nuspire

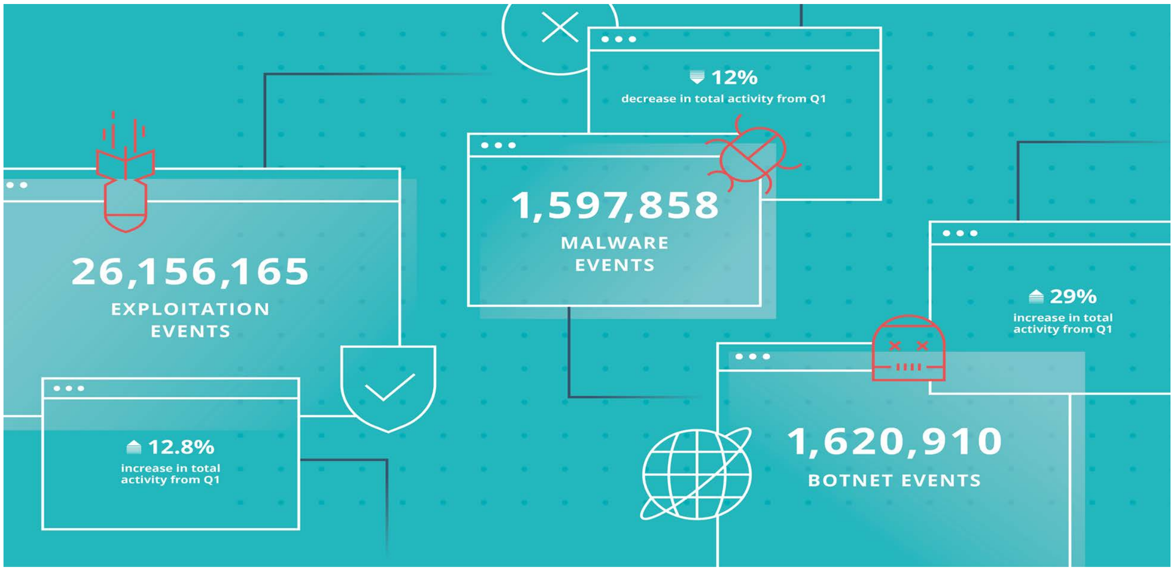
Managed Security Services: *How Midsize Organizations Can Solve Chronic Cybersecurity Challenges by Partnering with the Right MSSP*

FEATURING RESEARCH FROM FORRESTER

The Forrester Wave™: Midsize Managed Security Services Providers, Q3 2020

As cybersecurity threats and tactics continue to evolve, they are becoming increasingly more sophisticated and harmful. This is especially true now, in the pandemic-driven work from home (WFH) shift. New attack vectors and challenges for network administrators have been created; including VPN usage, home network security issues, personal device usage for business purposes and auditability of network traffic. Fortunately through most change, opportunity is created. The opportunity today is that many cyberattacks can be prevented. Meaning, organizations that stay abreast of the latest threat intelligence are able to take action to protect their digital perimeter and mitigate risk.

FIGURE 1 Nuspire Q2 2020 Threat Report


12%
decrease in total activity from Q1
1,597,858
MALWARE EVENTS
26,156,165
EXPLOITATION EVENTS
29%
increase in total activity from Q1
12.8%
increase in total activity from Q1
1,620,910
BOTNET EVENTS

IN THIS DOCUMENT

Solving Chronic Cybersecurity Challenges

Taking immediate action to prevent damage is largely dependent on the skills and resources available. Not all organizations have access to the latest threat intelligence—or the in-house expertise required to translate that intelligence into proactive response. In fact, 65% of organizations report a shortage of skilled cybersecurity staff.[1] This ongoing shortage puts additional pressure on existing security operations staff to perform highly important activities, including:

- Minimizing false positives
- Detecting intrusions
- Interpreting threat intelligence

[1] The (ISC)2 Cybersecurity Workforce Study, 2019

- Hunting threats down
- Monitoring and analyzing alerts
- Detecting intrusions

In addition to retaining enough talent (on average, three security analysts resign or are fired from an organization annually),[2] a key resource to effectively secure a digital perimeter is budget. Organizations that choose to maintain a security operations center (SOC) internally can expect to spend an average of $2.86 million annually.[3] As chief information security officers (CISOs) try to make pandemic impacted budgets stretch, continuously investing in the people, processes and technologies required to run an internal SOC is not always feasible.

A lack of in-house expertise and limited funding are two chronic cybersecurity challenges that often drive organizations to engage with a managed security services provider (MSSP). Outsourcing security operations is a proven way to secure security operations when you lack the necessary resources. Choosing an effective MSSP can provide the 24x7x365 eyes on glass needed to attain 360 degree visibility of your threat landscape. And, creating an extended team enables you to acquire the expertise needed to reduce false positives and mitigate risk while focusing internal teams on important business initiatives.

