ISG Provider Lens™

Cybersecurity - Solutions & Services

U.S. 2021

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

Infosys®

August 2021

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™

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All rights reserved. Reproduction of this publication in any form without prior permission is strictly prohibited. Information contained in this report is based on the best available and reliable resources. Opinions expressed in this report reflect ISG's judgment at the time of this report and are subject to change without notice. ISG has no liability for omissions, errors or completeness of information in this report. ISG Research™ and ISG Provider Lens™ are trademarks of Information Services Group, Inc.

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™

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

Identity and Access Management Software Market Trends

Identity and access management (IAM) has taken centerstage across enterprise initiatives and investments, with the realization that secured access and authentication will be the foundational step for protecting their information and technology assets. With the increase in digital and cloud-enabled environments, CISOs and IT teams should ensure

© 2021 Information Services Group, Inc. All Rights Reserved.

seamless management of increased identities that humans and machines require for supporting the digital ecosystem. Although password management has predominantly been the scope of the IAM, the evolution of technology and solutions have extended the capabilities to include advanced features and functionalities. Solution vendors are offering different flavors of IAM, with a focus on identity management, identity governance and administration (IGA), identity lifecycle management (ILM), privileged access management (PAM), customer IAM and access directory among other areas.

Customers are witnessing several benefits with cloud-based IAM. The service provides a single sign-on (SSO) to software-as-a-service (SaaS) solutions such as Microsoft 365, Google G-Suite, Salesforce and other SaaS-based enterprise resource planning (ERP) and human capital management (HCM) options. Cloud-based federated SSO provides secure identification for authorized data access in one place while serving as a proxy to all other applications. IAM solutions can eliminate the sprawl of privacy data to multiple applications and thereby reduce the risk of data breaches.

Data Loss Prevention Software Market Trends

Most enterprises consider data loss prevention (DLP) as an essential element of their data protection programs. A comprehensive DLP solution provides complete visibility into all data on the network whether the data is in motion, at rest or in use. DLP offers another venue to identity and comply with relevant data regulations such as HIPAA, GDPR and PCI-DSS. The ITAR is a U.S. DLP regulatory compliance that restricts and controls the exporting of technologies associated with defense and military. With such regulatory restrictions becoming stricter and severe with substantially higher fines for non-compliance in the event of breaches, DLP has earned a place at the top of the list in data protection investments from executives. GDPR non-compliance can cost a company up to 4 percent of global revenue, making data loss much more expensive than breach notifications and recovery.

These enhancements offer capabilities to detect and respond data exfiltration, irrespective of whether the actions were intentional or accidental. The infusion of artificial intelligence (AI) and machine learning (ML) technologies have given rise to the much-needed context, delivering on context-aware management to address previously undetectable leakages. This is also exacerbated due to the increased need to shift enterprise focus beyond the traditional perimeter, requiring visibility and context of the data as well as the user. The increased perimeter also means that the DLP functionality has been enhanced to cover newer use cases, including endpoint devices, storage, network devices, virtual systems and cloud environments.

Advanced Endpoint Threat Protection, Detection and Response Trends

Endpoint protection has gained even more critical importance with mobile devices, laptops, Internet of Things (IoT) gaining pervasiveness in today's business environment. Endpoint security solutions have evolved over the last three to five years, shifting away from limited antivirus software into a more advanced, comprehensive defense. This includes next-generation antivirus, threat detection, investigation, response, device management, DLP, and other considerations to face evolving threats. Endpoint security

© 2021 Information Services Group, Inc. All Rights Reserved.

is available on-premises (client server) as well as cloud-based (SaaS) options and in some cases as a hybrid model. Vendors are offering endpoint protection platforms (EPP) that can be deployed on the endpoint to protect against file-based, fileless and other types of malware through prevention, investigation and remediation capabilities. There are other vendors offerings systems that integrate EPP systems with endpoint detection and response (EDR) platforms to focus on threat detection, response and unified monitoring.

Technical Security Services Trends

The U.S. market is fragmented with hundreds of security providers that offer services for integration, system stress-testing and training. However, most of them do not have the adequate expertise or delivery capacity for enterprise-level engagements.

Many security solutions and technical security service providers compete in the U.S. market, covering all aspects of IT and business. These providers should determine how best to integrate all these vendor solutions with customer systems and business processes.

Several service providers are offering technical security services, including attack-surface reduction, digital identity management, cloud/infrastructure security, data security and others. Providers with a digital portfolio are adding advanced analytics capability and automated intelligence to provide security for application, cloud, digital identity, risk and threat operations services. Several others are pursuing platforms that are data-driven, AI-powered and digital to combine human intelligence with applied intelligence and digital technologies to drive intelligent operations. They are also investing in cutting-edge technologies, such as security and cloud automation, AI and analytics, and data and threat intelligence, in addition to enhancing their know-how of security products in order to recommend the best security products with protection and security supervision capabilities.

Strategic Security Services Trends

The market dynamics surrounding the advisory and consulting security services in the U.S. is driven by the technical and managed services capability of service providers. Traditionally, pure-play advisory and consulting firms with a specialization in security have gained foothold in the market. However, enterprises are no longer depending on powerhouses, including the Big Four consulting firms, but are scouting for service providers that can help them shift from consulting to actual implementation and management of their environment.

Enterprises expect consulting firms to advise on specific cyber risks and to benchmark clients against their peers. Strategic service providers are building knowledge centers and experience centers for employee training and skill enhancements. The aim of these centers is to learn from the experiences and implement unique cases with a set of pre-deployed and integrated industry tools. Extended team members, including those from managed and technical services, are expected to leverage these new use cases for training and upskilling themselves.

Several service providers are relying on the strength of their advisory capabilities to engage with customers on an outcome-focused approach with clear maturity milestones and outcomes that are to be delivered at each stage. Service providers are expanding

© 2021 Information Services Group, Inc. All Rights Reserved.

their global presence, allowing for a wide range of competences as well as a deep understanding of threat actors' tactics, techniques and procedures (TTPs). They apply this knowledge to get a holistic view of the entire supply chain and clients' security architecture.

Managed Security Services Trends

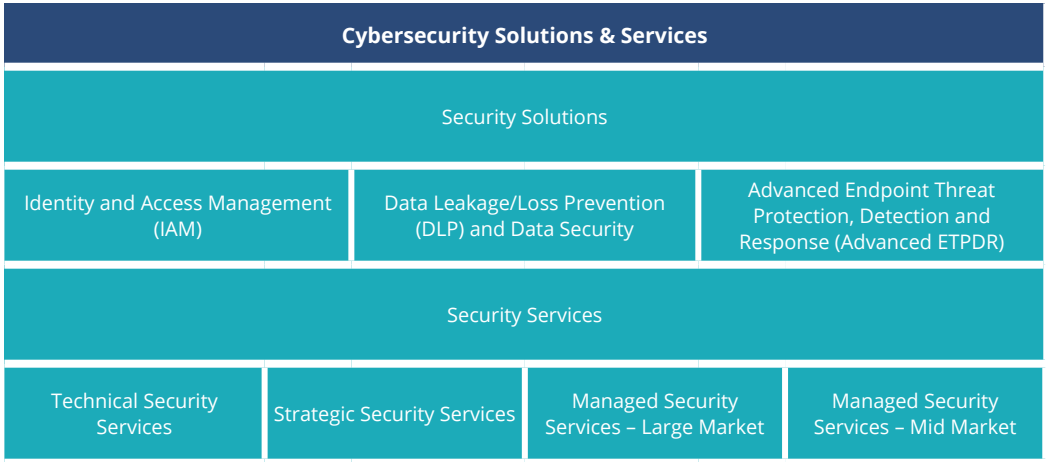
Managed security services are evolving from traditional monitor-and-react models to a more proactive one that includes both defensive and offensive capabilities. As advancements and sophistication have increased from both the protection and attack fronts, it has become increasingly difficult for organizations 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).

