SECURITY THEN AND NOW: FROM REACTIVE TO PROACTIVE

WHY YOU NEED SECURITY AS A SERVICE TO BATTLE TODAY'S CYBER THREATS

WHITE PAPER

FireEye

SECURITY CHALLENGES — AND THEIR SOLUTIONS — HAVE CHANGED DRAMATICALLY OVER THE LAST 40 YEARS. IN THIS PAPER WE EXPLAIN HOW YOUR SECURITY STANCE NEEDS TO CHANGE FROM A REACTIVE TO PROACTIVE ONE, AND HOW SECURITY AS A SERVICE CAN HELP.

In the 1970s, we had centrally controlled IT environments that, although complex, were relatively easy to manage from a security perspective. By the 1990s, security was getting more complicated due to the entry of distributed PCs, millions of which were being connected to the internet. Then the 2000s arrived with more mobility and more endpoints to protect in highly distributed environments. But even then, says Matt White, Senior Manager in KPMG's Cyber Security Practice, "if you go back [just] five years, people thought that if you got breached you hadn't bought the [right security] software.[1]

This is no longer the case.

Today, we have extremely complex environments to manage. Bring-your-own-device (BYOD) and bring-your-own-application (BYOA) policies allow users to access any cloud-based application on whatever device helps them be more productive.

Breaches are now thought of as inevitable. The security focus has changed from attempting to prevent breaches to correctly identifying and remediating attacks swiftly enough to contain and minimize any damage or loss.

Threat actors have also changed over the decades, from mischievous (to prove something) to malicious (to harm something) to advanced (to steal something). (Fig. 1.)

1 SC Magazine. "How to prepare for the inevitable: SC Roundtable sponsored by FireEye Mandiant." December 15, 2015.

FIGURE 1: BREAKING DOWN THE THREAT

CHALLENGES OF MODERN CYBER SECURITY

Today's security defenses are primarily still based on alerts generated by firewalls, intrusion detection systems and intrusion protection systems that can protect against known threats. But all those alerts have created the problem of alert fatigue, where analysts are inundated by false and duplicate alerts and miss important ones that can indicate serious advanced attacks.

Additionally, advanced persistent threat (APT) attackers behave quite differently than typical hacktivists or cyber criminals. APT attackers sneak into networks unnoticed. They remain in hiding as they spread through the environment and search for what they want. They stay in environments for long periods, siphoning off valuable data over months or years. And when you kick them out, they invariably return.

Given the rapidly evolving threat landscape, organizations are increasingly challenged to protect their key assets against unknown threats. But their technology and personnel are often inadequate or insufficient. The organizations also don't have a big-picture view of the cyber threat landscape. Their most formidable challenge is that their security teams are simply reacting to alerts and threats, which will ultimately fail to protect the organization from a major breach.

It takes a lot of effort to build a complete and robust security program. Many organizations rely on a trusted third party to help respond to incidents and evaluate the ongoing effectiveness of their security programs and operations to ensure they adequately mitigate risk. Called security as a service (SECaaS), this model mixes automated security technology with 24/7 manual analyses by human experts.

SECaaS doesn't mean you let go of your security function completely — you still have transparency into and control over it; it means you have the help of experts who have made security their core business and who stake their reputations on their ability to protect businesses like yours.

Beyond Reactive: the Modern, Proactive Cycle of Security Preparedness

Security preparedness is not a static state. Experts now say it's not a question of if you'll be breached, but when. In this new threat landscape, you need to be on constant alert — everything will depend on how fast you can respond and remediate when attackers hit. Fortunately, you can evaluate the state of your environment and security program by answering a few key questions and taking appropriate action to correct vulnerabilities, threats and breaches.

Have I been compromised? Determine the current state of your environment with a compromise assessment and security health check. If you have been compromised, you can take action to contain and block attacks. If you haven't, you have a clean bill of health, for now. But this doesn't mean you're safe from attack.

Am I at risk? Constantly test your network for vulnerabilities and fix anything that would make it easy for an attacker to compromise you. You can commission penetration and red team testing. For these tests, you ask a third party to think and act like an attacker intent on penetrating your environment. The strengths and vulnerabilities they reveal help guide improvements in your security program and environment.

Am I prepared? Continuously assess and update your overall security program — especially your incident-response plan. Engage experts to perform a response readiness assessment, or enact a tabletop exercise to practice responding rapidly and effectively to incidents.

