BINARY DEFENSE™ | 2019 White Paper

SOC-AS-A-SERVICE MAKES ENTERPRISE-GRADE SECURITY AFFORDABLE FOR THE SMB

Extend your security operations with a team of experts monitoring 24/7 for threats

Could Your Business Recover from a Serious Cyberattack?

What's the top worry of many small and medium-size businesses (SMBs) today? It isn't whether there will be an economic downturn, manufacturing delay, or some other major event.

Instead, these companies are increasingly worried about the aftermath of a serious cybersecurity attack.

For instance, nearly one-third of larger SMBs (150 to 250 employees) predict a successful cyberattack would be "extremely harmful" to their business, while 20 percent of all SMBs believe there is a high-to-definite likelihood their business would not survive after a successful cyberattack. [1]

They're right to be worried: Cyberattacks are more sophisticated than ever. It takes best-of-breed security tools and a dedicated, trained and experienced security staff working 24x7x365 to protect a business of any size.

The problem is that only larger companies can afford to deploy and operate this type of security coverage in house—and hackers certainly know this.

[1] "AppRiver Cyberthreat Index for Business: Q1 2019," AppRiver, January 2019

Types of Cyberattacks

Phishing

Emails attempting to trick the recipient into giving out sensitive information

Ransomware

Malware that blocks access to a victim's data until a ransom is paid

Distributed Denial of Service (DDos)

An attempt to take down a network by flooding it with traffic

Business Email Compromise

Attempt to defraud a company through a spoofed corporate email

However, staying ahead of hackers and protecting the business against cybersecurity attacks is no longer out of reach for SMBs. There's a new type of security service that brings enterprise-class technology, processes, skills, and experience to the SMB market at an affordable price. Called SOC-as-a-Service, it's becoming a necessity for companies that want to avoid the potentially devasting consequences of a successful cyberattack.

The Impact of a Successful Cyberattack

67%
OF SMBs EXPERIENCED A CYBERATTACK IN 2018

$1.4M
AVERAGE COST IN DAMAGES OR THEFT

$1.6M
ADDITIONAL AVERAGE IN COSTS DUE TO DISRUPTION OF OPERATIONS

Source: "2018 State of Cybersecurity in Small & Medium Size Businesses," Ponemon Institute LLC, November 2018

Why Hackers Get Through SMBs' Defenses

By identifying and responding to a potential cybersecurity threat immediately, companies can keep damage to a minimum. The problem is that for most businesses, the gap between the time when a breach occurs and the time when the business discovers the breach and takes steps to stop it is not hours or days, it's months. Most attackers only need a matter of minutes between the initial attack and the successful compromise of sensitive information. [2]

Why does it take so long for businesses to notice and respond to an attack? In a nutshell, it's because there are too many things to keep track of and too few people, with the right skills, to do so.

Let's look at the problem of too many things to keep track of. Computer systems, networking products, security software, and other technologies generate logs, which are detailed information about what is happening at any point in time. Security software, in particular, also generates alerts about any potential threats. All this data must be continuously reviewed by someone with the right security skills and know-how to recognize, investigate, and stop threats. This deluge of data is a huge problem for all businesses, but especially SMBs, because it requires time, people, and money to address.

Hiring and retaining people with cybersecurity skills is the other problem. Often the person or people handling security for an SMB also have other responsibilities within IT, which means they can't focus on security 100 percent of the time. Threats can then slip through the cracks because logs and alerts get reviewed only when there's time.

The "Negative Unemployment Rate for Cybersecurity Roles

Even if your business has the ability to hire dedicated security staff, there's an industry-wide talent shortage, with nearly half a million unfilled cybersecurity positions currently in North America.[3] According to industry analyst firm ESG, 53 percent of enterprises report a problematic shortage of cybersecurity skills at their organizations.[4]

[2] "2019 Data Breach Investigations Report," Verizon, 2019

[3] "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," (ISC)², 2018

[4] "The Cybersecurity Skills Shortage is Getting Worse," ESG, January 2019

Enterprises Are Getting Their SOCs On

More and more enterprises are turning to Security Operations Centers (SOCs for short) to address the problem of identifying and responding to potential cybersecurity threats as quickly as possible. A SOC is a centralized organization or function within a company that combines technology, staffing, and processes to achieve continuous awareness and response to cybersecurity issues as they arise.

The SOC has full responsibility for monitoring, detecting, investigating, analyzing, responding, mediating, and reporting on cybersecurity threats to the company. To accomplish all of this, SOCs are comprised of a team of experienced security analysts, many with specialized skills in the tools and technologies the company uses, as well as a thorough understanding of hackers' methodology.

Creating an in-house SOC can certainly help enterprises stay ahead of hackers and minimize the impact of attacks, but it's not a trivial or inexpensive solution to the cybersecurity problem.

A successful SOC requires:

- Purchasing, deploying, operating, and maintaining the various technology solutions needed by the SOC
- Hiring, training, and managing skilled security professionals to operate the SOC 24x7x365
- Creating and managing effective security processes to enable rapid identification, investigation, and response to threats

Even larger organizations find it difficult, if not impossible, to build an in-house SOC. SMBs may find it even more challenging due to lack of budget, resources, time and skill sets.

SOC-as-a-Service Levels the Playing Field

An alternative to building your own SOC can give your business all the benefits without the high cost, time, and resources of creating your own.

SOC-as-a-Service provides your business with the same level or higher protection as enterprises that have their own in-house SOCs, while costing no more than a full-time employee for mid-sized companies and even less for many smaller organizations.

1. Focus on the people who support the SOC and the processes they use to keep your business informed and protected. While many providers promote their technologies and automation more so than their security staff, processes, and standards for communication, successfully fighting today's threats requires the right people available all the time, communicating with your business one-on-one.

