ISG Provider Lens™

Cybersecurity - Solutions & Services

Managed Security Services - Large Accounts

U.S. 2021

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

August 2021

Customized report courtesy of:

CyberProof
A UST Company

About this Report

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of July 2021, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars ($US) unless noted.

The lead author for this report is Gowtham Kumar. The editor is Sabrina. The research analyst is Srinivasan P.N and the data analyst is Rajesh C. The quality and consistency advisor is Doug Saylors.

ISG Provider Lens™

ISG Provider Lens™

ISG Provider Lens™ delivers leading-edge and actionable research studies, reports and consulting services focused on technology and service providers' strengths and weaknesses and how they are positioned relative to their peers in the market. These reports provide influential insights accessed by our large pool of advisors who are actively advising outsourcing deals as well as large numbers of ISG enterprise clients who are potential outsourcers.

For more information about our studies, please email ISGLens@isg-one.com, call +49 (0) 561-50697537, or visit ISG Provider Lens™ under ISG Provider Lens™.

ISG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

For more information about ISG Research™ subscriptions, please email contact@isg-one.com, call +49 (0) 561-50697537 or visit research.isg-one.com.

EXECUTIVE SUMMARY

Major Trends Witnessed in U.S.

The U.S. is becoming a lucrative target for cyberattacks from a host of threat actors. While some sophisticated attacks have been state-sponsored to undermine the government's capability in protecting citizen privacy and state intelligence, most of them have used ransomware and malware for ransom payouts. The recent attack on SolarWinds has set a new precedence to formulate and enact stricter cybersecurity regulations and mandates to prevent such events of massive breach and spread across sectors. SolarWinds, an IT firm in the U.S., was the subject of a cyberattack that spread to its clients and went undetected for months, allowing hackers to spy on private companies including cybersecurity firm FireEye and the top strata of the U.S. government such as the Department of Homeland Security and Department of the Treasury.

The recent pipeline hack, on Colonial Pipeline, is another evidence of the lack of security protocols and measures against sophisticated ransomware attacks. Hackers and attackers are unrelenting with their methods and strategies in identifying vulnerabilities that not only create backdoors to critical systems but expose other weaknesses that could exploit connections with a larger ecosystem of channels, partners and customers. These advanced persistent threats require significant improvements in several areas and cannot be addressed by any single solution or platform. Enterprises need to rethink their security strategy with investments directed toward security solutions, including identity management, endpoint protection, and advanced data leakage and protection.

ISG Provider Lens™

The demand for these solutions has contributed to the growth of service providers that offer advisory, implementation and managed services, leading to strong partnerships with solution vendors. Service providers are realizing that the complex demands of end-user organizations can only be met with best-of-breed technologies creating the need for forging alliances, partnerships and co-innovation among security providers. Investments have been pouring in to build centers of excellence (COEs), intelligence labs, global security operations centers (SOCs), playbooks and frameworks, and these efforts emphasize the need for a collaborative approach to successfully mitigate advanced threats as well as prevent the spread across the ecosystem. End-user organizations and security providers are leveraging standardized approaches from trusted agencies including National Institute of Science and Technology (NIST), MITRE and several regional and country agencies. They have begun active collaborations with each other and with the vendor ecosystem. These initiatives and investments have resulted in strong growth for security solutions and services, especially for providers with a robust portfolio and distinctive competitive capabilities.

Cloud Security, Zero Trust Architecture and Treat Intelligence Gaining Traction

The growing sophistication from attackers as well as threat actors have necessitated the formulation of new strategies to reduce intrusion, with the need to authenticate and verify even trusted sources. According to the approaches from National Institute of Science and

Technology (NIST), zero-trust architecture is a cybersecurity plan that utilizes zero-trust concepts and encompasses component relationships, workflow planning and access policies. Organizations across the U.S. are realizing that a "trust but verify" approach should become the de facto policy to better secure against internal and external threats, especially in scenarios with complex and advanced persistent threats looming. Security service providers and solution vendors are increasingly leveraging this architecture as a foundational element for providing secure access to enterprise applications and services.

In addition, the growth of data within businesses and the ability to identify risk posture from this data has been spurring the interest for advanced threat intelligence. Organizations are no longer relying on reactive measures but demand a proactive, preventive stance to protect their data assets against treats and attackers. Enterprises that heavily invested in intellectual property (IP), patents, critical systems in healthcare, financial services and utilities are ramping efforts to isolate and deflect cyberattacks with error-free security measures. Real-time threat detection, enhanced visibility across the network and improved behavioral analysis of threat actors are being combined to provide advanced threat intelligence. This will further bolster the preparedness and awareness among enterprises and users to thwart cyberattacks.

Aggressive Initiatives from Federal Agencies

Based on the recent targeted attacks on U.S. enterprises, the Biden administration issued its "Executive Order on Improving the Nation's Cybersecurity" that prioritizes cloud and zero-trust security architectures, as well as prompting a reassessment of the U.S. federal government's cybersecurity policy. The new administration's comprehensive cybersecurity directive mandates new practices, workflows, architectures and deadlines. It further calls for "bold changes and significant investments" for government IT and operational technology (OT).

The U.S. Cyber Command and the National Security Agency works with the U.S. government, private industry, academia and international partners to achieve and maintain cyberspace superiority. This will be achieved by building resilience at home, implementing proactive defense strategies, and contesting adversaries' campaigns and objectives. These partnerships and collaborations will make it increasingly difficult for adversaries to operate. Furthermore, the Department of Homeland Security has decided to regulate cybersecurity in the pipeline industry. Such key infrastructure companies are expected to report cyber incidents to the federal government.

The success of these programs is based on the development of extensive new partnerships between public and private sector organizations.

