ESSENTIAL CYBER SECURITY FOR SMALL AND MIDSIZE ENTERPRISES

OVERVIEW

Many industry reports indicate that small and midsize enterprises (SMEs) are at particular risk from sophisticated cyber attackers. In fact, 77% of all cyber crime targets SMEs. But financial constraints can make it difficult for SMEs to obtain the resources they need to protect themselves against advanced threats.

An essential baseline of security needs a detect-and-prevent strategy to protect against advanced threats, with a response readiness plan for unforeseen incidents. Award-winning FireEye technologies help detect and stop multi-stage and multi-vector attacks. They arm security teams with accurate and contextual insights to immediately execute a response plan on their own or through a partner. Services from FireEye and its 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 CHALLENGE

Governments and large enterprises have known about advanced threats for some time and have gradually implemented security frameworks and adopted technologies to reduce the risk and impact of a data breach. These organizations typically have spending flexibility in their security budgets, or have legal or regulatory mandates to justify the cost of security. The challenge for SMEs is they lack the advantages of their larger counterparts, but face similar risks.

Although the news tends to focus on large breaches, SMEs are often the principal targets of cybercrime. Why? Because SMEs have more assets (such as credit card numbers, identity information, health information, intellectual property) than an individual, but less security than larger enterprises — putting them in the attackers “sweet spot.”

Many SMEs are also targets because they provide business process outsourcing (BPO) or information technology enabled services (ITES) to larger organizations. Attackers exploit this trust, infiltrate the weaker link and then move laterally to a more significant target. Attackers tend to follow the path of least resistance to attain their goals.

Large enterprises are increasingly scrutinizing their supply chain to identify providers who can demonstrate a high degree of cyber security due diligence. SMEs will need to implement higher levels of advanced prevention and detection capabilities to meet those requirements and grow their business.

Spear-phishing emails and ransomware are increasing risks for SMEs due to inadequate security. SMEs may not consider themselves targets, but weak security makes them easy targets for the smash-and-grab approach of ransomware.

Legacy signature-based security technologies are ineffective against these threats because they are often polymorphic, intentionally designed to avoid exhibiting any previous signature. Ultimately, SMEs need to address advanced threats and ransomware risks. This is because it’s been estimated that half of the small businesses that suffer a cyber attack go out of business within six months.

2 https://staysafeonline.org/
The Solution

Defending against today’s sophisticated attackers requires a security solution that prevents and detects advanced threats by:

- Being aware of the top threat vectors and malicious activity across those vectors.
- Spotting new threats, including never-before-seen (zero-day) attacks, and well known and commodity threats.
- Identifying advanced multi-stage and multi-vector attacks.
- Using cutting-edge intelligence to quickly recognize serious threats and threat actors.

FireEye Essential Security combines FireEye Network Security (NX) Essentials and FireEye Email Threat Prevention Cloud (ETP) to protect organizations against web- and email-based threats. Those two threat vectors account for 90% of cyber attacks. The Essential Security solution helps optimize your security budget by identifying only critical security issues without the distraction of false-positives that 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 as shown in Figure 1. Visibility into this linkage enables organizations to see how the two events are related and automatically blocks subsequent stages of the attack, such as attackers trying to transfer stolen data over the web. It also identifies and blocks subsequent attacks that use similar tactics, tools and procedures (TTPs).

The Essential Security solution helps organizations respond faster to threats with contextual, actionable intelligence. It also allows SMEs to stretch limited security budgets and reduce operational overhead by consolidating technology deployment, automatically blocking critical attacks and generating high-quality alerts to minimize wasted effort.

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.
DETECTION AND PREVENTION TECHNOLOGY

Network Security Essentials
FireEye Network Security Essentials is an affordable, plug-and-play network security solution that can be deployed in under 60 minutes. It minimizes the risk of costly breaches by detecting and stopping known and unknown network-based cyber attacks. 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) with conventional signature matching to detect common attacks and provides riskware protection to block spyware and adware. Unlike conventional or next-generation firewalls, stand-alone 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.

Email Security: Email Threat Protection Cloud (ETP)
Email is often the opening salvo of major breaches. FireEye ETP is a software-as-a-service (SaaS) offering that analyzes email for signs of spear phishing as well as commodity virus or spam threats.

Simplifying deployment with a cloud-based offering, ETP uses the 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.

Threat Intelligence
Cloud-based FireEye Threat Intelligence draws on our proprietary access to intelligence data from globally-deployed sensors and accompanies alerts from the FireEye solution. The intelligence, updated every 60 minutes, includes information on new malware profiles, vulnerability exploits and threat findings. It complements the MVX engine with cloud-enabled analytics and machine-learning technologies to detect advanced threats.

FireEye Dynamic Threat Intelligence (DTI) provides hourly updates on anonymously exchanged data on web-, email- and file-based threats across the FireEye global cloud network. The updates ensure the most recent attacks FireEye has seen across its global network of customers are found and blocked. DTI is available with Network Security Essentials.

FireEye Advanced Threat Intelligence (ATI) provides rich adversary and victim intelligence gathered by threat intelligence analysts and incident responders. As a result, FireEye attack alerts may include valuable contextual information, such as possible threat actor identity, likely motives and malware details. This makes the solution more efficient at detecting both highly targeted zero-day attacks and known malware and helps security professionals stay ahead of and stop threat actors. ATI is standard with ETP.

Deployment Options
The Essential Security solution can be deployed inline for greater control and real-time response to stop attacks in progress as shown in Figure 2.

Some organizations prefer to start with a more conservative approach, so it can also be deployed in out-of-band or monitor-only modes (BCC mode for ETP) as shown in Figure 3. In this deployment, all traffic is monitored for malicious activity and a report is generated but there is no automated prevention mechanism. FireEye or our partners can help you determine and deploy the option that best fits your needs.
BREACH PREPARATION

Remember that detection and prevention only solve half the problem. It is equally critical to analyze and respond to the technical, legal, financial and public relations impact of an unforeseen incident. FireEye strongly recommends establishing a response plan, ideally with a security partner. FireEye and its partners offer services for response plan development, response plan validation and incident investigation.

NEXT STEPS

SMEs are the target of choice for advanced attackers because they often have weak security measures, largely due to limited resources and less awareness of threats. To stay focused on growing your business and to minimize risk, an essential level of security is recommended. This includes security technologies and processes designed to defend against and respond to today’s sophisticated cyber attackers. Ultimately, they will give you greater confidence in the state of your security.

To learn more about FireEye security solutions designed to detect and prevent advanced attacks as well as prepare a suitable response plan in the event of a compromise, 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 4,400 customers across 67 countries, including over 250 of the Fortune 500.

For more information on FireEye, visit: www.FireEye.com