2. Look for a provider willing to divulge the qualifications of its security professionals who monitor, detect, and report threats to your business 24x7x365. The people staffing a SOC-as-a-Service should represent a range of disciplines across the cybersecurity landscape—everything from skills in reverse engineering of malware to threat hunting skills to an understanding of advanced hacker techniques and attack indicators.

3. Finally, look for a SOC-as-a-Service provider that integrates into your environment and not the other way around.

Conclusion

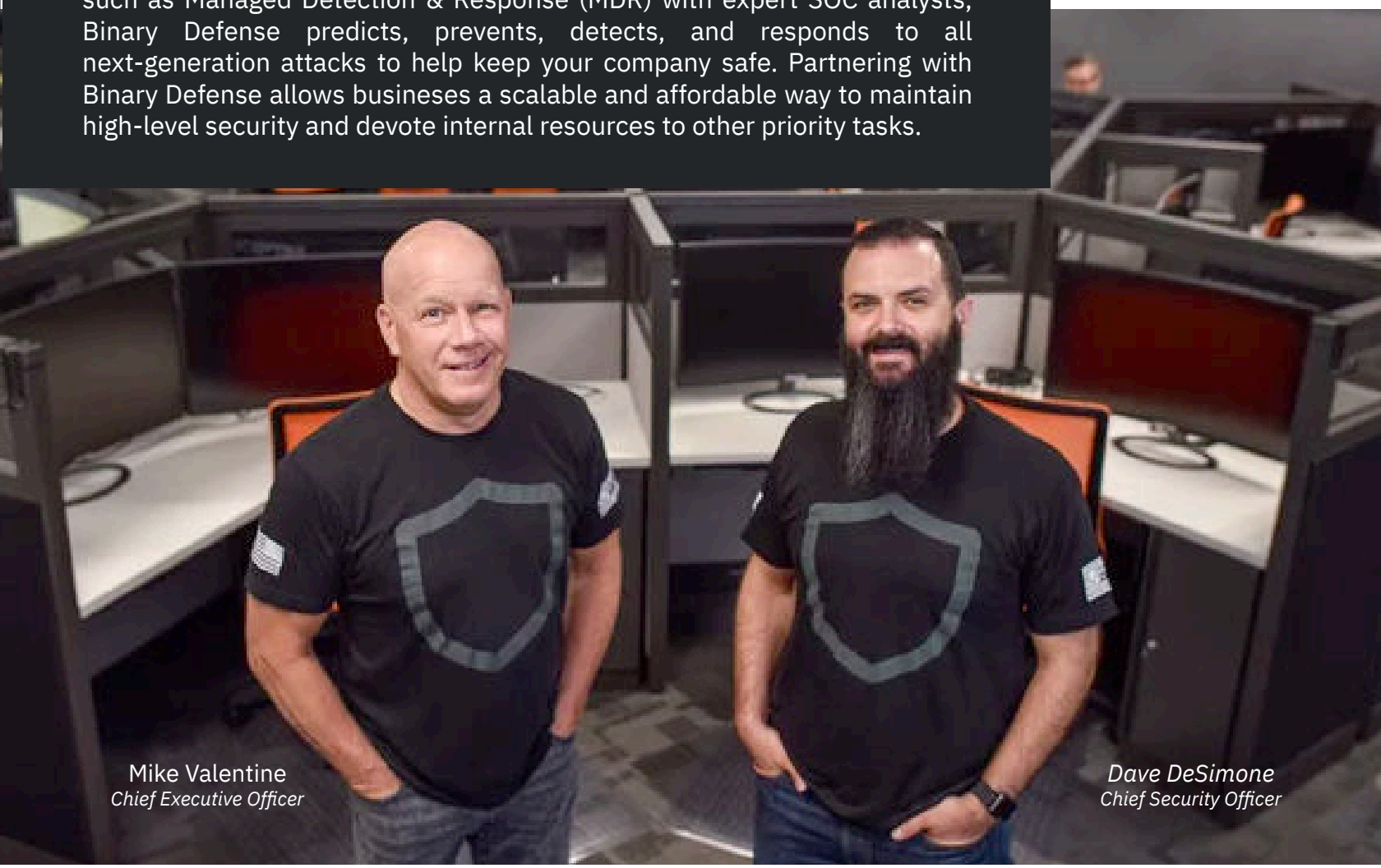
Every organization today needs the capabilities of a SOC to help protect against cyberattack. However, for a SOC to be effective, it requires ongoing investment in people, processes and technologies—which makes a do-it-yourself SOC extremely difficult to bring in house for all but the largest of companies.

The Binary Defense SOC-as-a-Service was created specifically to serve the needs of those businesses that don't have the budget, time, staff or skills for their own SOC. Our team of dedicated, highly-trained security analysts quickly integrate into your existing organization, then work to detect and analyze advanced attack patterns and alert you of malicious threats within minutes.

BINARY DEFENSE™

About Binary Defense

Binary Defense is the full-service security partner for organizations of all sizes and a global leader in advanced endpoint security solutions. The Binary Defense SOC-as-a-Service is always on duty to detect attacks and alert clients of threats. The Security Operations Center (SOC) is a true extension of your security team, offering personalized incident reports and escalation procedures. Pairing best-in-class protection technologies such as Managed Detection & Response (MDR) with expert SOC analysts, Binary Defense predicts, prevents, detects, and responds to all next-generation attacks to help keep your company safe. Partnering with Binary Defense allows businesses a scalable and affordable way to maintain high-level security and devote internal resources to other priority tasks.



LEARN MORE: BINARYDEFENSE.COM

600 ALPHA PARKWAY, STOW OH 44224 | 800-BINARY2

WWW.BINARYDEFENSE.COM