Have I planned sufficiently? Look ahead, beyond a breach, to determine possible long-term effects on your business. Build up your awareness of the latest technologies and protections that can help your company be more responsive. Consider paying a retainer to an incident-response firm to bolster your own resources. Have your security personnel refresh their security credentials to keep up in an extremely fast-moving field.

Have I been compromised? Yes, you're back where you started. Recognize that a clean bill of health only lasts so long. It's important to get periodic compromise assessments to ensure that nothing has slipped past your defenses.

THE BENEFITS OF SECURITY AS A SERVICE

How SECaaS works:

- Security technologies provided to your organization are not only the most up to date, but are continuously updated with minimal disruption to your business practices, and the updates do not rely on user compliance.
- Your organization gains access to deeper and broader security and expertise than you could cultivate in house so you don't have to recruit, hire and train them yourself, and they are continually enhanced without any effort from your organization.
- Alerts generated by your security systems are analyzed by experts around the clock and put into proper context so that no threat flies under the radar or gets missed..
- Accomplished SECaaS companies provide you with a single interface that gives you a transparent view of your security environment.

Accomplished SECaaS companies provide you with a single interface that gives you a transparent view of your security environment.

HOW TO EVALUATE SECURITY AS A SERVICE VENDORS

Not all SECaaS vendors are created alike. Here are questions to help you get to the core of exactly what a vendor should provide, and whether it will meet your needs.

Technology

Your objective here is to discover whether the vendor has an advanced technology platform that incorporates host and network solutions with real-time attack visibility.

- Does it automate functionality to accelerate response time and make its solution effective even when you have a small staff?
- Is its technology built to find and stop advanced attackers?
- Is its technology regularly updated to reflect rapidly changing attacker behavior and incorporate new innovations?
- How often does the vendor update its technology with information about the latest attacker infrastructure, tools and methodologies, and where does it get the information for those updates?
- How does the vendor package and deliver information and analysis on alerts, suspected attacks and new indicators of compromise (IOCs)?
- Does the vendor have a dedicated R&D team that continuously innovates on both commercial products and proprietary tools?

Intelligence

Your objective here is to determine the quality, breadth and depth of intelligence a vendor provides with its security offering.

- How does the vendor gain visibility into attacker behavior, activity, methodology and motivations?
- How does the vendor observe and monitor persistent attacker behaviors for targeted attacks that evolve over time?
- How timely and relevant is the intelligence that the vendor collects?
- How does the vendor's intelligence contribute to incident response?

Expertise

Your objective here is to assess how well the security professionals employed by the vendor understand the overall threat landscape and evolving, as-yet-unknown attacker tools, behaviors and motivations.

- What kind of experience does the vendor have in responding to critical, complex breaches?
- What types of attackers does the vendor have experience responding to?
- How has the vendor contributed as a first responder to publicized cyber breach incidents?
- How has the vendor established its authority as a security industry expert?

TIMES HAVE CHANGED—CHANGE WITH THEM

Cyber risks have changed considerably over the decades. Today, your adversaries are people: creative, nimble and persistent. They create new malware, probe for vulnerabilities and vary exploit tactics until they gain entry. Once inside, they cover their tracks and wait patiently, assembling a toolkit and formulating an attack plan over time as they watch and learn about your employees and your network. This is why a proactive rather than reactive approach to security is required now.

SECaaS vendors provide measurable, meaningful benefits to your security organization by providing world-leading security experts to monitor your network and systems with an advanced technology platform and the latest curated intelligence from around the world. Their capabilities allow you to detect, prevent, analyze and resolve security incidents quickly enough to mitigate the worst modern threats.

FireEye as a Service

Technology: Patented FireEye technology detects even the most complex and multifaceted threats. The FireEye R&D team innovates continuously to outsmart highly sophisticated threat actors. FireEye provide answers, not just alerts, through validated compromise reports that contain information about attackers and their intentions and tell you how to respond.

Intelligence: FireEye offers world-leading threat intelligence and is called on as an incident responder to almost every headline breach. FireEye curates the latest tactical intelligence discovered across its global defense community to build a dynamic intelligence network capable of finding threats in your environment fast and accurately.

Expertise: Expert FireEye security analysts monitor your environment 24/7 and provide ongoing compromise assessment, using FireEye technologies and Intelligence to detect signs of intrusion early, rapidly investigate and provide the answers you need to respond effectively to threats.

To learn more about how FireEye provides security as a service, visit:
www.FireEye.com/faas

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

www.FireEye.com

FireEye