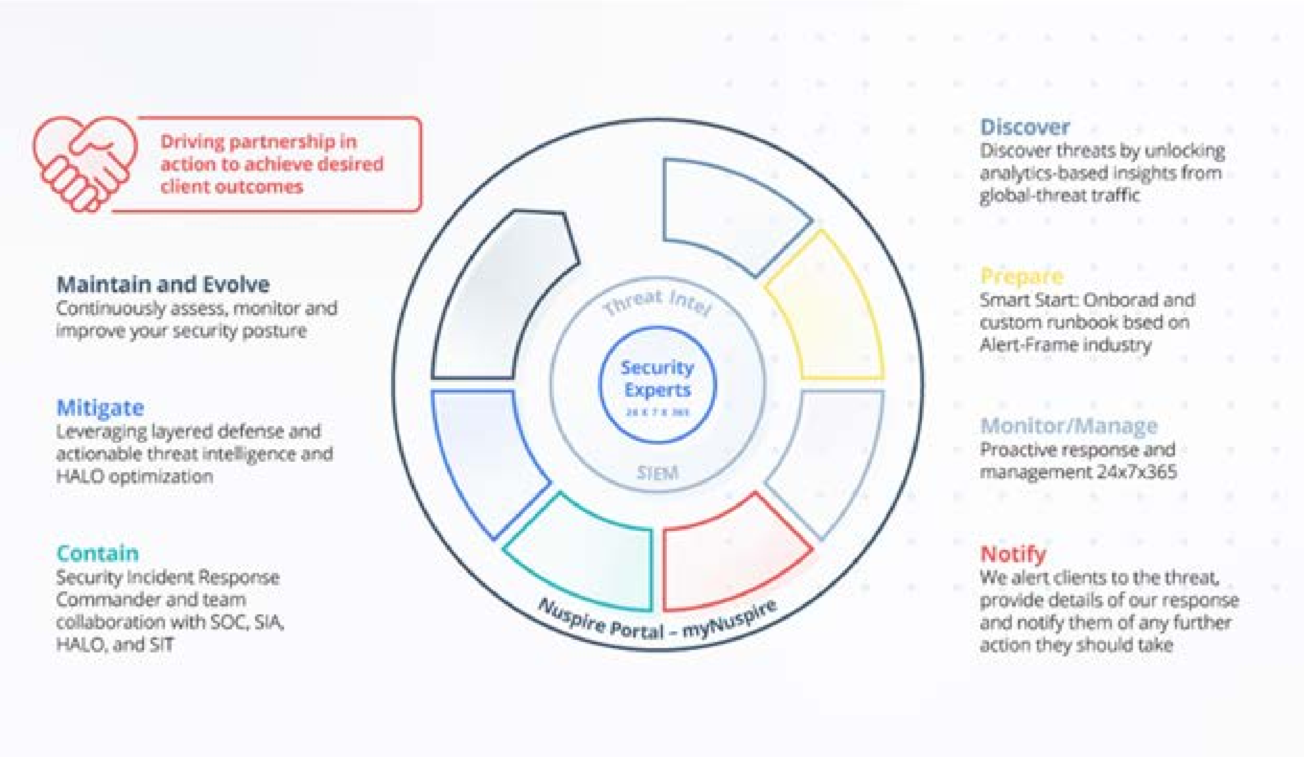
[2] Ponemon Institute© Research Report, The Economics of Security Operations Centers: What is the True Cost for Effective Results?, January 2020
[3] Ibid

Not All MSSPs are Created Equal

Partnering with a MSSP enables security leaders to share a workload that typically comes under fire from the latest threat, compliance requirement or technology challenge. MSSPs can absorb daily emergencies so organizations can prioritize activities and specializations. Using the right MSSP enables security leaders to leverage a pool of new skills and avoid overtaxing internal teams while filling coverage gaps.

While there are hundreds of MSSPs from which to choose, it is critical to choose a true partner that is the best fit for your organization. Your MSSP needs to understand your unique business needs, how your team is organized and identify gaps in coverage. Only after understanding your business needs can they then work around the clock to proactively monitor, detect, hunt and mitigate to protect your organization. Employing 24x7x365 proactive monitoring of your environment continuously, detects and responds to threats using real-time, proprietary analysis and enriched threat data. A pre-determined incident escalation process speeds response time and keeps everyone on the same page.

FIGURE 2 Nuspire Security in Action Methodology



Driving partnership in action to achieve desired client outcomes

Maintain and Evolve
Continuously assess, monitor and improve your security posture

Mitigate
Leveraging layered defense and actionable threat intelligence and HALO optimization

Contain
Security Incident Response Commander and team collaboration with SOC, SIA, HALO, and SIT

Discover
Discover threats by unlocking analytics-based insights from global-threat traffic