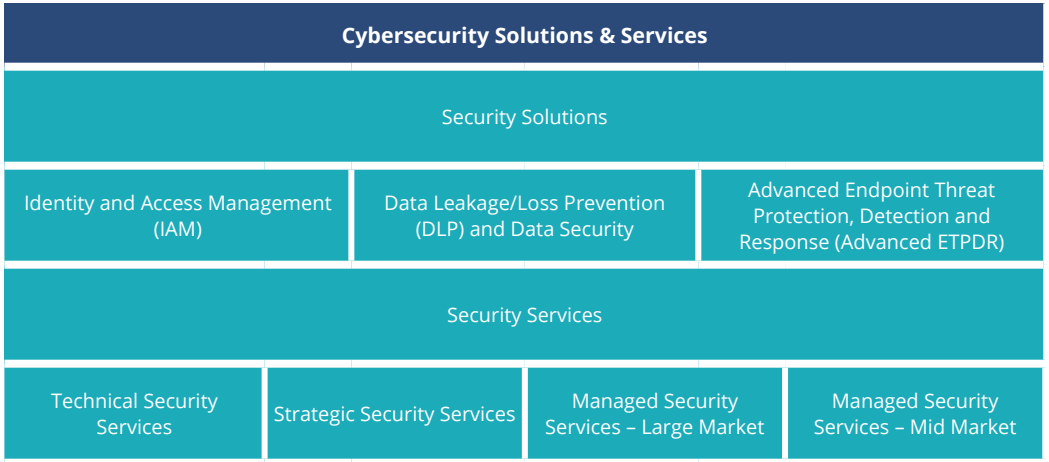
Managed Security Services Trends

Managed security services are evolving from traditional monitor-and-react models to a more proactive one that includes both defensive and offensive capabilities. As advancements and sophistication have increased from both the protection and attack fronts, it has become increasingly difficult for organizations to handle these complexities on their own. Moreover, as several organizations are working remotely with a distributed workforce, the situation demands for more efficient security services.

New security services are critical as configurations change how day-to-day business is conducted across all permutations of LAN, WAN, the cloud and the web. Many applications that were traditionally in-house and on-premises are now hosted, managed or used as a service. Portfolio offerings such as managed (digital) identity (IDaaS), threat hunting, counterintelligence and cloud security for private, public and hybrid designs are increasingly available. Bundled service packages are now common add-ons; for example, managed detection and response (MDR), EDR and security and compliance packages or generalized security hygiene packages. Specialized security operations center services exist for industries such as automotive or financial services, as well as for other areas such as operational technologies and connected devices (IoT, IIoT and ICS/SCADA).

Introduction

Simplified illustration



Source: ISG 2021

Definition

Enterprises are swiftly adopting new technologies to embark on digital transformation journeys to stay competitive and align with the ever-evolving needs of end users. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has led to an increase in exposure and a growing threat attack surface. Ransomware, advanced persistent threats, and phishing attacks emerged as some of the leading cyberthreats in 2020. Experian, SolarWinds, Zoom, Magellan Health, Finastra and Marriott were some of the leading entities that faced cyberattacks from hacking, malicious code, and ransomware in the past year.

Attackers are always looking for new and ingenuine ways to breach the defense mechanisms. This has led to an increase in their sophistication, as these attackers access different points in an enterprise IT ecosystem such as supply chain networks to breach security. In 2020, there was a rise

Definition (cont.)

in several other high-profile cyberattacks that targeted intellectual property, personal identifiable information (PII) and confidential records as well as client information within enterprises across the healthcare, hospitality, IT, finance and other industries. Data belonging to nation states was also being compromised. Apart from causing operational damage, these attacks impacted brand value, IT systems and the financial health of the targeted organizations.

The global threat scenario was further exacerbated in 2020 with the COVID-19 pandemic, which resulted in a large portion of employees working remotely, mainly from home. This new work model resulted in an increased use of collaboration tools and platforms and public networks, exposing users to phishing and other malicious threats. With this ever-changing threat landscape, enterprises should take a detailed and inclusive approach to cybersecurity to safeguard their businesses by implementing a mix of security products and services across areas such as IAM, data security and managed security services to achieve a robust secure framework that is suited to their needs and vision.

As the nature and complexity of cybersecurity threats continue to increase, hackers are constantly searching and targeting vulnerable sources and IT infrastructures. Some threats such as phishing, spear phishing and ransomware aim to benefit from the ignorance of people and their online behavior. The increased level of online activity, led by ecommerce and online transactions, has broadened the vulnerability stance and exposed end users to cybercriminals who are looking for any digital traces left behind. This makes users and IT endpoint systems with a low security posture and weak defense mechanisms an easy prey to cyberattacks.

The serious implications faced by enterprises from phishing and ransomware threats have led to the emergence of services to counter such advanced threats. These services and solutions extend beyond the basic perimeter and conventional security measures and offer continuous deep monitoring, inspection and protection, along with a structured incident response approach. In addition to the need for self-protection, laws and regulations such as the General Data Protection Regulation (GDPR) in Europe have led businesses to implement stronger safeguard measures to counter cyberattacks. Similar legislation exists in other countries such as Brazil and Australia to safeguard users from cyber threats and attacks.

Definition (cont.)

Cybersecurity has become an important practice area for enterprises due to its impact on businesses and their processes. However, IT executives often struggle to justify security investments to business stakeholders, particularly the CFO. Unlike other IT projects, it is not always possible to measure and demonstrate the return on investment (ROI) as well as quantify threat-related risks. Therefore, security measures are often at a low level and are not sufficient to address sophisticated threats. On the other hand, the availability of suitable technology does not always result in the elimination of vulnerabilities; many security incidents such as Trojan and phishing attacks are caused due to the ignorance of end users. Awareness-related aspects among end users may result in targeted attacks such as advanced persistent threats and ransomware, which impact brand reputation and cause data and financial losses in addition to operational outages. Therefore, consulting and user training continue to play a key role, together with up-to-date information and communications technology (ICT) infrastructure. The rising complexity of threats has also led to an increased focus on monitoring, detection and response services as well as signature-based protection and other security services to safeguard enterprises beyond the perimeter.

