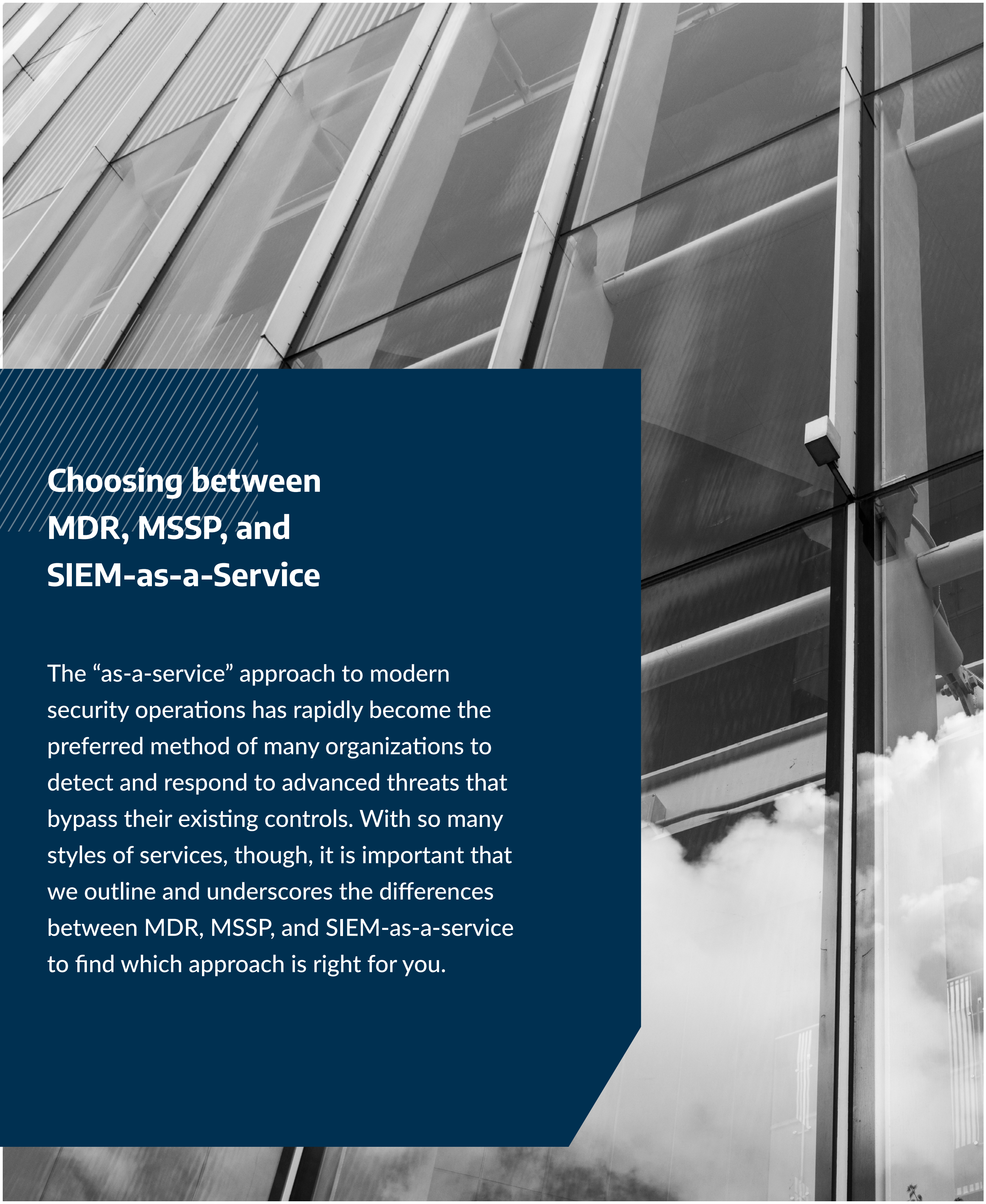
END CYBER RISK

WHITE PAPER

Choosing Between MDR, MSSP, and SIEM-as-a-Service

Table of Contents



Choosing between MDR, MSSP, and SIEM-as-a-Service

The "as-a-service" approach to modern security operations has rapidly become the preferred method of many organizations to detect and respond to advanced threats that bypass their existing controls. With so many styles of services, though, it is important that we outline and underscores the differences between MDR, MSSP, and SIEM-as-a-service to find which approach is right for you.

01

Cloud-Based Security Solutions Continue to Gain Momentum

As popular business applications are delivered through the cloud using a software-as-a-service (SaaS) model, security services are offered as a turnkey solution.

Demand for security operations solutions is driven by organizations of all sizes who are increasingly the targets of cyberattacks. These organizations realize that:

- There is an effectiveness problem caused by a shortage of cybersecurity skills among their IT staff, leaving them unable to detect and respond to advanced threats.
- Outsourcing portions of security strategy with a pay-as-you-go business model provides operational benefits.