© 2021 Information Services Group, Inc. All Rights Reserved.

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

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 1 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
1Kosmos	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Absolute Software	Not in	Product Challenger	Not in	Not in	Not in	Not in	Not in
Accenture	Not in	Not in	Not in	Leader	Leader	Leader	Not in
Alert Logic	Not in	Not in	Not in	Not in	Not in	Not in	Leader
Apple	Contender	Not in	Not in	Not in	Not in	Not in	Not in
AT&T	Not in	Not in	Not in	Not in	Not in	Contender	Leader
Atos	Product Challenger	Not in	Not in	Leader	Leader	Leader	Not in
Attivo networks	Not in	Not in	Contender	Not in	Not in	Not in	Not in
Avatier	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Axians	Not in	Not in	Not in	Not in	Contender	Not in	Not in
Beta Systems	Contender	Not in	Not in	Not in	Not in	Not in	Not in
BitDefender	Not in	Not in	Contender	Not in	Not in	Not in	Not in
Blue Voyant	Not in	Not in	Not in	Not in	Not in	Not in	Product Challenger

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 2 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
Broadcom	Leader	Leader	Leader	Not in	Not in	Not in	Not in
Capgemini	Not in	Not in	Not in	Leader	Leader	Leader	Not in
CGI	Not in	Not in	Not in	Market Challenger	Market Challenger	Contender	Not in
Check Point	Not in	Leader	Leader	Not in	Not in	Not in	Not in
Cisco	Not in	Not in	Market Challenger	Not in	Not in	Market Challenger	Not in
Cloud4C	Not in	Not in	Not in	Not in	Not in	Not in	Market Challenger
Cognizant	Not in	Not in	Not in	Market Challenger	Market Challenger	Market Challenger	Leader
Comodo	Not in	Contender	Product Challenger	Not in	Not in	Not in	Product Challenger
Computacenter	Not in	Not in	Not in	Contender	Not in	Not in	Not in
CoSoSys	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Crowdstrike	Not in	Not in	Leader	Not in	Not in	Not in	Not in
CyberArk	Leader	Not in	Not in	Not in	Not in	Not in	Not in
Cybereason	Not in	Not in	Rising Star	Not in	Not in	Not in	Product Challenger

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 3 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
CyberProof	Not in	Not in	Not in	Contender	Product Challenger	Leader	Not in
Cylance	Not in	Not in	Product Challenger	Not in	Not in	Not in	Not in
Deloitte	Not in	Not in	Not in	Leader	Leader	Leader	Not in
Digital Guardian	Not in	Leader	Not in	Not in	Not in	Not in	Not in
DXC	Not in	Not in	Not in	Leader	Leader	Leader	Not in
ESET	Not in	Not in	Market Challenger	Not in	Not in	Not in	Not in
EY	Not in	Not in	Not in	Product Challenger	Leader	Product Challenger	Not in
Fidelis Cybersecurity	Not in	Contender	Not in	Not in	Not in	Not in	Not in
FireEye	Not in	Not in	Leader	Not in	Not in	Not in	Not in
Forcepoint	Not in	Leader	Not in	Not in	Not in	Not in	Not in
Forgerock	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Fortinet	Contender	Not in	Leader	Not in	Not in	Not in	Not in
F-Secure	Not in	Not in	Not in	Not in	Not in	Not in	Market Challenger

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 4 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
Fujitsu	Not in	Not in	Not in	Product Challenger	Product Challenger	Contender	Not in
Happiest Minds	Not in	Not in	Not in	Contender	Contender	Not in	Contender
HCL	Not in	Not in	Not in	Leader	Leader	Leader	Leader
HelpSystems	Product Challenger	Product Challenger	Not in	Not in	Not in	Not in	Not in
Herjavec Group	Not in	Not in	Not in	Not in	Not in	Product Challenger	Leader
IBM	Leader	Leader	Not in	Leader	Leader	Leader	Not in
Ilantus	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Imperva	Not in	Product Challenger	Not in	Not in	Not in	Not in	Not in
Infosys	Not in	Not in	Not in	Leader	Leader	Product Challenger	Leader
Ivanti	Not in	Product Challenger	Product Challenger	Not in	Not in	Not in	Not in
Kasada	Not in	Contender	Product Challenger	Not in	Not in	Not in	Not in
Kaspersky	Not in	Not in	Leader	Not in	Not in	Not in	Not in
Keyfactor	Contender	Not in	Not in	Not in	Not in	Not in	Not in

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 5 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
KPMG	Not in	Not in	Not in	Product Challenger	Not in	Not in	Not in
Kudelski	Not in	Not in	Not in	Not in	Contender	Not in	Product Challenger
LTI	Not in	Not in	Not in	Product Challenger	Product Challenger	Contender	Leader
Lumen	Not in	Not in	Not in	Contender	Not in	Not in	Contender
Manageengine	Product Challenger	Contender	Not in	Not in	Not in	Not in	Not in
McAfee	Not in	Leader	Market Challenger	Not in	Not in	Not in	Not in
Micro Focus	Rising Star	Not in	Not in	Not in	Not in	Not in	Not in
Microland	Contender	Contender	Contender	Contender	Contender	Not in	Contender
Microsoft	Leader	Market Challenger	Market Challenger	Not in	Not in	Not in	Not in
Mphasis	Not in	Not in	Not in	Not in	Not in	Contender	Contender
Netskope	Not in	Product Challenger	Product Challenger	Not in	Not in	Not in	Not in
NTT	Not in	Not in	Not in	Product Challenger	Leader	Rising Star	Not in
Okta	Leader	Not in	Not in	Not in	Not in	Not in	Not in

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 6 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
Omada	Contender	Not in	Not in	Not in	Not in	Not in	Not in
One Identity	Leader	Not in	Not in	Not in	Not in	Not in	Not in
OneLogin	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
OpenText	Not in	Leader	Leader	Not in	Not in	Not in	Not in
Oracle	Leader	Not in	Not in	Not in	Not in	Not in	Not in
Orange Cyberdefense	Not in	Not in	Not in	Contender	Contender	Not in	Product Challenger
Palo Alto Networks	Not in	Product Challenger	Leader	Not in	Not in	Not in	Not in
Persistent	Not in	Not in	Not in	Contender	Not in	Contender	Contender
Ping Identity	Leader	Not in	Not in	Not in	Not in	Not in	Not in
Proofpoint	Not in	Market Challenger	Not in	Not in	Not in	Not in	Not in
PwC	Not in	Not in	Not in	Leader	Market Challenger	Not in	Not in
Qualys	Not in	Not in	Market Challenger	Not in	Not in	Not in	Not in
Rapid7	Not in	Not in	Leader	Not in	Not in	Not in	Rising Star

