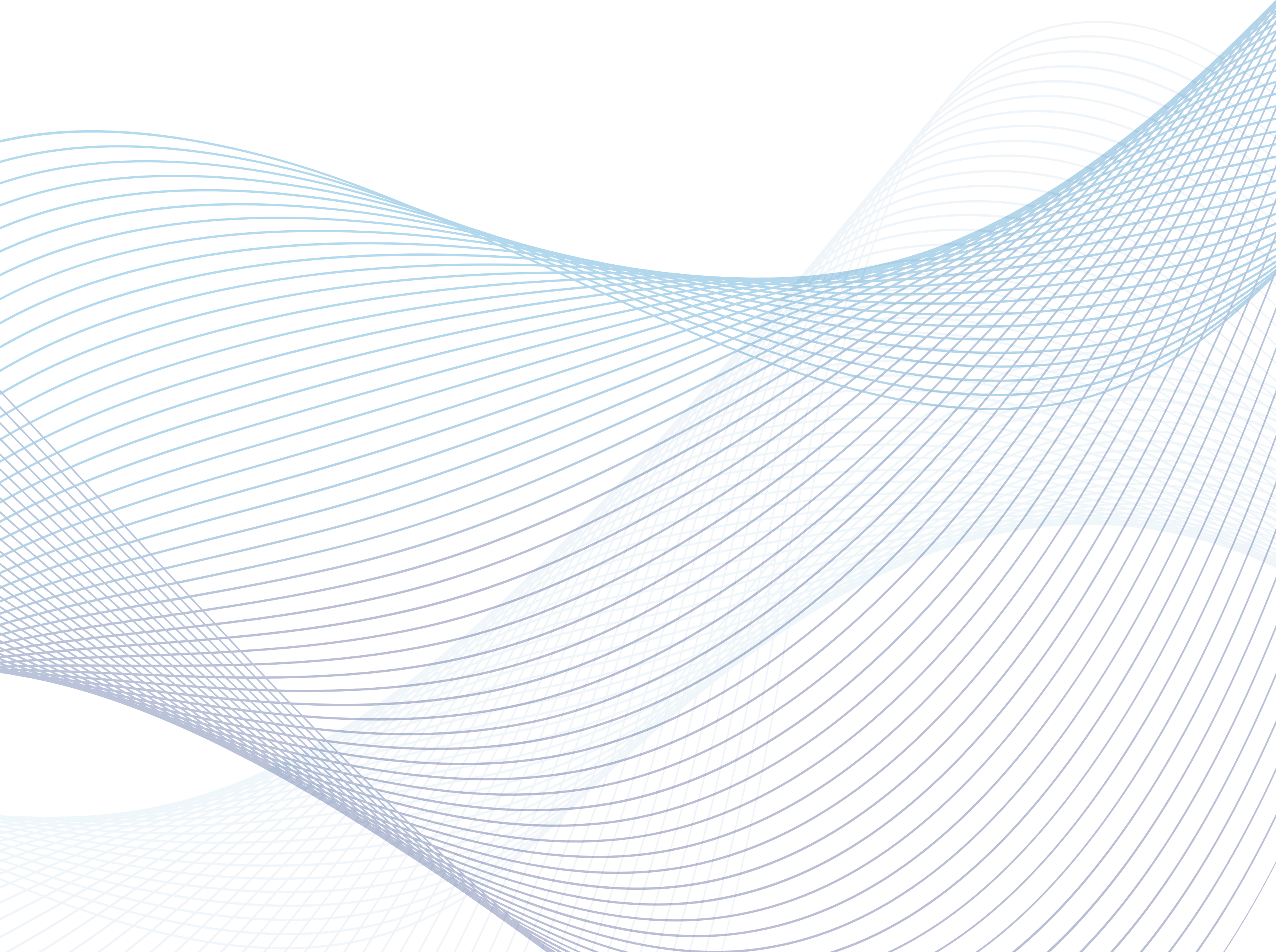
eSENTIRE®

5 Essential Questions to Ask Your Security Provider

And the answers you need to ensure your legacy MSSP can meet your long-term needs.



Introduction

Recognizing that defending against modern cyberthreats requires specialized technology and domain knowledge, many small and medium enterprises engage the support of Managed Security Services Providers (MSSPs). These providers promise a cost-effective way to detect and contain threats, allowing a company to meet governance requirements and focus on its core business.

Distinguishing between claims and reality.

However, not all security providers are created equal. Some undoubtedly have the combination of mature capabilities, a commitment to ongoing innovation and a modern, extensible platform to deliver the protection you need. Others focus on hypergrowth and customer acquisition, but aren't investing in the sustainable foundations needed to deliver what they're selling.

