Aite PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

APRIL 2021

Joseph Krull, CISSP, IAM, CISA, CRISC, CIPP
+1.210.421.8233
jkrull@aitegroup.com

SOC-as-a-Service: Add Talent and Automation to Your Cybersecurity Strategy

Financial services organizations are under constant cyberattack from a diverse group of assailants ranging from opportunist cyber criminals to highly motivated and resourced nation states. Attacks have increased in both frequency and sophistication and include ransomware, business email compromise, and theft of sensitive customer information. Organizations no longer have the luxury to investigate and respond to cyber anomalies and suspected attacks when resources become available; cyberattacks propagate quickly and can inflict significant brand damage. Organizations looking to augment cybersecurity capabilities with third-party services have a dizzying array of choices in the marketplace today. This report explains the various service options and provides examples of why an outsourced security operations center (SOC-as-a-Service) provides exceptional value to small and midsize financial services organizations as well as managed service providers supporting these organizations. This report also provides a case study demonstrating the value of SOC-as-a-Service.

INTRODUCTION

Small and midsize financial organizations are receiving the same sophisticated threats and attacks as major organizations; however, most don't have the resources to defend against them. These small and midsize firms generally have small cybersecurity teams or, in many cases, no dedicated on-staff cybersecurity professionals. Many of these organizations have looked to their information technology (IT) managed service providers (MSPs) or managed security service providers (MSSPs) to deliver cybersecurity capabilities, often with mixed results. Today's cybersecurity services marketplace is incredibly fragmented, with hundreds of MSPs and MSSPs offering a wide range of cybersecurity capabilities that are enticing for potential customers but incredibly difficult to deliver at a profit. The MSP, MSSP, and related technology solution provider markets are also a hotbed of merger and acquisition (M&A) activity, with more than 530 publicly reported deals in 2020 and more than 150 in the first quarter of 2021.[1]

This Impact Brief provides an overview of the services MSPs and MSSPs offer and focuses on the value offered by SOC-as-a-Service for small and midsize financial services organizations.

METHODOLOGY

This Impact Brief is based on briefings, discussions, and participation in virtual events with service providers, technologists, and IT professionals utilizing outsourced security services. Activities took place from November 2020 through March 2021.

THE MARKET

The market for cybersecurity services has become particularly crowded over the last four years as more and more MSPs and MSSPs seek to offload cybersecurity functions from organizations that cannot build and operate these services themselves. For many years, small and midsize financial services organizations attempted to keep up with cybersecurity defenses. They did so with a range of point products or solutions and well-meaning general IT specialists; however, over time, chief information officers (CIOs) came to realize that this strategy could not keep up with sophisticated cybersecurity risks. Today, there are more than 500 MSPs and MSSPs vying for cybersecurity business with a dizzying array of service offerings and technologies. This makes evaluation and comparison of the various services and the subsequent pricing particularly challenging for buyers of cybersecurity services.

During Aite Group discussions with service providers and IT professionals from November 2020 through March 2021, we examined the current state of the cybersecurity services market and identified five key trends that are impacting the market and small and midsize financial services organizations (Table A).

1. "Technology Company Mergers and Acquisitions: Annual M&A Lists," Channele2e, accessed March 25, 2021, https://www.channele2e.com/acquisitions/.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Table A: The Market

