ARCHONONE
INFORMATION TECHNOLOGY SOLUTIONS

BAE SYSTEMS
INSPIRED WORK

Managed Security Services buyer's guide

Introduction

Managed Security Service Providers (MSSPs) are responsible for protecting an organization's critical data and ensuring that they avoid data breaches. Thus, choosing an MSSP is an important decision that requires a careful, thorough assessment of the options. This whitepaper provides a useful framework to help prospective buyers assess MSSPs. It also provides helpful, probing questions that companies can use to vet potential providers.

MSSPs provide fully managed security services, not just security technology. Therefore, it is important to assess the three key elements of comprehensive managed security – technology, processes, and people. This whitepaper starts with what buyers should look for in a provider from a high-level, company perspective, then uses the "technology, process, people" framework to help buyers assess potential providers.

MSSPs help customers reduce costs and complexity, reduce information security risk, and reduce the compliance burden. This whitepaper will help customers reduce the amount of work and complexity involved in deciding which MSSP best meets the needs of their organization.

Table of Contents

Company

Company

Analyst validations

Start by looking at providers that are included in Managed Security Services reports by major analyst firms such as Forrester and Gartner. Providers included in these reports have the necessary industry experience, meet minimum customer requirements, and meet critical MSSP technology and service requirements. Analyst reports also highlight the strengths and weaknesses of providers and can help buyers choose a provider that meets their unique needs. Beware of providers that are not included in analyst reports – this may indicate that they lack industry experience, fail to meet the minimum customer requirements, or fail to meet technology and service requirements to be considered a true MSSP.

Questions to ask providers:

- Is your company featured in analyst research reports on MSSPs?
- Does your company meet the minimum customer requirements to be included in analyst reports?
- Does your company meet the minimum technology and service requirements to be considered a true MSSP by analyst firms?
- What are your company's strengths and weaknesses according to analysts?

Customer focus

Some MSSPs focus on serving global enterprises, others focus on mid-market or small to midsize businesses (SMBs). Some also choose to focus on a particular industry such as financial services or healthcare and optimize their solutions to meet the unique security and compliance needs of companies in these industries. Look for an MSSP that focuses on serving companies that are (1) your company's size and (2) in your industry. This will ensure that their solution is optimal in terms of product offering and price.

MSSPs that focus on SMBs offer inexpensive security solutions but lack the advanced security and compliance capabilities that larger players provide. MSSPs that focus on large enterprises have strong security capabilities but are often very expensive since they have global infrastructure to support. These providers also have a history of customer service issues for smaller customers.

The provider's core business is another important consideration. Beware of providers that sell MSSP solutions as an add-on to another primary business such as telecommunications or hardware. These providers often provide commoditized solutions and have poor customer service for managed security customers due to a lack of focus on these customers.

Questions to ask providers:

- Is managed security your core business?
- What percentage of your business is managed security?
- What size companies do you generally serve?
- How are your solutions optimized to meet the needs of companies this size?
- Do you have a specific industry focus?
- How are your solutions optimized to meet the unique needs of companies in this industry?

Customer base

The size of an MSSP's customer base is important for two reasons. First, a large customer base shows that the provide has the necessary experience in protecting customer networks and handling the complex technical issues that MSSPs face every day. Second, if an MSSP detects an emerging threat affecting one customer, it can immediately block that threat for all customers – so customers benefit from using a provider that has a large customer base because they have better insight on the global threat landscape. Prospective buyers should be wary of any MSSP that has a small customer base – these providers may lack the experience, security data, and visibility into the threat landscape to provide the advanced protection that customers need.

Questions to ask providers:

- How many managed security customers do you serve?
- Is your customer base large enough to provide insight into the global threat landscape?

A large customer base shows that the provide has the necessary experience in **protecting** customer networks.

