FireEye

EMAIL SECURITY

A Buyer's Guide

How to evaluate email security for advanced threat protection

Cyber attacks that began with an email

91%[2]

Emails that contained a malicious link or attachment

1 in 131[3]

Corporate losses from CEO fraud

$5.52B[4]

Demands on Email Security

Email is the main way that victims of advanced cyber attacks such as CEO fraud, also known as business email compromise (BEC), are targeted. Since more than 250 billion emails are sent each day,[1] it's not surprising that 91% of cyber attacks originate with an email,[2] and one in every 131 emails contain a malicious link or attachment.[3] While malware-based attacks are common, corporate losses from malware-less attacks such as BEC are an increasing threat.[4]

Today's high-impact email threats are not delivered in annoying spam messages. Instead, they hide in carefully designed spear-phishing campaigns and targeted attacks. End users click on seemingly harmless email messages that can download malicious malware, steal credentials and lead to fraudulent wire transfers. These sophisticated email attacks make it easy for cyber criminals to breach your organization, putting corporate and customer assets at risk.

The most successful attacks are sophisticated, multi-stage strikes that use several points (or vectors) of attack. They may begin with a spear-phishing email and incorporate an infected attachment, a link to a phishing site and an outside control and command (CnC) server. Many solutions cannot identify and correlate suspicious activity across an organization to stop multi-vector and multi-stage attacks.

Traditional signature-based and reputation-based defenses such as firewalls, email gateways, antivirus and anti-spam solutions cannot thwart newer and more sophisticated types of attacks. Signature-based products can only stop known threats. Unfortunately, today's attacks are highly targeted and utilize never-before-seen threats. In fact, 80% of malware is used only once and 68% is unique to a single organization.[5] Cyber criminals are constantly changing the game, using unique malware and fraudulent scams, and continually switching up the URLs of phishing sites so there's no signature to detect.

A new approach to email defense is needed to stop today's sophisticated multi-stage, multi-vector attacks. But how do you know if an email security solution can protect you from the creative, ever-changing ways cyber attackers try to compromise your systems? This guide can help. It gives you a checklist of questions to ask when evaluating or purchasing an email security solution.

> "The most devastating attacks by the most sophisticated attackers almost always begin with the simple act of spear-phishing."
>
> **Jeh Johnson**
> U.S. Secretary of Homeland Security

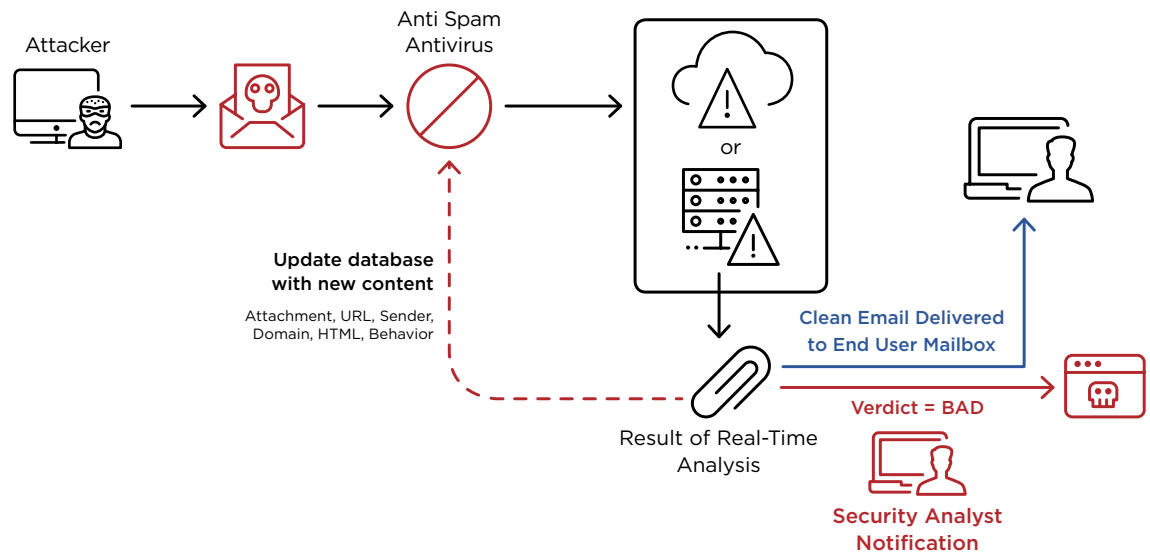
1 Radicati Group Email Statistics Report, 2017-2021
2 Phishme (2017). Phishing Defense Guide 2017.
3 C. Gonsalves (April 26, 2017). Criminals Scale Up Attacks, Ratchet Down Complexity.
4 Federal Bureau of Investigation (May 2018). 2017 Internet Crime Report.
5 J. Goldfarb (September 19, 2016). Detection Innovations.