According to Gartner, projected worldwide end-user spending is expected to grow to $304.9 billion in 2021 on public cloud services.[1]

$304.9B

Projected worldwide end-user spending on public cloud services.

18.4%

An increase from $257.5 billion spent in 2020.

The security-as-a-service market continues to outpace growth of the overall security space, which includes on-premises security product categories. The levels of cloud-based deployments of security controls vary considerably across different security technology segments. Security information and event management (SIEM) and identity and access management (IAM), and emerging controls such as threat intelligence enablement and cloud-based malware sandboxing, are increasingly adopted by organizations as a cloud-based security-as-a-service.

For some time, SIEM technology has been the go-to solution for many enterprises who need comprehensive visibility into cyberthreats across distributed IT infrastructure.

Yet, although these companies have large IT budgets for security staff and technologies, they've discovered SIEM solutions are capital intensive, complex, and cumbersome. For this reason, many firms gravitate towards managed security service providers (MSSPs), who–while helping

50%

of organizations will use MDR services by 2025.

$6 TRILLION

The expected amount of damages worldwide caused by cybercrime in 2021.

organizations monitor networks and systems and analyze threats–offer quick deployment and affordability through subscription models.

MSSPs, however, focus primarily on remote device management (configuring firewalls, intrusion detection and prevention systems, etc.) and spend less time on continuous threat detection and response. This means that by outsourcing the remote device management to third-party providers, organizations are obstructed from monitoring their own security posture and lose understanding of how best to respond to threats.

Managed detection and response (MDR) services arose to solve this problem. To some extent, MDR providers supply a cost-effective managed security operation center (SOC) to the midmarket. MDR providers part with the traditional MSSP model by providing a greater focus on threat detection and response. They recommend actionable responses to customers whenever remediation/mitigation actions need to be taken.

By 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment capabilities.[2]

02

SIEM: Powerful Technology, but Difficult to Manage

Large enterprises–especially those with large IT budgets for staff, process implementation, and advanced security technologies–have invested in SIEM solutions for years.

That's because SIEMs complete several critical functions, which includes:

ENHANCE: Overall transparency of network traffic.

DETECT: Threats or unusual activity that can elude other security controls.

STREAMLINE: Compliance reporting for regulated industries.

REDUCE: Time between detection and response for more effective incident response.

Because a SIEM collects log records from endpoint and network activity, security engineers have a complete record of everything that happens in a customer's IT environment.

This gives them the ability to identify indicators of compromise, malware intrusion, and other suspicious events. Having all log data in one place also simplifies compliance reporting. And finally, because every event is logged, a SIEM provides information security teams with the data they need to identify the origin of an intrusion, where it has spread, and the best way to respond to it.

Here's the problem: a SIEM is an expensive tool that takes up to six months to deploy.

It also requires 24x7 oversight from expert security engineers to work effectively. Many organizations who try to deploy and manage a SIEM on their own are unsuccessful, leading to a false sense of security from an improperly tuned solution. According to a Ponemon Institute research report[3], 70% of respondents say current SIEM technologies do not provide the most accurate, prioritized and meaningful alerts, which may be rooted in either technology failure or incorrect configurations.

61% of the respondents say they need a better understanding of the context associated with SIEM events, and 54% of respondents say a SIEM is "noisy" and generates a lot of low-level data and alerts that make it difficult to focus on what really matters.

What SIEM Users Are Saying

70%

say current technologies do not provide accurate alerts

61%

say they need a better understanding of SIEM events

54%

say SIEM is "noisy"

Some organizations have chosen to employ either a co-managed SIEM or a SIEM-as-a-service approach.

In this situation, a company purchases the SIEM technology and partners with a service provider who manages the SIEM on its behalf. This approach provides greater flexibility and control for the organization to define the outcomes it wants to achieve. Many SIEM-as-a-service providers have a deep understanding of their technology and can help in tuning and prioritizing alerts, however since their service tends to be strictly SIEM focused it is not ideal for organizations with a diverse security stack. A co-managed SIEM also tends to costs more than the MSSP and MDR options.

In this scenario, organizations pay both the capital expense of the SIEM platform, as well as the monthly cost for the service provider to manage it.

SIEM

PROS:

- High level of visibility in the environment
- Simplified Compliance and Reporting
- Service Providers have a deep understanding of their technology

CONS:

- Time consuming and costly to purchase, install, tune, and maintain
- High level of false positives and noise
- Service is limited to the SIEM itself and generally not the full security stack.

03

MSSP: Outsourced Security Management

Managed security service providers (MSSPs) is a common term for services that may focus on remote device management, vulnerability management, security event monitoring, and alerting.

These are generally seen as tier-1 level activities while MSSPs typically avoid the more complex tasks of triaging advanced threats, performing forensics analysis, and identifying networks and systems that are compromised.

Threat detection and response requires security experts with knowledge of the latest attack vectors, access to global threat intelligence, and in-depth knowledge of the customer's IT infrastructure.