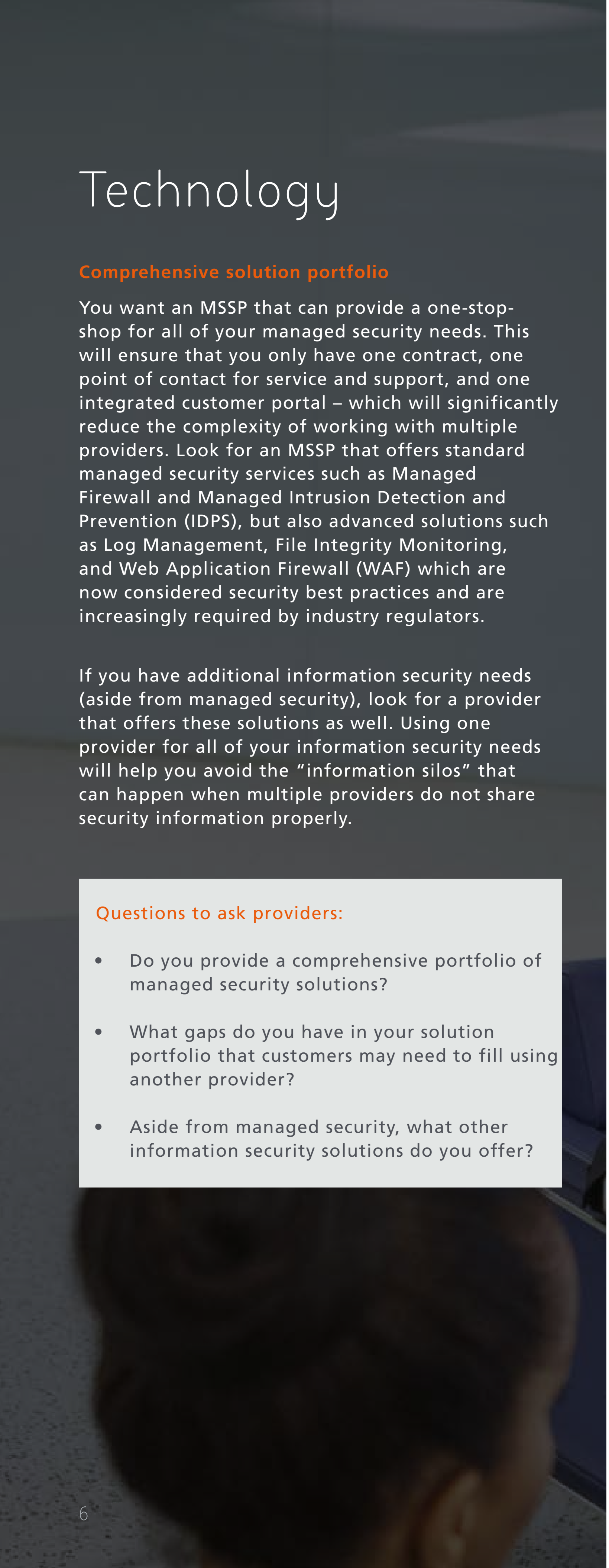
Financial stability

Financial stability is also an important consideration. You want your MSSP to be a reliable, long-term partner. You do not want to have to worry about changing providers on short notice because your MSSP went out of business. Also, companies that are not financially strong may be tempted to cut corners and could put your company's security at risk. Look for an MSSP that is profitable, financially stable, and can provide audited financial information upon request.

Questions to ask providers:

- Is your company profitable and financially stable?
- Do you provide audited financial information to customers upon request?

Look for an MSSP that is financially **stable**



Technology

Comprehensive solution portfolio

You want an MSSP that can provide a one-stop-shop for all of your managed security needs. This will ensure that you only have one contract, one point of contact for service and support, and one integrated customer portal – which will significantly reduce the complexity of working with multiple providers. Look for an MSSP that offers standard managed security services such as Managed Firewall and Managed Intrusion Detection and Prevention (IDPS), but also advanced solutions such as Log Management, File Integrity Monitoring, and Web Application Firewall (WAF) which are now considered security best practices and are increasingly required by industry regulators.

If you have additional information security needs (aside from managed security), look for a provider that offers these solutions as well. Using one provider for all of your information security needs will help you avoid the "information silos" that can happen when multiple providers do not share security information properly.

Questions to ask providers:

- Do you provide a comprehensive portfolio of managed security solutions?
- What gaps do you have in your solution portfolio that customers may need to fill using another provider?
- Aside from managed security, what other information security solutions do you offer?

Managed security platform

A Managed Security Platform is the back-end technology platform an MSSP uses to process and correlate security events, identify suspicious activity, and respond to security alerts. An MSSP's platform should go beyond basic security event monitoring by:

- Correlating security events across the customer's entire network to identify malicious traffic patterns
- Leveraging external research to constantly update databases of known attacks
- Leveraging a threat research team to reverse-engineer attack attempts and implement customized correlation rules to detect similar attacks in the future
- Enabling security analysts to immediately block attack sources across the entire customer base

Beware of providers using platforms that are limited to basic security monitoring, or those that provide "technology only" solutions that lack real-time, 24x7 monitoring. They will not be able to protect against the advanced threats that today's companies face.

Questions to ask providers:

- How does your managed security platform correlate security events? From what sources does it compile security events?
- What external research does the platform leverage?
- Do you have an internal threat research team to reverse-engineer attack attempts and implement rules to detect similar attacks in the future?