Market trends	Implications
MSPs and MSSPs are adding new or expanded cybersecurity services to remain competitive.	Many of these services require the support of specialized cyber professionals who are difficult to hire based on widespread shortages. Not all MSPs and MSSPs can afford relevant market salaries and keep their offerings profitable.
Many MSPs and MSSPs are closely aligning with selected cybersecurity technology vendors, particularly for endpoint and security information and event management (SIEM) capabilities.	MSPs and MSSPs are increasingly entering into complex and often exclusive relationships with individual cybersecurity vendors. These relationships can be negatively impacted if these technology vendors are acquired or exit the market, necessitating a rapid substitution of core products.
Small and midsize financial services organizations do not have the required resources to build and operate security operations centers, particularly if 24/7 coverage is needed.	The cost of operating a SOC is not trivial. For each required SOC analyst, the organization would need to allocate up to 3.8 staff for 24/7 coverage to consider vacations, absences, and inevitable turnover. Personnel costs account for the lion's share of SOC operating expenses.
The MSP, MSSP, and related technology solution provider markets are teeming with frequent M&A deals.	Market turmoil and frenetic M&A transactions can create unexpected impact on buyers of cybersecurity services. Each transaction can result in changes in technologies, pricing, and service coverage at the point of contract renewal.
Small and midsize financial services organizations require more advanced cybersecurity services to respond to ever-increasing sophisticated attacks.	Cybersecurity requirements have outpaced the traditional first-generation MSP and MSSP services of managed firewalls, managed intrusion detection systems, and log management. Organizations now require more sophisticated services to go beyond basic cybersecurity blocking and tackling to be able to react to and limit damage from cyberattacks.
Digital transformation initiatives and broader use of cloud services have increased cyber threats.	Small and midsize financial services have launched new digital products and have moved some of their operations to the cloud to differentiate and scale their services. Whether created in-house or provided by a partner, these services have changed or increased the attack surface. Web, mobile, and cloud-based services require constant and sophisticated monitoring and management to detect and mitigate cyber risks.

Source: Aite Group

COMPARISON OF CYBERSECURITY SERVICES

Buyers of cybersecurity services will be presented with a broad range of offerings that can often be difficult to quantify and compare. Service descriptions vary widely, while some basic categories of cybersecurity services do exist.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Many providers will indicate that they are integrating AI, machine learning, and/or automation into their service offerings, primarily to make the services more responsive and capable. Automation is already having a demonstrable impact on cyber defense, and improvements will continue in 2021 and beyond. Both the service provider and the supported organization benefit from automation. For the service provider, automation reduces the human requirements of the providers' services and enables or increases provider competitiveness and profitability. For the supported organization, automation results in more efficient and faster handling of cyber anomalies and reduction in remediation times.

Table B contains examples of generic cybersecurity services offered by MSPs and MSSPs.

Table B: Cybersecurity Services

Service category	Considerations for small and midsize financial services organizations
Managed SIEM: The provider will offer a SIEM capability based on event data collection and analysis, usually as a cloud-based service. The provider will supply the core infrastructure, management, and administration of the SIEM on a subscription basis.	A SIEM capability, while an integral part of cybersecurity operations, is not sufficient by itself to provide highly targeted organizations with coverage against cyberattacks.
Endpoint detection and response (EDR): The provider will offer agent-based monitoring of activities on desktops, laptops, and servers as well as some basic response and mitigation services.	EDR is a partial solution as the supported organization would still have to act in response to anomalous activities or actual indications of a cyberattack.
Managed detection and response (MDR); The provider will offer advanced threat detection as well as incident management and remediation services for cyber events. This is the fastest growing segment of today's cybersecurity services market.	The MDR provider's capabilities are suitable for organizations that elect to outsource cybersecurity services. However, not all MDR providers provide a SIEM capability that would likely need to be provided to meet regulatory and compliance requirements for logging. This would require a separate SIEM provider and increase complexity.
Extended detection and response (XDR): This offering goes beyond MDR to encompass additional telemetry and cyber services based on cloud workloads. This is a relatively recent market category that is still evolving in the marketplace.	XDR from some providers may be more than most small and midsize organizations can successfully integrate into their cybersecurity strategies. Pricing and technical requirements may exceed the organizations' budgets and integration capabilities.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

Service category	Considerations for small and midsize financial services organizations
SOC-as-a-Service: The provider offers the functionality of a security operations center based on a subscription model. The SOC is staffed by security analysts, threat intelligence specialists, and SIEM and EDR administrators. The SOC provides a 24/7 monitoring capability, operations and maintenance functions based on standardized runbooks, and a comprehensive cyber incident management capability.	SOC-as-a-Service will in most cases be the best fit for small and midsize organizations that move to outsource a broad range of cybersecurity functions and obtain a SIEM capability for regulatory requirements from a single provider.
Co-Managed SIEM and/or Co-Managed SOC – Some providers offer these options that require the supported organization to play an active role in the functioning of the service.	The co-managed options may not be suitable for organizations that have limited cybersecurity staff. Also, delineation of responsibilities can be complex and may result in poor handling of cyber events.

