WHITEPAPER

Why Choose MDR over MSSP or SIEM?

SOC-as-a-service has rapidly become the preferred approach to detect and respond to advanced threats that bypass your existing controls. This white paper explains why, and underscores the differences between SOC-as-a-service, MDR, MSSP and SIEM.

Cloud-Based Security Services Gain Momentum with SMEs

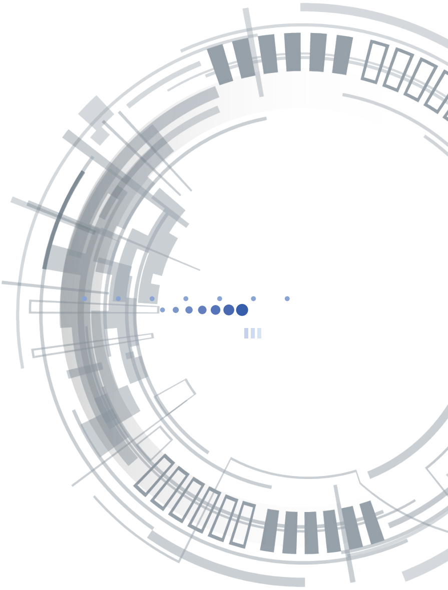
As popular business applications are delivered through the cloud using a software-as-a-service (SaaS) model, security services are offered as a turnkey security-as-a-service (SecaaS). Demand for SecaaS is driven by small to midsize enterprises (SMEs) who are increasingly the targets of cyberattacks. These organizations realize that:

1) There is a shortage of cybersecurity skills among their IT staff to detect and respond to advanced threats.
2) Outsourcing portions of security strategy with a pay-as-you-go business model provides operational benefits.

> “Demand for security-as-a-service (SecaaS) is driven by small to midsize enterprises (SMEs) who are increasingly the target of cyberattacks.”

According to Gartner[1], the cloud-based security market will be worth $9 billion in 2020, growing at a compound annual growth rate (CAGR) of 19.1%. 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 SMEs as a cloud-based security-as-a-service.

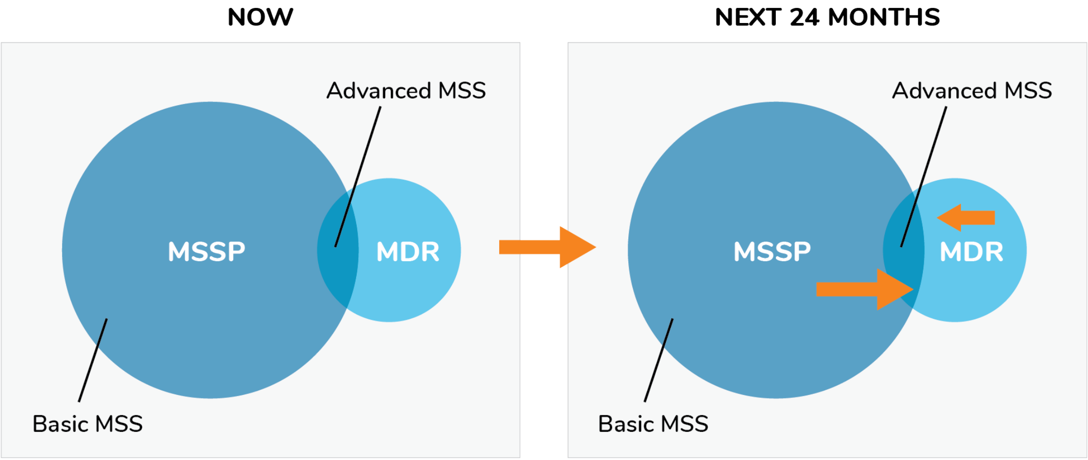
For some time, SIEM technology has been the go-to solution for large enterprises who need comprehensive visibility into cyberthreats across distributed IT infrastructure. Yet, although these companies have large IT budgets for security staff and technologies, they’ve discovered that SIEM solutions are capital intensive, complex and cumbersome. For this reason, many firms gravitate towards managed security service providers (MSSPs), who–while helping 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's 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.

According to Gartner[2], fewer than 1% of organizations have outsourced security services to MDR providers today. But by 2020, 15% of organizations will use MDR services, and 80% of worldwide MSSPs will offer MDR-type services.



Source: Gartner (May 2017)

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, including the following:

- **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 of every 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 24/7 oversight from expert security engineers to work effectively. Many SMEs who try to deploy and manage a SIEM solution on their own fail miserably. According to a 2017 Ponemon Institute research report[3], 70% of respondents say current SIEM technologies do not provide the most accurate, prioritized and meaningful alerts. 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

Some SMEs choose a co-managed SIEM, a hybrid approach where 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. A co-managed SIEM, however, 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.