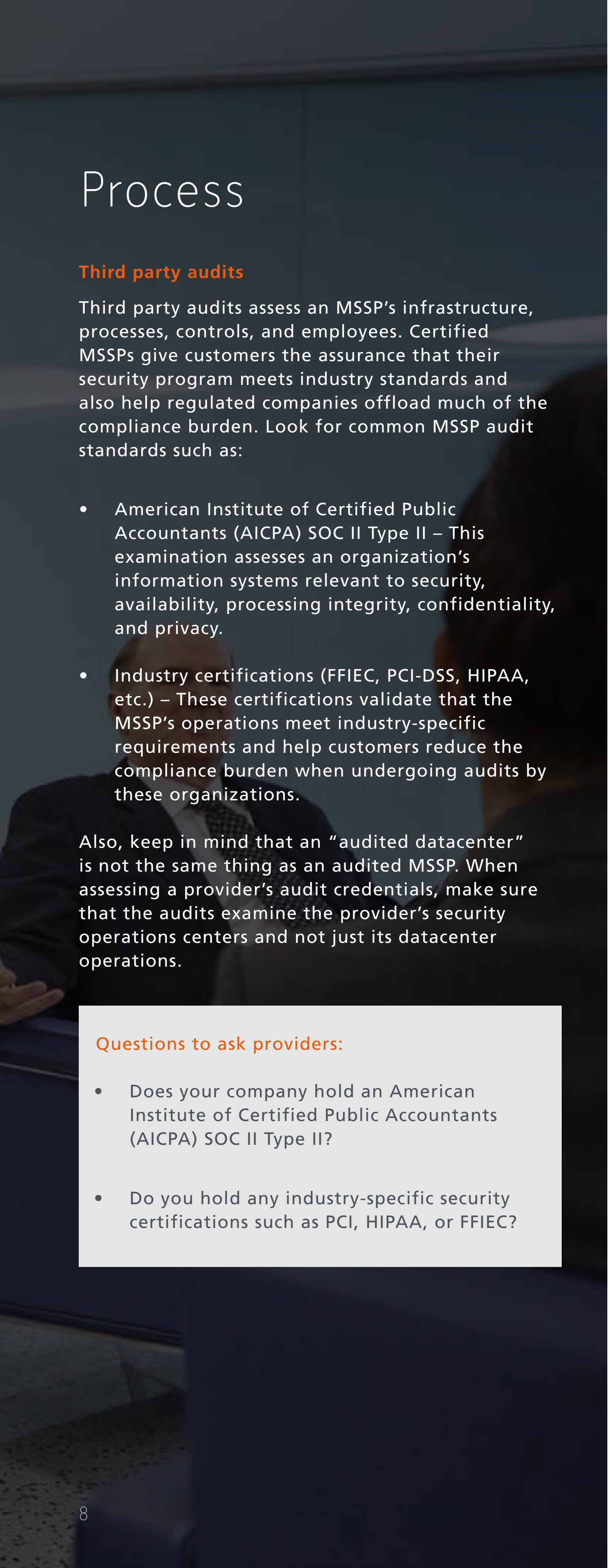
Customer portal

An MSSP's customer portal is the central repository where customers manage their account, submit customer support tickets, and view security reports. The customer portal should provide a comprehensive view of all network activity, through a single pane of glass. Your IT Managers will utilize your MSSP customer portal on a daily basis, so it's important that the portal is intuitive and user-friendly. It should include key features such as:

- Ability to submit support tickets and view change history
- Executive summary reports to provide a high level summary of network activity
- Detailed network activity reports to help IT Managers make better, more informed decisions
- Audit-ready compliance reporting, which significantly reduces the costs and headaches of meeting regulatory compliance. This is extremely important and valuable for highly regulated businesses.

Questions to ask providers:

- Does your portal include the ability to submit support tickets and view change history?
- Does your portal include both executive summary and detailed network activity reports?
- Does your portal feature audit-ready compliance reporting? Do the reports map to specific compliance mandates (PCI, HIPAA, FFIEC, etc.)?



Process

Third party audits

Third party audits assess an MSSP's infrastructure, processes, controls, and employees. Certified MSSPs give customers the assurance that their security program meets industry standards and also help regulated companies offload much of the compliance burden. Look for common MSSP audit standards such as:

- American Institute of Certified Public Accountants (AICPA) SOC II Type II – This examination assesses an organization's information systems relevant to security, availability, processing integrity, confidentiality, and privacy.
- Industry certifications (FFIEC, PCI-DSS, HIPAA, etc.) – These certifications validate that the MSSP's operations meet industry-specific requirements and help customers reduce the compliance burden when undergoing audits by these organizations.

Also, keep in mind that an "audited datacenter" is not the same thing as an audited MSSP. When assessing a provider's audit credentials, make sure that the audits examine the provider's security operations centers and not just its datacenter operations.

