when your email network experiences an outage. Whether the network is inaccessible due to natural disasters, power outages, or even regular maintenance, McAfee Email Protection provides options for keeping employees, customers, partners, and suppliers connected 24/7. The email continuity feature retains all messages sent or received during outages, intelligently synchronizing an accurate record of all message activity during that period until your email servers come back online.

Intelligence and threat reputation

McAfee Email Protection has another powerful tool in its arsenal—McAfee Global Threat Intelligence (McAfee GTI), the industry's most comprehensive threat intelligence service, which collects and redistributes real-time data from more than 100 million sensors across file, web, email, and network vectors. McAfee GTI's reputation analysis minimizes risk by blocking emails that come from suspicious sources, contain links that lead to suspicious websites, or have known malicious file attachments.

McAfee Email Gateway

Virtual appliance environments and system requirements

- VMware vSphere 4.x or higher
- VMware vSphere Hypervisor (ESXi) 4.x or higher
- Processor: Two virtual processors
- Available virtual memory: 2 GB
- Free hard disk space: 80 GB

Hardware appliance

- Available in two models and sold separately
- Also available on blade server form factor

For the third consecutive year, McAfee Email Protection was awarded a **five-star rating by SC Magazine.**

By significantly decreasing the probability that malware, phishing attacks, and advanced persistent threat attacks will infiltrate your network, your organization stays more secure, and the need for costly remediation is reduced.

Security challenges of hosted email

An increasing number of enterprise email addresses are being provisioned by hosted email services, such as Microsoft Office 365, Google Apps for Work, and others. Many hosted email solutions may offer security as part of their services. But is it enough? Probably not, as phishing attempts, spam, and graymail continue to crop up and the built-in security features are not equipped to prevent data exfiltration. Additionally, email outages associated with Office 365, as an example, can disrupt productivity. McAfee Email Protection provides enterprise-grade protection to defend against targeted phishing attacks and advanced malware during testing, migration, and post-migration. No matter when or where your mailboxes are deployed, McAfee Email Protection provides full coverage and email continuity.

Flexible Deployment Choices for Now and the Future

McAfee Email Protection gives you the flexibility to deploy email security your way. Choose from a cloud-based Software-as-a-Service (SaaS) solution, an on-premises solution (virtual appliance, hardware appliance, or blade server), or a hybrid combination of the two. With McAfee Email Protection, you can deploy your email security in a way that best fits your current needs and enables you to scale up or change direction in the future.

Regardless of your deployment choice, McAfee Email Protection gives you a single, centralized management console for consolidated reporting that allows you to easily measure the efficacy of your email security programs. Policies are applied for both cloud-based and on-premises components of the solution.

For information or to start an evaluation of McAfee Email Protection, contact your McAfee representative or visit **www.mcafee.com/emailsecurity**.

1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST: *McAfee Web Gateway Security Appliance Test*

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com