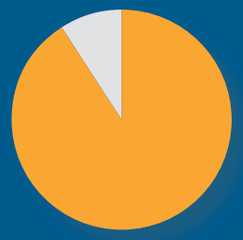
EMAIL SECURITY

A Buyer's Guide

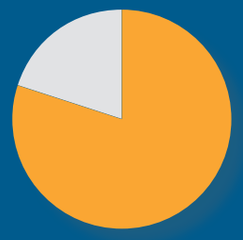
How to evaluate email security for advanced threat protection

FireEye



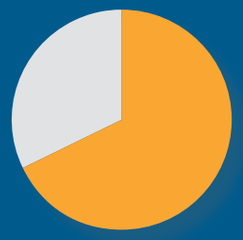
Cyber attacks that began with an email

91%[1]



Increase in ransomware attacks over previous year

400%[1]



Emails that contained a malicious link or attachment

1 in 131[2]

> "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

Demands on Email Security

Email is the main way that victims of advanced cyber attacks such as ransomware are targeted. In 2016, 91% of cyber attacks originated with an email[1], ransomware attacks (like the recent WannaCry attack which struck more than 300,000 systems) were up 400%[1] over the previous year and one in every 131 emails contained a malicious link or attachment.[2]

These increasingly sophisticated, malevolent messages trick users into clicking links, downloading attachments, sharing credentials or taking some action that activates ransomware, installs malware or gives cyber criminals access to business networks.

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 legitimate website compromised by cyber criminals 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, and endpoint antivirus 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.[3] Cyber criminals are constantly changing the game, using unique malware 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.

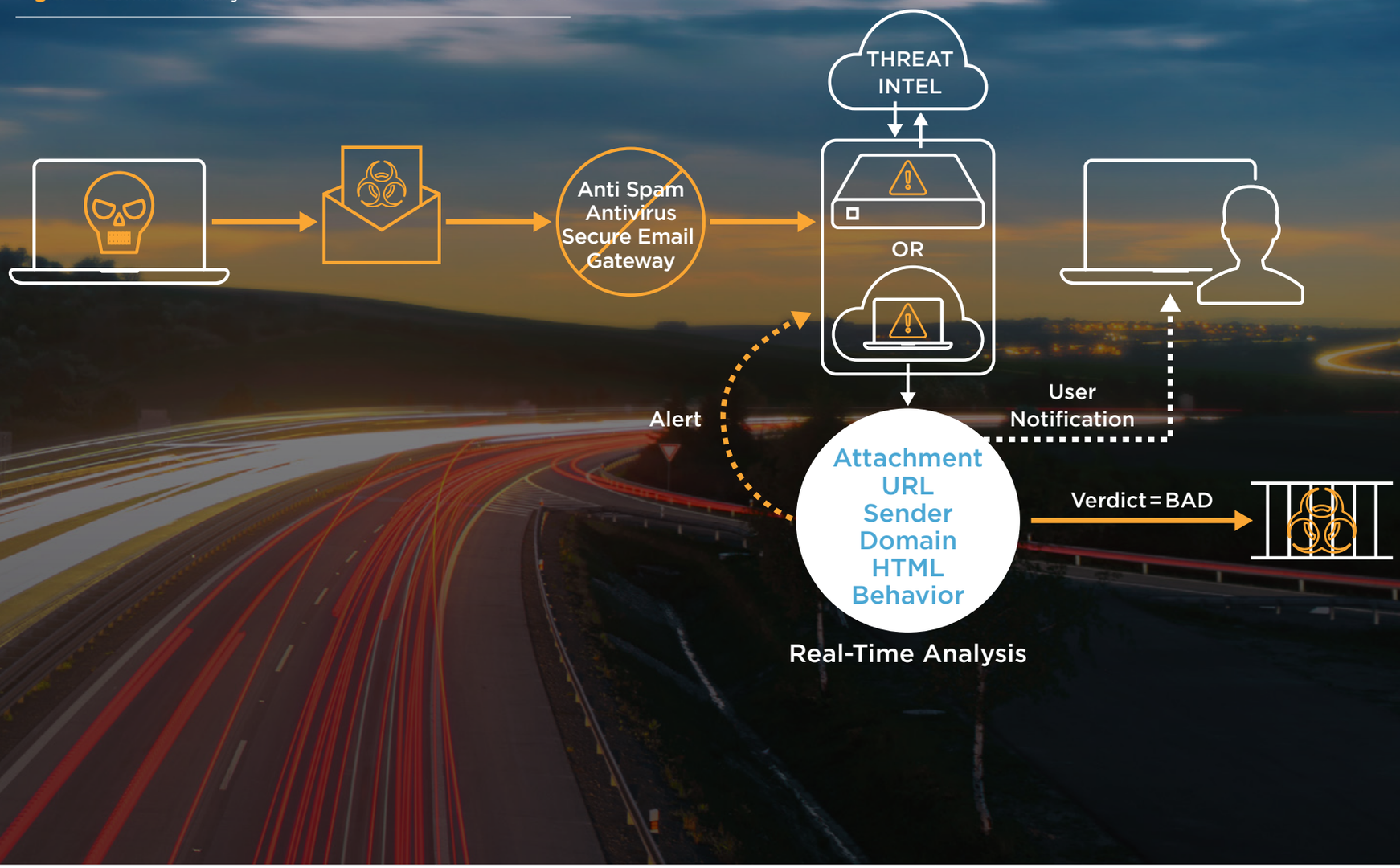
1 Phishme (2017). Phishing Defense Guide 2017.
2 C. Gonsalves (April 26, 2017). Criminals Scale Up Attacks, Ratchet Down Complexity.
3 J. Goldfarb (September 19, 2016). Detection Innovations.

