FireEye
SECURITY REIMAGINED

FireEye Network and Email Security

Better detection. Smarter alerts. Faster response.

OVERVIEW

As a customer of the FireEye Network Threat Prevention Platform (NX Series), you know that today's fast-evolving attacks are outpacing legacy security tools.

That's why your Network Threat Prevention Platform doesn't rely only on known signatures of previous threats. The FireEye Multi-vector Virtual Execution™ (MVX) engine confirms and block emerging and never-before-seen web attacks in real time. And it uses dynamic threat intelligence to help security teams tell serious threats apart from trivial alerts and false positives.

So far, so good. But what about blended (also known as multi-vector) attacks that come at your network through e-mail as well as the web? An estimated 90% of all attacks play out over both of these vectors.[1]

Simply adding a point solution from any security vendor to combat email threats is not the answer.

Most point solutions can't correlate threat intelligence from the individual solutions, so they miss multi-vector attacks. And when a threat is detected, these point tools don't act in coordinated way to stop them.

Without this correlation and coordination, security teams can easily get lost in the "noise" of too many alerts. They have trouble prioritizing which ones to investigate. And they can't respond quickly enough to the ones that matter. Managing information among multiple interfaces and data silos further hinders security professionals already stretched to the max.

SOLUTIONS THAT WORK TOGETHER TO BATTLE THE MOST SOPHISTICATED ATTACKS

FireEye Email Security is a powerful addition to the FireEye Network Threat Prevention Platform for fighting advanced attacks that use a blend of web and email tactics to infiltrate your environment.

Offered on premise through the EX Series appliance and in the cloud through the Email Threat Prevention (ETP) service, FireEye Email Security platforms protect against spear-phishing and other blended attacks that evade traditional defenses. Malicious email is often the opening salvo of multi-vector attacks. By using the Network Threat Prevention Platform with FireEye Email Security, security teams can correlate malicious URLs with the originating emails and the intended targets. This linkage enables security teams to see how the two events are related and automatically block subsequent stages of the attack, such as attackers trying to transfer stolen data over the web.

Together, FireEye Network and Email Security help security teams:

- **Detect attacks across critical attack vectors**—The web and email are two of the most common paths attackers use to get into your environment. The combination of Network Threat Prevention and Email Threat Prevention ensures that organizations are protected against both these critical links.
- **Detect blended attacks that point solutions miss**— Some threats aren't obvious when looking at isolated network or email activity. Even if point tools cover both vectors individually, they can miss threats because they can't correlate the related activities.

Saudi Aramco: FireEye NX and EX Together: Continuous Protection

The oil and gas industry is a prime target for all types of attackers. And as one of the biggest energy producers in the world, Saudi Arabia's Ministry of Petroleum and Mineral Resources faces a constant barrage of compromise attempts.

Knowing it could no longer rely on firewall and anti-virus technologies to stop sophisticated attackers, it began seeking a more advanced solution in 2011.

The ministry initially bought a FireEye Network Threat Prevention Platform (NX Series) appliance. Officials were impressed with the results—and acutely aware of email-borne threats. So it quickly added a FireEye Email Threat Prevention Platform (EX Series) to its deployment.

Despite being targeted routinely by sophisticated hackers, the ministry has kept its IT assets safe by using the Network and Email security platforms together. Using both FireEye products, the ministry has a unified, integrated platform to detect, prevent, analyze, and respond to today's threats.

"When it comes to detecting and preventing advanced attacks, the power of [the FireEye] Multi-Vector Virtual Execution™ (MVX) engine technology has no competition," said Wahid Hammami, the ministry's chief information officer. "It is the only defense available in the market to protect against zero-day attacks."

- **Respond faster to threats**— Working together, Network Threat Prevention and Email Threat Prevention correlate activity across web and email traffic for richer alerts. Complemented by contextual intelligence, these alerts provide a broader view of your security situation. Armed with this information, security teams can quickly prioritize alerts and mount an effective response.
- **Stretch limited security budgets**— With integrated anti-spam, and IPS capabilities, the Network and Email combination can consolidate deployments and block many attacks automatically—whether they're well-known threats or have never been seen before. FireEye MVX technology generates only high-quality alerts, reducing busywork. And a common architecture and interface helps further reduce overhead.

NEXT STEPS

If you've already deployed FireEye Network Threat Prevention, adding Email Threat Prevention is the next logical step to improve your security posture. FireEye Email Threat Prevention works with organizations of all sizes and infrastructures. And with flexible deployment options, it can nimbly evolve as your business infrastructure and needs change.

Visit the Enterprise Network Security solution and Email Security web pages for more information.

[1] Verizon 2014 Data Breach Investigations Report.