ENTERPRISE-GRADE SECURITY THAT SMALL AND MIDSIZE BUSINESSES CAN AFFORD

OVERVIEW

Most organizations depend on email and web protocols for business purposes. Accordingly, most cyber attacks begin with these protocols. Effective protection detects and prevents known commodity attacks as well as advanced, unknown attacks. Award-winning FireEye technologies accurately detect and stop advanced multi-stage and multi-vector attacks. They arm security teams with effective tools that enable operational efficiency by issuing significantly fewer false-positive alerts. These valuable solutions are designed to be easy to access and use and allow organizations to focus on growing their business.

FireEye pioneered this technology to detect advanced unknown attacks but it was initially deployed only by large enterprises. However, cyber attackers target organizations of all sizes. Small and midsize enterprises (SMEs) recognize they are not immune and that advanced threat protection is fundamental to their security framework.

SECURITY CHALLENGES

Small and midsize enterprises are faced with many security challenges, partly due to the dynamic nature of the cyber threat landscape and partly because of how SMEs attempt to operationalize security management within their organization.

Challenges related to the threat landscape generally stem from a lack of security visibility across the organization. Legacy perimeter detection and prevention technologies that rely on attack signatures struggle to identify today's threats. Attackers leverage techniques to change the tell-tale signature of malware so it appears just once in any given organization. In many cases, malware isn't even involved in the attacks.

Challenges related to security operations center on the fact that SMEs are often presented with too many security alerts that require action from human resources they lack. Many alerts are false positives and analyst time is wasted investigating non-security issues. Too many false positives can also hide true positives that require immediate interaction to mitigate further impact.

There are additional complications. To investigate alerts, SMEs must hire staff with appropriate security expertise. In most organizations, the security resource is part of the IT department, which creates conflicts of interest. SMEs that apply a layered defense-in-depth approach may be faced with multiple security technology tools that are frequently mismanaged, managed by security service providers or not managed at all. At best, this may result in excessive cost and at worst, it can present significant risk exposure. These challenges are all connected: SMEs must control costs while using very limited staff to manage many security tools that generate too many alerts.

FireEye

THE SOLUTION

The FireEye solution combines Network Security Essentials (NXE) and Email Threat Prevention Cloud (ETP) to protect organizations against web- and email-based threats.[1] Those two vectors account for 90% of cyber-attacks. The solution helps optimize your security budget by identifying critical security issues without the distraction of false positives that unnecessarily burden the scale and timeliness of incident response.

The powerful FireEye Multi-Vector Virtual Execution™ (MVX) engine is at the heart of these FireEye technologies. It helps identify advanced, multi-stage attacks and blended threats that span multiple attack vectors, including the web and email, that otherwise may not appear malicious when viewed in isolation.

The correlation of malicious URLs with spear-phishing emails is critical to identifying the opening salvo of many multi-vector attacks. The Cloud MVX engine provides visibility into these linkages, enabling organizations to see how the two events are related and then automatically block subsequent stages of attacks, such as attackers trying to transfer stolen data over the web. It also identifies and blocks subsequent attacks that leverage similar tactics, tools and procedures (TTPs).

With a high degree of automation, efficiency and efficacy, this solution enables organizations to improve their security posture and simplify deployment and day-to-day management of both network and email security.

Network Security Essentials

Network Security Essentials is an affordable, plug-and-play network security solution that can be deployed in under 60 minutes to minimize the risk of costly breaches.

In addition to the patented, signature-less Cloud MVX engine, Network Security Essentials includes Intelligence-Driven Analysis technology that identifies and blocks known and unknown threats. The Intelligence-Driven Analysis technology is a collection of contextual, rule-based engines that detect and block malicious activity based on the latest machine, attacker and victim intelligence. An intrusion prevention system (IPS) detects common attacks with conventional signature matching and provides riskware protection to block spyware and adware. Unlike conventional or next-generation firewalls, IPS-only or anti-virus (AV) software, Network Security Essentials detects both known and unknown (zero-day) attacks with high accuracy while generating low rates of false positives, freeing security teams to focus on the alerts that matter.