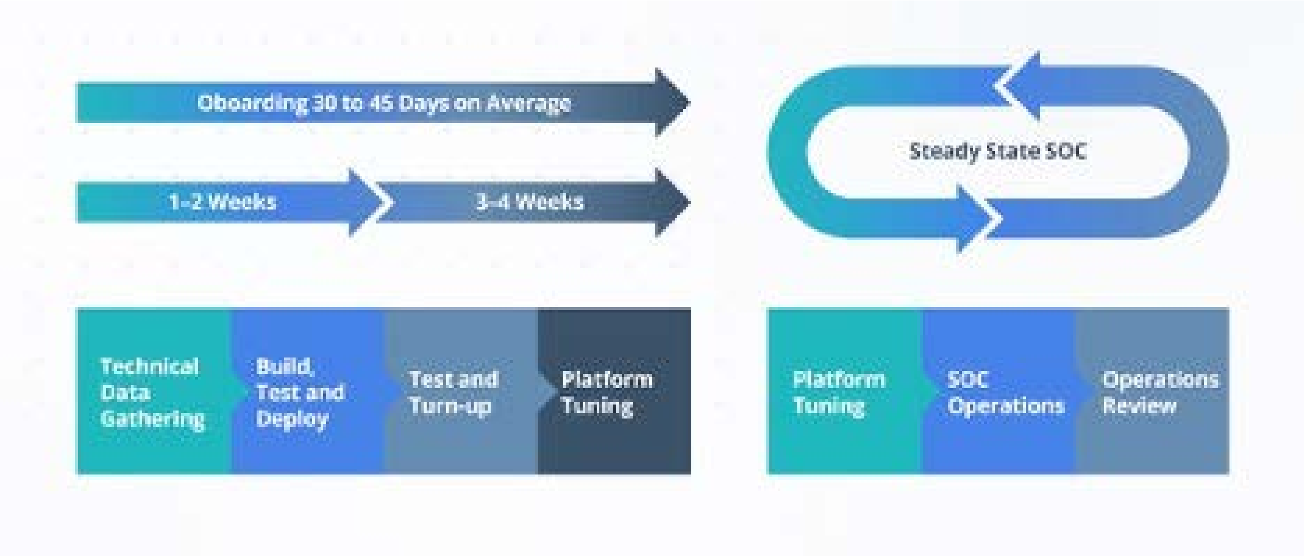
Prepare
Smart Start: Onborad and custom runbook bsed on Alert-Frame industry

Monitor/Manage
Proactive response and management 24x7x365

Notify
We alert clients to the threat, provide details of our response and notify them of any further action they should take

Once you‘ve vetted capabilities, it is also important to understand a MSSP‘s onboarding and support process. Will you be gaining a true partner—available to address your needs 24x7x365—or a phone tree? Effective onboarding includes processes that clearly establish the expectation for how clients want incidents handled. It also communicates what to expect in the first 30, 60, 90 days of the engagement and what service level agreements will be in place to assure you are truly gaining an extension of your team.

FIGURE 3 Nuspire Smart Start Onboarding Process



Choosing the Right MSSP

Thoroughly vetting a MSSP's capabilities and approach is critical to ensure a successful partnership. A proper vetting also includes getting answers to important questions including:

- Do you have a runbook that is customized to my unique environment, processes and rules?
- What is the process you use to customize security services, and do you provide monthly reviews to apply learning and revise procedures?
- Do you have a formalized onboarding process that includes a deep discussion about risk, goals, industry and asset inventory? How often is the process updated?
- How do you correlate and prioritize data, and do you have more than one source of intelligence?
- Do you rely on our organization to have a specific technology to integrate with yours or I need to rip and replace my current technology stack?
- Do you provide multiple sources of threat intelligence that are correlated to an actionable step?
- Are your security analysts responsive and available whenever we need them?
- Are your security analysts proactively hunting for threats that we may not be aware of?

Selecting the right MSSP is also aided by leveraging third-party industry research to understand best practices and to rank partners based on capabilities and approach. "As legacy MSSP approaches become outdated and less effective, improved threat intelligence and integrations will dictate which midsize MSSPs will lead the pack. Vendors that can provide those capabilities position themselves to successfully deliver midsize MSSP success to their customers."[4]

[4] The Forrester Wave™: Midsize Managed Security Services Providers, Q3 2020

The Forrester Wave™: Midsize Managed Security Services Providers, Q3 2020

The 12 Providers That Matter Most And How They Stack Up

by Jeff Pollard and Claire O’Malley

August 11, 2020

Why Read This Report

In our 26-criterion evaluation of midsize managed security services providers, we identified the 12 most significant ones — BlueVoyant, Cipher, ControlScan, CyberProof, Delta Risk, Encode, InteliSecure, Kudelski Security, Nuspire, Proficio, Rapid7, and StratoZen — and researched, analyzed, and scored them. This report shows how each provider measures up and helps security and risk professionals select the right one for their needs.

Key Takeaways

CyberProof, Rapid7, And Kudelski Security Lead The Pack

Forrester’s research uncovered a market in which CyberProof, Rapid7, and Kudelski Security are Leaders; InteliSecure, BlueVoyant, Delta Risk, and StratoZen are Strong Performers; and Cipher, Encode, Proficio, ControlScan, and Nuspire are Contenders.

Threat Intelligence And Microsoft Integrations Are Key Differentiators

As legacy MSSP approaches become outdated and less effective, improved threat intelligence and integrations will dictate which midsize MSSPs will lead the pack. Vendors that can provide those capabilities position themselves to successfully deliver midsize MSSP success to their customers.