Scope of the Report

The ISG Provider Lens™ Cybersecurity – Solutions & Services 2021 study aims to support ICT decision-makers in making the best use of their tight security budgets by offering the following:

- Transparency on the strengths and weaknesses of relevant providers
- A differentiated positioning of providers by market segments
- A perspective on local markets

For IT providers and vendors, this study serves as an important decision-making basis for positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also leverage the information from ISG Provider Lens™ reports while evaluating their current vendor relationships and potential new engagements.

Provider Classifications

The provider position reflects the suitability of IT providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions IT providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between US$20 million and US$999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above US$1 billion, with activities worldwide and globally distributed decision-making structures.

Provider Classifications

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly.

Leader

Leaders have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

Product Challenger

Product Challengers offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

Market Challenger

Market Challengers have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

Contender

Contenders offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in both products and services and a sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

Provider Classifications (cont.)

Each ISG Provider Lens™ quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star. Number of providers in each quadrant: ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).

Rising Star

Rising Stars have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

Not In

The service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.

Cybersecurity - Solutions & Services Quadrants

ENTERPRISE CONTEXT

Managed Security Services - Large Accounts

This report is relevant to enterprises across industries in the U.S. for evaluating providers of managed security services.

In this quadrant report, ISG highlights the current market positioning of providers of managed security services to enterprises in the U.S., and how each provider addresses the key challenges faced in the region.

Without the appropriate managed IT support, IT systems are vulnerable to exploitation. As more crucial processes move onto the cloud and cybercriminals become even more sophisticated, there is an even greater need for a smarter way of improving security. As a result, the demand for cloud security, security operations center (SOC) services, Internet of Things (IoT) and operational technology (OT) security and zero trust security has been increasing among enterprises over the past few years.

Managed security service providers (MSSPs) established their own, dedicated, co-managed or virtual SOCs within the region to serve enterprises. The managed security services (MSS) market in the U.S. is mainly driven by the growing need for security solutions across various end-user industries. Regulation and compliance pressure will increase the demand for MSS in the region.

The following can use this report to identify and evaluate different service providers:

Chief information officers (CIOs) should read this report to better understand how the current processes and protocols impact an enterprise's existing systems as well as the security needs for the adoption and integration of new capabilities.

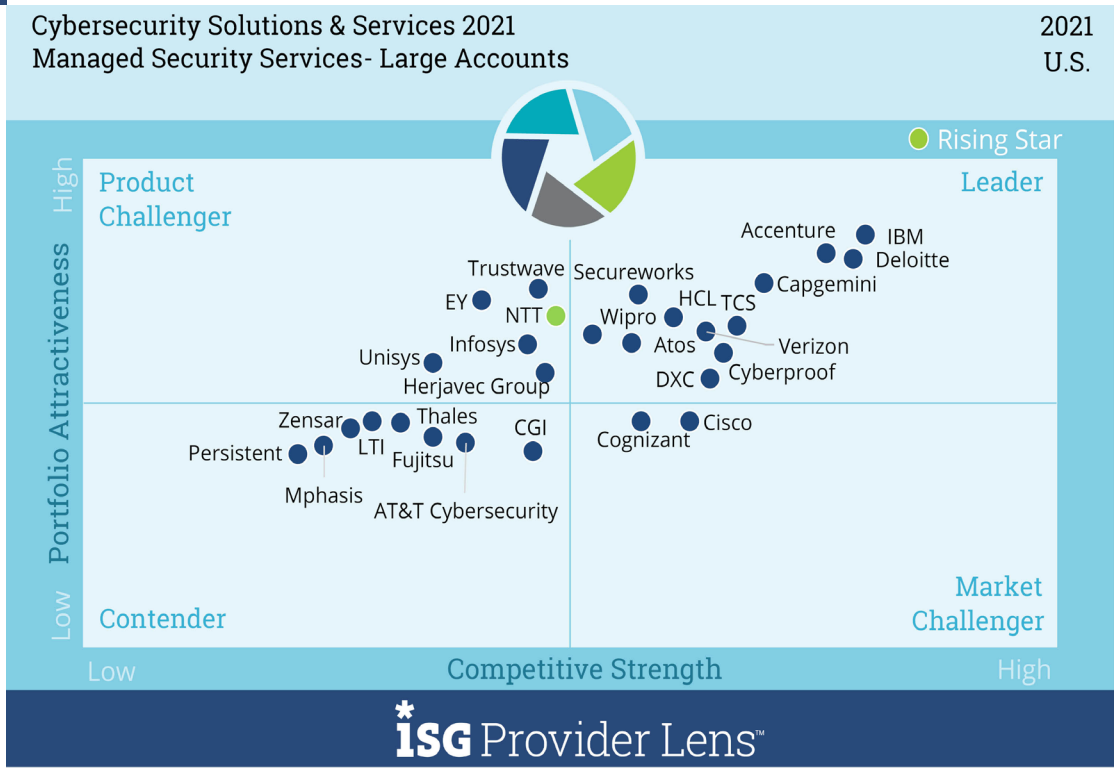
Chief technology officers (CTO)s handling operations and services should read this report to acquire in-depth knowledge on emerging technologies and solutions to gain strategic directions as well as partnership options with relevant service providers. CTOs can also ensure the deployment of appropriate security platforms and solutions, enabling competitive advantage.

Security leaders should read this report to understand the relative positioning and capabilities of MSSPs. The report also compares the technical capabilities of various service providers in the market.

MANAGED SECURITY SERVICES - LARGE ACCOUNTS

Definition

Managed security services comprise the operations and management of IT security infrastructures for one or several clients by a security operations center. Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, antivirus operations, IAM operation services, DLP operations and all other operating services to provide ongoing, real-time protection without compromising on business performance. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate the best-of breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.