Source: Aite Group

THE VALUE OF SOC-AS-A-SERVICE TO ORGANIZATIONS

As noted in the previous table, SOC-as-a-Service will be the best fit for most small and midsize financial services organizations. The primary benefits of SOC-as-a-Service are economics and cybersecurity coverage. Aite Group heard from several sources that organizations substituting their in-house security operations center for a SOC-as-a-Service provider can see up to an 80% reduction in annual spend. A capable and proven SOC-as-a-Service provider will be able to perform nearly all the required cybersecurity and regulatory support functions as well as allow the organization to focus on management oversight regarding the successful performance of the SOC provider.

A SOC-as-a-Service provider will bring advanced technologies to the engagement. These are normally well beyond the reach of small and midsize organizations to procure, implement, deploy, and maintain independently. Examples include enhanced detection, user behavior and entity behavior analytics, risk analysis weighting, and incorporation of threat intelligence data. Coupled with advanced automation and AI/machine learning, these technologies will benefit the organization and the service provider.

Outsourcing to a SOC-as-a-Service provider does not completely release the organization from cybersecurity requirements. The organization will still need to have a structure to define cybersecurity strategy and risk appetite, and the CIO or other designated executive will be responsible for informing and guiding key stakeholders of cyber-related risks. The CIO or designated representative will also remain responsible for cyber-related interactions with examiners, regulators, and auditors. However, a capable SOC-as-a-Service provider will successfully offload the day-to-day cybersecurity functions and be ready to jump into the action in the event of a cyber incident.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

If properly planned, designed, and implemented, the SOC-as-a-Service will essentially be a logical extension to the organization's IT staff. The CIO or designee will need to ensure that the provider has access to required resources and information. This will allow the provider to customize runbooks, create incident response procedures, and keep current communications plans for both daily operations in the event of cyber incident.

The SOC-as-a-Service provider will, in most cases, provide the supported organization with relevant reports and data regarding cyber health and risk levels. Many SOC-as-a-Service providers currently do this via web-based dashboards.

Although a SOC-as-a-Service relationship allows an organization to offload key cybersecurity functions, to be successful, the partnership requires active interest and involvement by a responsible member of the supported organization's CIO or designated representative. Otherwise, it is unlikely that the provider will receive sufficient input and feedback to best serve the organization.

THE VALUE OF SOC-AS-A-SERVICE TO MANAGED SERVICE PROVIDERS

MSPs have added cybersecurity services to their offerings, as these services are often in demand by their clients and can bring their clients additional recurring revenue. Many MSPs have attempted to create homegrown cybersecurity offerings but encountered challenges related to product fit, limited in-house cybersecurity expertise, and difficulties in attracting cybersecurity professionals who are in high demand. Facing these challenges, many MSPs have elected to enter partnerships with MSSPs and MDR providers to offer cybersecurity services. The bulk of the actual work is offloaded to the MSSP or MDR provider, but the MSP may need to retain responsibility for the services. Depending on the contract, this may leave very little revenue for the MSP or dictate uncompetitive pricing to the client. If a client requires cybersecurity services from multiple providers (e.g., MDR plus SIEM), it can further complicate the role of the MSP and add contract complexity.

