COMCAST BUSINESS | MASERGY

Security Services RFP Questions

Finding a Trusted Partner for Detection & Response

Table of contents

Click to jump to the section of interest

Introduction

IT leaders are increasingly aware of the security risks and resource limitations they're up against today, which is why a large majority of mid-size companies lean on Managed Security Services Providers (MSSPs) or Managed Detection & Response (MDR) services to step up their security posture. These providers can be a big help given what companies face these days.

Security Challenges Today

- **More attack surfaces:** Work-from-anywhere business models have widened attack surfaces with cloud apps and infrastructure, mobile and personal devices, smaller and more distributed remote offices, and business partners all heightening risks
- **Clever threat actors:** With the increasing number of security attacks, including rising ransomware threats, every business is now a target for cyber criminals — not just large or mid-size companies managing intellectual property and customer data
- **Strategic vision impediments:** Many mid-market companies lack even basic security programs leveraging widely accepted security frameworks.
- **Financial limitations:** 24/7 security monitoring and response operations are required today, but it is expensive and time consuming to build this capability in-house
- **Operational hurdles:** Finding qualified security talent to staff security operations is challenging in today's competitive marketplace

With this low starting point, you'd think it would be easy for an outside provider to step in and provide meaningful value. But the truth is that many MSSPs and MDR services fall short on the job. The biggest provider pitfalls include...

Biggest Provider Pitfalls

- Security alert factories that overwhelm clients with often poorly triaged and un-actionable to-do's
- Insufficient incident resolution — even when alerts pass a triage test, the security analysts and their processes don't exhaustively drive the incident to final resolution
- Under-skilled analysts lacking experience with the ever-growing list of security tools as well as the expanding IT environment
- Underwhelming services and customer experiences, including phone support staffed with script readers
- Limited service level agreements, making it hard to hold providers responsible for under performing response times

So, how do you ensure you're getting the right combination of expertise, operational excellence and effective security tech stack all in one provider? This evaluation framework includes RFP questions to help you upgrade your provider.

What an Effective Provider Looks Like

Both MSSPs and MDR providers must be able to assist clients with a comprehensive approach — not just more alert-generating security products. An effective approach must entail:

- **Process:** Security operations and service delivery based on best practices and proven frameworks, as well as automation technologies to speed response
- **Expertise:** Cyber risk management mindset, with highly qualified security analysts that have a passion for helping customers and fighting cybercrime
- **Technology:** A flexible yet quick-to-deploy tech stack must enable the detection and response mission across all environments and work with existing tools

What most mid-market leaders struggle with are sound security processes based on proven frameworks and focused on the specific risk management needs of the business. Worse, most companies don't have any formal security program in place, and that's a fundamental roadblock for managing cyber risk. Gartner's "Market Guide for Managed Security Services" sums this up well by advising that an effective security program is: "60% process, 30% expertise, and 10% technology."

Effective security programs are

60%
process

30%
expertise

10%
technology

Process

Evaluating a provider's operations and service delivery

When it comes to a security attack, time is not on your side. The longer it takes your team to contain the threat, the more damage and cost to your business. And if 50% of your employees work from home it typically takes 58 days longer to identify and contain a breach. This explains why MSSPs and MDR providers must be able to quickly and efficiently detect, respond, and also recover.

58 Days

The additional time it takes to to identify and contain a breach when employees work remotely

Providers should also help clients build and improve their security program, aligning it with the customer's chosen security framework. These are some of the most well-respected security frameworks, which should serve as a general game plan for your provider that the customer team has chosen to follow.

