RocketCyber
A Kaseya COMPANY

HOW TO CHOOSE THE RIGHT MANAGED SOC SOLUTION

A Buyer's Guide for Selecting a Managed Detection & Response Solution

When it comes to cybersecurity, small and midsize businesses (SMBs) are constantly fighting an uphill battle — and the attackers always seem to have the advantage. While cybercriminals only need to successfully exploit one threat vector to land a hit, businesses have to detect and stop threats across a constantly expanding list of vectors, including email, endpoints, networks and the cloud. Having the right tools to detect and vanquish threats is vital for businesses to keep attacks at bay.

A Managed Security Operations Center (SOC), also known as a Managed Detection and Response (MDR) solution, is one of those tools. However, not every Managed SOC is the same, and they won't all align with the needs of your business. Since there are many things to inquire about and factors to consider when choosing a Managed SOC service, this guide will help you make the smartest Managed SOC choice.

TODAY'S THREAT LANDSCAPE IS FILLED WITH DANGER

The threat landscape businesses face today is rapidly evolving and more dangerous than ever before. Cybercriminals have become adept at mounting stealthy and sophisticated attacks that tax IT teams at companies of every size. However, SMBs are particularly ripe targets for their schemes for a variety of reasons, including:

- A lack of enterprise cybersecurity solutions in place. **One in three small businesses with 50** or fewer employees rely on free or consumer-grade cybersecurity tools for their entire cyber defense.
- The belief they won't be targeted because they are too small. However, **55% of ransomware attacks** now involve companies with fewer than 100 employees.
- A low level of investment in basic protective tools like firewalls or email security. In fact, **one in five companies** do not use any endpoint security whatsoever.

A CYBERATTACK IS AN EXISTENTIAL THREAT TO ANY BUSINESS

Many SMBs are undergoing digital transformation while struggling to hire the cybersecurity personnel they need to maintain security. At the same time, a challenging economy means everyone is working a little bit harder these days, including the bad guys. This unfortunate combination of factors creates a perfect storm of danger for SMBs, bringing potentially devastating results in its wake.

- An estimated **60% of SMBs go out of business** after being hit with a cyberattack
- Business financial losses from ransomware have grown **by nearly 70%**
- The cost of a data breach has climbed by 12% in two years to **a record-high $4.35 million**

WHAT IS MANAGED DETECTION & RESPONSE (MDR)

With MDR SMBs can turn cybersecurity management over to the experts in the form of a SOC. This provides knowledge and expertise without adding headcount costs and managerial overhead. The primary function of a Managed SOC is to rapidly analyze, detect and respond to cyberthreats that bypass traditional cybersecurity tools.

Comprehensive MDR will cover:

Endpoint security: Protect your endpoints with Windows and macOS event log monitoring, advanced breach detection, malicious files and processes, threat hunting, intrusion detection and third-party, next-gen AV integrations — at a minimum.

Network security: Gain new levels of network protection with firewall and edge device log monitoring integrated with real-time threat reputation, DNS information and malicious connection alerts.

Cloud security: Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and overall Secure Score.

In MDR, analysis is done by collecting information from a variety of sources like endpoints, cloud services and firewall logs. From this telemetry, trained SOC analysts can:

- **Investigate suspicious activities**
- **Proactively hunt for hidden latent threats**
- **Respond to and remediate early-stage threats**
- **Spot and stop cyberattacks**
- **Take care of problems before they become disasters**

HOW MANAGED SOC SERVICES FIT INTO SECURITY BEST PRACTICES

Turning to a Managed SOC to oversee cybersecurity needs goes a long way towards ensuring your organization is following cybersecurity best practices, including:

Taking a defense-in-depth approach: An organization practicing this tactic will have a variety of security tools and controls layered throughout their network, creating a more resilient barrier between cybercriminals and a company's systems and data.

Using a cybersecurity framework: Using one of the standard cybersecurity frameworks (CSFs) is an easy and effective way to ensure a company is covering all of its bases, especially if that company faces compliance requirements around information security. Some frequently used security frameworks include NIST, CIS and CMMC.