The Forrester Wave™: Midsize Managed Security Services Providers, Q3 2020

The 12 Providers That Matter Most And How They Stack Up

by Jeff Pollard and Claire O'Malley
with Joseph Blankenship, Melissa Bongarzone, and Peggy Dostie

August 11, 2020

Table Of Contents

Related Research Documents

The Forrester Wave™: Global Managed Security Services Providers, Q3 2020

Now Tech: European Managed Security Services Providers, Q2 2020

Now Tech: Global And Emerging Managed Security Services Providers, Q2 2020

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Midsize MSSPs Are Desperately Seeking Innovation

Forrester's 2020 evaluation shows that the midsize managed security services provider (MSSP) market is stagnating, as the market pivots to focus on pure managed detection and response (MDR) capabilities. MDR capabilities provide immense value for security teams, but they make up only a small subset of what most MSSPs offer. Every vendor has budget and roadmap limitations — just like their customers — so more efforts directed at MDR also requires them to neglect making improvements in the core set of capabilities the MSSP may offer. Regulation, not surprisingly, is also causing midsize MSSPs to struggle with data sovereignty. The General Data Protection Regulation (GDPR) is in place, making informalized, ad hoc approaches to managing customer data across multiple international borders a potential problem for midsize MSSPs.

However, the evaluation also showed strong players in the midsize space, with unique approaches and perspectives tailored to their target customers. Forrester dubs these vendors as midsize not because of a limited array of capabilities or insignificant customers, but because of smaller revenues and their recent emergence in the market compared with the larger global MSSPs security leaders are more familiar with. Midsize customer references show extreme satisfaction with their chosen MSS partner and often selected it against larger counterparts because they appreciated the new and refreshing approach to MSS delivery.

As a result of these trends, midsize MSSP customers should look for providers that offer:

- **Threat intelligence that tells the whole story.** Midsize MSSPs offer a vast selection of threat intelligence sources and threat intelligence data. However, the strongest current offerings take their threat intelligence capabilities one step further by providing the full story of that data, along with next steps based on the information, guiding customers to other areas of concern that need investigation. Security buyers should prioritize vendors that supplement their threat intelligence with suggested next steps that take into account the full context; these vendors should also provide prescriptive steps and actions to help customers understand what they should do before considering an incident complete.
- **A true extension of their team.** The happiest customers didn't sign on with their vendor just to outsource and replace the security function at their organization. Instead, their MSSP supplements and augments their internal teams. Look for midsize MSSPs where collaboration and teamwork are interwoven and prioritized as much as technical capabilities. The best MSSPs strike this balance for all of their customer relationships.
- **Integrations that support growing cloud — and Microsoft — security solutions.** The tech titans, Microsoft specifically, continue to disrupt cybersecurity space.[1] MSSPs have taken note and are now catering their solutions for easy integrations with Microsoft's security suite along with other cloud and API-event collection technologies. They understand that their customers are also investing in Google Cloud Platform (GCP), AWS, and Azure, so they've adapted their solutions to support those as well. Customers should pick an MSSP that understands and supports, with integrations, as much of their cybersecurity technology estate as possible.

Evaluation Summary

The Forrester Wave™ evaluation highlights Leaders, Strong Performers, Contenders, and Challengers. It's an assessment of the top vendors in the market and does not represent the entire vendor landscape. You'll find more information about this market in our "Now Tech: Global And Emerging Managed Security Services Providers, Q2 2020."

We intend this evaluation to be a starting point only and encourage clients to view product evaluations and adapt criteria weightings using the Excel-based vendor comparison tool (see Figure 1 and see Figure 2). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 1 Forrester Wave™: Midsize Managed Security Services Providers, Q3 2020

