FireEye®

Email Security Powered by Oracle Cloud

Overview

Email remains the primary method used to initiate an advanced attack or deliver ransomware because it can be highly targeted and customized to increase the odds of exploitation. While legacy anti-spam filters and antivirus software are good at catching traditional, mass phishing threats with known malicious attachments, links and content, they cannot catch sophisticated and targeted spear-phishing and impersonation attacks designed to bypass these traditional solutions.

Most secure email gateways mitigate against traditional spam and viruses, but lack the automated analysis needed to catch spam campaigns and more dangerous threats from the first time they're seen. They rely on commodity anti-spam filters and antivirus software designed to react to new threats sent in large volumes. Typically responses can take several minutes and polymorphic techniques can delay detection further, leaving a global gap exploited by spammers and cyber threat actors. Firewalls don't help; they can't examine email traffic that is typically sent over Transport Layer Security (TLS) connections to deliver ransomware and spear-phishing campaigns.

To prevent today's spam campaigns, the activation of ransomware, and spear-phishing and impersonation attacks an email security solution needs to evolve quickly to adapt to the threat landscape. It must focus on threat protection that:

- Detects threats from the first time they're seen without relying on signatures
- Identifies critical threats with minimal false positives
- Blocks inline to keep threats such as ransomware out of the environment
- Uses cyber threat intelligence gained from the frontlines to respond quickly to protect the organization

Why Your Current Email Security Solution Isn't Secure Enough

A data breach puts the information, people and processes an organization is responsible for at risk. It disrupts business, tarnishes the organization's reputation and compromises customer trust. The average cost of a data breach is $3.62 million[2] and they are often initiated by phishing emails. It's likely that the volume of emails stolen through the years is greater than all other forms of data theft combined.[3]

Email is an easy target for cyber attackers. To determine if your current solution(s) are secure, you must ask:

1. Do your email security solutions detect attacks from the first time they're seen and block the most dangerous cyber threats including malware-laden attachments and URLs, credential-phishing sites and impersonation attacks?

2. Do they enable efficient response to alerts by blocking threats, telling you which matter and providing intelligence on what to do?

3. Do you have access to the latest, contextual intelligence available to rapidly adapt to the evolving threat landscape?

4. Do your email security solutions integrate with your other security tools and work across threat vectors and protect against blended attacks?

5. Are they flexible and scalable to change as your business does?

91% of cyber attacks begin with a spear-phishing email.[1]

---

1   PhishMe (2016). "Enterprise Phishing Susceptibility and Resiliency Report."
2   Ponemon Institute LLC (June 2017). "2017 Cost of Data Breach Study: Global Overview."
3   Mandiant, A FireEye Company (2017). "M-Trends 2017 A View From The Front Lines."

Powered by
ORACLE®
Cloud

1

As email threats have evolved, cloud-based email subscription services have seen widespread adoption.
Organizations are migrating information, operations and assets to the cloud. Given the rate that public cloud services and Internet-connected devices are growing, it's not surprising that cyber threats targeting the cloud, and the need for cloud-based security, will increase.

FireEye Email Security Powered by Oracle Cloud combats advanced email-borne attacks. An antivirus and anti-spam (AVAS) add-on provides protection against spam campaigns and impersonation attacks. It addresses the need for a comprehensive cloud-based email security offering to protect against spam campaigns, and targeted and advanced threats for organizations that wish to fully embrace the cloud.
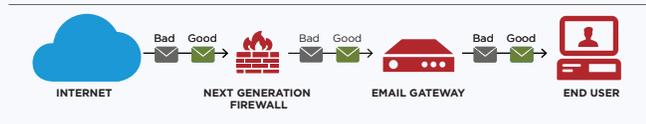
2

Outdated defenses give organizations a false sense of security. Email gateways that rely on commodity intelligence, and third-party signatures and reputations aren't purpose built to detect threats from the first time they're seen. Similarly, a firewall can't stop ransomware and spear-phishing campaigns delivered by email.

Figure 1. Traditional security solutions fail to detect targeted cyber attacks.

Architecturally these technologies can't hold email while they analyze it. This means they allow the delivery of emails to users that contain malware-laden attachments and URLs, and impersonation attacks.

FireEye Email Security helps organizations of all sizes minimize the risk of costly breaches. It accurately detects and blocks spam campaigns, and advanced and targeted attacks hiding in emails that other email security solutions miss. In fact, one leading secure email gateway, deployed ahead of FireEye, missed more than 185,000 malicious email attachments in a single day.[4]

3

Legacy, signature-based intelligence feeds can't evolve quickly enough to stop today's email-borne attacks. Those feeds cannot help anticipate attacks or guide responses. In fact, the numerous security technologies and software incorporated as point solutions has led to a huge uptick in alerts. In-house detection, rather than relying on signature and reputation updates from third-parties, allows the FireEye Email Security to evolve much faster and immediately block spam campaigns when something new is found. Algorithms analyze message sender and domain for spoofing of known names within the recipient domain to stop increasingly prevalent impersonation attacks such as CEO fraud that don't involve malware or malicious URLs.

FireEye Email Security knows what to block based on intelligence gained from firsthand investigations. This insight also provides security teams with alert context to simplify alert prioritization. Malicious emails are quarantined and actionable contextual intelligence accelerates containment of advanced threats with in-depth information about the attack and attacker.

Globally shared real evidence enables immediate blocking of previously unknown attacks and accelerates threat response. Threats are identified with minimal noise and false positives. This ensures security team resources are focused on real attacks, reduces operational expenses and minimizes organizational risk.