Moreover, leveraging a cybersecurity framework helps a business accomplish five major security goals:

IDENTIFY

Find security weak points where a company may be over or under invested.

PROTECT

Locate every possible vector that needs to be defended and take steps to add the right protection to keep cybercriminals from slipping through.

DETECT

Spot security problems before the bad guys do and thwart cyberattacks.

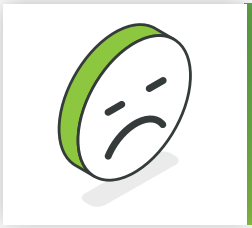
RESPOND

Take action to close security gaps and isolate threats quickly in emergency situations.

RECOVER

Get the business back on its feet with minimal downtime in the event of a cyberattack and repair damage from a security incident.

If the worst does happen, minimizing the time from discovery to recovery is the most important factor in keeping your business afloat.



*The global mean time to identify and contain an average data breach is **277 long, expensive days**. This climbs to 326 days if ransomware is involved.*

Investing in strong security and following security best practices is a smart, holistic and comprehensive way to set a company up for security success today and in the future. Taking an inefficient, one-off approach leaves dangerous security gaps, creates management challenges and adds unnecessary layers of complexity.

CHOOSING BETWEEN BUILDING A SOC OR LEVERAGING A MANAGED SOC

Many MSPs and SMBs envision building a SOC, only to discover how complex and costly a task it actually is. Leveraging a Managed SOC lowers the barrier to entry, making MDR easy and affordable. Keep these key points of consideration in mind when considering your options:

Personnel: Most SOCs are 24/7/365 operation centers. Creating your own means that you will need to have a large enough team on the payroll to handle its needs.

Availability: Many sophisticated attacks tend to start on a Friday evening while even more occur on holiday weekends. Ensuring personnel are available at off times or during holidays can be difficult and expensive.

Talent: Obtaining and retaining talent is a challenge. Unfortunately, the market demand for security professionals far outweighs the market availability. This drives up the cost of hiring cybersecurity professionals and makes it harder to keep trained experts on staff.

Investment: Advanced cybersecurity tools aren't cheap and can be costly to set up. For example, in a SOC, you'll need many defensive tools like threat intelligence feeds and malware analysis solutions, as well as experienced staffers who can utilize them to their fullest extent.

IDENTIFYING THE KEY CAPABILITIES OF A MANAGED SOC SERVICE

The right Managed SOC service will include these key capabilities:

- ✔ **24/7/365 service:** The SOC must be operational every hour of every day, all year long. This is the most crucial factor to consider since many attackers try and time their attacks when companies have less staff available, especially over holiday weekends — ransomware attack rates **climb by about 30%** during the winter holiday season.
- ✔ **Integrated threat intelligence:** Threat intelligence is the lifeblood of a SOC. Ensure the SOC you choose brings in multiple threat feeds to quickly identify the latest emerging threats.
- ✔ **Threat hunting:** To find and neutralize threats, a SOC must always have experienced cybersecurity analysts on hand. These experts will proactively hunt for latent threats and other security dangers that could be hiding in a company's network.
- ✔ **Expert analysis:** A SOC is only as good as its cybersecurity experts. Ensure the analysts and threat hunters your SOC relies on are true cybersecurity experts, trained to detect suspicious behavior as well as stealthy threats.
- ✔ **Time to resolution:** These days, it's less of an "if' and more of a "when" a company will face a cyberattack. Discovering a cyberattack quickly and limiting the damage that it does is critical to a company's survival. Ask how the SOC will respond to and remediate an incident.
- ✔ **SIEM-less log monitoring:** Find out if you're required to deploy a security information and event management system (SIEM) for the SOC to function. Ideally, you want to have a Managed SOC solution that does not require a SIEM — technology that can be very costly and cumbersome to manage.
- ✔ **MITRE ATT&CK alignment:** It's one thing to have a CSF in place but another to be able to leverage the MITRE ATT&CK framework in the event of an attack. Understanding how the MITRE ATT&CK framework can help prevent and mitigate cyberattacks is important for incident response.
- ✔ **Intrusion monitoring:** The right SOC will be able to detect suspicious activity in real time, including connections to terrorist nation-states and unauthorized TCP/UDP services, as well as backdoor connections to command-and-control servers.

