MASERGY

WHITE PAPER

The managed security services provider survival guide

WHAT YOU'LL LEARN

- How to know when you're not spending enough on security
- The difference between traditional security services and managed detection and response
- Three primary criteria for evaluating managed detection and response providers

Do you need a survival guide to find the right Managed Security Services Provider (MSSP)? Don't get stuck in "analysis paralysis." Forrester Research and Masergy joined forces to help IT professionals navigate the world of outsourced security services and managed detection and response solutions. The following is a summary of a webinar with Masergy V.P. of Security Craig D'Abreo and Forrester Principal Analyst and featured speaker Jeff Pollard, who offer insights and recommendations for enterprises seeking to understand the MSSP market and how to evaluate providers.

Introduction

Today's threat landscape is a highly asymmetric battlefield that heavily favors the attacker. To survive, most organizations need security partners with a comprehensive solution set including advanced machine learning as well as incident response plans backed by 24/7 continuous monitoring. But the security services market has become so saturated that it can be difficult to decide who should be trusted to protect your most important asset--your company data. Choosing an MSSP can also be daunting, because the selection process is about more than just the features of a given cybersecurity solution. It's a contract to deliver services over a number of years, and once selected, you're committed to learn to work with your MSSP.

The differences: security monitoring services versus detection and response services

While most enterprises are familiar with managed security services that provide 24/7 monitoring and distill masses of security system log (syslog) alerts down to a small number of action items and follow-up tasks for IT teams, many professionals are still familiarizing themselves with managed detection and response services (MDR). MDR expands the scope of security monitoring services by helping customers not just identify the top-priority alerts but also respond to them, taking real action.

MDR benefits

MDR is advantageous for one simple reason--it helps enterprises cover more ground. While it is perhaps obvious, it deserves the call out: It covers detection and response, driving to incident resolution. Instead of budget battling between investments in detection, prevention, and response, MDR covers it all. You have both detection and response capabilities within the service and technology suite.

The Business Case for MDR

Even with traditional security monitoring services augmenting their efforts, IT departments still struggle to stay afloat. Executives continue to find their teams overtasked and understaffed, according to Forrester's Data Global Business Technographics® Security Survey.

The goal with managed detection and response is that someone is taking an active role inside your environment and performing actions that you have given them permission to perform. That's very different from traditional services, which simply monitor alerts and create a prioritized list of action items.

Security Ops struggle to stay afloat

64% find that day-to-day tactical activities take up too much time.

62% say their security team is understaffed.

64% say they adopt SaaS security offerings because the rest of their environment is already outsourced.

Source: Forrester's Global Business Technographics® Security Survey

The rise of MDR: market evolution

The continually overtasked IT team is one of the key reasons MDR is an industry on the rise. Enterprises have been interested in as-a-service solutions, and many purchased technology that they simply couldn't support from a personnel and skill sets perspective. With the rapid expansion of the security industry offering endpoint visibility and control, enterprises began realizing the need for the extra security coverage; however, many couldn't run those technologies on a 24/7 basis. Therefore, investments were underutilized and not optimized. As these dynamics collided along with the recent rise in cybersecurity and ransomware attacks, the stage was set for MDR. Enterprises were asking their partners for more help, and providers were more than willing to serve those needs. Adding response tasks to their list of offerings is often a natural extension of their business model.

Three primary criteria for evaluating MDR partners

Given that partners are now being trusted to act on behalf of enterprise IT teams, executives should deepen their evaluation criteria and look for additional characteristics in their service partner.

- **The threat intelligence lifecycle:** How does your company arrive at its threat intelligence, and how is it incorporated into the response strategy?
- **Experience in execution:** Can your service offer best practices in response plans and do you have mature processes backed by service level agreements?
- **Commitment to the mission of security service:** How do you create a culture of service? Are you primarily (or originally) a software company or services company?

"I'd say if you're spending less than 10% of your IT budget on security, you're blissfully ignorant. If you're spending 11-20% or 21-30%, you're starting to become more aware of what's happening."

Jeff Pollard, Principal Analyst, Forrester

Security spending: how much is enough?

While no amount of spending will ensure total security, a Forrester report provides helpful insights in demonstrating how much IT spend is likely NOT enough. A study titled Security Budgets 2018: Uncertainty Trumps Normalcy finds that companies that spend between 0-10% of their IT budget on security have low situational awareness and poorer visibility into their security posture.