The right security provider quickly identifies and—crucially—contains attacks as they happen on your behalf, preventing breaches in real time; the wrong provider overwhelms your already overtaxed IT or security team with alerts and forces them to interpret the data and attempt to contain threats on their own.

How can you spot the difference and make the right decision?

Finding a security provider who will deliver to expectations—24x7, month after month, year after year—often comes down to knowing what questions to ask.

The Five Essential Questions to Ask Your Security Provider

#1 - How much of the threat surface does your platform cover?

Rapidly detecting threats and responding effectively requires coverage of the entire threat surface as any gap or blind spot provides an opportunity for threat actors to establish a beachhead and evade detection.

Today, covering an entire threat surface means security solutions must address:

- **Endpoints:** to protect against malware, fileless attacks, zero-day attacks and advanced persistent threats, to recognize suspicious or abnormal activity and to prevent lateral movement
- **Network:** to protect against brute force attacks, service exploits attempts, active intrusions, drive-by attacks, malicious connections and executables, port scans, DoS/DDoS attacks and web application attacks
- **Cloud:** to extend MDR capabilities into the Infrastructure- and Software-as-a-Service (IaaS and SaaS) domains
- **Logs:** to correlate multiple events into a single incident, to map threats to affected resources, to perform ad hoc queries on stored data for forensics and to accelerate investigations and decrease response times
- **Insider Threats:** to protect against advanced persistent threats and malicious insiders

Of course, prospective MDR security providers will simply say, “Yes!” when you ask them if they cover the entire threat surface, so be sure to ask for details and make them list—*and actually explain*—their coverage.

	ENDPOINTS	NETWORK	CLOUD	LOGS	INSIDER THREATS
COVERAGE	East/West (internal, lateral)	North/South (ingress/egress)	IaaS and Saas environments	Contextual awareness	Behavioral
FORENSIC CAPTURE	Endpoint telemetry	Packet capture and traffic metadata	Cloud provider logs and real-time telemetry	Multi-month archival	NetFlow, endpoint, DNS, logs

Collectively, these solutions cover the entire threat surface and equip security analysts with critical forensic data to aid in thorough investigation and rapid containment.

#2 - Is your security platform cloud native?

Delivering effective cybersecurity requires being able to consume a vast stream of telemetry and events from a wide range of signal sources (Question #1). It requires being able to process that data to identify attacks while avoiding false positives and false negatives (Question #3). It requires equipping a team of analysts and threat hunters with the tools they need to investigate and research advanced, evasive attacks (Questions #3 and #4). And it requires having the ability to continuously upgrade detection and defenses because, as we know, things are always changing.

These requirements demand a cloud-native security platform.

While “cloud ready” means that a solution can be deployed in the cloud, “cloud native” goes much farther: cloud native means a platform was architected, was designed and was built specially for the cloud.

Cloud native is about how a platform is developed, not about where it’s deployed. A cloud-native approach employs a service-based architecture in which processes and activities are self-contained and optimized to leverage the agility and flexibility afforded by the cloud itself.

In cybersecurity, a cloud-native platform offers important advantages over legacy approaches—advantages that provide real, important benefits for cybersecurity providers and the clients who depend on them. For example:

- A cloud-native architecture is more easily extensible, which means more features, sooner, to enable analysts and protect clients
- A cloud-native platform offers higher performance because the services inside it can maximally utilize the cloud’s compute, storage and network resources; this performance is necessary to ingest and process the growing streams of data which need to be processed to keep up with real-time threats
- A cloud-native platform can effortlessly scale to handle increased workloads without degradation to performance or client experience

Building a cloud-native platform takes time, expertise and investment—it requires completely rearchitecting systems and overhauling software development methodologies. This level of commitment means there’s no quick catch-up option for providers who’ve been left behind with legacy architectures.

For any one incident, or even over the short term, the difference between a cloud-ready platform and cloud-native platform might be tough to spot. But over the long term the gap between the two will grow as the cloud-native platform gains new capabilities, better equips human analysts and threat hunters, gracefully scales with new data sources and—ultimately—continues to provide defense against everything threat actors can throw at you.

#3 - How does your platform ingest and process data?

Mitigating risk requires a platform that can ingest and process information from critical sources, providing threat visibility across varied and dynamic environments.

To enable rapid detection and effective containment, the best combination is a cloud-native, machine learning-led platform plus expert security analysts who sift through the noise of thousands of alerts each day to hunt the real threats and disrupt them before they disrupt your business.