EASY INTEGRATION OF THE SOC IS KEY FOR OPERATIONS AND COST EFFECTIVENESS

Cost is always a top concern when considering making security moves. You want to be sure you've got everything covered but you also don't want to pay for extraneous bells and whistles. Opting for a Managed SOC should save you money over establishing your own. To make it even more cost-effective, choose a Managed SOC that smoothly integrates with leading types of endpoint, networking and cloud solutions, including:

AV/AM Monitoring with Bitdefender, Cylance, Deep Instinct, SentinelOne, Sophos, Webroot, Windows Defender

Firewall Analyzer & Monitoring with Barracuda, Cisco Meraki, Fortinet, Juniper, pfSense, SonicWall, Ubiquiti, Untangle, WatchGuard

Email and DNS Monitoring with Graphus, Barracuda, DNSFilter, IRONSCALES, Microsoft 365, Google Workspace

PSA ticketing support platforms — a must-have integration to effectively and efficiently streamline security and operations activities

MAKE SURE YOU DON'T ENCOUNTER NASTY SURPRISES AS YOU GROW

A SOC that's merely "good enough" right now isn't the right solution. Your business is dynamic and ever-changing. You need a Managed SOC service that grows as you do, with simplified pricing that makes sense throughout your relationship. Pricing that's volume-based or by the terabyte leads to bills that balloon quickly. An ideal solution is priced by the number of endpoints you maintain, so as your endpoint infrastructure grows, you can manage costs along the way. This is especially important for MSPs as they pick up new customers and those customers' businesses expand and contract.

LOOK FOR WORLD-CLASS SUPPORT

Don't settle for weak support or a lack of innovation when you choose your Managed SOC. You should be able to discuss your security needs with your Managed SOC provider and feel comfortable asking questions. Your provider should also make an effort to keep you up to date on new integrations and what's going to happen in upcoming development cycles.

It's also critical to choose a Managed SOC provider that continues to innovate. The cybersecurity landscape is a fast-moving world, with new threats and risk factors popping up every day. Your SOC must be able to keep up with the changing demands of today and be ready to face the threats of tomorrow, so you can be confident that your security is in good hands.

TRANSFORM YOUR SECURITY WITH KASEYA'S MANAGED SOC

Stop advanced threats with Kaseya's Managed SOC — a world-class MDR solution that offers an innovative, affordable and effective way to power up your security. By partnering with us, you can gain access to an elite team of cybersecurity veterans that will help you hunt for threats and triage them. They will be available 24/7/365 to dive in immediately and work with your team when actionable threats are discovered.

Kaseya's Managed SOC includes:

Continuous monitoring: Round-the-clock protection with real-time advanced threat detection.

Advanced security stack: A 100% purpose-built platform backed by decades of experience, optimized for managed service providers and their customers.

Breach detection: Thwart sophisticated and advanced threats that bypass traditional AV and perimeter security solutions.

Threat hunting: Focus on other pressing matters while an elite cybersecurity team proactively hunts for malicious activities.

No hardware requirements: Patent-pending, cloud-based technology eliminates the need for costly and complex on-premises hardware

LEARN MORE ABOUT ROCKETCYBER | SCHEDULE A DEMO

About RocketCyber

RocketCyber, a Kaseya company, and its managed security operations center (SOC) platform, makes advanced threat protection easy and efficient. The RocketCyber cloud platform identifies malicious and suspicious activity that evades traditional cyber defenses and delivers round-the-clock monitoring to detect and respond to threats across endpoints, networks, and cloud attack vectors.