JANUARY 2019

WHITEPAPER

SECURITY-AS-A-SERVICE HAS ARRIVED

INTRODUCTION

Finding the most effective and affordable way to secure your environment is not a simple choice. Between the changing topography of the cyberthreat landscape, the continual increase in security events and incidents; the shortage of skilled cybersecurity professionals; and, let's face it, the price tag associated with maintaining a secure environment and reducing cybersecurity risk is not getting any cheaper.

Businesses searching for solutions to these problems are increasingly looking to third parties for answers, giving them 3 options—traditional managed security service providers (MSSPs), managed detection and response (MDR) offerings, and security-as-a-service (SECaaS) solutions. Each approach is a response to the pressures of protecting an ever more complex environment that demands speed, agility, and advanced threat detection. But, whereas the reactive approach of traditional managed security services is on passive monitoring of physical and some logical infrastructure that stops at alerting, SECaaS enables the delivery of proactive and reactive security tools in less than 2 minutes. In this way, SECaaS is the result of the natural evolution of managed security services—it addresses the shortcomings of traditional MDR offerings and is the response to the shifting needs and priorities of businesses that have looked to MSSPs for help in the past.

Done right, SECaaS could be the answer to your cybersecurity needs. But how should small- and medium-sized businesses (SMBs) and enterprises make that decision?

> SECaaS enables the delivery of proactive and reactive security tools in less than 2 minutes.

WHAT'S IN A NAME?

First, let's define what we mean by managed security services, MDR, and SECaaS, and how they differ from one another. Simply put, MSSPs deliver outsourced monitoring and management of a customer's existing security infrastructure. As part of the service, MSSPs remotely monitor and/or manage security devices, such as firewalls and intrusion prevention solutions (IPS) solutions, and provide 24/7/365 coverage. These organizations typically stop at alerting to a potential threat and don't provide response and remediation services except as a premium add-on service. For many, this means they are on their own to resolve alerts.

In recent years, MDR has emerged as a solution to mid-sized organizations and enterprises that need better threat detection, the reduction of false positives, and the help with incident response (IR) that MSSPs fail to provide. Traditional MDR solutions provide threat intelligence-driven detection that uses behavioral-based detection and go beyond simple alerting to include forensic investigation as well as threat hunting to identify attacker activity—privilege escalation and lateral movement—that may otherwise slip by unnoticed.

SECaaS is another option for consumers in the wider MSSP and MDR market—designed to deliver and provision managed security capabilities from the cloud. Cloud-based delivery of a holistic SECaaS product can take the best parts of traditional MDR and managed security offerings and extend them across any environment—public, private, or hybrid cloud, as well as on-premise—proving its value faster and addressing a broader range of security concerns than traditional methods. SECaaS also reduces costs, offering subscription-and/or consumption-based pricing, and simplifies cybersecurity through consolidated management and rapid response.

For the past several years, the security space has touted SECaaS as a potential solution to the challenges posed by a complex threat landscape and the shortage of qualified cybersecurity professionals. But, not all SECaaS is the same. The definition has been muddled by marketing speak, with vendors calling themselves SECaaS just because they can deliver software updates from the cloud. SECaaS vendors, however, can do much more—they can deliver capabilities such as advanced threat detection, threat hunting, and remediation with the speed, cost savings, and agility consistent with operating in the cloud.

FEATURES	TRADITIONAL MSSP	SECaaS
Ease of implementation (DevOps ready)	Average 45 days	<2 min
Prevention, detection and response	Alerting only	99.999% threats blocked; response included
Average time to detect and elminate threats	99 days	1 day
Visibility & threat management across environments (public, private, or hybrid cloud & on-premise)	On-premise ONLY	✓
Audit-ready compliance (HIPAA, PCI, & GDPR)	No	✓
Subscription-and/or consumption-based pricing	Fixed contract	✓
Patching	Client owned	✓
Vendors	SCWX, IBM, etc.	Armor

FACING CHALLENGES

Innovation has always been a double-edged sword. Advances in technology have had the side effect of expanding attack surfaces for organizations, while broadening the threat landscape. As companies embrace digital transformation and as the complexity of their environments grow, protecting everything from cloud workloads to interconnected devices is becoming more difficult.