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 7 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
RSA	Leader	Not in	Not in	Not in	Not in	Not in	Not in
SailPoint	Leader	Not in	Not in	Not in	Not in	Not in	Not in
SAP	Market Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Saviynt	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Secureworks	Not in	Not in	Not in	Product Challenger	Leader	Leader	Not in
SentinelOne	Not in	Not in	Product Challenger	Not in	Not in	Not in	Not in
SLK Group	Not in	Not in	Not in	Not in	Contender	Not in	Contender
Sophos	Not in	Product Challenger	Leader	Not in	Not in	Not in	Not in
TCS	Not in	Not in	Not in	Leader	Rising Star	Leader	Market Challenger
Tech Mahindra	Not in	Not in	Not in	Market Challenger	Not in	Not in	Leader
Thales	Market Challenger	Not in	Not in	Market Challenger	Market Challenger	Contender	Not in
Trend Micro	Not in	Leader	Leader	Not in	Not in	Not in	Not in
Trustwave	Not in	Not in	Not in	Not in	Product Challenger	Product Challenger	Not in

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services - Quadrant Provider Listing 8 of 8

	Identity and Access Management (IAM)	Data Leakage/Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services Large Accounts	Managed Security Services Midmarket
Unisys	Product Challenger	Not in	Not in	Leader	Product Challenger	Product Challenger	Leader
ValueLabs	Not in	Not in	Not in	Contender	Not in	Not in	Contender
Varonis	Not in	Leader	Not in	Not in	Not in	Not in	Not in
Verizon	Not in	Not in	Not in	Rising Star	Market Challenger	Leader	Not in
VMware Carbon Black	Not in	Not in	Product Challenger	Not in	Not in	Not in	Not in
Watchguard	Not in	Product Challenger	Not in	Not in	Not in	Not in	Not in
Wipro	Not in	Not in	Not in	Leader	Leader	Leader	Leader
Zensar	Not in	Not in	Not in	Contender	Product Challenger	Contender	Contender
Zscaler	Not in	Rising Star	Not in	Not in	Not in	Not in	Not in

© 2021 Information Services Group, Inc. All Rights Reserved.

Cybersecurity - Solutions & Services Quadrants

ENTERPRISE CONTEXT

Identity and Access Management (IAM)

This report is relevant to enterprises across all industries in the U.S. and evaluates the ability of solution vendors to offer software and associated services to meet unique demands for securely managing enterprise user identities and devices.

In this quadrant report, ISG highlights the current market positioning of IAM providers in the U.S., and how each provider addresses the key challenges faced in the region. U.S. enterprises engage with solution vendors that offer access management, identity governance and administration, privileged access management, and customer IAM. These IAM should be cloud native, risk aware, and an all-in-one converged solution, built on a zero trust framework.

All-in-one converged IAM solution includes password management, access enforcement, identity governance and administration, authentication, identity analytics, and privileged access management. However, most enterprises find it difficult to integrate external applications with IAM solutions.

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

IT and technology leaders should read this report to understand the relative positioning and capabilities of providers of IAM solutions and services. The report also compares the technical capabilities of various service providers in the market.

Security professionals should read this report to understand how vendors and their IAM tools comply with security and regional laws, and how these players can be compared with each other.

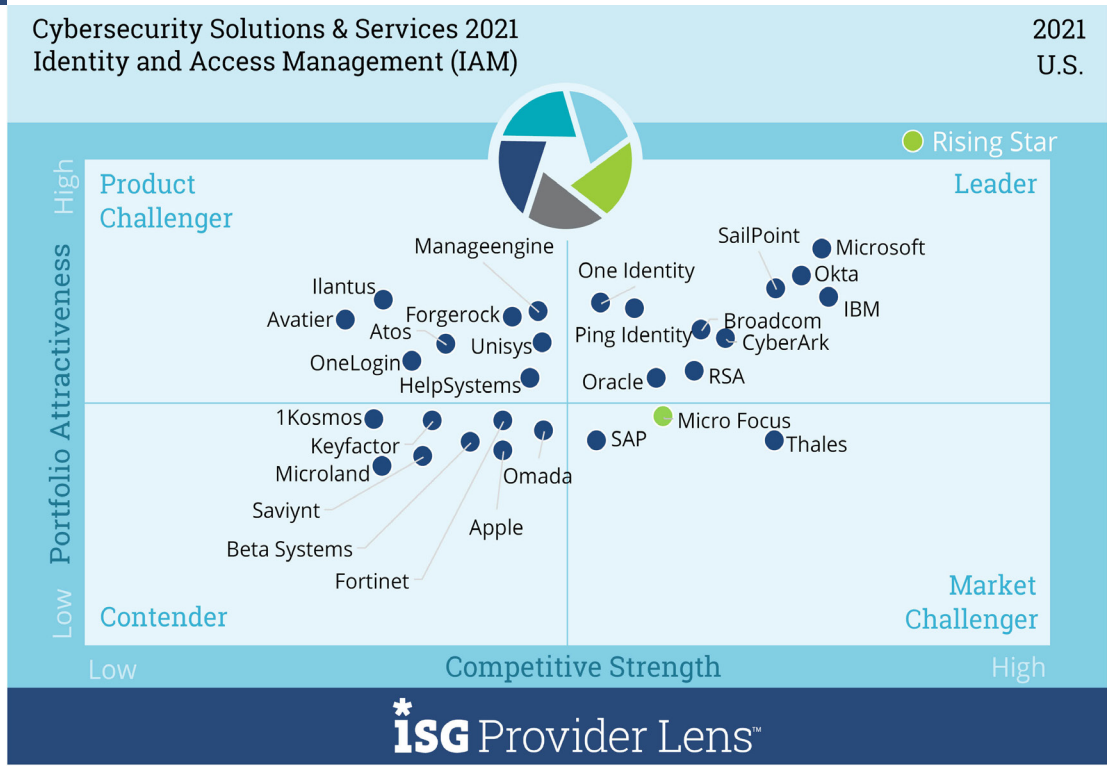
Compliance and governance leaders should read this report to understand the landscape of IAM as it directly affects compliance with region's data and privacy related legislations.

© 2021 Information Services Group, Inc. All Rights Reserved.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Definition

Identity and access management (IAM) vendors and solution providers are characterized by their ability to offer proprietary software and associated services to meet the unique demand for securely managing enterprise user identities and devices. This quadrant also includes software as a service based on proprietary software. Pure service providers that do not offer an IAM product (on-premises or cloud) based on self-developed software are not covered here. Depending on the organizational requirements, these solutions could be deployed in several ways such as on-premises, on cloud (managed by customer), as-a-service model or a combination thereof.



Source: ISG Research 2021

© 2021 Information Services Group, Inc. All Rights Reserved.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Definition (cont.)