Source: ISG Research 2021

MANAGED SECURITY SERVICES - LARGE ACCOUNTS

Eligibility Criteria

- The service provider should be able to provide security services such as detection and prevention, security information and event management (SIEM), and security advisor and auditing support remotely or at the client site.
- The provider should hold relevance, in terms of revenue and number of customers, in the respective country for managed security services.
- It should not be exclusively focused on proprietary products but can manage and operate the best-of-breed security tools.
- The provider should possess accreditations from vendors of security tools.
- Security operations centersshould be ideally owned and managed by the provider and not predominantly by partners.
- The provider should maintain certified staff; for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

Observations

Managed detection and response includes components of the traditional model where a service provider monitors for anomalies in networks, servers, firewalls, log activity, web traffic, etc. and generates alerts during non-typical conditions. Furthermore, clients are increasingly engaging with providers to coordinate the incident response team. Cybersecurity and fusion centers have emerged, not to replace security operations centers but to expand and extend security operations. These centers leverage advanced technologies such as AI, machine learning, edge computing, blockchain and other tools that can ingest large volumes of data, produce smart analytics, deliver layered security, push back criminals and open lines of business communication and collaboration, while giving insights into how threats morph, move and multiply.

Clients engage service providers in several different ways. They may fully outsource security operations, ceding control and decision making to providers and tying their automated response protocols to customized risk tolerances. Others will use a subscription or license agreement scenario for a SIEM platform so they can maintain control over operations. Quite a few engage managed security service providers (MSSPs) on a hybrid basis to supplement some existing in-house capacity or skillset with services that fill the gaps or enhance vigilance.

MANAGED SECURITY SERVICES - LARGE ACCOUNTS

Observations (cont.)

Finally, clients in the U.S. are seeking innovative performance-based contracts where older style response time service-level agreements (SLAs) are irrelevant to a ransomware attack. They seek to share the risk with security service providers when a breach or attack is not prevented. Focus might be placed on functionality and availability of the tool or platform, ensuring that analysts act promptly when anomalies occur and successfully automate actions wherever possible.

From the 85 companies assessed for this study, 28 have qualified for this quadrant with 11 being Leaders and one as a Rising star.

- **Accenture** has a 7,000-member strong cybersecurity team that applies strategy and transformational processes to client engagements. It is further complemented by network of global fusion and operation centers specialized in more than a dozen industry verticals.
- **Atos** MDR uses advanced security analytics on endpoints, user behavior, applications and network for deeper multi-vector detection. Atos AIsaac® leverages more than 75 AI models that enable automated hunting and data mining.
- **Capgemini's** global network of Cyber Defense Centers (CDCs) provides advanced, analytics-driven SIEM services that combine incident detection and response as well as monitoring.
- **CyberProof** approaches its clients with use case methodology that aims to identify and map business risks against the most likely attack scenarios. The identification of these gaps improve their detection and response capabilities against the MITRE ATT&CK matrix.
- **Deloitte** is heavily focused on managed detection and response over other traditional managed security elements. It offers a proactive threat hunting service to identify and investigate advanced threats by using telemetry from EDR tools and logging data from the cyber data lake.
- **DXC Technology** has invested significantly in creating differentiators and best practices that are embodied in its Cyber Reference Architecture and Cyber Maturity Review, combined with the intellectual property within blueprint accelerators.
- **HCL** offers a structured approach to their key offerings including managed protection services, cybersecurity monitoring and incident response, security assurance services, IAM operations, GRC operations, security of things operations, and cloud-security-as-a-service operations.

MANAGED SECURITY SERVICES - LARGE ACCOUNTS

Observations (cont.)

- **IBM** has invested in a new advisory and managed services offering called Cloud Native Security Services aimed at reducing the risk of cloud misconfiguration and offering insights into potential threats.
- **Secureworks** has an extensive portfolio of managed services which includes managed firewall and intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor the security hygiene of thousands of clients with flexible delivery models.
- **TCS** leverages its more than 12 threat management centers and over 200 security operations centers, of which most are client specific. It has invested in creating platforms for most of the managed security services that can integrate with existing technology stacks.
- **Verizon's** advanced security operations center solutions are fully customizable cybersecurity event-monitoring solutions, designed for enterprises to maximize their SIEM and related security investments.
- **Wipro** leverages its team of security operations center operators with a 24-by-7-by-365 service delivery window to analyze system-prioritized alerts in near real time. Their managed security services business caters to customer needs, spanning across intelligence, protection, detection, remediation, response and recovery. It has
- **NTT** has brought application security in-house with the acquisition of WhiteHat and has also integrated a zero-trust framework into its consulting services. extending it to integration and managed services as well.

ACCENTURE

Overview

Accenture is ranked among the top IT and business services firms and generated US$44.3 billion in revenue in 2020, reporting across five industry groups. It has more than 506,000 employees in over 120 countries. Often growing through acquisitions, it provides professional services, including outsourcing and managed technology and cybersecurity, to 4,000 clients. Its 7,000-member strong cybersecurity team applies strategy and transformational processes to client engagements. The company has a network of global fusion and operation centers that specialize in more than a dozen industry verticals.

Strengths

Skilled team and Fusion centers: The Accenture team has more than 500 skilled cybersecurity professionals in North America, with more than 90 cyber specialists focused exclusively on industrial control systems. The company has an expanding network of nine cyber fusion centers that build on the proficiency of its own internal cyber defense team in Accenture Labs, including its elite hacker group called Fusion-X.

Advanced analytics and intelligence capabilities: Accenture combines its internal resources with the expertise of external security researchers and technology partners to utilize an advanced analytics capability and automated intelligence to provide managed security for application, cloud, digital identity, risk and threat operations services.

Expanding partnerships and investments: Accenture maintains partnerships with more than 200 technology companies across the security ecosystem; some of them include Netskope, Okta, Ping Identity and Tanium. This allows the company to be vendor agnostic while transforming strategic recommendations into action plans.