Adding the innovation of attackers to this situation makes for a combustible mix. It is no secret that security events are continuing to challenge the controls that organizations of all sizes have put in place. The amount of malware in the wild remains a challenge, particularly for small and midsized businesses (SMBs). In addition, there are cases where sophisticated attackers may try to hide their actions inside a network by reducing the use of malware and avoiding detection by antivirus, IDS, and other security tools.

Addressing these challenges takes a combination of people, processes, and technology, with the first "p" in that triumvirate posing a challenge all its own. ISACA's recent "State of Cybersecurity 2018 Part 1: Workforce Development" report highlights the difficulty of finding staff that can handle security operations internally. Sixty-one percent of respondents to ISACA's survey said that half or less of their applicants for open security positions are qualified, with 30%of these respondents indicating that less than 25% of applicants are qualified. In addition, 25% said it took 3 months to fill an unfilled cybersecurity position, while 26% said it took 6 months or more.

Meanwhile, the price of failing at cybersecurity remains high. According to the Ponemon Institute's "2017 Cost of Data Breach Study", the average cost globally of the breaches analyzed for the report was $141 per compromised record, translating to a cost of $3.62 million. Having a strong incident response (IR) capability reduced the average cost by roughly an estimated $19 per record, the report found.

For many organizations, outsourcing security is a way to bridge the gap between their security resources and the needs posed by the risks they face. According to the Ponemon Institute's "2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB)" report, when asked what the biggest challenges were to their cybersecurity's effectiveness, 73% cited insufficient personnel, while 56% blamed a lack of budget. Driven to reduce costs and complexity, many organizations want to do more with managed security providers to meet the demands of protecting their environment. The services most often used are monitored and managed firewalls, IDS/IPS, and secure gateways for messaging or Web traffic, the survey found.

As security risks facing large and small organizations grow more prevalent and sophisticated, outsourcing security is an increasingly attractive option.

What percentage of your organization's IT security operations are supported by MSSPs?	FY 2017	FY 2016
None	47%	54%
Less than 10%	10%	11%
10% to 25%	12%	13%
26% to 50%	11%	9%
51% to 75%	9%	9%
75% to 100%	10%	4%
Total	**100%**	**100%**
Extrapolated Value	**21%**	**16%**

SECAAS CAN SEPARATE ITSELF FROM THE PACK

Pursuing managed services offers the promise of cost savings, the removal of the burden of managing security, and the expertise of security professionals who are beyond what organizations typically have in-house. SECaaS providers stand out by mixing what is best about traditional MDR and MSSP offerings and then taking advantage of the cloud to meet the needs of today's organizations.

While traditional MSSPs and MDR providers are poised to take advantage of the opportunity presented by the same factors driving interest in SECaaS, there are factors that set it apart. For example, both traditional MSSPs and SECaaS turn CapEx to OpEx. However, MSSPs often use fixed or annual contracts, removing the flexibility customers can get from SECaaS solutions that use a consumption-based model.

The ability to monitor cloud environments while protecting on-premise infrastructures distinguishes SECaaS. A client portal that offers both visibility into an organization's cloud and on-premise environments, as well as self-provisioning and management capabilities is a critical piece of this puzzle; it provides visibility and empowers organizations to leverage cloud computing's scalability.

A client portal should also offer access to cybersecurity experts who can investigate and respond to sophisticated attacks. Their expertise can potentially reduce attackers' dwell-time in environments that are not protected by an internal IR team (or one on retainer) or the ability to handle response and remediation in-house.

TIME

The challenges facing today's companies underscore a simple fact—a new security approach is needed. Answering the call requires a solution that enables the quick deployment of new protections across on-premise, cloud, and hybrid IT environments and provides a unified view of the organization's IT security posture. By leveraging the cloud, SECaaS vendors can quickly deploy security, while implementation for MSSPs can take weeks. A holistic SECaaS offering that provides a fully featured stack of security controls backed by proactive threat hunting and IR equal to that used by the federal government provides higher levels of control and visibility and allows the focus to stay on what matters most—your business.

