Nemertes

Better data. Better decisions.

MSSP Buyers Guide

What to look for in a modern managed security services provider.

By John Burke, CTO

Johna Till Johnson, CEO

Nemertes

November 2021

© Nemertes 2021

Table of Contents

Introduction: An MSSP Is in Your Future **- 3 -**

From Anywhere to Anywhere On Anything *- 3 -*

What To Look For In An MSSP **- 4 -**

Structure and Stability: The Power of Mature Process *- 5 -*

Expertise and Stability: Constellations of Cybersecurity Stars *- 5 -*

Structure and Expertise: Guidance on Security Models and Frameworks *- 5 -*

Expertise: Knowledge and Experience *- 6 -*

Stability: Relationships Driving Resolution *- 6 -*

From AntiX to ZTNA: A Well-Stocked, Intelligent Toolchest **- 6 -**

Integrate, Orchestrate, Automate *- 7 -*

Tools That Learn Not to Trust: AI Driving Security *- 7 -*

Defending the High Ground: The Advantages of Position *- 7 -*

Risky Business: Busines Risk Should be the Center of MSSP Thinking **- 8 -**

Conclusion and Recommendations **- 8 -**

ISSUES AND QUESTIONS: AN MSSP CHECKLIST **- 9 -**

© Nemertes 2021

Introduction: An MSSP Is in Your Future

Organizations of all sizes face a major challenge: how to provide solid cybersecurity without adopting an open-ended expansion of the cybersecurity staff, toolset, and budget.

Security challenges continue to broaden even as risks deepen. It was challenging enough securing a traditional enterprise environment consisting of users in company facilities accessing resources in company data centers over company networks, with a sharply defined perimeter between the enterprise and the rest of the Internet. That world no longer exists.

From Anywhere to Anywhere On Anything

The new world is much harder to secure:

- Since 2020, more than half—56% then, and climbing—of enterprise workloads run outside enterprise data centers, split roughly evenly between SaaS and IaaS/PaaS, and typically across multiple vendors in each category.
- During the pandemic, the majority of office staff shifted to working remotely, and even though some will return to work, many will not. Nemertes' *Next-Generation Networking 2021-22 Research Study* finds 33% of staff will continue to work remotely. And many that do return to work will be working from the office only part of the time; on average, staff will work remotely 39% of the time.
- Use of personal devices on company WLANs is common, nearly ubiquitous.
- Intelligent devices continue to take up residence in corporate networks (part of the "Internet of Things") and many are designed with little concern for security.
- The agile and DevOps revolutions have made direct manipulation of infrastructure by developers and applications far more common, and further reaching, both increasing risk and decreasing the time cybersecurity teams have to react to compromises.

Against the backdrop of this open intermingling of environments, devices, and populations, the world of bad actors has evolved dramatically as well. In a context of fully mature black markets for vulnerabilities, exploits, infrastructures from which to launch attacks, and even fully baked attacks delivered in a SaaS model, enterprises need to defend not just against old-fashioned cyber-criminals, malware, and attempts to steal protected information but also against ransomware and state actors and non-governmental hactivists.

To be sure, the cybersecurity industry is keeping pace, with a defense for every attack and a mitigation for every risk. Point solutions spring up like mushrooms after spring rains, established solutions sprout new capabilities, big companies buy small companies. The marketplace gets steadily more complex, and enterprise security environments do too.

Unfortunately, the market is not doing such a bang-up job of producing security professionals to sort through, select, deploy, and wield this mighty arsenal. Cybersecurity experise is hard to find and steadily more expensive, especially in the areas, like cloud and IoT, where enterprises are most

© Nemertes 2021

likely to get out over their skis and open up threat surfaces without sufficient knowledge to mitigate the new risks.

And as hard as it is to find—and afford!—appropriately skilled staff, it is harder still to get enough of them to staff a 24/7 SOC able to provide robust incident response per guidance from NIST and basically everyone else.

As a result, most enterprises have cybersecurity teams that are smaller than they need. Those undersized teams are pulled in three directions:

- responding to incidents
- managing existing security infrastructure and processes including normal monitoring
- implementing new initiatives including deploying and becoming expert in new technologies

The result is typically an endless game of "whack-a-mole" with no prize for success. Deployment and integration of each new wave of technologies typically precedes complete normalization of the preceding wave and its associated changes to practices and process.

52%

Successful companies based on MTTC are 52% more likely to have a SOC than their less successful counterparts.

As importantly, many security professionals still situate all their thinking about security, unconsciously, within a mental context that is no longer correct and useful. Perimeter-based thinking is stubbornly persistent, leading among other things to difficulty embracing the idea of Zero Trust ("Why should I go to 'deny-all' communications security amongst our own servers—aren't they all friends?") and difficulty seeing how to implement it ("That is a lot of ACLs to constantly manage, or too many firewalls.").