MSSP: Outsourced Security Management that Lacks in Important Areas of Cybersecurity

Managed security service providers (MSSPs) focus on remote device management, vulnerability management, security event monitoring and alerting. MSSPs typically lack the necessary skills to triage advanced threats, perform forensics analysis, and identify 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 provide the following capabilities:

- **Off-the-shelf technology for a cloud-based or on-premises SIEM;** and in some cases, a co-managed SIEM owned by the customer
- **Remote device management** of security products, such as firewalls, intrusion detection/prevention systems, web/email gateways, Active Directory
- **Managed endpoint protection** (EPP)
- **Remote or on-site incident response** provided by a separate retainer
- **Continuous monitoring** of network traffic and log management
- **Regulatory compliance reporting**

Security Information and Event Management:

Pros

- Customers maintain complete control
- SLAs depend on in-house capacity to deliver
- Strong user and entity behavior analytics

Cons

- High upfront costs and complexity
- Up to 6 months to deploy and see value
- Requires 24x7 oversight of skilled security engineers

Managed Security Service Providers:

Pros

- Focus on remote device management
- Provide basic monitoring and alerts that do not require deep security expertise
- Managed endpoint protection via antivirus

Cons

- Limited knowledge of customer's IT environment
- Limited security skills (if any) for threat triaging and analysis
- Limited network monitoring capabilities

MSSPs configure preventive security controls and provide basic alerts, but they expect customers to perform their own triage, analysis and response. System alerts are sent to customers without any 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.

MDR: Outsourced Threat Detection and Response–and More:

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.

MDR providers target two primary groups of buyers: 1) small and midsize businesses with limited investments in security resources (tools/staff); 2) midsize enterprises that are investing in security resources, but seek partners to augment in-house capabilities

MDR services provide the following capabilities to end customers:

- **Proprietary technology stack for SIEM** included in service price
- **24/7 monitoring** of events/logs, suspicious activity, and alerts
- **Continuous networking monitoring**
- **Threat detection,** triaging, forensics analysis
- **Remote incident investigation** and response recommendations
- **Vulnerability assessments**
- **Regulatory compliance reporting**
- **Security advisors** who act as extensions of end-customers' IT and security teams

MDR service providers invest heavily in advanced analytics that leverage commodity big-data platforms like Hadoop, invest in elastic computing like Amazon Web Services, and subscribe to multiple third-party threat intelligence sources that track the latest attack vectors.

Managed Detection and Response:

Pros

- Focus on threat detection, triaging and forensics analysis
- 24/7 monitoring of network/systems, suspicious activity, and alerts
- Incident response with actionable intelligence

Cons

- No remote perimeter device management (firewalls, IPS/IDS, web/email gateway)
- Incident response requires the customer's participation
- Limited reporting ability outside of compliance or security-related functions, such as network performance or operations data

The following table captures the similarities and differences between MSSP and MDR providers.

Characteristics	MSSP	MDR
Security event log and context sources	Event source agnostic. Data sent to provider is determined by the customer.	Proprietary technology stack provided and network sensor deployed at customer premises.
Remote device management	Yes, vendor-agnostic for most common security controls (firewalls, intrusion detection/ prevention systems, web-gateways)—or tools deployed with MDR-type services.	Only for provider's own technology stacks.
Compliance reporting	Yes	Yes
Service interface	Portal and email act as the primary interfaces, with secondary access to analysts provided via chat functions and phone	Rely on more direct communication (such as voice or email) with analysts, rather than portals.
Incident response support	Both remote and on-site support provided by a separate retainer.	Lightweight, remote IR support typically included in basic services. On-site IR provided by retainer.
Incident containment	When remote. Manage all security controls for customer. Offer MDR-type services–such as managed endpoint detection and response (EDR).	Provided using technology stack or customer-owned technologies, leveraging scripts and APIs to programmatically make changes.
Service-level agreements (SLAs) for incident detection and response	Yes	Rarely

Source: Gartner[4]

Soc-as-a-Service: The Solution SMEs Need

A security operations center (SOC)-as-a-service is a turnkey solution that offers MDR capabilities and more. It uses a cloud-based SIEM platform to collect and correlate log data and network flows from network sensors deployed on customer premises. It includes 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 service.

Arctic Wolf offers the industry-leading SOC-as-a-service. The AWN CyberSOC™ service 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 and 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
  1) infrastructure-as-a-service (IaaS) environments like AWS
  2) software-as-a-service (SaaS) environments like Office365
  3) security-as-a-service (SecaaS) environments like Okta
- **Predictable pricing** based on a company's number of employees, servers and deployed network sensors

To find out more, contact Arctic Wolf Networks today. For an overview or trial deployment of AWN CyberSOC, please call 1-888-272-8429 or email at ask@arcticwolf.com.

[1]. Gartner Market Trends: Global Demand for Cloud-Based Security Is Growing Through 2020, Gartner, Published: 5 Apr 2017.

[2]. Gartner: Market Guide for Managed Detection and Response Services; 31 May 2017

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

[4]. Gartner: Security Event Monitoring Options for Midsize Enterprises, 12 Oct 2017

SOC2 Type II Certified

Contact us
arcticwolf.com
1.888.272.8429
info@arcticwolf.com