Caution

Accenture's price point is suited for large organizations rather than small and mid-sized companies.

2021 ISG Provider Lens™ Leader

With its advanced monitoring, analysis and reporting capabilities as network of fusion centers for intelligence, the company is uniquely positioned to provide managed security services to enterprises in the U.S.

ATOS

Overview

Atos is large French technology transformation and digital services company with US$13 billion in annual revenues, of which more than US$1 billion is attributed to big data and cybersecurity. It employs more than 6,000 security professionals and operates through a network of 14 global security operations centers in addition to a cadre of tactical security software and hardware solutions. Along with managed security, Atos also provides consulting services to assess programmatic security needs as well as integration and implementation expertise to execute recommendations.

Strengths

Advanced detection and response capabilities: Atos' managed security services offer a full spectrum of sophisticated detection and response services round the clock and across the globe and is called advanced detection and response service. The service establishes highly resilient security practices to counter today's advanced persistent and sophisticated threats. The service also comes with a CERT service add-on to ensure seamless and swift response to threats after they are detected.

Superior threat intelligence: Managed detection and response (MDR) is an advanced managed security service that provides threat intelligence, threat hunting, security monitoring, incident analysis and incident response. The service is driven by the Atos AI platform – AIsaac®. Atos MDR uses advanced security analytics on endpoints, user behavior, applications and network for deeper multi-vector detection. For faster responses, it uses auto threat containment to stop the spread of attacks, and the security orchestration, automation and response (SOAR) module from AIsaac® helps provide rapid response.

Sophisticated training models: Atos AIsaac® leverages more than 75 AI models that enable automated hunting and data mining to detect security incidents. In addition, the AIsaac® SOAR module has automated investigation of detected alerts and containment for detected security incidents. Its threat anticipation feature automates the identification of assets that are affected by latest threat or vulnerability advisories.

Caution

Atos' services are designed for large enterprises and a small percentage of mid-sized firms, making its pricing unaffordable to small organizations.

2021 ISG Provider Lens™ Leader

Atos' success is attributed to its sophisticated team of security experts, combined with an innovative AI platform and network of security operations centers that ensure round-the-clock advanced threat detection and response.

CAPGEMINI

Overview

Capgemini addresses the entire breadth of business needs, from strategy and design to managing operations. The company relies on its deep industry expertise of fast-evolving fields such as cloud, data, AI, connectivity, software, digital engineering and platforms. Its collective experience, industry knowledge and insights into the global security market have made it an expert in combating emerging advanced threats, underpinned by more than 53 years of successfully delivering managed IT and security services to some of the world's most recognizable brands.

Strengths

Tailored and client-specific services: Capgemini's security operations center offerings are created around sector-specific requirements, risk profiles and critical data assets, as well as current security strategies and levels of protection. They are delivered through a variety of options, including managed, dedicated, satellite and hybrid security operations center delivery models, that are tailored to client requirements.

Sophisticated security network: Capgemini's global network of Cyber Defense Centers (CDCs) provides advanced, analytics-driven SIEM services that combine incident detection and response as well as monitoring based on multiple threat intelligence feeds to keep clients' data, users and IT assets safe.

Cloud-based portfolio: Capgemini provides a comprehensive portfolio of security services to address the challenges presented by cloud adoption with a complete end-to-end global managed security offering for hybrid cloud estates, including on-premises, public, private and multi-cloud. With a philosophy to "think like an attacker," the company protect clients by using a combination of threat intelligence, robust architectures and a highly industrialized and automated service delivery model.

Caution

Though Capgemini has renewed its focus on the midmarket, its services are still out of reach from smaller companies.

2021 ISG Provider Lens™ Leader

Capgemini differentiates itself through client intimacy, innovation and reputation as trusted provider of security services. These are complemented by a strong team of security experts, helping the company to maintain its leadership in the U.S.

CYBERPROOF

Overview

CyberProof is part of the UST Global group offering security services to better manage incident detection and response. Operating across 26 countries, the company is among the five strategic Microsoft Gold Partners and leverages the vast regional presence and clientele of UST Global to secure digital ecosystems and mitigation services. It is planning to expand with new offerings to its consulting and services portfolio.

Strengths

Comprehensive and advanced functionalities: CyberProof provides continuous security event monitoring, threat detection and response services by leveraging the CyberProof Defense Center (CDC) platform – a cloud-based single pane of glass interface with built-in orchestration, automation, and collaboration features to facilitate co-sourced security operations. CDC integrates with clients' existing infrastructure and security investments to provide a single pane of glass view of security operations and centralized activities.

Intelligent and contextual assistant: CyberProof SeeMo is an intelligent virtual assistant that converts threat intelligence and vulnerability-related context to alerts. It also automates manual steps taken by human analysts such as enriching event data, proactively querying external sources and responding to analysts' requests by providing contextualized and actionable information.

Use-case based methodology: CyberProof's Use Case Factory is an agile, risk-driven supply chain that identifies and maps business risks against the most likely attack scenarios. It uses these to identify gaps in its detection and response capabilities against the MITRE ATT&CK matrix. These use cases are then developed and implemented across tailored packages of detection rules, response playbooks and integrations and automations that will prevent those attack scenarios from exceeding the defined response window.

Caution

CyberProof has started gaining momentum but should aim at reducing reliance on UST Global clients for expanding its growth in the managed security service market.

2021 ISG Provider Lens™ Leader

CyberProof delivers intelligence-led security services, complemented by its detection and response capabilities and use-case playbooks. The company has elevated its status as a trusted provider of managed security services for the midmarket in the U.S.