Security Blindness

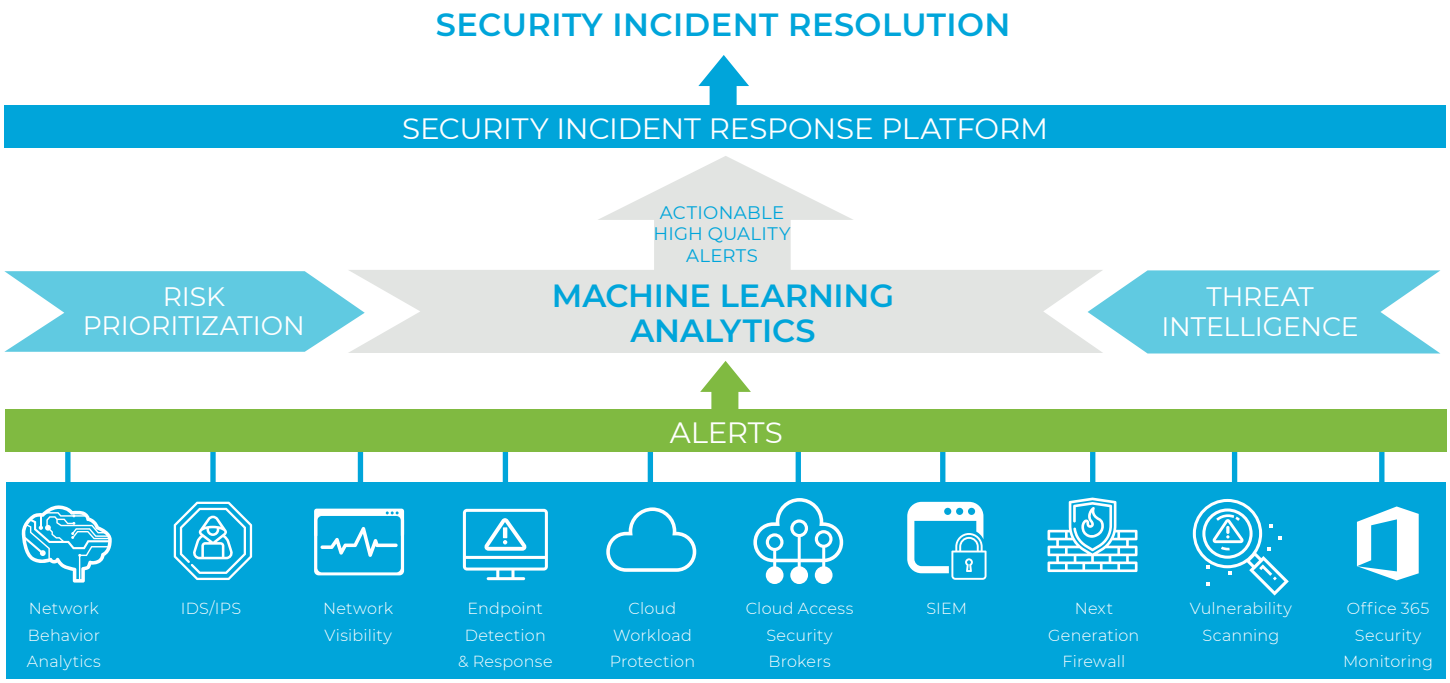
0-10%
IT spending

Security Awareness

11-30%

Detection and response service: a holistic ecosystem

As the scope of traditional security services expands, so too does the framework of service offerings. Today's comprehensive detection and response solutions are more holistic ecosystems. Take Masergy's MDR solution as an example:



"You'll notice a theme throughout the entire Masergy Managed Security Services platform—we take in various sources of security data and the goal is to correlate that information with other pieces of data coming into the platform," said Craig D'Abreo, V.P. of Security at Masergy. "We believe this is an extremely important piece of any advanced security infrastructure."

Detection and response: case studies

MDR alerts to Wanna Cry attack

- **Customer:** Financial services organization
- **Detection:** Patches for each operating system were available prior to the Wanna Cry outbreak, and most organizations were vulnerable without the patch. Behavioral analytics detected suspicious activity on unpatched machines across the network.
- **Response and further investigation:** Analysts acted quickly to quarantine the infected host and utilized DNS logging and additional vulnerability scans to identify what other machines could be susceptible to this attack.

"We didn't have a specific security signature looking for this activity. This all came up as a result of behavioral analytics. Masergy's deployed sensors revealed the anomalous behavior. It allowed us to determine something suspicious was going on," recalled D'Abreo. "This case is a great example of how people, process, and technologies must work together to build the most effective detection and response program."

CASB system flags HIPAA violations

- **Customer:** Healthcare company
- **Detection:** CASB (cloud access security broker) data leakage prevention alerts flagged activity as a potential HIPAA violation. Using OneDrive (a sanctioned application for file sharing) an employee accidentally shared files and personal health information with a third party.
- **Response and further investigation:** Masergy immediately quarantined the files and built additional custom policies and data leakage prevention alerts to detect any future activity on unstructured data. Security training programs were also amended.

"CASB solutions provide very helpful data containerization capabilities that can be used to prevent situations like these," explained D'Abreo. "Job functions may require employees to view certain files with sensitive information, but when it comes to copying and pasting that information into other third-party systems, technology should stop the user. With data containerization, you can do just that."

Cloud workload protection defends against phishing

- **Customer:** High-tech company
- **Detection:** Cloud Workload Protection recognized a new workload engaged in command and control activity and flagged it as an unusual anomaly.
- **Response and further investigation:** Masergy shut down the rogue instance and quarantined the user account. Additional forensics determined the workload was initiated by an unauthorized user account, created after a phishing attack gained customer credentials.

"There's really no way to organically monitor security activity within cloud infrastructures," added D'Abreo. "This is why our customers deploy Cloud Workload Protection in every single one of those instances within their virtual private cloud environment. Not only can you run vulnerability scans against each of the instances, but you can also set up very specific configurations for security monitoring."

Conclusion

Service partnerships have become the common approach used to survive and mitigate cybersecurity risks today. Backed by professional teams, IT leaders are better positioned to deliver on tactical security demands and supply their organizations with the specialized talent needed to respond to evolving security threats. MSSPs act as an extension of the enterprise IT team, underlining the importance of making a wise selection. In the end, managed detection and response is more than just securing an endpoint or monitoring a network. Security partners are active defenders of intellectual property and should be experienced responders committed to the mission of service.

About Masergy

Masergy 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.

Packet Fusion

Ellen Pensky
ellen@bumblebeemarketing.net