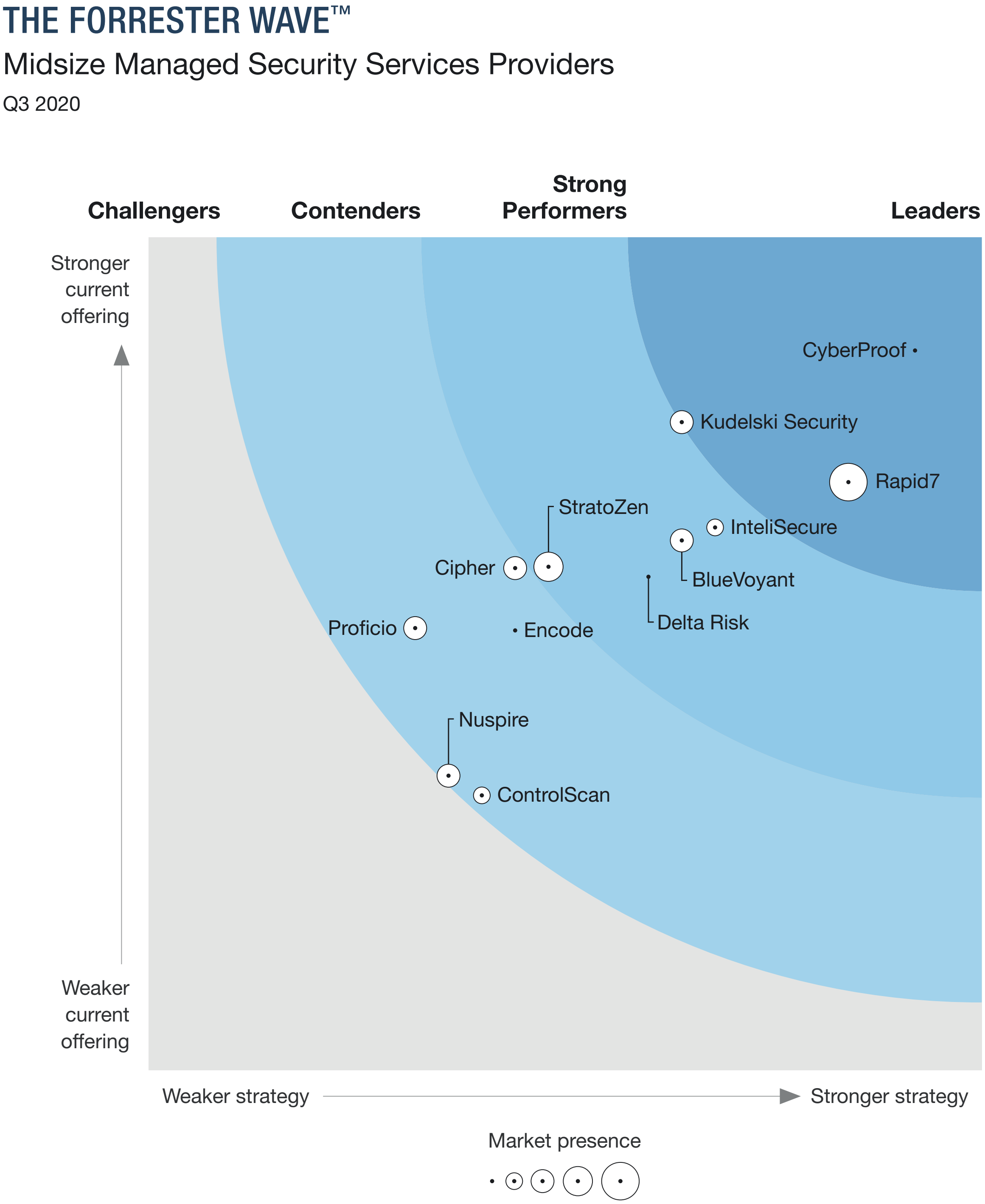


FIGURE 2 Forrester Wave™: Midsize Managed Security Services Providers Scorecard, Q3 2020

	Forrester's weighting	BlueVoyant	Cipher	ControlScan	CyberProof	Delta Risk	Encode
Current offering	50%	3.18	3.01	1.65	4.32	2.96	2.64
Event analysis and correlation: network/endpoint and application	20%	3.00	2.32	1.00	5.00	1.66	3.00
Solution usability	14%	2.50	2.50	2.50	4.00	3.00	3.00
Event collection and environment integrations	20%	3.00	4.80	2.70	3.80	3.90	3.00
Business and technical value	5%	2.00	1.00	1.00	5.00	4.00	3.00
Analytics and automation	20%	4.00	2.00	1.50	4.00	3.00	2.00
Incident management process	16%	3.00	4.00	1.00	5.00	3.00	2.00
Reporting capabilities	5%	5.00	3.00	1.00	3.00	3.00	3.00
Strategy	50%	3.20	2.20	2.00	4.60	3.00	2.20
Service provider roadmap	20%	3.00	1.00	3.00	5.00	3.00	3.00
User experience roadmap	20%	3.00	1.00	3.00	5.00	3.00	1.00
Go-to-market approach	10%	3.00	3.00	3.00	3.00	3.00	3.00
Talent management	10%	5.00	1.00	1.00	3.00	3.00	1.00
Delivery model strategy	10%	3.00	3.00	1.00	5.00	3.00	1.00
Research, development, and innovation management	20%	3.00	3.00	1.00	5.00	3.00	3.00
Partnerships and alliances	10%	3.00	5.00	1.00	5.00	3.00	3.00
Market presence	0%	2.50	2.50	2.00	1.00	1.00	1.00
Number of clients	50%	3.00	4.00	1.00	1.00	1.00	1.00
Overall service revenue	50%	2.00	1.00	3.00	1.00	1.00	1.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 2 Forrester Wave™: Midsize Managed Security Services Providers Scorecard, Q3 2020 (Cont.)

	Forrester's weighting	InteliSecure	Kudelski Security	Nuspire	Proficio	Rapid7	StratoZen
Current offering	50%	3.26	3.89	1.77	2.65	3.53	3.02
Event analysis and correlation: network/endpoint and application	20%	2.34	5.00	2.34	2.32	5.00	3.66
Solution usability	14%	2.50	5.00	2.00	1.00	3.50	3.00
Event collection and environment integrations	20%	4.80	2.00	1.00	2.80	2.80	3.00
Business and technical value	5%	5.00	4.00	3.00	2.00	3.00	4.00
Analytics and automation	20%	3.00	4.00	1.00	3.00	3.00	3.00
Incident management process	16%	3.00	4.00	2.00	4.00	3.00	2.00
Reporting capabilities	5%	3.00	3.00	3.00	3.00	5.00	3.00
Strategy	50%	3.40	3.20	1.80	1.60	4.20	2.40
Service provider roadmap	20%	5.00	3.00	1.00	1.00	5.00	3.00
User experience roadmap	20%	5.00	3.00	1.00	1.00	3.00	3.00
Go-to-market approach	10%	3.00	3.00	3.00	1.00	5.00	5.00
Talent management	10%	1.00	3.00	1.00	1.00	5.00	1.00
Delivery model strategy	10%	3.00	5.00	1.00	1.00	3.00	1.00
Research, development, and innovation management	20%	1.00	3.00	3.00	3.00	5.00	1.00
Partnerships and alliances	10%	5.00	3.00	3.00	3.00	3.00	3.00
Market presence	0%	1.50	3.00	2.50	2.50	5.00	3.50
Number of clients	50%	1.00	2.00	5.00	2.00	5.00	5.00
Overall service revenue	50%	2.00	4.00	0.00	3.00	5.00	2.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Vendor Profiles