MSSPs configure preventive security controls and provide basic alerts while the emphasis lies with the customers to perform their own triage, analysis, and response. System alerts are sent to customers, often without additional context or recommended containment and remediation actions. Customers choosing this model must already have the necessary security expertise to determine the validity of given alerts and take appropriate follow-up actions.

MSSP may be the preferred choice of organizations that feel they have adequate expertise within their staff but are simply overwhelmed with the more menial tasks of running their security operations.

In these cases, an MSSP would provide the lower level alerting and management of the environment while handing off the responsibility for any detailed analysis and response to the customer to complete.

MSSP

PROS:

- Remote management of common security technologies
- Works with your current security stack
- Incident Response retainers are often available
- Compliance reporting available

CONS:

- Advanced Analysis and Response is the responsibility of the customer
- Lack of context or guidance
- High level of noise since all alerts are forwarded to the customer
- Expertise must be provided by the customer

04

MDR: Outsourced Threat Detection and Response

While MSSPs and SIEM solutions may do some things really well, no security offering can do it all.

Because of this, many organizations struggle to piece together a complete picture of their cybersecurity strategy. Managed Detection and Response is designed to fill this gap and enhance customer security operations through guidance and support.

MDR providers tend to target two primary goals: 1) Providing security operations to organizations lacking in-house expertise and capabilities while 2) Augmenting established security teams who feel they are overwhelmed by events and need additional expertise.

MDR can be seen as a hybrid approach in many situations where technology alone is not enough to secure an environment. Managed detection and response providers will often invest heavily in advanced analytics, big data platforms, and emerging threat intelligence, as a means to eliminate much of the noise customers are experiencing and instead allow them to focus on only the true positive alerts. This requires these MDR provides to use their own experts to leverage the customer's security stack for the highest level of visibility and context.

Unfortunately, not all MDR adheres to the same standards. There are some providers who offer MDR services tied solely to the products they sell, offering to manage their endpoint or network tool as a form of "MDR". This is less an MDR solution and more of a managed tool service with limited visibility. In many of these cases, these providers have strict contracts that do not allow them to view or manage any tool outside of the one they are assigned to.

If you are considering MDR be sure to research the full scope of your providers service to ensure they are offering the greatest level of security operations.

MDR

PROS:

- Diverse technology support
- Expertise and guidance
- Eliminates noise and false positives
- Full visibility into the environment

CONS:

- Not all MDR providers are equal
- Requires some customer resources
- Technology is not always included

05

Security Operations: The Solution Modern Day Organizations Need

/// Arctic Wolf uses a cloud-based SIEM-like platform to collect and correlate log data and network flows from resources deployed on customer premises along with endpoint data.

Arctic Wolf provides experienced security engineers who focus on threat detection, forensics analysis, and prioritizing incidents for customers. Vulnerability assessment and compliance reporting is also part of the comprehensive solution.

To find out more, contact Arctic Wolf today. Experience the only purpose-built, cloud-native security operations platform.

Contact our cybersecurity experts to learn more.

CONTACT US

Arctic Wolf® is the leader in security operations and delivers the following capabilities above and beyond MDR:

Named Concierge Security® Teams (CSTs) for each customer account who act as trusted security advisors and extensions to customers' IT staff.

Hybrid AI (human-augmented machine learning), which provides 10X better threat detection with 5X fewer false positives.

Security optimized data architecture that dynamically scales, ingests, parses, and analyzes unlimited amounts of log data.

Customizable rules engine that enables CSTs to tailor services to specific customer needs.

Cloud monitoring of Infrastructure-as-a-service (IaaS) environments such as AWS Software-as-a-service (SaaS) environments such as Office365 environments and SaaS-delivered Access Management such as Okta.

Predictable pricing based on a company's number of employees, servers, and deployed network sensors.

[1] Gartner Forecasts Worldwide Public Cloud End-User Spending to Grow 18% in 2021; November 2020

[2] Gartner: Security Event Monitoring Options for Midsize Enterprises; 12 Oct 2017

[3] Ponemon Institute: Challenges to Achieving SIEM Optimization; March 2017

| Public

ARCTIC WOLF

END CYBER RISK

About Arctic Wolf

Arctic Wolf® is the market leader in security operations. Using the cloud-native Arctic Wolf® Platform, we help organizations end cyber risk by providing security operations as a concierge service. Arctic Wolf solutions include Arctic Wolf® Managed Detection and Response (MDR), Managed Risk, and Managed Cloud Monitoring—each delivered by the industry's original Concierge Security® Team. Highly trained Concierge Security® experts work as an extension of internal teams to provide 24x7 monitoring, detection and response, as well as ongoing risk management to proactively protect organizations while continually strengthening their security posture.

For more information about Arctic Wolf, visit arcticwolf.com

Contact Us

arcticwolf.com
1.888.272.8429
ask@arcticwolf.com