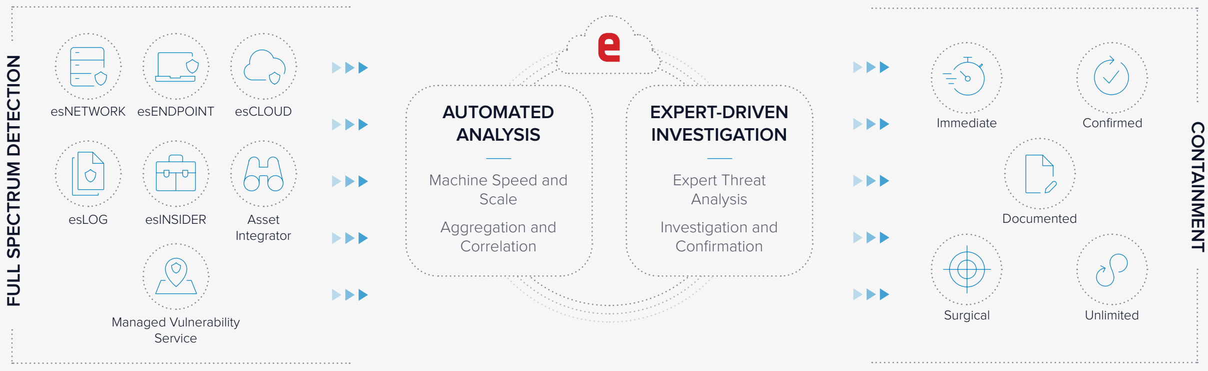
When evaluating potential security providers be sure to ask exactly how they ingest and process data from their customer base. What security tools are supported and how do they map to security visibility and response? What processes and technologies are in place? How are they continually improving their capabilities? What metrics monitor operational effectiveness?

Plenty of MSSPs and IT solution providers can deploy and manage security technology—but modern cybersecurity that can tackle today's evolving and evasive threats is less about operating security technology and more about analyzing data and enabling threat hunters and SOC analysts to respond and contain threats.

Only a combination of the right platform and the right people can deliver what's needed.

Full-spectrum coverage creates a constant stream of forensic data and telemetry from an expansive threat surface. In practice, a mid-market company can easily generate 10,000 alerts per day. Most mid-market companies can process—at most—500 to 1,000 alerts per day, but bear in mind that processing "only" 500 alerts per day requires an analyst processing at a little faster than one alert per minute for eight hours straight. Most IT teams are neither built nor staffed to perform this function. What about evenings? And weekends? Criminals don't adhere to the boundaries of the traditional workday. Your cybersecurity defenses shouldn't either.

SIEM vendors suggest that seeing thousands of alerts on a single pane of glass is the solution, but this approach does nothing to address the true foundational challenge: how can your security provider process a never-ending—and ever-growing—stream of security alerts with a zero-trust approach in mind? There's no point in outsourcing the problem of running the technology if the security provider can't deal with the problem of processing the alerts to enable their people.



Modern cybersecurity requires the ability to efficiently ingest and process enormous volumes of threat signals; the vast majority of MSSPs, private SOCs and self-proclaimed MDR providers simply aren't equipped to do so.

#4 - How do you respond to threats?

A key differentiator among security providers is how they define the term “response.” Unfortunately, for most, it essentially means they are processing alerts and sending “true” or “valid” alerts to your IT or security team. This puts the burden on your personnel to then conduct threat hunting, diagnose potential malware and understand how to remediate.

Minimizing threat actor dwell time is of critical importance, because skilled attackers can cause damage and exfiltrate sensitive data in short order. Consider that most criminals need only 15-25 hours to breach perimeter defenses, identify valuable data and extract it, and modern ransomware can rapidly spread throughout a network before being simultaneously activated.

An effective security response boils down to:

- Correctly identifying events which require a response, while eliminating false positives and false negatives
- Containing and remediating the threat, quickly and completely

A security provider who simply flips alerts over to you isn’t providing a real response; neither is a security provider who correctly diagnoses an incident, but then expects you to handle the actual response component.

Companies need real security partners who will identify events and proceed to contain and remediate them quickly. Of course, being able to do so is very much dependent upon how well-equipped the security provider is to ingest and process data, to conduct the necessary investigations and to leap into action.

Another important and related question to investigate is “How does the security provider respond to you?” If you were to call up the provider’s SOC hotline at 9:00pm and ask a question about a case in progress, how long would it take before you were speaking with a real expert who could take the time to thoroughly answer your questions and address any concerns.

Asking “How do you respond to threats?” and understanding the fine print—even for so-called “concierge” services—before you sign any agreements has the potential to prevent some unwelcome surprises.