Questions to ask providers:

- Does your company hold an American Institute of Certified Public Accountants (AICPA) SOC II Type II?
- Do you hold any industry-specific security certifications such as PCI, HIPAA, or FFIEC?

Alert escalation and incident response procedures

Once an MSSP's Managed Security Platform aggregates security events, security analysts must classify potential security incidents and investigate all suspicious activity. Alert escalation and incident response procedures are critical because they determine how the MSSP responds to security incidents. Look for an MSSP that has escalation and response procedures that are clearly defined and fully audited by third parties to ensure compliance with industry best practices. Be sure to ask for specific examples of how the provider has responded to potential incidents in the past. Beware of any provider that lacks clearly defined procedures – this indicates that they are not well prepared to respond quickly and methodically to protect your network from malicious attacks.

Questions to ask providers:

- What is your process for classifying security incidents?
- What are your alert escalation procedures?
- What is your response plan for suspected security breaches?
- Are these security processes fully audited by third party auditors such as the AICPA (SOC II Type II)?
- Can you provide examples of how your team has responded to security incidents in the past?

Threat research capabilities

The attack landscape is constantly changing and hackers are constantly finding new ways to infiltrate company networks. Threat research teams enable MSSPs to provide advanced protection against these evolving threats. By analyzing the latest vulnerabilities and threats to customer networks, then implementing customized behavioral signatures and SIEM correlation rules to protect against these threats, threat research teams ensure that MSSPs deliver the latest and best protection to customers.

Some MSSPs simply compile threat alerts from publicly available sources, but lack a true threat research team. Look for an MSSP that goes beyond this basic level of protection with a threat research team that is dedicated to combating the advanced, sophisticated threats that today's companies face.

> Some MSSPs simply compile threat alerts

Threat intelligence

Threat information which is received but not efficiently and properly reviewed, understood, analyzed and actioned, will not contribute to the defense of an organization. To be effective, in addition to having subscribed to or obtained reliable sources of threat information, an organization must have the ability to process that information and convert it into intelligence that informs them about the nature and details of a threat and ultimately turn that intelligence into defensive capability which rapidly enhances the ability of the organization to protect itself from that threat.

When evaluating MSSPs, make sure that they have an ongoing process for continually integrating threat intelligence into their infrastructure and technology solutions.

Questions to ask providers:

- Do you have a dedicated threat research team?
- How many analysts are dedicated to evolving threat research?
- What processes do you have to continually integrate threat intelligence into your solutions?

Beware of providers that lack a full team

People

Highly trained and experienced security analysts

MSSP Security Analysts utilize cutting-edge analytical techniques to protect customer networks 24x7 and are a critical component of an MSSP solution. They should be highly trained, experienced, and certified by leading security organizations. Look for analyst certifications such as CISSP, GSEC, CEH, CCSP, CCNA, CISM, and Security+. Beware of providers that lack a full team of certified analysts, or those that put too much emphasis on "technology only" solutions and not enough emphasis on their analysts – their importance in protecting customer networks simply cannot be understated.

Questions to ask providers:

- Do you monitor customer networks 24x7 by certified security analysts?
- What certifications do your analyst hold?
- How many years of experience do they have?

Customer support

Your IT Managers will need to interact with your MSSP's customer support team on a regular basis to request configuration changes, upgrade technology, seek advice on the changing threat landscape, and troubleshoot security and networking issues. Therefore, it is critical to choose an MSSP with a strong customer support record. Look for an MSSP that devotes substantial resources to customer support and that has strong procedures to measure and report customer satisfaction statistics. Be wary of MSSPs that have too many lines of business (such as telecommunications providers, hardware providers, etc.) competing for resources as this may have an adverse impact on customer service.

Questions to ask providers:

- How many employees do you have dedicated to customer service and support?
- How do you measure your customer support track record?
- Do you share customer satisfaction ratings with customers?

We are BAE Systems

We help nations, governments and businesses around the world defend themselves against cyber crime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analyzing huge volumes of data. These, combined with our cyber special forces - some of the most skilled people in the world, enable us to defend against cyber attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We employ over 4,000 people across 18 countries in the Americas, APAC, UK and EMEA.

BAE Systems
265 Franklin Street
Boston
MA 02110
USA
T: +1 (617) 737 4170

BAE Systems
154 University Avenue, 2nd Floor
Toronto, ON
M5H 3Y9
Canada
T: +1 (647) 777 2000

Victim of a cyber attack? Contact our emergency response team on:

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com

CREST

CESG Certified Service
Cyber Incident Response

CPNI
Centre for the Protection of National Infrastructure

BAE Systems, 265 Franklin Street, Boston, MA 02110, USA
E: learn@baesystems.com | W: baesystems.com/businessdefense
linkedin.com/company/baesystemsai
twitter.com/baesystems_ai