Our analysis uncovered the following strengths and weaknesses of individual vendors.

LEADERS

- **CyberProof excels with its virtual analyst, SeeMo.** SeeMo enhances the vulnerability and threat intelligence context behind each alert as well as automating steps of the incident investigation and remediation process to accelerate workflows. Rather than resting on the advantages SeeMo provides, CyberProof has a strong roadmap of future features and planned improvements. The roadmap focuses on providing benefits for its clients in addition to its internal service delivery personnel, something not all MSSPs always consider.

  Customer references note CyberProof's automation, flexibility, and highly skilled staff as key differentiators. Reference customers stated that CyberProof's communication behind the scenes and global footprint for service delivery (with data sovereignty as a particular area of concern as the company grows) as areas for improvement. Companies looking for an MSSP that provides high-context alerts and is well versed in automation, orchestration, and remediation should consider CyberProof.

- **Rapid7 leads with exceptional reporting.** Rapid7 offers clients access into the InsightIDR compliance dashboard with customized reporting. Clients also get a customer advisor for further assistance, providing a valuable, easy-to-understand dashboard. The customer advisor sets the vendor apart from competitors because most MSSPs struggle to provide meaningful dashboards and reporting. Rapid7 has a definite focus on MDR and endpoint. The vendor also offers insider threat monitoring with user behavior analytics (UBA) capabilities. Recent acquisitions improved network analysis and visibility (NAV) and analytics, making the portfolio comprehensive enough to become a viable alternative to traditional MSSPs.

  Rapid7's cloud platform support is limited to purely Rapid7 products, with integrations available for other security products such as enterprise detection and response (EDR) tools. However, reference customers raved about how Rapid7's dedicated staff provides a huge benefit. They remarked that the staff is not only there to answer any question but also to provide guidance on industry trends not specific to services. Customer references also said that service delivery limits exist due to the limited geographic footprint of Rapid7 SOCs in the US and UK. Existing Rapid7 clients should consider expanding services, and companies looking for a well-integrated alternative to legacy MSSPs should investigate Rapid7.

- **Kudelski Security tailors services for customers' individual needs.** Kudelski Security's Cyber Fusion Center (CFC) gathers and analyzes threat intelligence, making recommendations for remediation steps specific to each customer. These are blended to create a white glove experience for clients. Kudelski Security continues to expand in North America. It uses the funding and scale of its parent organization to fuel this growth, while operating as an engine to drive innovation.

Industrial control system (ICS) services differentiate Kudelski Security from its competitors. The vendor is one of the few providers with clear ability to deliver MSS for ICS environments that were not solely dependent on vendor hardware solutions. Reference customers praise Kudelski Security's technical expertise, IR, and detection capabilities as well as the high-touch nature of service delivery. However, references expressed frustration with the onboarding process and said portal training is problematic. References would also like to see improvements in the vendor's limited cloud capability. Companies seeking a white glove, context-heavy MSS, as well as those looking for an MSSP that can provide ICS native MSS, should strongly consider Kudelski Security.

STRONG PERFORMERS

› **InteliSecure centers its offering on data protection and human behavior.** The vendor's Critical Asset Protection Program (CAPP) identifies and maps critical data as it relates to each customer's business, leading to a service that understands the value of the data it protects. This data-security-led approach, different from most MSSPs, emerged from analytics and alerting derived from traditional infrastructure to drive SOC use cases. InteliSecure goes to market with a targeted approach that includes the precise scenarios where it will provide value for clients with data security use cases as the primary driver of value.

InteliSecure currently lacks automation capabilities and relies on its customers to make those automation investments before it's able to leverage them. Customer references noted occasional slow escalations due to technical issues and lengthy resolution times for internal tickets as problems that needed to be addressed. Reference customers identified InteliSecure's innovation with a data security service and its vendor-neutral approach as strengths. Companies concerned about sensitive data leakage and/or theft should take a look at InteliSecure.

› **BlueVoyant makes security services compliance friendly.** The Wavelength client portal allows customers to continuously view their security posture. The portal also provides a transparent interface for clients to observe the tasks and efforts of BlueVoyant analysts, so clients understand exactly what the service does for them. BlueVoyant's security service centers on Microsoft's security portfolio, including Azure Security Center and Azure Sentinel. This makes its approach unique as an MSSP emphasizing cloud platforms for service delivery. Despite taking an innovative approach to cloud-based service delivery, BlueVoyant's collaboration methods aren't as innovative, relying on dated methods to connect with clients.