MSPs can benefit from engaging SOC-as-a-Service providers to offer a broad range of outsourced cybersecurity services to their small and midsize customers. The advantages associated with this model include uncomplicated pass-through of more comprehensive cybersecurity processes and simplified contracting. MSPs that can bring capable SOC-as-a-Service providers to their clients should be able to solidify their client relationships and seek new clients via joint MSP/Soc-as-a-Service marketing efforts.

SOC-AS-A-SERVICE DIFFERENTIATORS

Capabilities and service level quality can vary widely between SOC-as-a-Service providers. Potential buyers of cybersecurity services should look for SOC-as-a-Service providers that can offer the following:

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- **Simplified setup and service initiation:** SOC-as-a-Service providers should have detailed and tested plans, procedures, and timelines for starting the service. This will include distribution and installation of agents, adapting runbooks to the specific customer environment, and granting access to reporting. This will also include briefing and training designated members of the supported organization.
- **Highly reliable anomaly detection and reduced false positives:** The SOC-as-a-Service provider should be able to demonstrate that the service can accurately and quickly detect cyber anomalies and cyberattacks. False positives can significantly impact the reliability, efficiency, and credibility of the service, and the SOC-as-a-Service provider should be able to demonstrate how false positives are minimized.
- **Highly intuitive dashboards:** Organizations should be able to measure their cyber risks against an established baseline or framework. Ideally, the dashboards should display an overall risk score to allow personnel without cybersecurity experience to quickly assess the overall state of cyber health.
- **Robust logging and analysis:** The service should include log collection, aggregation, and analysis to support regulatory compliance and review by examiners, assessors, and auditors.
- **Contract flexibility:** For MSP's, the ability to either use the MSP's contract or the SOC-as-a-Service provider's contract directly with the supported organization can support commercial success.
- **Highly responsive cybersecurity specialists:** This is the most important aspect of a SOC-as-a-Service provider. Buyers should look at the qualifications, training, tenure, and certifications of security analysts, threat intelligence specialists, and SIEM and EDR administrators. The provider should be able to offer references from other clients, particularly any that have needed to use the provider's remediation and incident response services.

CASE STUDY

Aite Group spoke with the chief information security officer (CISO) and senior infrastructure engineer at Alpha Theory, a financial services software company focused on portfolio optimization for global institutional investors. The company supports clients with more than US$200 billion in assets under management. Alpha Theory had engaged a well-known MSSP with less than favorable results. The CISO noted that a combination of the lack of transparency regarding alerts, poor provider performance, and high monthly fees drove a decision to suspend the contract and bring cybersecurity services back in-house. During the tool selection phase for the in-house build, Alpha Theory was introduced to AgileBlue, a Cleveland, Ohio-based SOC-as-a-Service provider.

After a brief review of AgileBlue's services, the CISO said he realized that SOC-as-a-Service would be ideal for Alpha Theory's business and alleviate the need to invest in infrastructure and personnel while protecting the company from sophisticated cyberattacks. The CISO also noted that AgileBlue's service offering would help Alpha Theory demonstrate capabilities to help their

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

clients meet U.S. Securities and Exchange Commission requirements. AgileBlue initiated services at the end of January 2021.

The CISO and senior infrastructure engineer expressed satisfaction with the ease of implementation. Specifically, they noted the "one click" deployment of agents, strong controls around how the agents securely communicate with AgileBlue, and elimination of the need to reboot endpoints after agent installation. The experienced senior infrastructure engineer told Aite Group that implementation of AgileBlue was the smoothest agent deployment he had encountered. The CISO was particularly pleased with a comprehensive project plan provided by AgileBlue to facilitate the deployment and the team's ability to work with AgileBlue's dedicated support team. The CISO and senior infrastructure engineer accessed AgileBlue's web-based portal to review monitoring activities and cyber health, and they reported that this portal provides them all they need to manage cybersecurity operations and respond to queries.