Frameworks for Your Security Strategy

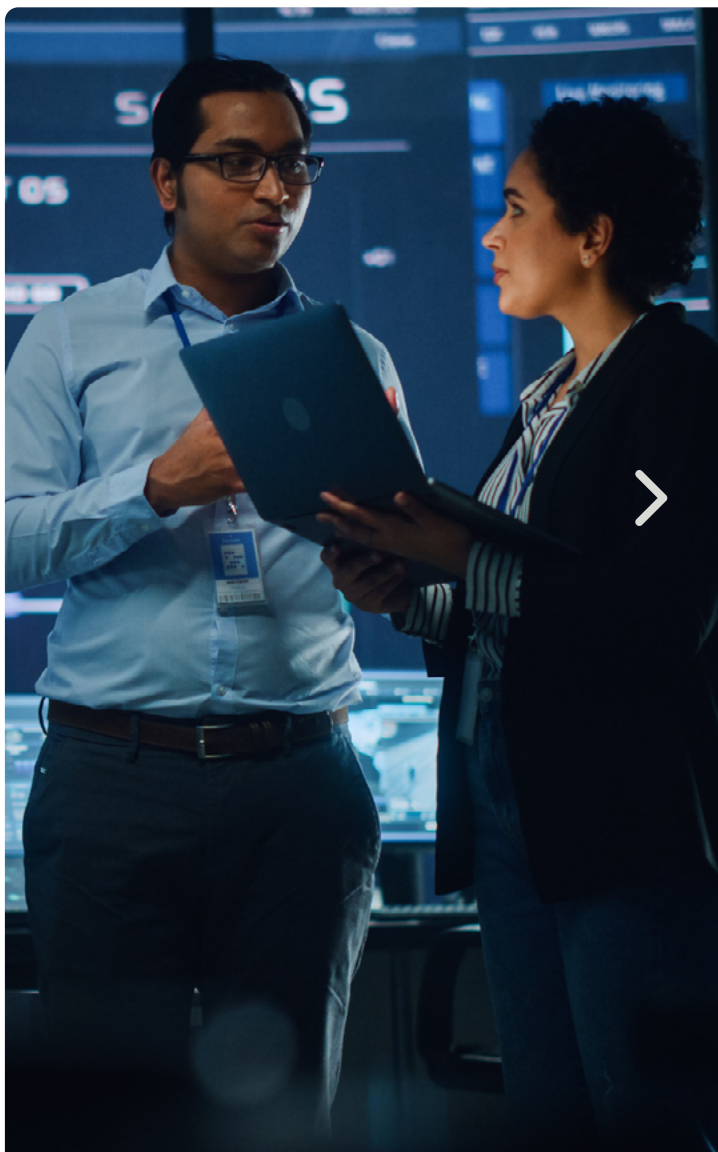
National Institute of Standards and Technology: Cybersecurity Framework
The most widely adopted framework for comprehensive security programs.

Center for Internet Security: The 18 CIS Critical Security Controls
More prescriptive than the NIST CSF (above), but arguably this framework is easier to understand and implement. It's often a good starting point for organizations without any security program in place.

Forrester Research: Zero Trust
This strategy complements the base frameworks above and is for more "security mature" organizations ready to implement Zero Trust practices. It's also the most effective strategy for managing cyber risk, but can be disruptive to existing practices and norms.

Operations and Service: Key Questions to Ask

- **Guiding Strategies:** How does your provider use industry standard security frameworks as a guiding strategy for client programs?
- **24/7 Service:** Does your provider have global Security Operations Centers (SOC) and locations for "follow the sun" services? Do these SOCs support any regional privacy requirements, such as GDPR compliance regulations?
- **Proven Processes:** Does your provider bring a balance of mature incident response processes and the need for adopting new techniques with expanding scope of security tools and attack vectors? How are newly recognized threat indicators recycled into the customer based continuous improvement?
- **Customizable Processes:** These same proven processes must also support some degree of customizability to support specific client's needs. Can your provider integrate with your ticket system? Do they have flexible processes that fit with your own corporate standard operating procedures or compliance needs?
- **Easy to Work With:** Does your provider deliver prioritized alerts, consumable insights, and clear action items to explain incidents and mitigate threats? How will they help you make security control adjustments to prevent similar incidents in the future? Are the providers' analysts laser focused on solving the security incident at hand?
- **Effective Response:** Can your provider share their defined incident response process for each type of tool or threat — i.e. endpoint, cloud, network? How do they automate response (e.g. carefully with critical decision points always landing with skilled analysts, not script)? Do they use contextual enrichment or SOAR technologies (i.e. Security Orchestration Automation and Response tools)? What SLAs or commitments does the provider make in terms of urgent threat notifications and responsiveness? What are their mean time to detect and contain metrics?
- **Support Systems:** Will you have a single point of contact for expert security support?