As a result, all but the largest and best-resourced organizations struggle with successfully implementing cybersecurity via a fully-insourced model. Having a SOC (security operations center) correlates strongly with success (based on the median total time to contain, MTTC, a threat). Successful companies based on MTTC are 52% more likely to have a SOC than their less successful counterparts. But most organizations can't afford to staff or manage a SOC, and for those companies, an externally managed SOC, i.e. one that's part of a managed security services offering, is the answer. Companies with fewer than 2500 employees see an improvement in MTTC of 50% when moving to an externally managed SOC.

50%

Companies with fewer than 2500 employees see a 50% improvement in MTTC when moving to an externally managed SOC.

The conclusion? For most companies, the best option going forward is to partner with one or more managed security services providers (MSSPs).

What To Look For In An MSSP

A managed security services provider is still a managed services provider, and one should seek in an MSSP all the things one seeks in any other kind of MSP: structure, expertise, and stability. These manifest in several ways.

© Nemertes 2021

Structure and Stability: The Power of Mature Process

An MSSP should structure its work internally and its work with you around rock-solid processes, well defined and fully documented, from on-boarding through all phases of delivery, until offboarding (should it occur). This is as much for their benefit as yours. Solid processes allow them to more easily bring their new staff up to speed on how to do things correctly without disrupting the services delivered. Solid processes should also help the MSSP meet all SLAs and be able to show that services are, verifiably, delivered in accordance with your specific requirements, because those requirements have been properly documented and communicated.

Maturity is important. It means the provider has learned how to deliver a service consistently. But, that level of comfort and familiarity with a standard way to do things makes it easier for the MSSP to also safely bend those processes to meet a given company's specific needs, integrate with their unique processes. (This can't and shouldn't be without limit, of course; one of the big reasons to outsource to an MSSP is to take advantage of their ability to do things well, and under-cutting that by making them adhere to incumbent processes arbitrarily —which, let's face it, were not meeting needs in some important ways or why the outsourcing?— is a waste of the opportunity.)

To achieve this broad and deep bench, the ideal MSSP will have good staff retention and great programs for training and certifying staff.

Expertise and Stability: Constellations of Cybersecurity Stars

One major advantage of working with an MSSP is that it can maintain the kind of deep bench of expert staff most enterprises can't. This ensures continuity of service in the face of staff turnover and means there are extra pairs of hands available to help in an emergency. Further, if it is not a specialist operation focused on one particular piece of the puzzle (e.g. factory floor security) it will also be maintaining some depth of support across a broad spectrum of security areas and solutions categories.

To achieve this broad and deep bench, the ideal MSSP will have good staff retention and great programs for training and certifying staff.

Structure and Expertise: Guidance on Security Models and Frameworks

Across industries, cybersecurity professionals are expected to be familiar with security operational models, threat taxonomies, and controls frameworks promulgated by both government and independent standards organizations. For example, the National Institute of Standards and Technology (NIST) has published scores of standards documents including the 800 series, on cybersecurity concepts such as secure software development or supply-chain risk management, and the 1800 series on cybersecurity practices such as securing industrial IoT. These, along with publications and models from the Center for Internet Security, the Cloud Security Alliance, the MITRE Corporation, and others, define the common vocabulary and conceptual framework of modern cybersecurity. An MSSP should be able to guide clients in improving their alignment with such standards, and as needed help staff adopt and get comfortable with the appropriate concepts, vocabularies, and processes.

© Nemertes 2021

Expertise: Knowledge and Experience

Relevant to the client's enterprise, that is. In searching out an MSSP partner, each organization should strive to find one that understands and has experience helping secure companies in their industry. Especially for financial services and healthcare, vertical-specific (and even sub-vertical specific, e.g. banking vs. insurance) compliance requirements are crucial considerations in planning and managing cybersecurity.

Similarly, an ideal MSSP will also be familiar with the cybersecurity and compliance implications of the enterprise's specific business practices. If the company processes credit card information, the MSSP should understand PCI DSS. If it is a healthcare provider, the MSSP had better know its HIPAA from its HITECH. A manufacturer? The MSSP had better understand the cybersecurity implications of ISO9001, and ISO27001:2013 Annex A. Although the controls and mitigations different kinds of enterprises are ultimately responsible to have in place are overlapping subsets of the same broad set of practices and tools, it is crucial that the people managing your security know which ones pertain to you specifically.

And, the ideal MSSP will have experience dealing with the different compliance regimes that apply based on where the enterprise operates. Requirements will vary by country, state/province/etc., and even by city in some regions.

Stability: Relationships Driving Resolution

As with most managed service provider relationships, an enterprise can work best with an MSSP when the teams they work with, both account management and technical, are stable; that is, that they get to work with the same people over time. This sort of relationship should minimize the enterprise's need to escalate concerns above their usual points of contact, but the relationship should have a well-defined escalation mechanism anyway.