DELOITTE

Overview

Deloitte is a large global consultancy with more than 300,000 employees. The London-based company has about one-quarter of its workforce and offices in the U.S., giving it a capacity to deliver advisory services to the largest of global enterprises based in the region. Its offering includes strategic, technical and managed security services. Deloitte's professionals in the U.S. address client concerns in risk management, threat intelligence, vulnerability management, penetration testing and incident response, as well as malware and forensic analysis.

Strengths

Dedicated focus on MDR services: Deloitte is heavily focused on managed detection and response over other traditional managed security elements, offering a proactive threat hunting service to identify and investigate advanced threats by using telemetry from EDR tools and logging data from the cyber data lake and SIEM platforms in addition to other tools. These tools enable an end-to-end service called Cybersecurity Intelligence Center Network that can bring clients from prevention and detection to containment, remediation and recovery.

Established thought leadership: Over the years, Deloitte has established itself as a sought-after leader in cyber intelligence and can influence beyond its client base and markets. Given its background in audit and compliance, it applies these skills to assess the maturity of systems and governance structures alike. The company also trains and coaches its clients' in-house security teams and leadership.

Strong team and industry partnerships: Deloitte has more than 2,000 cybersecurity professionals dedicated to managed security services, and its teams draw on the experience of serving several of the large Fortune 500 companies. Its strategic alliances with key technology and cloud providers, including Google, Amazon Web Services and Microsoft, further exemplify its ability to deliver customized and flexible solutions and services.

Caution

Due to its premium pricing strategy and reputation as a leading provider of consulting services, Deloitte is not a suitable provider for small and mid-sized enterprises.

2021 ISG Provider Lens™ Leader

Deloitte has earned reputation as a strong leader in the managed security services market owing to its experience and expertise gained from solving complex challenges for large enterprises.

DXC TECHNOLOGY

Overview

DXC Technology is a U.S. multinational corporation that provides business-to-business information technology services. For 2020, it reported revenues of US$19.58 billion with 138,000 employees globally. DXC's enterprise technology stack includes analytics and engineering, applications, cloud and security and IT outsourcing. Its global network of more than 12 security operations centers and more than 3,000 security professionals across the globe are available 24-by-7-by-365 to respond to the immediate needs of clients.

Strengths

Strong experienced team of professionals: DXC's comprehensive managed security offerings, security consulting and global scale allow it to address security on an end-to-end basis. With more than 3,500 security staff and 12 security operations centers on five continents, the company has a global presence that ensures a wide service distribution. DXC's teams have gained significant management and advisory expertise from large and complex security engagements, including with many of the Global Fortune 500 companies.

Leveraging innovative technologies: DXC is ranked among the largest MSSPs and leverages AI, analytics, intelligence, orchestration and automation to remediate across business boundaries. It specializes in the areas of cyber defense, secured infrastructure, digital identity and data protection. Its security solutions deliver better business outcomes to help enterprises thrive on change.

Investments for expansion and differentiation: DXC has invested significantly in creating differentiators and best practices that are embodied in its Cyber Reference Architecture and Cyber Maturity Review, combined with the intellectual property within blueprint accelerators, allowing it to drive client value. It has also made strategic acquisitions over the years, including Syscom (a ServiceNow partner), Virtual Clarity, Luxoft and TESM, enabling security to be part of the design and transformation journey.

Caution

DXC should further market and showcase its security operations center capabilities to drive its growth in the managed security services market.

2021 ISG Provider Lens™ Leader

DXC has successfully integrated innovative technologies through a strong team of experienced security professionals spread across connected security operations centers, allowing it to maintain its leadership in the U.S.

HCL

Overview

HCL Technologies (HCL) is a multinational IT services and consulting company headquartered in Noida, India. The company has offices in 32 countries with a worldwide network of R&D innovation labs and delivery centers and over 159,000 employees. HCL Cybersecurity & GRC Services offers a wide portfolio of offerings with the relevant depth and breadth of security and risk domain. Backed by its robust managed security frameworks, HCL's portfolio forms a strong suite of cybersecurity offerings that cover the full scope of managed security services.

Strengths

Comprehensive and holistic portfolio: HCL's key offerings for managed security services fall under broad security pillars. These include managed protection services, cybersecurity monitoring and incident response, security assurance services, IAM operations, GRC operations, security of things operations, and cloud-security-as-a-service operations. The company has 23 dedicated security operations centers in the U.S. to offer its services.

Strong security platform: HCL offers managed security services through its next-generation Cybersecurity Fusion Centers (CSFC) that are powered by its advanced Fusion Platform. CSFC Fusion Platform enables a rapid threat response by automating manual and repetitive processes to drive context-driven investigation. It also provides robust reporting and business intelligence with standard dashboards.

Flexibility in delivery and execution capabilities: HCL CSFCs bring together cross-functional expertise across apps, cloud, datacenter, network and workplace centered on security. This approach of leveraging the "fusion of knowledge" across all centers helps in delivering improved operations and a single point of contact for customers in case of any exigency.

Caution

HCL's commitment to increasing its U.S. footprint and investments to improve delivery capabilities is likely to alleviate existing concerns on localized support.

2021 ISG Provider Lens™ Leader

HCL's robust portfolio of offerings, backed by its experienced security professionals and expertise gained through CSFCs, will continue to propel its leadership status in the U.S.

IBM

Overview

Founded in 1911 and headquartered in Armonk, New York, IBM offers computer hardware, middleware and software as well as hosting and consulting services in areas ranging from mainframe computers to nanotechnology. With 8,000 dedicated professionals around the world, it is one the largest enterprise security providers, gaining 1,900 cloud patents and 1,400 AI patents within a year. Its managed security offerings are based on the SIEM platform and is backed by more than 400 tier-1 and 2 analysts for handling threat detection and investigations through a network of global security operations centers as well as regional, tactical and security research centers.

Strengths

Strong team of security professionals: IBM's security offering is among the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by IBM Security X-Force research, enables enterprises to effectively manage risk and defend against emerging threats. IBM's large clientele is a testament to its capabilities; it caters to 49 of the top 50 global financial services companies and banks, 14 of the top 15 global healthcare companies, and 27 of the top 30 global energy and utility companies.