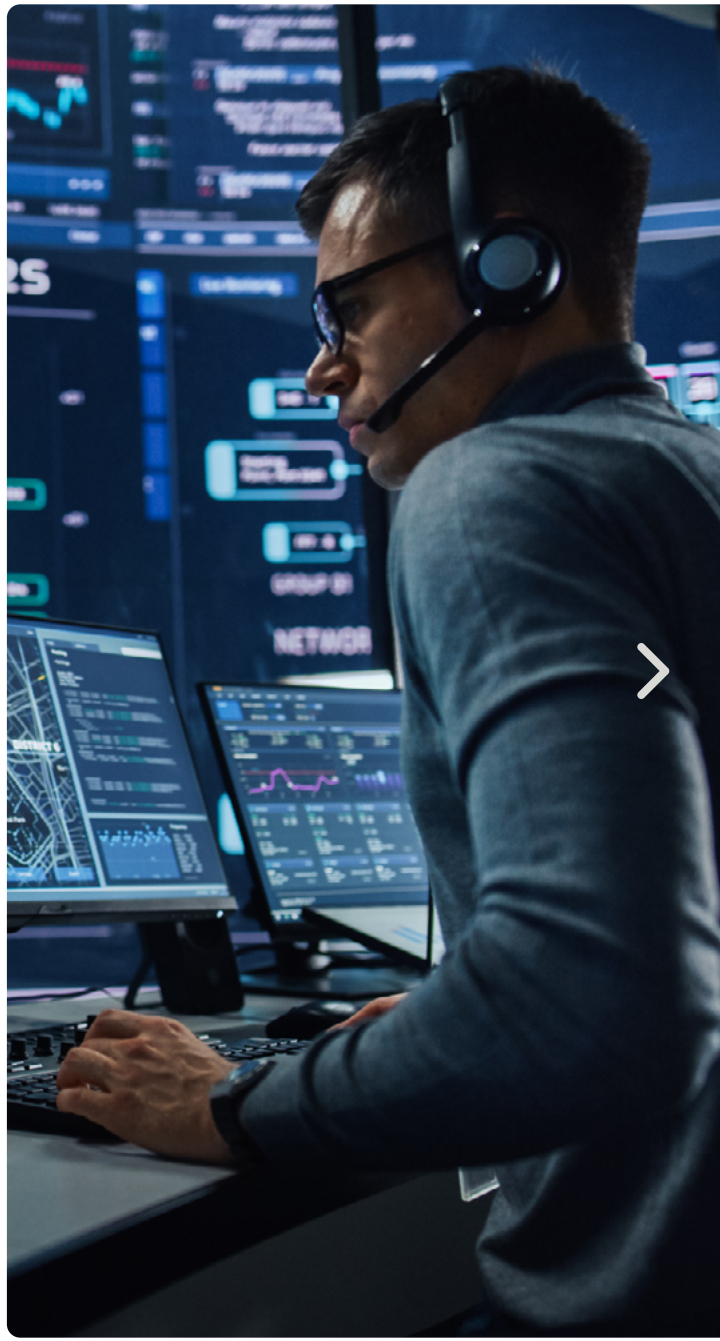
Expertise

Evaluating the ability to source & train security talent

The rubber meets the road with the quality of the providers' security analysts. Professionals make or break the overall effectiveness of the managed security service.

Talent: Key Questions to Ask

- **Talent Quality:** Does the provider have a defined strategy for hiring and retaining the best security talent? What level of talent will answer the phone when clients call with an urgent question?
- **Certified Analysts:** What is the average tenure of your provider's analysts and what certifications do they hold? What continual training programs do they offer their analysts?
- **Strategic Review:** Does your assigned analyst(s) take the time to understand your business and its specific security risks? Do they bring needed expertise to the table to help you with continual improvement of your security program (see security frameworks) for continual improvement, ultimately shifting to a proactive, instead of reactive, mindset?
- **Experience:** How long has your provider been handling security for clients in your industry? Who are they working with currently and will they serve as a reference?
- **Compliance:** What do they know about your compliance needs?



Technology

Expanding tools and creating a consolidated tech stack

Over the last decade plus, the Managed Detection and Response service segment has sprung up because of the clear need. Nearly all organizations can use help — not just large enterprises. The highly asymmetric nature of cybersecurity has proven that protection strategies, while still mandatory, do regularly fail. Hence the need for catching the attacker's kill chain with detection and response, before major damage is done in the form of data exfiltration. This requires a specific technology strategy.

While most large enterprises have the budget, expertise, and resources to figure out the required tech stack on their own, largely all mid-market companies cannot. Therefore, they rely on providers to bring these capabilities to the table in a manner that is non-disruptive, fast to deploy, and cost effective — not always an easy task.

Having said that, most mid-market companies have already made significant security investments and it makes enormous financial and operational sense for the security provider to leverage these existing tools as much as reasonably possible. The goal: consolidate point solutions to create a holistic approach to security. Establish a unified threat management platform where all alert information and log data comes together and is evaluated by an advanced analytics engine and optimized to deliver a correlated picture of your security posture and prioritized list of identified threats.

Tech Stack: Key Questions to Ask

- **Flexibility with Existing Tools:** Can you reasonably leverage your existing security technology investments like next-gen firewalls and endpoint security? Or do you need to rip and replace your tools?
- **Monitoring the Entire Environment:** Does the provider's tech stack monitor and cover:
  - **Endpoint:** Endpoint Protection and Endpoint Detection and Response Services — Too many "Detection and Response providers" are really just managed Endpoint security providers and don't have coverage beyond the endpoint
  - **Cloud:** Iaas with Cloud Workload Protection and SaaS with Cloud Access Security Brokers (CASB) technologies
  - **Network:** Network Detection and Response, including visibility tools, next-generation cloud firewalls, secure web gateway, Intrusion Detection & Protection Systems: IDS/IPS, or even SASE solutions that combine SD-WAN with a toolbox of network security technologies and services
- **Consolidation and Analytics:** How does the provider consolidate all tech-born data feeds into one management system, applying machine learning and behavioral analytics to drive correlation faster, more intelligent detection and response?
- **Deployment:** Does the provider's tech stack deploy quickly leveraging cloud technology and with minimal disruption? Does the provider have a well-defined deployment strategy which leverages cloud infrastructure as much as possible, but recognizes that sometimes CPE is needed?