Capability #1

Filter Spam, Detect and Stop Attacks, Including Spear Phishing and Impersonation

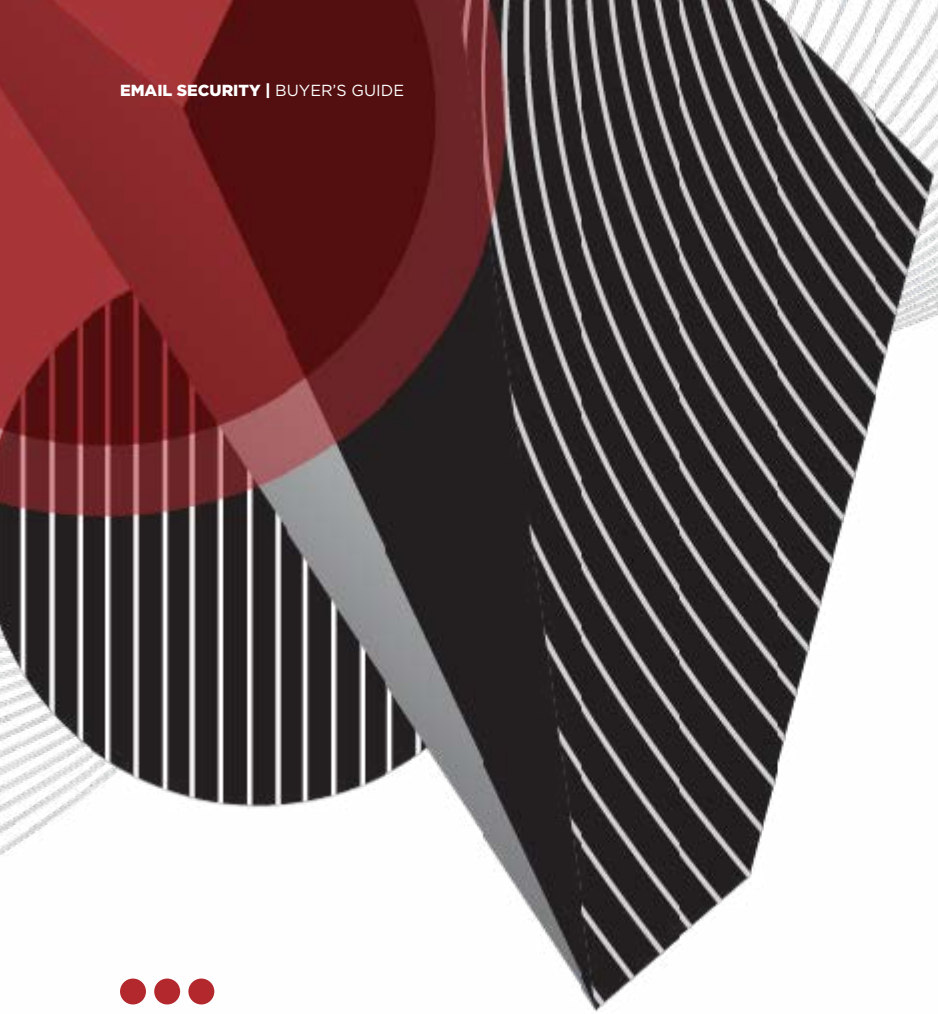
Cyber criminals are continually modifying their tactics to sneak past signature-based email security. They target specific individuals with spear-phishing emails, spoof senders, create unique malware for each attack, and set up phishing websites to steal login and other user information. Each time a new threat appears, signature-based and reputation-based solutions must be updated. But by the time this occurs, cyber criminals have gotten the message past your defenses and into the user's mailbox.

Figure 1. Email security solution with spam filtering and advanced threat protection.



Ask these questions when evaluating email security solutions

- Does it use multiple technologies including machine learning to accurately detect attacks?
- Does it automatically analyze, detect and quarantine advanced attacks inline and the first time they are seen? Does it also update its content database?
- Can it detect socially engineered phishing emails, credential-phishing sites, sender spoofing and malware hidden in email attachments, links and content?
- Does it analyze suspicious email traffic to identify zero-day, impersonation and multi-stage attacks and ransomware?