Cloud-native service expansions: IBM launched a new advisory and managed security offering called Cloud Native Security Services. These services are aimed at reducing the risk of cloud misconfiguration and offering insights into potential threats by enabling centralized visibility and monitoring of native security controls across cloud environments. The services suite also includes container security services that will cater specifically to clients' container environments.

Regional and global presence: IBM is well situated in the U.S. to handle the security needs of global enterprises. Its U.S. network of security operations centers and tactical centers is spread across Boulder and Atlanta, which can coordinate with other security operations centers across the world. These centers host regional and global capabilities that comply with local/regional data sovereignty requirements and time zones.

Caution

IBM should enhance its messaging to attract small and mid-sized enterprises. Furthermore, the company is still unable to shed its strong brand association with large organizations.

2021 ISG Provider Lens™ Leader

IBM has an innovative service portfolio, complemented by its cutting-edge research in AI, analytics and automation. The company has also made investments in the right expertise, giving it a leadership status in the U.S.

SECUREWORKS

Overview

Secureworks is a publicly traded U.S. company that provides information security solutions to global enterprises. Dell Technologies owns 86 percent of its common stock. Secureworks has more than 2,600 employees in eight countries and relies on five security operations centers, a security center of excellence, two primary data centers and a public cloud capacity to deliver security services to over 4,000 clients. Its fiscal year 2021 revenues increased 1.5 percent to US$561 million, with 75 percent originating from U.S. clients.

Strengths

Strong in-house capabilities: Secureworks has been focusing on managed security services and frontline security operations services for more than 20 years. Its proprietary Red Cloak™ Threat Detection and Response (TDR) is a cloud-native software and security analytics application that analyzes client environmental factors against the MITRE's ATT&CK framework. The software is offered in-house or through a fully managed or hybrid engagement model and delivers relevant and validated threat activity alerts to clients.

Comprehensive managed portfolio: Secureworks' portfolio of managed services is extensive. Its managed firewall and IDS and IPS monitor the security hygiene of thousands of clients and facilitates with flexible delivery models. Its advanced threat services help clients detect and respond faster. SIEM services provide 24-by-7-by-365 real-time monitoring and correlation to reduce false positives and provide a consolidated view of endpoints, applications, networks and cloud environments.

Experienced incident response: Secureworks performed more than 1,300 incidents response engagements last year. The company offers both emergency response and retained incident management services. It also evaluates and trains in-house teams for conducting readiness assessments of teams and processes. It runs workshops and practice events to help develop incident response playbooks with varied use cases.

Caution

Secureworks has built its recurring revenue stream by focusing on selling more services to existing large accounts. Despite having a dedicated sales team for the midmarket, the lack of attention has led to client frustration.

2021 ISG Provider Lens™ Leader

Secureworks offers cyber threat intelligence and managed security services round the clock, backed by security expertise and in-house intellectual capabilities. With these attributes, the company has secured a leadership position in the U.S.

TCS

Overview

Founded in 1968 in Mumbai, India, TCS offers IT and consulting services. The company posted revenues of US$23 billion for fiscal year 2021 with operations in 149 locations across 46 countries and a workforce strength of nearly 489,000. As a company with a wide range of IT services, consulting and business solutions, it has been partnering with many of the world's largest businesses in their transformation journey. TCS is investing to secure enterprises across their cloud, IoT and mobile footprints as well as evolving technologies such as 5G and quantum computing.

Strengths

Strategic offshore/nearshore capabilities: TCS has set up more than 12 threat management centers and currently over 200 security operations centers, of which most are client specific. It has dedicated security operations centers for end-to-end security service delivery and the onshore security operations centers are part of initiative to build more onshore capabilities. Services such as security monitoring are more offshore based, with advanced services such as fraud management, digital forensics, compliance, red team testing, threat hunting having a heavier onshore presence.

Planned investment to enhance offerings: TCS has invested in creating platforms for most of the managed security services that can integrate with existing technology stacks of clients to optimize the total cost of ownership (TCO) and provide holistic coverage of security controls. This allows clients to on board the service at incremental levels of maturity over a period, aligning with their roadmaps across various services. This risk-based approach helps clients to align the security services as per business need with low-entry and exit barriers.

Strong foundational framework: TCS provides a holistic reporting framework that represents the cybersecurity posture of the enterprise across four views and six dimensions. These can calculate security metrics from ingested data across various security tools such as managed detection and response, vulnerability management, IAM and CSPM technologies.

Caution

TCS' should focus on investing in marketing and showcasing its security operations center capabilities to further expand in the managed security services market.

2021 ISG Provider Lens™ Leader

TCS' capabilities in integrating security with complementary technologies and building intelligent security operations centers for creating a comprehensive coverage of advanced security threats are a testament to its leadership in the U.S.

VERIZON

Overview

Verizon is a multinational telecommunications conglomerate headquartered in New York City. The company offers a suite of management and data security services through Verizon Business Group. It manages more than six forensics labs, enabling incident response around the globe. The labs process nearly 1.7 trillion security events every year to improve the threat library. Other thought leadership investments include Verizon Threat Research Advisory Center and weekly cyber intelligence summary.

Strengths

Sophisticated and flexible offerings: Verizon delivers global managed security solutions, combining intelligence and analytics, including advanced security operations and managed threat protection services, threat intel and response services, forensic investigations and identity management. Its cybersecurity services offerings are designed to ensure flexibility, assurance and operational support through a single interface.

Broad portfolio of services: Verizon offers core managed security services around four key areas: identify, protect, detect and respond, and recover. Its portfolio of services is broad and includes managed IDS/IPS, firewalls, web gateway, monitoring, identity management, incident management, proactive penetration testing, threat detection, vulnerability assessments, management, resolution, analytics, managed SIEM, security orchestration automation and response (SOAR), and MDR.

