EMAIL SECURITY FOR GOVERNMENT ORGANIZATIONS

OVERVIEW

Government networks and critical infrastructure around the world are under a constant state of attack. The threats evolve daily as nation states, cyber criminals and hacktivists stress government cyber defenses to their breaking points.

Traditional security solutions such as firewalls and email gateways fail to detect targeted cyber attacks. To prevent the activation of ransomware and spear-phishing attacks an email security solution needs to proactively adapt to the threat landscape. It must focus on advanced threat protection that:

- Detects threats in real-time 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 protect the organization and help speed up response

Why Your Current Email Security Solution Isn't Secure Enough

A data breach puts the information, people and processes a government organization is responsible for at risk. It disrupts business, tarnishes the government entity's reputation and compromises the public's trust. The average cost of a data breach is $4 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 cloud-based email security solutions comply with FedRAMP requirements?
2. Are they designed for advanced threat detection and protection?
3. Are your intelligence feeds signature based?
4. Do your email security solutions integrate across threat vectors to protect against blended attacks?

Ninety-one percent of cyber attacks begin with a spear-phishing email.[1]

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

FireEye

1 As email threats have evolved, cloud-based email subscription services have seen widespread adoption. Government organizations are migrating information, operations and assets to the cloud. Supporting cloud products and services must meet Federal Risk and Authorization Management Program (FedRAMP℠) requirements and be deemed FedRAMP compliant.

The FireEye Government Email Threat Prevention (ETP) service meets the FedRAMP security requirements and has been granted an Authority to Operate (ATO) by the U.S. Department of the Interior (DOI). It is the first email security service focused on advanced threat protection to be FedRAMP authorized.

FedRAMP

2 Outdated defenses give organizations a false sense of security. Email gateways that rely on commodity intelligence, anti-spam filters and antivirus software aren't purpose built for advanced threat protection. 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 that contain malicious URLs and malware-laden attachments to users.

FireEye Email Security helps government organizations of all sizes minimize the risk of costly breaches. It accurately detects, quarantines and immediately stops advanced and targeted attacks hiding in emails that other email security products 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 provide insight on attacker motivations, characteristics and methods. 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.

An email security solution for advanced threat protection can reduce the risk of compromise for government organizations if it: 1) knows what to block, 2) is deployed inline and 3) blocks threats in real-time. FireEye Email Security knows what to block based on intelligence gained from firsthand investigations, and simplifies alert prioritization to contain critical threats faster.

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 website appearing on dynamic URLs 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, Network Security and Endpoint Security integrate seamlessly 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 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 content from even being delivered to the end user.

Email Security (EX Series) is a family of on-premises appliances. FireEye Government Email Threat Prevention (ETP) is cloud based, with nothing to install. It is ideal for organizations migrating their email infrastructure to the cloud. It integrates seamlessly with cloud-based email systems such as Microsoft Office 365 with Exchange Online Protection. It's also available with inline anti-spam and antivirus protection (Fig. 2).

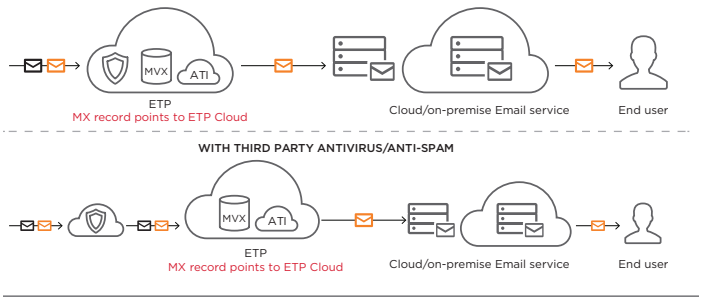

Figure 2. Government Email Threat Prevention (ETP) – inline deployment.

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.

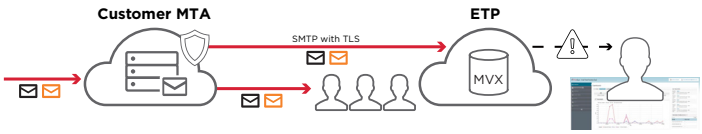

Figure 3. Government ETP – BCC mode.

FireEye or its authorized partners can help you determine and deploy the option that best fits your needs.

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, government entities need email security focused on advanced threat protection. This includes security technologies and cyber threat intelligence gained from firsthand investigations of the cyber attacks that matter.

To learn more about how FireEye Email Security detects and stops advanced and targeted attacks, please visit **www.FireEye.com/email** or contact your local sales representative.

About Fireeye, Inc.

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

www.FireEye.com