IAM solutions are aimed at collecting, recording and administering user identities and related access rights, as well as providing specialized access to critical assets including PAM. They ensure that access rights are granted based on defined policies. To handle existing and new application requirements, the solutions are increasingly embedded with secure mechanisms, frameworks and automation (for example, risk analyses) within their management suites to provide real-time user and attack profiling functionalities. Solution providers are also expected to provide additional features related to social media and mobile users to address their security needs that go beyond traditional web and context-related rights management.

Eligibility Criteria

- The service provider should have relevance (in terms of revenue and number of customers) as an IAM product vendor in the respective country.
- IAM offerings should be based on proprietary software and not on third-party software.
- The solution should be capable of being deployed in either or through a combination of on-premises, cloud, IDaaS and a managed (third-party) model.
- The solution should be capable of supporting authentication either or by a combination of SSO, multifactor authentication (MFA), risk-based and context-based models.
- The solution should be capable of supporting role-based access and PAM.
- The IAM vendor should be able to provide access management for one or more enterprise needs such as cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.
- The solution should be capable of supporting one or more legacy and newer IAM standards including, but not limited to, security assertion markup language (SAML), open authorization (OAuth), OpenID Connect, WS-Federation, WS-Trust and system for cross-domain identity management (SCIM).
- To provide secure access, the portfolio should offer one or more of the following: directory solutions, dashboard or self-service management and lifecycle management (migration, sync and replication).

© 2021 Information Services Group, Inc. All Rights Reserved.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations

The rise of the remote enterprise and work-from-home options as a result of the COVID-19 pandemic have contributed to the growth of the IAM market. With the immediate onset of pandemic, organizations were prioritizing on MFA to help employees and contractors gain unfettered access, while requiring services outside the enterprise network perimeter. MFA and SSO continue to be the de facto solution approach for several large and small organizations as it offers higher levels of security and meet compliance requirements. MFA is a legal requirement in some jurisdictions and is a best practice in IAM. Two-factor authentication (2FA) is generally the default method where MFA is required. However, as the situation evolved with the need for a hybrid workforce, passwordless capabilities as well as zero-trust access and least privilege access have gained traction among enterprises. Several CISOs and solution vendors expect passwordless and zero-trust access to gain higher priority, as they eliminate even smaller possibilities of attackers gaining access.

Many vendors are also including contextual and adaptive functionalities, adding to the extra layers of security to protect against potential threats. Analytics-driven user and entity behavior data are being leveraged to ensure higher trust levels, and the integration with IAM creates proactive remediation based on the detection of real-time user behavior. The market is also witnessing the rise of vendors that offer real-time biometric identification and leverage blockchain-based identity access to ensure enhanced levels of security.

PAM is another aspect of access governance that is gaining traction. Most IAM vendors have included it as part of the standard offering within their IAM portfolios, adding specialized functionalities including user and entity behavior analytics (UEBA), and these are becoming more relevant in cases where organizations leverage AI and robotic process automation (RPA) bots for their operations. As these functionalities need to be treated like human accounts, contextual capabilities and the behavior of these bots are used to provide PAM, securing the enterprise completely from human and non-human entities.

© 2021 Information Services Group, Inc. All Rights Reserved.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations (cont.)

Cloud computing is driving two important trends in the changing, competitive IAM landscape. Many vendors are moving IAM from on-premises to the cloud or are building solutions that accommodate both. More clients are also demanding pay-as-you-go models or IAM as a service (IDaaS). These trends have a major impact on established vendors on two different fronts. Porting products that are designed for on-premises usage to run in the cloud requires significant investments by the vendor but offers little in the way of product differentiation as the functionality mostly stays the same. In addition, shifting from a traditional licensing model that involves paying upfront plus a monthly fee significantly affects the provider's cash flow and, potentially, its ability to invest in R&D. As a result, many established providers are witnessing a rapid growth of cloud-native IAM products at a competitive pricing through as-a-service business models.

From the 85 companies assessed for this study, 29 have qualified for this quadrant with 10 being Leaders and one a Rising Star.

- **Broadcom** sold off its security consulting and services businesses to bolster its productized focus and leverage its brand presence for improving its revenue base and partnerships with service providers.
- With the acquisition of Idaptive in 2020, **CyberArk** delivers an AI-based, security-first approach that is adaptive and leverages context awareness for managing identities. The C3 Alliance has more than 100 technology partners and industry leading product integrations.
- **IBM** offers a diverse portfolio of offerings that encompass IAM, cloud access management and authentication, IGA, PAM, consumer identity and access management (CIAM) and hybrid access management system.
- **Microsoft** is creating a true zero-trust mindset to ensure effective protection, organizational resilience and a future of security. Microsoft Azure AD offers traditional features such as SSO, Lightweight Directory services, rights management, certificate services and federation services.
- With more than 7,000 integrations, **Okta** products have gained significant appeal among several corporate executives. The solutions have enabled client enterprise workforces to rely on SSO across multiple cloud services providers.

© 2021 Information Services Group, Inc. All Rights Reserved.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations (cont.)

- **One Identity** relies on growing organically with investments to expand portfolio that serve as a one-stop-shop addressing a wider audience and aggressively expand partner network to promote sales growth
- **Oracle** offers a structured approach leveraging functional groups to provide directory services, access management and identity management. These solutions are further enhanced by their analytics services which covers fraud detection and heuristic behavior analysis.
- **Ping Identity** offers integration kits and agents to other identity and service providers, which help in extending access management systems as well as enabling authentication, authorization and data synchronization.
- **RSA** helps enterprise users to speed time-to-deployment and time-to-value with its launch of best practices and blueprints around implementation creating set of use cases, ecosystem integrations and recommendations.
- The acquisition of ERP Maestro will enable **SailPoint'**s clients to closely manage separation-of-duties controls for critical ERP business systems. ERP Maestro's SaaS-based platform supports SAP SuccessFactors.
- **Micro Focus** (Rising Star) leverages its integrated platform across cloud, SaaS, web services, microservices and IoT to offer identity, access and privilege management with authentication and authorization capabilities. This has also enabled the foundation for a single unified view of identity across complex hybrid environments.

© 2021 Information Services Group, Inc. All Rights Reserved.

ENTERPRISE CONTEXT

Data Leakage/Loss Prevention (DLP) and Data Security

This report is relevant to enterprises across industries in the U.S. for evaluating providers of DLP and data security products.

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

Due to the COVID-19 pandemic, working from home has become the new normal. As a result, it has become crucial to ensure a secure mobile workforce, enforce security in bring-your-own-device (BYOD) environments and secure data on remote cloud systems.

Enterprises look for DLP solutions that can offer personal information protection and compliance, intellectual property (IP) protection and data visibility. These enterprise DLP solutions are comprehensive software packages for physical and virtual solutions. The increase in the number of enterprise digital assets has, in turn, resulted in the massive growth of structured and unstructured data. Hence, large enterprises are actively investing in DLP solutions. Digital DLP solution functionalities are extending into the cloud and advanced threat protection.

In the U.S., the adoption of DLP among mid-sized enterprises is increasing. Enterprises' digital transformation strategies such as cloud adoption, IoT and analytics are driving the adoption of DLP solutions.