BlueVoyant is working through the pains expected when companies grow quickly. Customer references brought up the limitations of the BlueVoyant portal not showing detailed security information and lower-level analysts who lacked knowledge, leading to inconsistent client experience. They did, however, rave about BlueVoyant's vertical expertise, especially in financial services. BlueVoyant's threat intelligence and technical aptitude, especially for cloud platforms, are notable strengths. Companies seeking an MSSP with a cloud-led approach, transparent portal, and extensive financial services expertise should consider BlueVoyant.

- **Delta Risk uses its ActiveEye platform as a cloud-first integration point.** The vendor's ActiveEye platform covers discovery, detection, investigation, response, and reporting. ActiveEye is cloud native and uses the benefits of a cloud approach to offer comprehensive integrations with EDR tools, cloud infrastructure providers, SaaS solutions, and SIEM platforms. By developing and controlling the intellectual property of this cloud-based platform, Delta Risk can maximize the value it creates as a service delivery platform. This is advantageous because Delta Risk isn't dependent on integrations with third-party commercial tools for full-service delivery.

  Much of the portal remains opaque to clients, only viewable by Delta Risk analysts. This hides some of the value Delta Risk provides through the activities it performs on clients' behalf. Specifically, reference customers identified Delta Risk's customer support and general lack of transparency as areas for improvement. Customer references praised Delta Risk's expansive partnerships, cloud native expertise, and wide range of available integrations as key strengths. Midmarket companies seeking a platform-based approach that heavily leans toward managed SOC-as-a-service use cases should investigate Delta Risk.

- **StratoZen's executive summary expresses the technical value of its MSS.** The vendor's portal-delivered executive summary shares alert, incident, and escalation summaries. It also provides valuable tactical and operational service-related data that clearly describes the benefits clients receive. StratoZen possesses strong understanding of its target market, recognizing that not all clients can — or will — understand the service. In many cases, StratoZen is the entirety of the security program for most of its small business and midmarket clients, so it emphasizes that in its approach to service delivery. This is reflected in the vendor's approach to customer support, as it helps these small clients understand their network infrastructure.

  StratoZen's knowledgeable analysts were praised by customer references. References also noted rapid time-to-value through ease of deployment and rapid onboarding and analyst flexibility as pluses. However, reference customers identified confusing alerts and the lack of a mobile application for customer-to-analyst communication as minuses. Firms looking for in-depth discovery on monitored devices to enhance situational awareness, and those with limited or no security staff, should strongly evaluate StratoZen.

CONTENDERS

- **Cipher looks to MDR to propel its existing managed SOC approach.** The vendor uses the traditional managed SOC approach, supplemented by Portolan, its cyberintelligence orchestration tool, as the backbone of service delivery. Customer demand made MDR services a focus for Cipher. MDR expands the service portfolio of Cipher to the endpoint, but it is not a transformation of the existing business model to a new one. The managed SOC portion demonstrates Cipher's expertise on common SIEM platforms, like Splunk, as well as SOC workflow, especially for detection and response.

Cipher's extensive reporting capabilities provide value, but the data used is isolated to technical security data. This limitation requires customer effort to translate and apply findings to the overall business. Customer references note Cipher's Splunk expertise and complementary set of available professional services as strong points in their relationship. On the downside, they commented that incident analysis in alerts wasn't always as detailed as desired. Reference customers also stated that internal communication within Cipher needs improvement. Companies considering a shift to MDR that also require SIEM expertise should consider Cipher as a potential MSS partner.

- **Encode uses MDR to complement its managed SOC service.** Encode focuses on 24x7 MDR and SOC-as-a-service. The vendor provides traditional SIEM reports from its report repository, SOCStreams, which offers a comprehensive set of reports. Encode has a broad expertise on multiple SIEM platforms, such as AWS GuardDuty, Elastic, and QRadar, and has substantial expertise with EDR and network traffic analysis third-party security solutions. The shift to MDR means that Encode now focuses on the endpoint in addition to delivering its legacy monitoring- and analytics-based response and remediation services.

  Encode's remediation efforts are limited, based on the premium a customer is willing to pay. Customer references indicate that general email alerts aren't as comprehensive as they'd like. Specifically, reference customers called out the slow development of new features and the vendor's struggle to support cloud platforms. On a positive note, reference customers do like Encode's agility, impressive knowledge of the security vendor landscape, and meaningful alerts with few false positives. Companies beginning the shift from a SIEM-based set of security services to an MDR-first approach should take a look at Encode.

- **Proficio uses benchmarks and threat intelligence to guide client security decisions.** Proficio calculates a risk score using its ThreatInsight solution to identify alert criticality. ThreatInsight extends the calculated risk score to peer groups, creating a strategic metric for clients to compare against current trends. Unfortunately, while competitors turned toward cloud platforms and MDR, Proficio remains an ArcSight- and Splunk-centered vendor. Therefore, Proficio needs substantial innovation before reaching service parity with the rest of the market.

  Proficio needs to address this in the future to remain competitive with others in this Forrester Wave. Customer references mention Proficio's log monitoring and incident response activities, as well as their responsiveness, as positives. But they shared concerns about reporting limitations, a substandard executive dashboard, and limited communication methods as weaknesses. Companies with an on-premises ArcSight implementation that want deep ArcSight-specific expertise should consider Proficio.