Capability #2

Quickly Recognize and Respond to High-Priority Threats

In a typical week, organizations receive an average of 17,000 alerts. Yet a mere 19% of those alerts are reliable, and overburdened security teams are able to investigate only 4% of those.[6] Even worse, most email security solutions don't tell you anything about these alerts to determine which are real threats so you can prioritize and respond to them. As a result, true attacks are frequently missed, leaving your organization exposed to risk.

6 Ponemon Institute (January 2015). The Cost of Malware Containment.

Organizations receive **an average of 17,000 alerts.** Overburdened security teams are able to investigate only 4% of those.

Ponemon Institute
"The Cost of Malware Containment"

Ask these questions when evaluating email security solutions

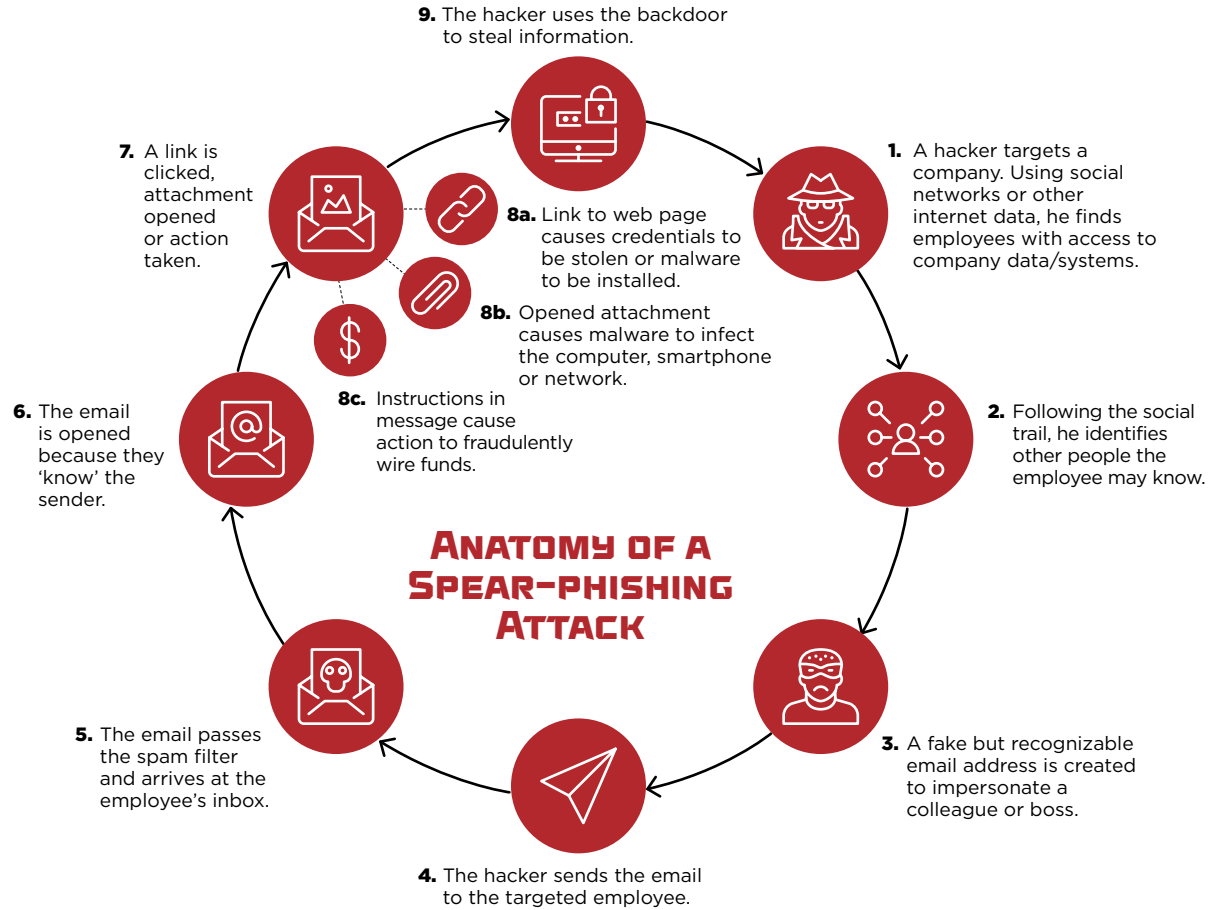
- Does it generate false positives at a rate of less than one per forty million URLs analyzed?
- Does it provide insight into both the attack and the attacker to make it easier to prioritize alerts and respond to threats?
- Does it use intelligence gleaned from experts who investigate the world's most consequential breaches?
- Can it quickly validate threats by executing them in isolation and block them in real time?