MACHINE LEARNING + **EXPERT PEOPLE**

6
investigations every minute

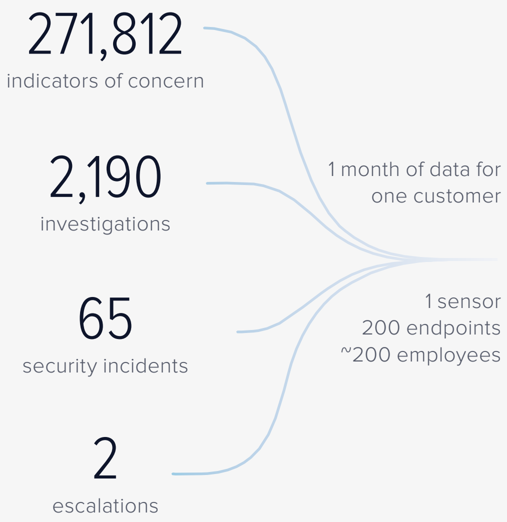
35
seconds to begin triage

20
minutes to isolation and containment

450
malicious IP addresses analyzed per day

646
confirmed security incidents per day

400+
new indicators of compromise (IOCs) per day



271,812
indicators of concern

2,190
investigations

65
security incidents

2
escalations

1 month of data for one customer

1 sensor
200 endpoints
~200 employees

eSentire equips world-class SOC analysts with advanced technologies to enable rapid, effective response to cybersecurity threats.

#5 - How do you overcome the cybersecurity skills gap?

Essentially, modern cybersecurity requires a combination of advanced threat detection technologies, extensive processes to monitor and react to the signals generated and recognized by those technologies and—most importantly—expert analysts who decide if and when a response is needed.

Many MSSPs and companies who try to build a private SOC capability find out the hard way that operating and scaling an effective SOC requires overcoming a major hurdle: the global cybersecurity skills shortage—estimated by (ISC)2 to have surpassed four million professionals.

To put this in perspective, staffing a SOC to achieve 24x7x365 coverage requires a minimum of 12 people once you factor in paid time off, sick leave and employee churn. And that's simply providing a minimum of one analyst at all times. It's reasonable to wonder how your security provider can guarantee that your alerts are being reviewed by skilled professionals.

Operating a SOC in this environment and over the long term demands a mature approach to talent recruitment and retention. At eSentire we employ a six-point methodology we developed over the last ten years which includes:

- Establishing a talent pipeline to maintain access to cybersecurity professionals despite the global shortage
- Taking care of your SOC analysts to prevent the burnout which is the number one problem cited in surveys of cybersecurity professionals
- Establishing quality assurance processes to help analysts grow while also ensuring customers receive the best possible service
- Investing in tools and technologies to continually improve operational effectiveness, efficiency and human-machine collaboration in the face of ever-increasing threat signals
- Providing continuous education and certification support to help SOC analysts level-up with new skills and credentials
- Providing career advancement opportunities whether someone is interested in deep technical growth, a managerial path or exploring other roles within the organization

In normal operating circumstances, these programs ensure your security provider can out-recruit and outperform MSSPs and private SOCs. In trying circumstances—including natural disasters and unforeseen events—the operational foundation laid by these programs is vital to maintaining cybersecurity service continuity.

eSentire isn't an MSSP that just bolted on MDR. We're the category creator with the depth, breadth and customer trust that comes from nearly 20 years of proven success.

We pioneered development and operation of effective, resilient, and world-class SOCs **(learn more)** ★

Boasting a world-class Net Promoter Score of 72

Customer retention is 97%

Understanding MDR

Managed Detection and Response means different things to different people, which creates real confusion when you’re trying to find the right MDR partner.

Read The Definitive Guide to MDR to learn about:

- The current marketplace definition of MDR
- Technical criteria and detailed questions to evaluate MDR providers
- The strengths and weaknesses for each of the seven categories of MDR

This instructive eBook will help you make more informed cybersecurity choices that align with your business objectives, in-house security resources and risk tolerance levels.

eSENTIRE

The Definitive Guide to
Managed Detection and Response (MDR)

Balancing Risk, Cost and Capabilities.

eSENTIRE®

About eSentire:

eSentire, Inc., founded in 2001, is the category creator and world's largest Managed Detection and Response (MDR) company, safeguarding businesses of all sizes with the industry-defining, cloud-native Atlas platform that removes blind spots and enables 24x7 threat hunters to contain attacks and stop breaches within minutes. Its threat-driven, customer-focused culture makes the difference in eSentire's ability to attract the best talent across cybersecurity, artificial intelligence and cloud-native skill sets. Its highly skilled teams work together toward a common goal to deliver the best customer experience and security efficacy in the industry. For more information, **visit www.esentire.com** and follow **@eSentire**.