- **ControlScan offers managed SIEM and MDR for the midmarket.** ControlScan understands the needs of midsize organizations. These companies often have third-party compliance requirements that require sophisticated security expertise but can't find an MSS partner that works well with midsize organizations that have some enterprise needs. ControlScan designed its MSS to address this underserved market. The vendor seeks to offload tactical security tasks from customer teams to ControlScan analysts. Technology partners supplement ControlScan's current MSSP capabilities, with MDR becoming an important focus in the near term.

ControlScan's data storage is limited to only the US, which can create data sovereignty issues. Reference customers applaud ControlScan's knowledgeable employees, alert accuracy, and customer support teams. However, customer references also mention limited vulnerability scanning capabilities and limited report customization as areas for improvement. Midsize companies seeking a North American MSSP should investigate ControlScan.

- **Nuspire provides MSS for small businesses that lack security expertise.** Nuspire maintains a laser focus on the security needs of the small business clients it serves. The vendor has to balance innovation and improvement with the fact that many customers are using the service because third parties require them to or to satisfy a compliance mandate. Nuspire prioritizes time-to-value for clients with strong onboarding processes that clearly establish the expectations for how clients want incidents handled. The vendor provides standardized and compliance-focused reporting capabilities. This enables clients with little or no security expertise to demonstrate that the service is enabled, working, and valuable. On the downside, Nuspire has limited cloud capabilities and no automation currently available, which is not unreasonable given that its target customers are small businesses.

  Customer references note flexibility, ease of use, and responsiveness as Nuspire's biggest strengths. However, customers critiqued Nuspire's limited service portfolio as an understandable, but obvious, weakness. SMBs with third-party requirements, compliance mandates, and limited-to-no security expertise should take a hard look at Nuspire.

Evaluation Overview

We evaluated vendors against 26 criteria, which we grouped into three high-level categories:

- **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave graphic indicates the strength of its current offering. Key criteria for these solutions include threat intelligence, data sovereignty, business value, technical value, cloud security analytics/dashboard integration, collaboration methods, and reporting capabilities.
- **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. We evaluated service provider roadmaps, user experience roadmaps, talent management, and partnerships and alliances.
- **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's number of clients and overall service revenue.

VENDOR INCLUSION CRITERIA

Forrester included 12 vendors in the assessment: BlueVoyant, Cipher, ControlScan, CyberProof, Delta Risk, Encode, InteliSecure, Kudelski Security, Nuspire, Proficio, Rapid7, and StratoZen. Each of these vendors has:

- **Smaller annual MSS revenue than global MSSP firms.** Each participant has $55 million or less in annual revenue.
- **A complete suite of managed security services.** We included vendors that offer a complete suite of managed and monitored solutions that enhance customers' existing security investments and workflows.
- **Mindshare with Forrester clients.** Forrester clients often discuss the participating vendors during inquiries and interviews. Alternatively, the participating vendor may, in Forrester's judgment, have warranted inclusion because of technical capabilities and market presence.

FORRESTER®

Supplemental Material

ONLINE RESOURCE

We publish all our Forrester Wave scores and weightings in an Excel file that provides detailed product evaluations and customizable rankings; download this tool by clicking the link at the beginning of this report on Forrester.com. We intend these scores and default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs.

THE FORRESTER WAVE METHODOLOGY

A Forrester Wave is a guide for buyers considering their purchasing options in a technology marketplace. To offer an equitable process for all participants, Forrester follows The Forrester Wave™ Methodology Guide to evaluate participating vendors.

In our review, we conduct primary research to develop a list of vendors to consider for the evaluation. From that initial pool of vendors, we narrow our final list based on the inclusion criteria. We then gather details of product and strategy through a detailed questionnaire, demos/briefings, and customer reference surveys/interviews. We use those inputs, along with the analyst's experience and expertise in the marketplace, to score vendors, using a relative rating system that compares each vendor against the others in the evaluation.

We include the Forrester Wave publishing date (quarter and year) clearly in the title of each Forrester Wave report. We evaluated the vendors participating in this Forrester Wave using materials they provided to us by June 4, 2020, and did not allow additional information after that point. We encourage readers to evaluate how the market and vendor offerings change over time.

In accordance with The Forrester Wave™ Vendor Review Policy, Forrester asks vendors to review our findings prior to publishing to check for accuracy. Vendors marked as nonparticipating vendors in the Forrester Wave graphic met our defined inclusion criteria but declined to participate in or contributed only partially to the evaluation. We score these vendors in accordance with The Forrester Wave™ And The Forrester New Wave™ Nonparticipating And Incomplete Participation Vendor Policy and publish their positioning along with those of the participating vendors.

INTEGRITY POLICY

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Endnotes

[1] See the Forrester report "CISOs, Get Ready To Pay More As Tech Titans Enter The Security Market."

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

nuspire

ABOUT NUSPIRE

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24×7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser-focused on delivering an extraordinary cybersecurity experience that exceeds client expectations. For more information, visit www.nuspire.com and follow @Nuspire.