DELIVERING THE POWER OF THE CLOUD

It's not just reduced costs, the following benefits are provided by vendors that can deliver security from the cloud:

Scalability & Speedy Provisioning:
SECaaS can easily adapt to the growing or shrinking needs of its customers and enables the quick provisioning and de-provisioning of users and devices.

Fast Updates & Uniform Protection:
With SECaaS, protections are continuously updated to provide the most current security defense, streamlining the updating process and reducing complexity.

Easy Policy Definition & Management:
Policies are centrally defined and managed, making them easy to push to users and devices regardless of physical location.

Web-Based Management Portal:
SECaaS providers should offer a management console that provides unified control of your managed services and real-time visibility into your security.

AGILITY, THREAT DETECTION, & RESPONSE

With the threat landscape growing more complex, managed security services remain a viable alternative for businesses that either cannot afford or cannot find the in-house expertise they need to protect their applications and data. From underneath the managed security umbrella, SECaaS has emerged with a combination of best-of-breed technologies that leverage the capabilities of the cloud to deliver cost savings, threat detection, remediation, and agility to companies of all sizes. While there are some similarities between the offerings of traditional MSSPs and MDR vendors, each is missing pieces of the puzzle, and customers are forced to either buy both types of services or lose out on the capabilities offered by one in favor of the other. The gap between the needs of companies and what many MSSPs are delivering has led to customer turnover and forced many to consider a new approach. For businesses perturbed by the rising cost and complexity of securing an increasingly interconnected, distributed environment in-house, a SECaaS vendor that provides an integrated bundle of services is an effective option. Instead of buying additional security technologies, organizations adopting a SECaaS solution can augment their security efforts and bolster their defenses.

PICKING THE RIGHT PROVIDER

SECaaS empowers businesses to focus on their core competencies. Hand off your security management to skilled professionals mandated to protect your environment 24/7/365. While choosing which security approach and provider is best for your organization, bear in mind the following considerations:

Know Your Needs:
The first step is to determine what your needs are as an organization and establish criteria for the provider that meets your security and regulatory compliance requirements. Also, carefully examine the gaps that may exist between your security controls and the ones provided by the vendor.

Incident Response:
SECaaS vendors that offer IR capabilities across on-premise, hybrid, and cloud environments can aid organizations by reducing both downtime and the amount of money that needs to be spent if there is a data breach.

Integrated Solutions:
If the SECaaS provider can offer multiple integrated solutions, organizations will benefit from the unified visibility and management across different security functions and environments, whether on-premise or in a public, private, or hybrid cloud. It also eliminates the CapEx that comes from buying new security technologies for more protection.

Price Points Matter:
Cloud computing is known for a lower cost of ownership, but it is not always delivered. Performing a price comparison for on-premise solutions and cloud service providers is an important piece of deciding which vendors and approach are best for you.

Vendor's Security:
Cloud providers should have high levels of security. Be sure to ask the vendor about how they will protect your data and access to their systems. his is particularly important for regulatory compliance reasons.

Check their Record:
If you are handing even part of your security mandates to a third party, it is always imperative to ensure they have a track record of excellent service. Customer support is vital with any managed security service, as is the experience of their staff. Ideally, the service will provide not only best-of-breed protection and expertise, but also solutions that deliver audit-ready compliance.

ABOUT ARMOR

Armor is a cloud security company that takes the complexity out of protecting your data, whether it resides in a private, public, or hybrid cloud—or in an on-premise IT environment. We provide managed security solutions that give you a clear picture of threats facing your organization. This allows us to provide you with the people and security resources to stop attacks before they happen and react quickly and effectively when they do, keeping your data safe and compliant. Wherever you are on your cloud journey, Armor can help. We make cybersecurity simple.

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167