

ESSENTIAL SECURITY FOR SMALL AND MIDSIZE ENTERPRISES

OVERVIEW

An essential baseline of security needs a prevent-and-detect strategy with a response readiness plan for unforeseen incidents.

Award-winning FireEye technologies help detect and stop advanced multi-stage and multi-vector attacks with high accuracy. They arm security teams with accurate and contextual insights to immediately execute a response plan on their own or through a partner. Services from Mandiant and FireEye partners also complement these proactive technologies to help organizations with incident response.

These effective solutions are designed to be easy for SMEs to access and use, and allow them to focus on growing their business.

THE SOLUTION

The FireEye solution combines FireEye Network Security Essentials and FireEye Email Threat Prevention Cloud (ETP) to protect organizations against web- and email-based threats. Those two vectors account for 90% of cyber-attacks. It helps optimize your security budget by identifying only 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 FireEye technologies. It helps identify advanced multi-stage attacks and blended threats that span multiple attack surfaces, 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 identify the opening salvo of many multi-vector attacks. Visibility into this linkage enables organizations 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. 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 simplify deployment and day-to-day management of both network and email security, and improve their security posture.

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. It uses the MVX engine to analyze web traffic to detect exploits, malware executables and multi-protocol callbacks. It also includes an Intrusion Prevention System (IPS) to detect common attacks with conventional signature matching and provides riskware protection to block spyware and adware. Unlike conventional or next-generation firewalls, IPS or antivirus (AV) solutions, Network Security Essentials detects both known and unknown (zero-day) attacks with high accuracy while generating low rates of false positives. Network Security Essentials can be deployed in either inline or monitor-only mode.

Email Security: Email Threat Protection Cloud (ETP)

Email is often the opening salvo of 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 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 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.

BREACH PREPARATION

Detection and prevention only solve half the problem. It is equally critical to plan for technical, legal, financial and public relations for an unforeseen incident. FireEye strongly recommends establishing a response plan, ideally with a security partner. Mandiant Consulting from FireEye offers services for response plan development, response plan validation and incident investigation.

SAMPLE CONFIGURATIONS:

Key factors that lead to appropriate bundled solutions are: the number of email boxes to monitor, the volume of network traffic traversing the internet, the nature of the data or transactions you're trying to protect and the level of security awareness possessed by your board of directors and business leaders. Let FireEye help you define the most appropriate solution modelled after these sample configurations.

	SMALL	MEDIUM	LARGE
Number of Employees	100	1000	2000
Network Traffic	50 Mbps	100 Mbps	250 Mbps
Possible Solution	ETP 100 seats NX 2400	ETP 1000 seats NX 4400-100	ETP 2000 seats NX 4400-250

NOTE: Contact your partner for appropriate security response plan development services.

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 security solutions designed to detect and prevent advanced attacks as well as prepare a suitable response plan, please visit www.fireeye.com or contact your local sales representative.

ABOUT FIREEYE

FireEye protects the most valuable assets in the world from today's cyber attackers. Our combination of technology, intelligence, and expertise helps eliminate the impact of breaches. The FireEye Global Defense Community includes over 4,400 customers across 67 countries, including over 250 of the Fortune 500.

For more information on FireEye, visit:

www.FireEye.com

FireEye, Inc.

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

www.FireEye.com