Flexible Deployment Options

Network Security Essentials requires an on-premise virtual or physical appliance that can be deployed in either inline or monitor-only mode. Network Smart Node, the on-premise appliance, can be deployed across a range of locations, from the primary network perimeter to remote and branch offices — anywhere that has direct Internet access. The downloadable virtual machine image (Figure 1) is favored because it's cost effective and quick to deploy. Network Smart Nodes use Intelligence-Driven Analysis technology and signature-based IPS detection to identify and protect against suspicious activity. They use an encrypted connection to send suspicious objects that require further analysis to the Cloud MVX service in the FireEye private cloud. The Network Smart Node and Cloud MVX service is also available as an integrated hardware appliance (Figure 2). FireEye recommends the 50 Mbps option for small enterprises and 100 Mbps for midsize enterprises.

Email Security: Email Threat Protection Cloud

Email is often used to initiate major breaches. ETP is a cloud-based, software-as-a-service (SaaS) offering that analyzes email for signs of spear phishing as well as commodity virus or spam threats. ETP uses patented Cloud MVX technology to proactively prevent advanced email attacks. It also provides inline anti-spam and antivirus protection. ETP can protect both on-premise and cloud-based mailboxes with either inline or monitor-only deployment.

Threat Intelligence

Cloud-based FireEye threat intelligence accompanies alerts from the FireEye solution. The intelligence, updated every 60 minutes, includes information on new malware profiles, vulnerability exploits, adversary and victim intelligence and threat findings. It complements the Cloud MVX engine with cloud-enabled analytics and machine learning technologies to detect advanced threats. As a result, FireEye alerts may include critical contextual information such as possible threat actor identity, likely motives and malware details, to help security professionals detect and stop highly targeted zero-day attacks and known malware.

[1] Verizon 2015 Data Breach Investigations Report

SAMPLE CONFIGURATIONS

Factors to consider when assembling a solution include: the number of email boxes to monitor, the volume of network traffic traversing the system, the virtualized or physical environment, the adoption of cloud-delivered services and the level of security awareness possessed by senior business leaders and your board of directors. FireEye and its partners can help you choose or design a solution to match your needs, modeled after these sample configurations.

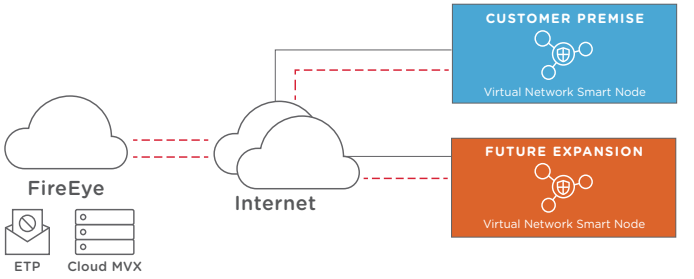

FIGURE 1. ETP CLOUD AND CLOUD MVX WITH VIRTUAL APPLIANCES

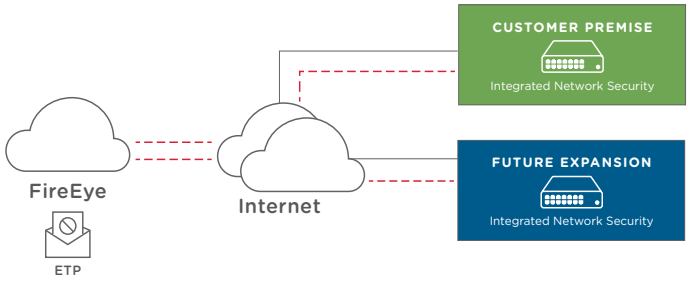

FIGURE 2. ETP CLOUD AND PHYSICAL INTEGRATED NETWORK SECURITY APPLIANCES

	SMALL #1	SMALL #2	MEDIUM #1	MEDIUM #2
DEPLOYMENT TYPE	**VIRTUAL/ CLOUD**	**PHYSICAL APPLIANCE**	**VIRTUAL/ CLOUD**	**PHYSICAL APPLIANCE**
Number of Employees	200-250	200-250	450-550	450-550
Network Traffic	50 Mbps	50 Mbps	100 Mbps	100 Mbps
Proposed Sample Solution	ETP 200-250 seats Virtual NX1500 Cloud MVX	ETP 200-250 seats Integrated 2500NXE1	ETP 450-550 seats Virtual NX2500 Cloud MVX	ETP 450-550 seats Integrated 2500NXE2

NEXT STEPS

SMEs are the target of choice or opportunity for advanced attackers because of their weak security measures, which are largely due to limited resources and a lower awareness. To grow the businesses and reduce risks, it is critical to maintain an essential level of security. And that necessitates confidence in the state of security, as well as the security program, tools and processes.

To learn more about FireEye, visit:
www.FireEye.com

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. The company has 5,000+ customers across 67 countries, including 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