When the MSSP has to act in response to a compromise, an attack, or a new vulnerability, it should be focusing ad-hoc communications on that action. It should explain what has happened to trigger the response, what they have and have not done in response, what they plan yet to do, and what actions they need the customer to take. At the end of the resolution, the MSSP should close the loop with the client by reviewing how policies and controls should change, if necessary, to reduce the risk of a similar compromise in the future.

From AntiX to ZTNA: A Well-Stocked, Intelligent Toolchest

In addition to having staff familiar with the full spectrum of relevant cybersecurity technologies, an enterprise should expect an ideal MSSP to be able both to supply any needed tools and to work with tools an enterprise already has on hand. Getting the MSSP to leverage the customer's existing investments in tools, such as SIEM and ticketing systems can reduce spending on the MSSP and improve portability should the customer decide to seek a different provider. It can have the added benefit of increasing the "stickiness" of staff assigned to that account, since they will have trained on a tool not standard to the MSSP.

An ideal MSSP should be able both to supply any needed tools and to work with tools an enterprise already has.

© Nemertes 2021

On the other hand, it also makes it harder for the MSSP to maintain the depth of staffing the customer desires—it undercuts the advantages of playing to the MSSP's strengths. Providing its own tools lets the MSSP leverage its own investments not just in the tool but in staff trainings, experience across its customer base, and certifications.

An ideal MSSP should work with on-premise, cloud, and hybrid tools to defend all staff working anywhere using all services from anywhere.

A full-service MSSP should be able to work with on-premise tools, cloud tools, and hybrids in defense of the typical combination of on-premise, mobile, and remote staff utilizing a hybrid service delivery environment. It should ideally have experience with the full spectrum of security technologies, from foundational technologies like endpoint protection and security information and event management (SIEM) to newer systems for providing zero-trust network access (ZTNA) or sandboxed web access in a secure web gateway as a service.

Integrate, Orchestrate, Automate

The MSSP should have experience not only with the tools in their silos but also with knitting them together using security automation and response (SOAR) systems, and applying behavioral analytics to the mass of log data created across all environments to help drive a robust managed threat detection and response (MTDR) service. The SOC and ultimately the customer must not spend time worrying over anomalous but unthreatening events, nor on real attacks quashed by automatic defenses.

Tools That Learn Not to Trust: AI Driving Security

Deep analytics, applying machine learning and artificial intelligence techniques, are the only scalable and sustainable solution to the problem of identifying the events requiring human attention and response amid the sea of notifications and alerts an infrastructure will generate. They also power any real approach to zero trust, providing for ongoing updates to the granular trust map that undergirds zero-trust based on observed behavior in the environment. Zero trust means zero implicit trust, including not assuming something in the network is still trustworthy just because it was when you let it connect initially. The all-environments perspective is crucial, given the proliferation of multi-channel attacks. Analytics can provide the end-to-end visibility into behavior across all networks and within systems that can drive decisive action at the optimal place: on the endpoint, in the WAN, the LAN, the data center, or the cloud.

MSSPs that are themselves one of the enterprise's cloud or network service providers can secure that service more deeply than third parties can reach.

Defending the High Ground: The Advantages of Position

Some MSSPs can also bring to bear additional security services and functionality based on the advantage of their position. If they are themselves one of the enterprise's service providers, they can take security on the service deeper, below where third parties can reach. An IaaS or network services provider can address some threats at the physical level, for example, by isolating the hardware used to serve the customer.

© Nemertes 2021

They can exercise packet-drop options anywhere in their infrastructure, from ingress to core to egress, not just at a customer edge.

Moreover, a service provider can see what is happening across their whole infrastructure, not just the parts serving this one customer. This visibility allows them to pour additional relevant data into their cybersecurity machine learning and AI systems. That broader knowledge of real threats and attacks in the wild can then inform the trust map of a customer's zero trust deployment, accelerating their development of institutional immunity to new infections without themselves having to experience an infection.

Risky Business: Busines Risk Should be the Center of MSSP Thinking

As with any in-sourced cybersecurity, an MSSP should center its activity on risk. It should, with the customer, prioritize protections, services, and mitigations based on risk assessment. That assessment, both the initial pass during onboarding and ongoing refreshes thereafter, should focus on risks faced by the specific customer enterprise, informed by industry-specific threat intelligence, the experiences of other customers, and the vulnerabilities it finds in the customer's systems and processes. With a risk-based approach, cybersecurity leaders can frame the discussion in financial terms: balance the costs of defense, mitigation, response, and recovery against the projected financial impacts associated with various attacks and compromises. Risk as translated into potential financial impact also makes an effective metric for gauging the effectiveness of security programs and improvements in security posture, and an important factor for leadership to weigh in new and transformative digital business initiatives.