- **SIEM:** Does the provider offer a turnkey managed SIEM technology or service? Even with advanced machine learning security analytics, SIEM remains foundational for any effective security program, and if you don't have one (including via your provider), you are not setting yourself up for success. Does the managed SIEM support out-of-the-box security tool integrations? Can it support your log search and investigation needs? Does it scale well, including across geographies?
- **Zero Trust Capabilities:** How can the provider help you gain insight into user-based and identity analytics as well as gain control over application-level security policies and network-level enforcement? Do they offer Zero Trust Network Access capabilities?
- **SOAR Automation:** Does the provider enable its security operations center with SOAR technologies?

Understanding SOAR: Importance and Best Practices

Correlation is key to success, and SOAR tools help tie everything together. They serve as the glue that brings the strong points of each individual technology into one environment. SOAR systems are where incident analysis and triage are performed through a combination of AI-based intelligence and human investigation. Using SOAR, security teams define, prioritize, and drive standardized incident response activities through digital workflows. Moreover, they can leverage the technology to automatically respond to security threats, keeping analysts focused on only the most urgent and important events.

While SOAR is not always a customer-facing tool, it undoubtedly improves the efficiency and effectiveness of security analysts. It should be carefully implemented with critical decision points always landing upon the experience of the qualified analyst—not automation script. Look for evidence that the provider has thoughtfully implemented automation so that “mistake automation” isn’t also a consequence.

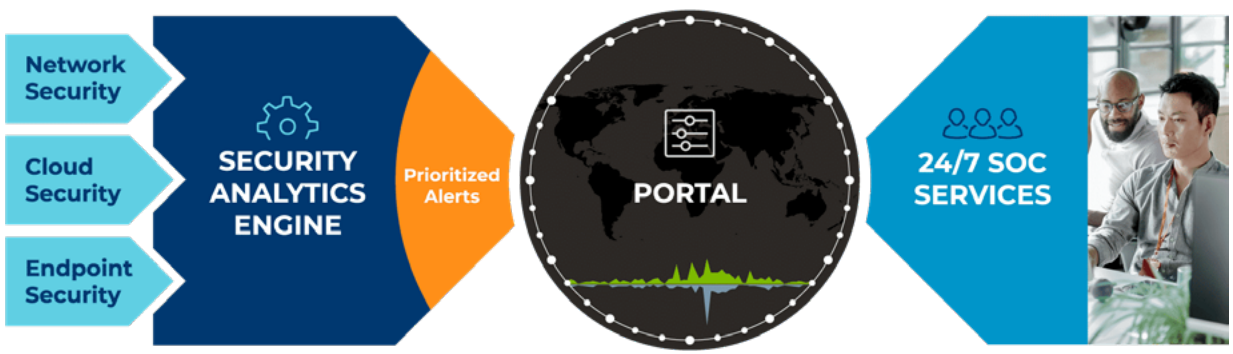
True Partners Should Be Effective Business Enablers

Any IT leader that finds themselves “pumping” or even “slamming the brakes” on their digital transformation initiatives every time a security issue comes to light likely doesn’t have the right security controls and program in place. Ultimately, the organization is responsible for committing the resources and leadership oversight needed to implement a formal security program. However, with a program in place, the provider should be a valuable asset to ensure the appropriate technology, process, and expertise is in place to proactively manage cyber risks that come with the digital transformation strategy.

For example, many mid-market companies are aggressively adopting Software as a Service. However, SaaS also creates risks such as phishing attacks and data loss that must be addressed proactively, otherwise it’s inevitable that a security breach will happen. A provider that offers CASB coupled with response services, understands these risks, and puts the appropriate security controls and practices in place for the organization, ensuring effective risk management and success of the digital transformation strategy. This enables executive confidence in their strategy and ultimately accelerates the business plan.

Masergy Has Your Security Services Covered

There is a lot of confusion and overlap in the market regarding the different types of security services: Managed Security Services (MSS) versus Managed Detection & Response (MDR) versus Security Operations Centers (SOC) services or SOC as a service (SOCaaS). This guide can help untangle the differences. At the end of the day, Masergy covers all three of these arenas with security technology, expertise, and process all in one solution.



Learn more about Masergy's Managed Security Services.

GET A FREE CONSULTATION

About Masergy

Masergy, a Comcast Business company, is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.