ISG Provider Lens™

© 2021 Information Services Group, Inc. All Rights Reserved.

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

Chief information security officers (CISOs) should read this report to understand the products of DLP vendors and their relative position with individual strengths, thereby ensuring the organization's information and data security.

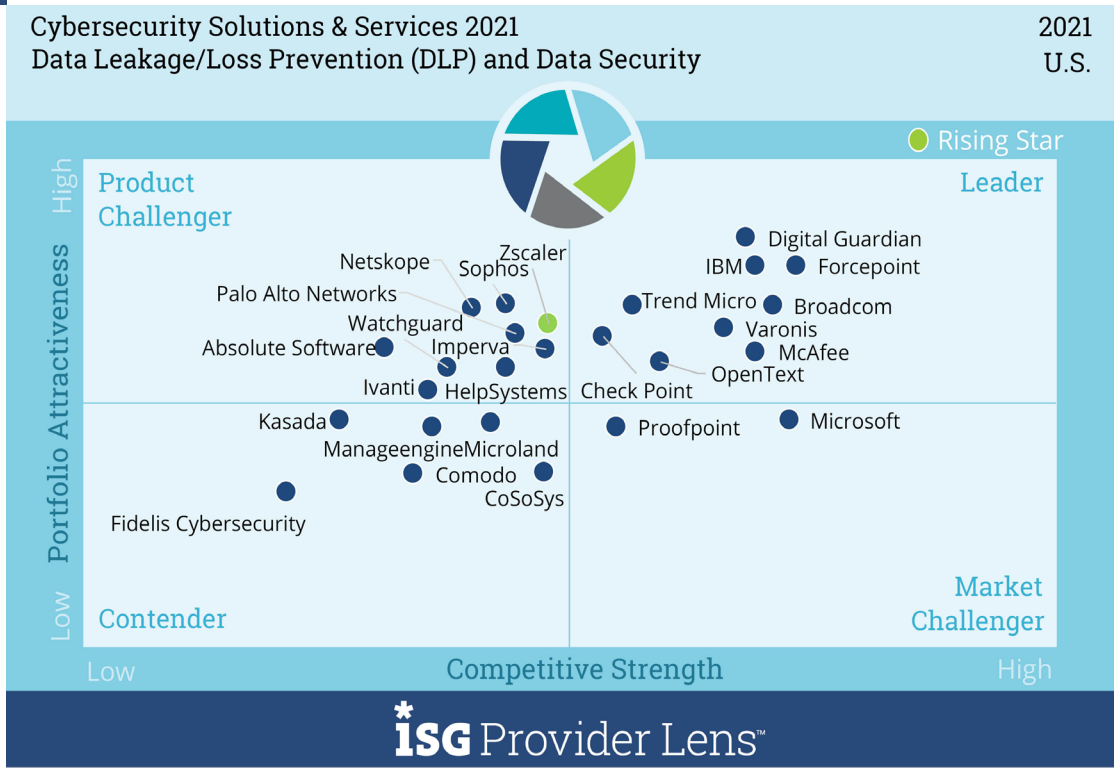
Chief security officers (CSOs) should read this report to understand the relative positioning and capabilities of providers to help them effectively plan and select DLP-related solutions. The report also shows how the product and market capabilities of each provider differ from the rest in the market.

Security architects should read this report to understand how providers of DLP solutions fit their initiatives and needs compared with each other.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition

DLP vendors and solution providers are characterized by their ability to offer proprietary software and associated services. This quadrant also includes software as a service based on proprietary software. Pure service providers that do not offer a DLP product (on-premises or cloud-based) based on self-developed software are not covered here. The solutions can identify and monitor sensitive data, provide access for only authorized users and prevent data leakage. Vendor solutions in the market are characterized by a mix of products that can provide visibility and control over sensitive data residing in cloud applications, endpoint, network and other devices.



Source: ISG Research 2021

© 2021 Information Services Group, Inc. All Rights Reserved.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition (cont.)

These solutions should be able to discover sensitive data, enforce policies, monitor traffic and improve data compliance. They are gaining considerable importance as it has become more difficult for enterprises to control data movements and transfers. The number of devices, including mobile, that are used to store data is increasing in enterprises. These are mostly equipped with an internet connection and can send and receive data without passing it through a central internet gateway. The devices are supplied with a multitude of interfaces, such as USB ports, Bluetooth, wireless local area network (WLAN) and near-field communication (NFC), which enable data sharing. Data security solutions protect data from unauthorized access, disclosure and theft.

Eligibility Criteria

- Service provider should hold relevance (in terms of revenue and number of customers) as a DLP product vendor in the respective country.
- The DLP offering should be based on proprietary software and not on third-party software.
- The solution should be capable of supporting DLP across any architecture such as the cloud, network, storage or endpoint.
- It should be able to protect sensitive data across structured or unstructured data, text or binary data.
- It should be offered with basic management support including, but not limited to, reporting, policy controls, installation and maintenance, and advanced threat detection functionalities

© 2021 Information Services Group, Inc. All Rights Reserved.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Observations

Traditional DLP solutions do not offer sophisticated on-demand and real-time threat detection capabilities and have also become outdated leading to operational annoyances, including false positives and noise. They were aimed at protecting the enterprise from frontlines by acting as a holistic protective barrier but have become ineffective in the face of insider threats, ransomware and advanced malware. The DLP market is not only continuing to change from a product feature perspective but also in the way the protective solution is being acquired by customers and thus the go-to-market strategies pursued by DLP providers.

Current solutions offer advanced functionalities that are intended to provide increased visibility associated to location and usage of data as well as related assets within the enterprise. In addition, vendors are offering solutions that can apply data leakage and protection policies based on the content and context of the data, user and the enterprise. DLP is also an essential component of security frameworks (ISO, NIST, COBIT, etc.) and an important input to user and entity behavioral analysis (UEBA). Several vendors in the market are gaining certifications and aligning their solutions to these frameworks, including MITRE ATT&CK®, to ensure the highest levels of data protection to their clients.

While choosing a DLP solution, enterprises should view their needs from a wide perspective. Many factors determine if the solution or suite of solutions is optimal for each enterprise. Some of them include the sensitivity of the data being protected, the velocity with which it changes, the need for a visibly compliant solution, tolerance for risk, investigative resource requirements and the net effect on productivity. Other considerations include an appetite for outsourcing, the need for vendor support, partner network, and a product development roadmap that aims to keep solutions current with the changing data security landscape.

From the 85 companies assessed for this study, 26 have qualified for this quadrant with nine being Leaders and one a Rising Star.

- **Broadcom's** more than 100 certified technology partners as well as rich set of application programming interfaces (APIs) to simplify integrations with ICD, has helped create a coordinated approach to threat protection, detection and response.

© 2021 Information Services Group, Inc. All Rights Reserved.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Observations (cont.)