Although the AgileBlue service has only been in place for just over two months, the CISO noted that he and his team are already seeing strong benefits from the service. Specifically, these benefits include a much smoother auditing process and what the CISO is positioning as a competitive advantage for Alpha Theory during discussions with prospective clients. In essence, the CISO reported that Alpha Theory is now receiving a complete range of cybersecurity services at roughly 10% of the monthly cost of the previous MSSP.

During Aite Group's subsequent discussions with AgileBlue and its client, the company cited three major differentiators they believe are contributing to its success in the marketplace and keeping its clients successfully monitored. The first is providing its clients with enhanced visibility regarding cyber risk via the AgileBlue analytics reporting dashboard. Next is the AgileBlue proprietary risk scoring algorithm, including industry comparisons and risk analysis trends. And finally, AgileBlue asserted that its proprietary Silencer technology significantly reduces false positives, with a 95% confidence score on incident alerts based on its proprietary machine learning and user behavior analytics.

RECOMMENDATIONS

Aite Group recommends that buyers from small and midsize financial service organizations take the following actions related to outsourcing cybersecurity services:

- Assess the listed capabilities of cybersecurity services providers. Determine the types of services that are needed based on the organization's risk appetite, regulatory requirements, budget, and level of active participation. Capabilities should be mature and successfully deployed to similar organizations.
- Carefully consider the commercial profiles of each potential cybersecurity services provider. As the market has experienced frenetic M&A transactions in 2020 and into 2021, look for indicators that the provider may be a target for acquisition. This would add complexity or cancel out potential benefits from a long-term relationship.
- Look for simplified and intuitive risk and cyber health reporting—ideally in the form of web-based dashboards that can be interpreted by noncyber professionals.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

- Qualified staff and responsiveness of the provider's cyber specialists are critical for success. Organizations should focus on the provider's ability to quickly address cyber issues, risks, anomalies, vulnerabilities, and respond to cyber events.
- Compared to other cybersecurity services, SOC-as-a-Service will most likely be the best fit for small and midsize financial services organizations. Include SOC-as-a-Service providers in request for proposals or look for SOC-as-a-Service offerings from MSPs.

CONCLUSION

- Small and midsize financial organizations are receiving the same sophisticated threats and attacks as major organizations; however, most do not have the resources to defend against them. The use of outsourced cybersecurity services can help close that gap.
- The landscape of cybersecurity services includes hundreds of providers offering a broad array of capabilities ranging from basic blocking and tackling, all the way to sophisticated remediation and incident response offerings. The MSP, MSSP, and related technology solution provider markets are experiencing frequent M&A deals, making supplier commercial profile analysis an important of service provider selection criteria.
- The use of AI, machine learning, and automation help cybersecurity service providers more quickly identify cyber anomalies, respond to incidents, and perform remediation actions.
- SOC-as-a-Service offers a broad range of cyber capabilities that can be used as a logical extension of an organization's IT staff. Small and midsize financial services should consider SOC-as-a-Service when contemplating outsourcing of cyber functions.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com

ABOUT AITE GROUP

Aite Group is a global research and advisory firm delivering comprehensive, actionable advice on business, technology, and regulatory issues and their impact on the financial services industry. With expertise in banking, payments, insurance, wealth management, and the capital markets, we guide financial institutions, technology providers, and consulting firms worldwide. We partner with our clients, revealing their blind spots and delivering insights to make their businesses smarter and stronger. Visit us on the web and connect with us on Twitter and LinkedIn.

CONTACT

For more information on research and consulting services, please contact:

Aite Group Sales
+1.617.338.6050
sales@aitegroup.com

For all press and conference inquiries, please contact:

Aite Group PR
+1.617.398.5048
pr@aitegroup.com

For all other inquiries, please contact:

info@aitegroup.com

RELATED AITE GROUP RESEARCH

Better, Stronger, Cheaper Cybersecurity: Doing More With Less in a Crisis Economy, June 2020.

101 Arch Street, Suite 501, Boston, MA 02110 • Tel +1.617.338.6050 • Fax +1.617.338.6078 • info@aitegroup.com • www.aitegroup.com