Capability #1

Detect and Stop Attacks, Including Spear Phishing and Ransomware

Cyber criminals are continually modifying their tactics to sneak past signature-based email security. They target specific individuals with spear-phishing emails, 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 with Advanced Threat Protection



? Ask these questions when evaluating email security solutions

- Does it use multiple signature-less technologies to accurately detect attacks?
- Does it automatically analyze, detect and quarantine advanced attacks inline and the first time they are seen
- Can it detect socially engineered phishing emails, credential-phishing sites and malware hidden in email attachments, links and content?
- Does it analyze suspicious email traffic to identify zero-day and multi-stage attacks and ransomware?

Ask these questions when evaluating email security solutions

- Does it generate false positives at a rate of less than one per one million items 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 #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.[4] 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.

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

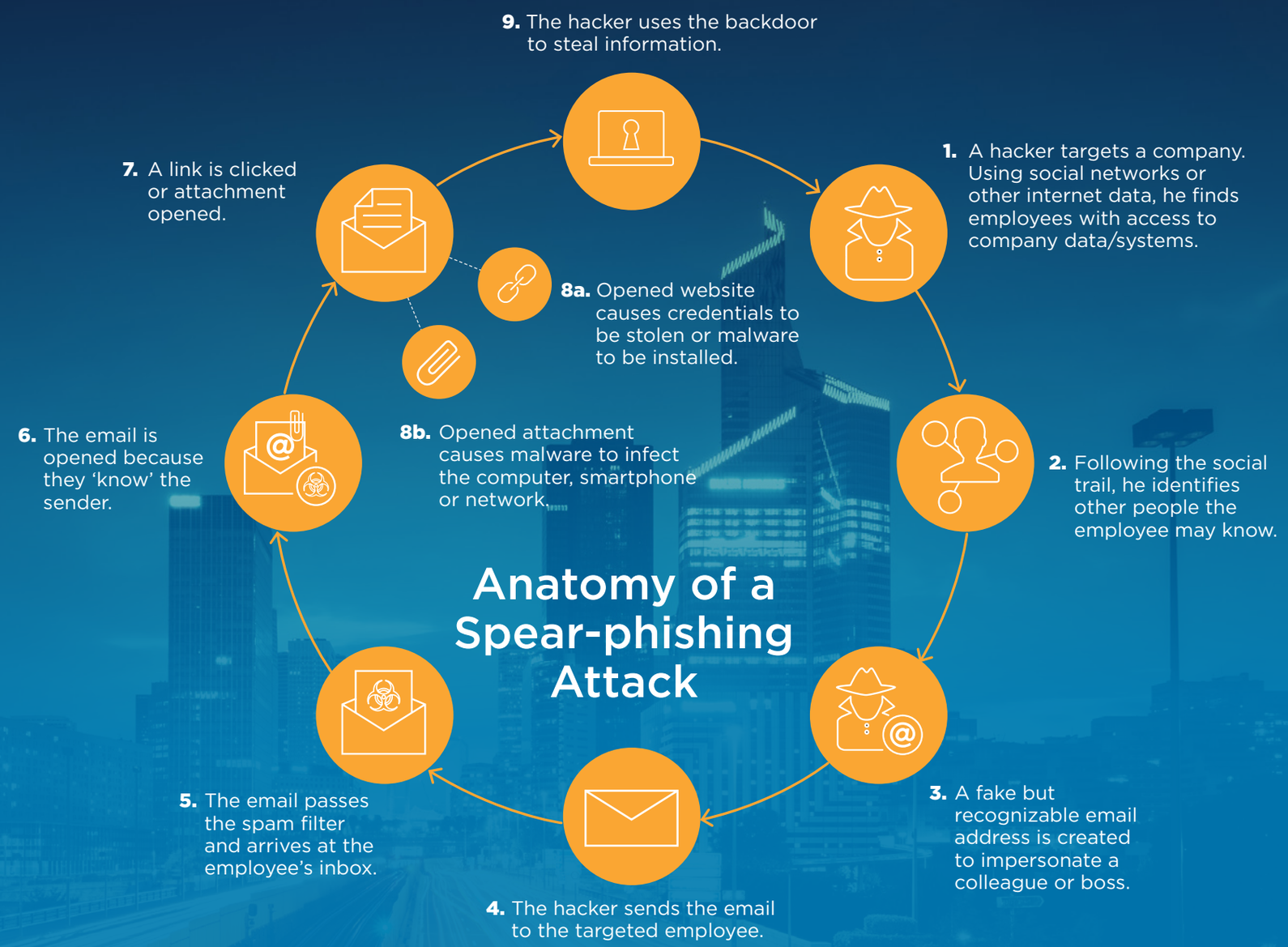
> Organizations receive **an average of 17,000 alerts**. Overburdened security teams are able to investigate only 4% of those.
>
> **Ponemon Institute**
> "The Cost of Malware Containment"

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?
- Is the intelligence feed updated in real time with real evidence 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. **Victims saw their stock prices drop 15%.**
>
> **Vanson Bourne**
> The Impact of Spear Phishing," 2016

Capability #4

Protect Your Entire 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 that integrates email with 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?

> "99% of malware is sent via email or web server. 80% of crimeware is email-based."
>
> **Verizon**
> "2017 Data Breach Investigations Report"

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.

? 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 GDPR data privacy laws 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 $20 billion annual investment in IT security.[5] The majority of these attacks start with a malicious 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 them in real time.

$20 billion

Annual investment in IT security

5 S. Piper (2013). Definitive Guide™ to Next-Generation Threat Protection: Winning the War Against the New Breed of Cyber Attacks.

Critical Elements of Email Security

> "The volume of email stolen through the years is likely **greater than all other forms of electronic data theft combined.**"
>
> **Mandiant**
> "M-Trends 2017:
> A View From The Front Lines"

You need an email security solution that:

				
Automatically detects and stops sophisticated 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, worry-free 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 Threat Prevention (ETP) is best suited for cloud-based and hybrid deployments and FireEye Email Security (EX series) is designed for on-premises deployment.

To learn more, visit
www.fireeye.com/email

FireEye is the leader in intelligence-led security-as-a-service. 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 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
877.FIREEYE (347.3393)
info@fireeye.com

fireeye.com

FireEye®