4

Many attacks combine network (web) and email tactics in multiple stages to evade web-only and email-only defenses, which focus on just one stage of an advanced attack.
A single cyber attack may be comprised of sophisticated malware that exploits a zero-day vulnerability, a spear-phishing email, a malicious URL and a complex network of command servers for controlling compromised devices and stealing targeted assets.

While ransomware attacks start with an email, a callback to a command-and-control server is required to encrypt the data. These email-led, multi-stage attacks easily evade sandboxes, which analyze files in isolation. By the time most security products discover a problem, the victim's data is already encrypted. FireEye Email Security and Network Security work together to detect and stop blended attacks. Together, they correlate the attack life cycle to trace attacks back to an original spear-phishing email and threat actor.

---

4   FireEye Blogs (July 20, 2016). "Gaps In Email Threat Detection Open The Door to Cybercrime."

FireEye Email Security and Multi-Vector Virtual Execution Technology
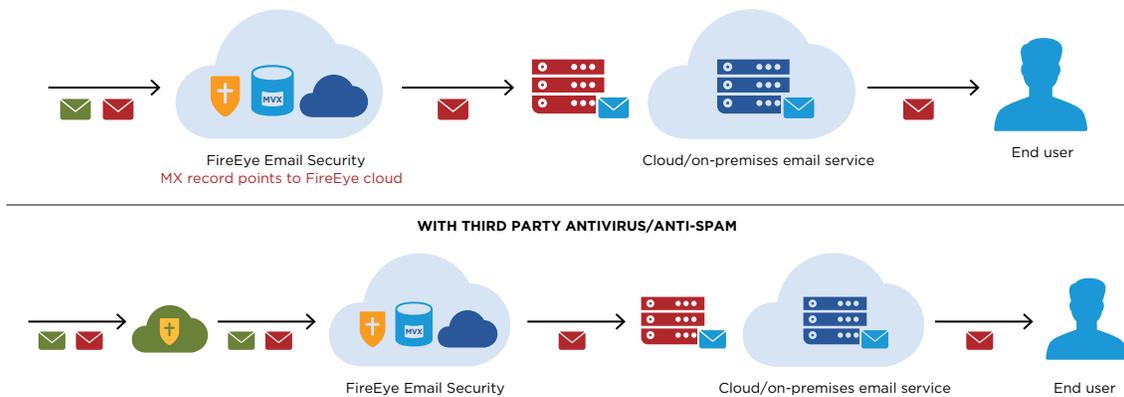
At At the core of FireEye Email Security is Multi-Vector Virtual Execution™ (MVX) technology. MVX is a purpose-built, dynamic analysis engine that inspects suspicious objects for hard-to-detect exploits and attacks hidden in attachments and URLs. Malicious emails are quarantined in real time for further analysis or deletion. With the use of attack and attacker intelligence gained from firsthand investigations, threats are identified with minimal noise and false positives are nearly nonexistent. This frees security teams to focus on investigating and responding to real attacks and using scarce resources efficiently.

Flexible Deployment Options

FireEye Email Security can be deployed inline for greater control and real-time response to stop attacks in progress. Especially with attacks such as ransomware, where prevention is the only effective defense, inline deployment keeps malicious and malware-less content from even being delivered to the end user.
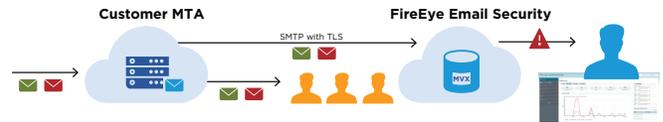
FireEye Email Security – Cloud Edition, with nothing to install, is ideal for organizations migrating their email infrastructure to the cloud. It integrates seamlessly with cloud-based email systems such as Microsoft Office 365. An AVAS add-on is available with inline anti-spam and antivirus protection for stopping new spam campaigns and impersonation attacks from the first time they're seen (Fig. 2).

Some organizations prefer to start with a more conservative approach, and FireEye Email Security can be deployed in out-of-band or monitor-only modes (Fig. 3). In this deployment, all traffic is monitored for malicious activity and a report is generated, but there is no automated prevention mechanism.

Figure 3. FireEye Email Security – Cloud Edition – BCC mode.

FireEye Email Security – Server Edition is a family of on-premises appliances. FireEye or its authorized partners can help you determine and deploy the option that best fits your needs.

The Value of Oracle Cloud

Oracle Cloud combines the elasticity and utility of public cloud with the granular control, security and predictability of on-premises infrastructure to deliver high-performance, high availability and cost-effective infrastructure services.

Figure 2. FireEye Email Security – Cloud Edition – inline deployment.

Key Features

Performance

FireEye Email Security - Cloud Edition leverages the performance of Oracle Cloud Infrastructure to deliver the highest performance possible for analysis, detection and resolution of email vunerabilities.

Elastic and on-demand compute

FireEye leverages Oracles Cloud Infrastructure to rapidly scale up as many servers needed to cope with the largest attacks, ensuring that you are protected at all times no matter what the attack is.

Next Steps

Today's sophisticated cyber attackers and dynamic threat landscape necessitate that organizations understand their threat profile. This involves knowing what assets are at risk, focusing on fast threat detection and response, and resolving incidents quickly. To stay focused on their missions and to minimize risk, organizations need email security focused on detecting and blocking email-borne threats from the first time they're seen. This includes security technologies and cyber threat intelligence gained from firsthand investigations of the cyber attacks that matter.

To learn more about FireEye's partnership with Oracle please visit: **www.fireeye.com/oracle**

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

Powered by
ORACLE
Cloud