- **Check Point** leverages advanced functionalities from several AI engines, which combines behavioral and contextual intelligence to offer layered protection across different stages of protection.
- **Digital Guardian** adopts a data risk discovery approach to offer visibility before creating policies by showing where sensitive data is located and how it flows as well as the risk areas. The platform adopts a use case-based approach towards known data types or user groups.
- **Forcepoint's** Dynamic Data Protection combines user and data activity from monitoring and enforcement points across endpoint networks and cloud, allowing it to gain more context from behavior.
- **IBM's** Guardium® solution is provided as preconfigured appliances shipped by IBM or as software appliances installed on the IBM platform. The platform is designed to be configured for a single database or thousands of heterogeneous databases located across the enterprise.
- **McAfee** leverages third-party technology partners to help in maximizing intelligence sharing offering a unified experience in managing all DLP violations through a centralized console. The Raw DLP event data is shared with McAfee Behavioral Analytics to detect risky user behavior.
- **OpenText** made acquisitions including Carbonite and Webroot to strengthen their cyber resilience portfolio and comprehensive information management offering. This helps maintain business security and continuity to better manage cyber threats, data loss, endpoint protection, forensic investigation and remediation.
- **Trend Micro's** Integrated DLP uses an exhaustive list of identifiers to identify specific data by patterns, formulas, positioning and more to create contextual awareness. The DLP solutions also provide advanced fingerprinting to secure unstructured data and IP that reside on or off the network.
- **Varonis** acquired Polyrize that provides software maps and analyzes relationships between users and data across cloud applications and services, gaining capabilities in simplifying cloud data access control and analyzing cloud activity.
- **Zscaler** Cloud DLP platform offers instant analysis of violations and creates reports to highlight compliance concerns and can forward DLP evidence data and session metadata to third-party DLP solution providers. The company is a Rising Star in this space.

© 2021 Information Services Group, Inc. All Rights Reserved.

ENTERPRISE CONTEXT

Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)

This report is relevant to enterprises across industries in the U.S. for evaluating providers of advanced endpoint threat protection, detection and response products.

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

Today's organizations require advanced protection against an increasingly sophisticated threat environment. In addition to endpoint detection and response, advanced endpoint security solutions include artificial intelligence (AI), machine learning (ML), security analytics and real-time threat intelligence.

With the increasing adoption of BYOD, employees are accessing company data on their own mobile devices. However, this practice raises safety and management concerns, demanding the use of advanced end-point security solutions to protect critical company data. The retail industry in North America is governed by the Data Breach Disclosure Law, the Payment Card Industry (PCI) Data Security Standard (DSS), and the Payment Application Qualified Security Assessor (PAQSA). Similarly, several other regulatory trends are boosting the adoption of advanced endpoint threat technology in each sector.

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

Chief information security officers (CISOs) should read this report to understand the products of advanced endpoint threat protection vendors and their relative position with individual strengths, thereby ensuring the organization's information and data security.

Chief security officers (CSOs) should read this report to understand the relative positioning and capabilities of providers to help them effectively plan and select advanced endpoint threat protection related solutions. The report also shows how the product and market capabilities of each provider differ from the rest in the market.

Chief technology officers (CTOs) should read this report to decide the technologies to adopt and embrace in the workplaces.

Security architects should read this report to understand how providers of advanced endpoint threat protection solutions fit their initiatives and needs compared with each other.

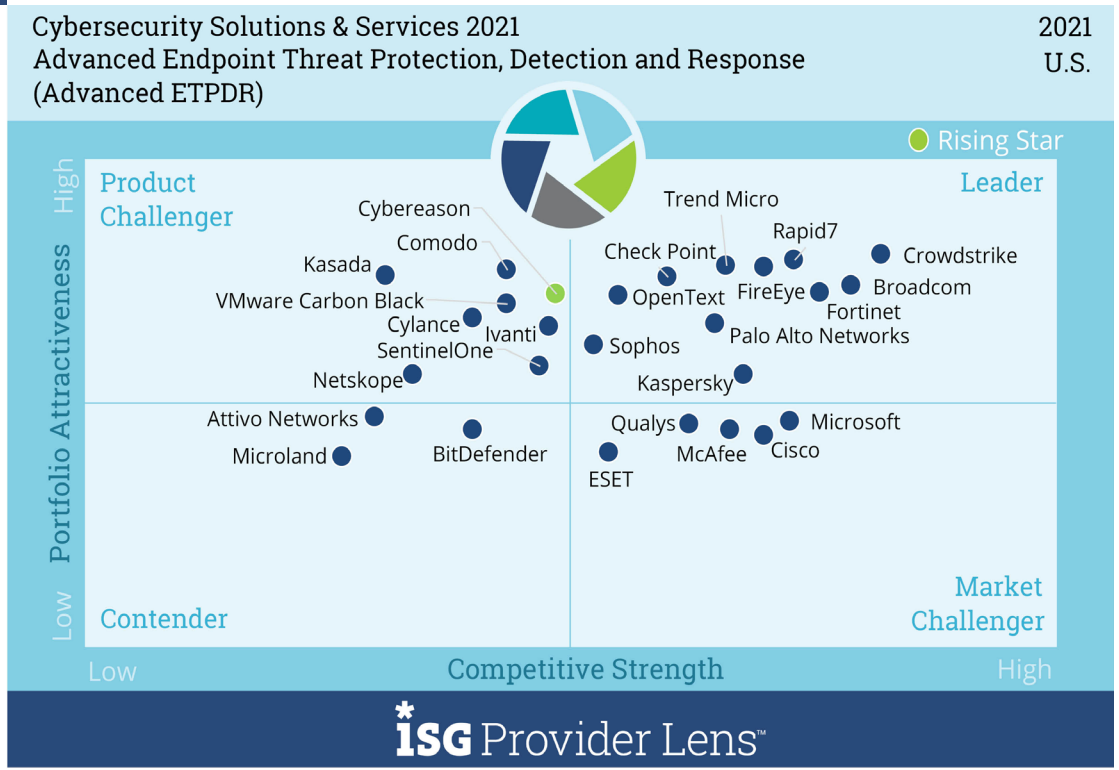
© 2021 Information Services Group, Inc. All Rights Reserved.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION AND RESPONSE (ADVANCED ETPDR)

Definition

Vendors and providers of advanced endpoint threat protection, detection and response (ETPDR) solutions are characterized by their ability to offer proprietary software and associated services. This quadrant also includes software as a service based on proprietary software. Pure service providers that do not offer an advanced ETPDR product (on-premises or cloud-based) based on self-developed software are not covered here. This quadrant evaluates providers that offer continuous monitoring and total visibility of all endpoints and can analyze, prevent and respond to advanced threats.

These solutions go beyond plain signature-based protection and offer protection from adversaries such as ransomware, advanced persistent threats (APTs) and malware by investigating the incidents across the complete endpoint landscape. They should be able to isolate the infected endpoint and take the necessary corrective action or remediation. Such solutions comprise a database, wherein the information collected from network and endpoints is aggregated, analyzed and investigated. Each solution has an agent that resides in the host system to offer the monitoring and reporting capabilities for the events.



Source: ISG Research 2021

© 2021 Information Services Group, Inc. All Rights Reserved.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION AND RESPONSE (ADVANCED ETPDR)

Eligibility Criteria

- Service provider should hold relevance (revenue and number of customers) as an advanced ETPDR product vendor in the respective country.
- The advanced ETPDR offering should be based on proprietary software and not on third-party software.
- The solution should provide comprehensive and total coverage and visibility of all endpoints in the network.
- It should demonstrate effectiveness in blocking sophisticated threats such as advanced persistent threats, ransomware and malware.
- It should leverage threat intelligence, analyze, and offer real-time insights on threats emanating across endpoints.