Capability #3

Identify and Prepare for Future Attacks

Today's cyber attacks are multi-stage and multi-vector, often incorporating spear-phishing emails, malware, credential-phishing websites and CnC servers. To anticipate, plan for and respond to these attacks, you need in-depth information about attacks and attacker motivations, characteristics and methods. This type of intelligence enables you to "connect the dots" across attack vectors to spot potential attacks.

Signature-based intelligence and reputation-based feeds used by traditional email security products can't provide this information. They need to be updated every time a new threat appears. This takes time, so the intelligence they do provide is often received too late to be effective against evolving threats. Even worse, it tends to increase false positive alerts, making it difficult to spot real attacks while providing a false sense of security.



Ask these questions when evaluating email security solutions

- Is the intelligence derived from hundreds of thousands of hours of incident response engagements, a global network of sensors collecting real-time intelligence, and hundreds of analysts and researchers to provide contextual insights with alerts that identify the most critical threats for response?
- Can it be quickly updated while operating inline based on proprietary, email-specific threat intelligence about newly detected attacks?
- Does it give you visibility into the entire lifecycle of an attack — exploit, malware execution, callbacks (multi-stage) and malware — delivered in fragments (multi-flow)?
- How credible are the sources of intelligence and how are they validated?

> "The average impact of a successful spear-phishing attack: **$1.6 million.**"

Vanson Bourne
"The Impact of Spear Phishing," 2016

Capability #4

Protect Your Broader Environment by Working with Integrable Solutions

When a security infrastructure consists of point solutions that don't integrate, you get a complex, disjointed system that's plagued by false alerts, offers limited visibility and often misses multi-stage attacks because of a lack of correlation across vectors. It's also nearly impossible to create integrated workflows, which can dramatically reduce the time it takes you to go from detection to investigation to response. The result? Your organization is exposed to greater risk.

Ask these questions when evaluating email security solutions

- Is it part of a comprehensive security platform and ecosystem that integrates other critical security components, such as network and endpoint security?
- Does it share threat information with network and endpoint security products?
- Can you create integrated, automated workflows to speed up the detection to remediation process?

Capability #5

Grow and Adapt to Your Business Needs

Most organizations are in a constant state of flux. New business acquisitions. Growth. Moving to the cloud. You need an email security solution that protects your investment by adapting to these changes. When a security product can't evolve to meet these new challenges, it exposes your organization to increased costs and greater risk and opens the door to attacks.

> "96% of social attacks use email."
>
> **Verizon**
> "2018 Data Breach Investigations Report"

Ask these questions when evaluating email security solutions

- Does it offer flexible deployment options to fit your environment such as cloud and on-premises?
- Does it easily integrate with cloud-based email systems such as Microsoft® Office 365™ and Gmail™?
- Can it be deployed in active protection or monitor only mode?
- Is it available with inline anti-spam and antivirus protection?
- Does the cloud-based solution comply with SOC 2 Type II certification for security and confidentiality, European Union data privacy requirements and FedRAMP security requirements?

Invest Wisely in Cyber Security

Today's highly sophisticated, targeted, multi-stage, multi-vector attacks are extremely effective at evading traditional defenses despite a $96 billion annual investment in IT security.[7] The majority of these attacks start with a malicious or a malware-less email. Spear phishing is the weapon of choice because it works. Criminals will continue to use email attacks as long as organizations continue to rely on ineffective, outdated security that cannot detect threats in real time.

$96 billion

Annual investment in IT security

7 Gartner (December 2017).

Critical Elements of Email Security

You need an email security solution that:

- Automatically detects and stops advanced email-borne attacks
- Quickly identifies, prioritizes and enables response to high-priority threats
- Prepares for future attacks
- Integrates with multiple security solutions
- Grows and adapts to your business needs

An email security solution that offers this combination of capabilities — rapid detection, response and visibility into an attack — is the best way for organizations to effectively prevent email-borne attacks.

About FireEye Email Security Solutions

FireEye develops solutions that meet all critical requirements for combating modern and future cyber threats. FireEye Email Security - Cloud Edition is best suited for cloud-based and hybrid deployments and FireEye Email Security - Server Edition is designed for on-premises deployment.

To learn more about FireEye, visit: **www.FireEye.com/email**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

FireEye®