A business risk approach frames cybersecurity as balancing defense, mitigation, response, and recovery costs against the projected financial impacts of attacks and breaches.

Conclusion and Recommendations

An ideal MSSP

- Brings with it all the virtues of any good MSP in terms of staffing and process maturity
  - Staff training programs, solid retention, long account tenures
  - Documented escalation paths, SLAs
- Wields a broad and robust cybersecurity toolset, expertly
  - Brings their preferred or works with your preferred; premise, cloud, and hybrid
  - Gets staff certified with key tools
  - Uses AI- and ML-powered analytics crossing all service environments
- Provides well-structured and responsive SOC and MTDR services
  - Works with standard and custom playbooks for incident response
  - Utilizes a security orchestration, automation, and response solution
- Monitors and secures resources across all the environments the enterprise uses to provide IT services: multiple external clouds, private data centers, and enterprise edge resources
- Monitors and secures access for all user populations whether on premises, remote, or working in a hybrid of the two, and across the enterprise's entire geographic footprint

© Nemertes 2021

- Takes a risk-centered approach to planning, executing, responding to, and reporting on cybersecurity posture and events
- Understands the cybersecurity implications of the customer's industry, business practices, and geographical footprint and has other customers of similar size and footprint
- Can do more than just provide managed security services, opening the possibility of deepening the security surrounding another key service

IT and cybersecurity professionals evaluating MSSP options should seek all those things, evaluate multiple possible partners (including combinations of partners), and seek a short-term initial engagement to make sure the relationship works before signing longer term contracts (presumably at more favorable rates).

About Nemertes: Nemertes is a client-centric research-based advisory and consulting firm that analyzes the business value of emerging technologies. Since 2002, we have provided strategic recommendations based on data-backed operational and business metrics to help enterprise organizations deliver successful technology transformation to employees and customers. Simply put: Nemertes' better data helps clients make better decisions.

© Nemertes 2021

MSSP CHECKLIST

Relationship Foundations

- ☐ **Staffing and Skills:** Ask how many staffers will be assigned to your account, how many other accounts each staffer supports, and their specific skills and technology certifications. How long do staff typically stay with an account and with the MSSP?
- ☐ **Industry and business expertise:** Ask the provider to demonstrate expertise in your industry, ideally both via reference accounts and through a thorough demonstration of knowledge of relevant regulations and compliance requirements.
- ☐ **Geographic familiarity:** Has the provider worked in your geographies, and is it familiar with the relevant privacy regulations (e.g. GDPR) or other compliance requirements that apply?
- ☐ **Relationship management:** Ask the provider to walk you through their onboarding and offboarding processes, including any aspects specific to your industry, location, and practices. Ask if they can help transfer your services from an existing MSSP (e.g. get custom runbooks and scripts, transfer software licenses, and ensure destruction of any of your data the old MSSP may retain).

Strategy

- ☐ **Risk-based approach:** What is the provider's approach to assessing and communicating risks? Ask what sources it draws on, (e.g. which industry threat intelligence feeds, how many other customers' experiences). How does it assess and prioritize risk mitigations? How does it communicate all this?
- ☐ **Incident resolution approach:** Have the provider describe in detail how it addresses incidents, including escalation path, proactive notifications, responses, and after-action adjustments to policies, systems, and processes.
- ☐ **Proactive improvement approach:** How does the provider help you improve your overall cybersecurity posture and processes? How does it leverage industry standards from NIST, CIS, CSA, the ISO, and others? How are suggestions for improvement communicated?

Services

- ☐ **SOC and MTDR:** Do you provide complete service—monitoring, detection *and* response—without customer assists, or do you only assist in response, or only advise on response
- ☐ **Environment coverage:** Which components of your environment does the provider protect? Endpoint, network, cloud, on-premises?
- ☐ **Intelligence feeds:** To which intelligence feeds does the provider subscribe? How are they integrated into its solutions?
- ☐ **Passive response vs. active threat-hunting:** Does the provider conduct threat-hunting? What is its process for doing so?

Tools and Technologies

- ☐ **Toolset options:** Does the provider supply all relevant tools? Will it work with your existing toolsets? Is a flexible mix of BYO and provider-supplied an option?
- ☐ **Automation:** What type of SOAR and other solutions does the provider bring to bear to accelerate responses to incidents? Do they have standard runbooks? If so, can they be customized? If not, how do they work with clients to develop custom runbooks?
- ☐ **ML, AI, and analytics:** What types of ML, AI, and other analytics does the provider bring to bear, and in which scenarios?
- ☐ **Metrics and dashboarding:** Which metrics does the provider report on? How are they tracked? What type of dashboarding does the provider use to communicate them?

© Nemertes 2021