Advanced and customizable security operations center: Verizon's advanced security operations center solutions are fully customizable cybersecurity event-monitoring solutions, designed for enterprises to maximize their SIEM and related security investments with a monitoring and analytics ecosystem that is customized to their exact specifications and business requirements. It provides far more flexibility to meet specific client requirements.

Caution

Verizon is well known for its technical and communication capabilities. At the same time, the company should showcase its consulting and advisory offerings with relevant use cases.

2021 ISG Provider Lens™ Leader

Verizon's advanced security operations center capabilities and investments to enhance its services portfolio through technology partnerships have helped it to win large clients in the U.S.

WIPRO

Overview

Wipro uses proprietary tools, AI, automation and analytics to help organizations comply with data privacy regulations such as the GDPR, Privacy Shield and HIPAA. The company has more than 190,000 dedicated employees to serve clients across six continents, providing solutions and services on cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies. Based on the recent business structure changes, its cybersecurity and risk services fall under a global business unit and address customer needs across all the four strategic market units.

Strengths

Exhaustive portfolio of offerings: Wipro's managed security services business caters to customer needs, spanning across intelligence, protection, detection, remediation, response and recovery. The service offerings include Secure Eye, security intelligence and analytics, managed services, endpoint security, security assurance, cloud security, infrastructure posture/compliance and integrated identity services.

Playbook as a service: Powered by Cortex SOAR, this service enables enterprises to streamline and consolidate security alerts and automatically enrich and track responses. It provides a shared library of more than 142 playbooks to choose from for on-demand playbook development with support from custom integrations.

Security intelligence as a service: Wipro delivers integrated, automated and comprehensive capabilities that provides visibility into a client's entire data center and cloud environment. It has team of security operations center operators with a 24-by-7-by-365 service delivery window to analyze system-prioritized alerts in near real time. machine learning algorithms are further leveraged to identify abnormal behavior for analysis.

Caution

Wipro's business structure changes should reflect its commitment to security as a core part of the business in the coming months to ensure continued success.

2021 ISG Provider Lens™ Leader

Wipro's in-depth portfolio and sophisticated cybersecurity platform have allowed it to scale to high client requirements for comprehensive managed security offerings in the U.S.

RISING STAR: NTT

Overview

NTT came into existence in 2019 as a subsidiary of NTT Group (Nippon Telegraph and Telephone Corp.), combining and rebranding all of NTT's global IT services, including NTT Security. Backed by one of the world's largest telecoms with annual revenues of over US$100 billion, the company has about 120,000 employees globally, of whom 2,000 are cybersecurity professionals. It offers a wide portfolio of products and services and has two U.S.-based security operations centers and eight more across the globe.

Strengths

Breadth of offering: NTT provides a broad range of managed cybersecurity services and technologies, covering device management, threat detection, enterprise security management, web application firewall, and SIEM.

Unique intelligence through AI and machine learning: NTT's threat detection and response uses vendor and proprietary intel feeds to cross-correlate and identify threats that require action. The company applies machine learning to its continuously refreshed datasets from managed client infrastructure, its own global backbone, and in-house Global Threat Intelligence Center with commercial intel feeds and security operations center network. In this way, it demonstrates a unique threat intelligence capability that validates incidents and reduces alert fatigue by virtually eliminating false positives.

Leading edge: With the acquisition of WhiteHat, NTT has brought application security in-house, while a zero-trust framework has been adapted into its consulting services and applied to integration and managed services as well. The company handles the convergence of traditional IT with new and contemporary factors such as the IIoT and OT to apply security expertise across several industry verticals. It has also made considerable efforts to upgrade its managed security user portal and reporting capabilities as well as to provide flexible service bundles and pricing to improve the client and user experience.

Caution

With the low-visibility changeover and consolidation of brands and subsidiaries, the NTT brand has suffered from some market confusion and ambiguity over its purpose.

2021 ISG Provider Lens™ Rising Star

NTT presents a broad portfolio and strong capability. With a growing presence in the U.S., it is expected to reach the leader status within 24 months.

Methodology

METHODOLOGY

The research study "2021 ISG Provider Lens™ Cybersecurity – Solutions & Services" analyzes the relevant software vendors/service providers in the U.S. market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology

The study was divided into the following steps:

1. Definition of 2021 ISG Provider Lens™ Cybersecurity – Solutions & Services U.S. market
2. Use of questionnaire-based surveys of service providers/vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities and use cases
4. Use of ISG's internal databases and advisor knowledge and experience (wherever applicable)
5. Detailed analysis and evaluation of services and service documentation based on the facts and figures received from providers and other sources.
6. Use of the following key evaluation criteria:
   - Strategy & vision
   - Innovation
   - Brand awareness and presence in the market
   - Sales and partner landscape
   - Breadth and depth of portfolio of services offered
   - Technology advancements

Authors and Editors

Gowtham Kumar, Author

Lead Author

Gowtham Sampath is a Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Industry Services and Analytics Solutions & Services market. With more than a decade of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries. He is also authoring articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Srinivasan PN, Author

Senior Analyst

Srinivasan is a senior analyst at ISG and is responsible for supporting and co-authoring Provider Lens™ studies on Insurance BPO Industry, Mainframe Ecosystem, Cybersecurity Ecosystem and AWS Ecosystem. His area of expertise lies in the space of engineering services and digital transformation. Srinivasan has over 6 years of experience in the technology research industry and in his prior role, he carried out research delivery for both primary and secondary research capabilities. Srinivasan is responsible for developing content from an enterprise perspective and author the global summary report. Along with this, he supports the lead analysts in the research process and writes articles about recent market trends in the industry.

Authors and Editors

Jan Erik Aase, Editor

Director and Principal Analyst

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor. Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.

ISG Provider Lens™ | Quadrant Report
August 2021

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.