Observations

As hackers and attackers become more sophisticated to bypass detection, platforms and solutions targeting endpoint protection are also gaining enhanced functionalities and features. They can detect and protect against unknown malware, exploits and threats before systems are compromised. Some of the solutions devise capabilities of routing all sources of identified or presumed threats to virtual containment environments where the threat is nullified either by deletion or through the completion of its script. These containment environments are completely purged once the data is analyzed for exploit's attack methods to further enhance threat detection based on context and behavior. Several vendors have been offering solutions in these areas with distinctive advantages and complementary capabilities to create a comprehensive portfolio with competencies to address growing threats from specific routes. Some of these vendors, including CrowdStrike, Kasada, Comodo, Rapid7, Cybereason, Fortinet, FireEye, Ivanti and Carbon Black among others, have witnessed significant growth over the year.

Vendors are also adding complementary capabilities such as machine learning and analytics to enable real-time intelligence to quickly identify and detect threats. One of the key aspects of advanced endpoint solutions is their capability to prevent threats from reaching the enterprise IT environment and keeping it isolated from attackers. The market is expecting more advanced features that will offer heightened intelligence in identifying threats based on behavior 100 percent of the time as well as the route of the threat to pinpoint attackers.

© 2021 Information Services Group, Inc. All Rights Reserved.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION AND RESPONSE (ADVANCED ETPDR)

Observations (cont.)

From the 85 companies assessed for this study, 27 have qualified for this quadrant with 11 being Leaders and 1 a Rising Star.

- **Broadcom** provides real-time threat visibility and management options across on-premise, cloud or hybrid infrastructures using a single agent for attack surface reduction, attack prevention, breach prevention and EDR with a single console.
- **Checkpoint's** security teams leverage their security operations center (SOC) to filter through high volumes of alerts and reduce network blind spots to expose and stop cyberattacks with speed and precision.
- **CrowdStrike's** acquisition of Humio will expand its extended detection and response (XDR) capabilities by ingesting and correlating data from any log, application or feed to deliver actionable insights and real-time protection.
- **FireEye** identifies attacks and behavior to prevent sophisticated threats using a broad set of capabilities such as advanced detection, response, and proactive and adaptive investigation as well as real-time threat intelligence.
- **Fortinet's** Security Fabric and FortiGuard Labs provide a robust foundation for XDR with a common data structure, correlated telemetry, unified visibility, native integration and seamless interoperation.
- **Kaspersky's** newest endpoint offering is tailored for organizations with limited security expertise and resources, led to a significant increase in sales of Kaspersky Endpoint Security Cloud solution, specifically in the SMB segment.
- **OpenText's** MDR service is the latest addition to its security portfolio, with the newly launched EnCase™ Endpoint Security CE 21.1 delivering additional out-of-the-box detection rules that are aligned to the MITRE ATT&CK framework.
- **Palo Alto Networks'** Cortex XDR agent provides a comprehensive prevention stack that leverages AI-based local analysis using a local ML model with data sets from global sources.

© 2021 Information Services Group, Inc. All Rights Reserved.

ADVANCED ENDPOINT THREAT PROTECTION, DETECTION AND RESPONSE (ADVANCED ETPDR)

Observations (cont.)

- **Rapid7** has been acquiring cloud-based firms, Alcide.IO (Kubernetes security) and DivvyCloud (CSPM), to improve its cloud-native security platform and continuous management of risk and compliance across cloud environments.
- **Trend Micro** Apex One™ is a critical component of their endpoint offering allowing users to add security and investigation capabilities and offers threat detection, response and investigation within a single agent.
- **Sophos** EDR leverages a deep learning neural network to offer on-demand access to curate threat intelligence that is trained on hundreds of millions of samples to look for threat indicators.
- **Cybereason** (Rising Star) integrates endpoint telemetry with behavioral analytics to detect and end cyberattacks anywhere on enterprise networks, extending across IT environments.

© 2021 Information Services Group, Inc. All Rights Reserved.

ENTERPRISE CONTEXT

Technical Security Services

This report is relevant to companies across all industries in the U.S. for evaluating providers that do not have exclusive focus on their respective proprietary products but can implement and integrate other vendors' products or solutions. This covers integration, maintenance and support for IT security products or solutions.

In this quadrant, ISG defines the current market positioning of providers of implementation and integration services for security products and solutions in the U.S., and how each provider addresses the key challenges faced in the region. The report assesses providers that specialize in security products and solutions integration, maintenance and support offerings. These set of effective programs by providers help organizations safeguard their sensitive information, data and other digital assets from advancing digital threats.

The key implementation or integration tasks include identity and access management (IAM), enterprise vulnerability management, etc. The U.S. is already a mature market when compared with other regions and countries. It faces high demand for technical security services, driving the growth of most service providers in this space. ISG research shows that the supply of required talent workforce is the major factor driving the demand. Also, the demand for implementation and integration of solutions and products is increasing among enterprise customers in the U.S. This has led to the consolidation of many service providers, as implementation capabilities lag behind the demand.

The leading service providers intend to develop their own proprietary interfaces to integrate with various vendor solutions and plug solution gaps. However, with large number of providers offering this service, a gap still exists. Most service providers operate in one specific region or one industry vertical. Few service providers are focused or partnered with couple of industry tools and solutions and lack the wide enterprise implementation capability. Enterprise customers, thus, partner with large providers that can offer enterprise-wide implementation, thereby neglecting small, niche providers for such implementation services.

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

Marketing and sales leaders should read this report to understand the relative positioning and capabilities of service partners that can help them effectively develop and define a cybersecurity strategy, with the necessary assessments to related systems.

Chief strategy officers should read this report to understand the relative positioning and capabilities of service partners to collaborate with and develop an effective cybersecurity strategy.

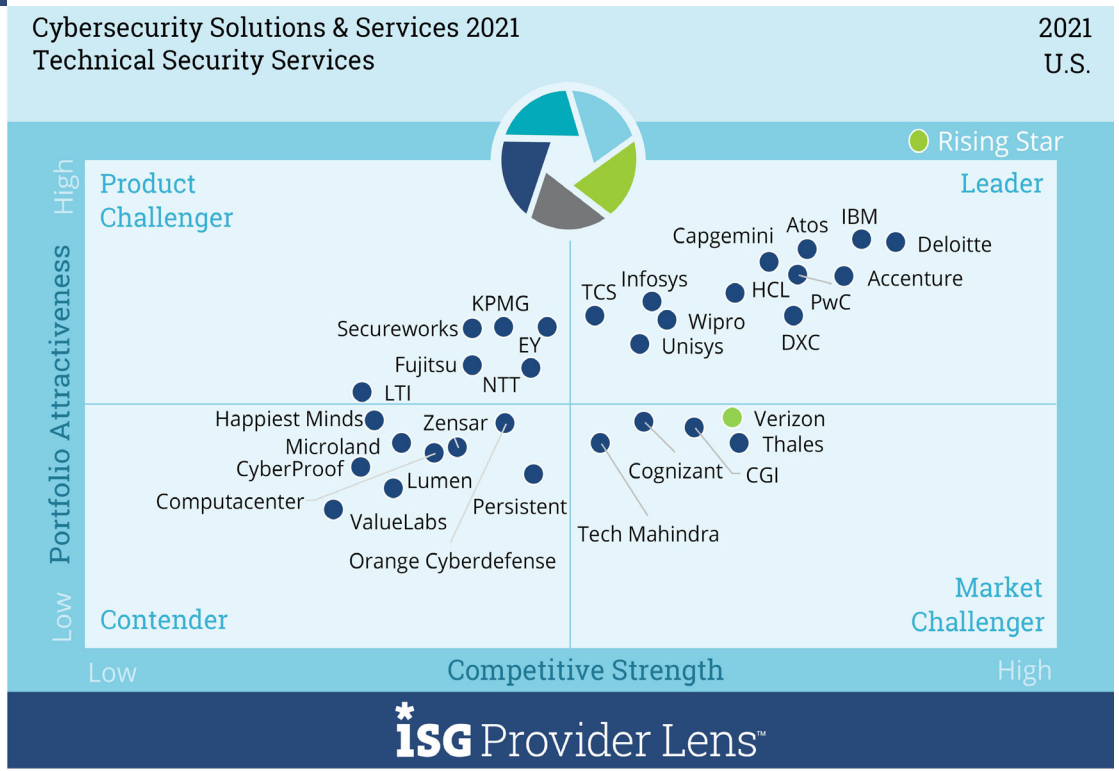
Security and data professionals should read this report to understand how providers comply with the security and data protection laws in the U.S.

© 2021 Information Services Group, Inc. All Rights Reserved.

TECHNICAL SECURITY SERVICES

Definition

This quadrant examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions. The category of technical security services covers integration, maintenance and support for IT security products or solutions. The services address all security products, including antivirus, cloud, and data center security, IAM, DLP, network security, endpoint security and unified threat management (UTM).



Source: ISG Research 2021

© 2021 Information Services Group, Inc. All Rights Reserved.

TECHNICAL SECURITY SERVICES

Eligibility Criteria

- The service provider should demonstrate experience in implementing security solutions for companies in the respective country.
- The provider should not be exclusively focused on proprietary products.
- It should be authorized by vendors to distribute and support security solutions.
- The provider must have certified experts to support its security technologies.
- It should be able to participate (desirable, not mandatory) in local security associations and certification agencies.

Observations

Despite the considerable number of technical service providers in the U.S., gaps still exist. Leading service providers are developing proprietary platforms and interfaces to integrate the varied vendor solutions and plug security gaps. The creation of a successful security environment requires a large ecosystem of technology partners and skilled solution specialists to provide swift security technology integrations that go beyond the out-of-the-box use cases and signatures that come with technologies. These cybersecurity products should be interoperable with a large ecosystem of technology and business partners across the globe to provide clients with superior technology and innovation.

With partners, they create a go-to-market plan, co-create offerings and ensure that resources are trained and certified in the latest technologies. This enables an excellent reach and differentiated services that meet client needs.

Service partnerships have developed into a leading sales channel for vendors. They support client relationships and are trusted to estimate system capacity, write requirements and train customer staff. Security products require high-performing appliances and intricate cloud and network configurations. Technical security consultants also match requirements to appliance models and software and accordingly design the implementation architecture and project plan.

© 2021 Information Services Group, Inc. All Rights Reserved.

TECHNICAL SECURITY SERVICES

Observations (cont.)

These partnerships also provide repeatable architectures and technical blueprints that provide efficient and effective security solutions. They help enterprises detect threats and respond to attacks rapidly, thus enabling security orchestration and automation across the security and IT organization.

Technology vendors and service providers are investing in proprietary technologies with content gained from vast research leveraging labs, centers of excellence as well as partnerships and rich experience from complex deployments. These are being used to create powerful and structured use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture.

When considering a new security solution, technology mature clients understand that the skillset of the technical security service provider that will engineer, architect and integrate the solution is of equal importance as the functionality of the tool itself. Furthermore, clients are looking to bundle software, hardware and long-term service support for increased savings opportunity. The diversity of security tools and partnerships with vendors ensures that U.S.-based clients are given the best security solution advice and configuration from service providers.

From the 85 companies assessed for this study, 32 have qualified for this quadrant with 12 being Leaders and one as a Rising star.

- **Accenture** continues its investments to combine human intelligence with applied intelligence and digital technologies to drive intelligent operations. The services also combine analytics capabilities to collect and analyze the vulnerabilities of more than 71,000 products from over 1,000 vendors.
- **Atos'** acquisition of Eagle Creek Software Services (Eagle Creek), a technology and management consulting company specialized in Salesforce enterprise implementations for clients across North America.
- **Capgemini** leverages cutting-edge technologies, such as security and cloud automation, AI and analytics, data and threat intelligence, as well as its in-depth know-how of security products.
- **Deloitte's** more than 8,600 dedicated cyber risk service practitioners offer customization solution packages for clients based on size, industry and business needs. These services are combined with a function-leading toolset from its targeted partnership network and proprietary solutions.

© 2021 Information Services Group, Inc. All Rights Reserved.

TECHNICAL SECURITY SERVICES

Observations (cont.)

- **DXC Technology** leverages security by design principles, the company offers cyber defense, digital identity, data protection and secured infrastructure. These services are designed to help clients safely run, transform and grow their business across the entire enterprise stack.
- **HCL** relies on its large set of skilled experts in multiple security technologies and its Transformation & Integration services are delivered by seasoned subject matter experts who are placed across the globe.
- **IBM's** showcases a strong portfolio with their integrated security services aimed at protecting critical assets as well as offer quick response and recovery from disruptions as well as managing the complete threat lifecycle.
- **Infosys** relies on their comprehensive portfolio which includes Cyber Next Platform, which offers pre-built, ready-to-use solutions and services for security monitoring, security analytics, threat intelligence and advanced security controls.
- **PwC** leverages a multidisciplinary team of specialists in the areas of digital, people and organization as well as business resilience, forensics, financial crime and human-centric design.
- **TCS** invests heavily in alliances with technology vendors for service development and a go-to-market strategy and positions them collectively within the service model.
- **Unisys** uses their understanding of how clients are targeted and then creating a security architecture to address these areas with a strong focus on providing an ecosystem of solutions addressing specific threats.
- **Wipro** combines detection, triaging, orchestration, contextualized incident management and investigation into a seamless experience to reduce the mean time to respond (MTTR) for every incident.
- **Verizon** (Rising Star) leverages its active partnerships with a wide base of industry leading and best-of-breed technology companies to increase bench strength and help enhance Verizon's consulting service delivery.

© 2021 Information Services Group, Inc. All Rights Reserved.

INFOSYS

Overview

Headquartered in Bangalore, India, Infosys is a multinational IT company that provides business consulting, information technology and outsourcing services. It has a global presence in 46 countries and posted revenues of US$14 billion in fiscal year 2021 with more than 250,000 employees and 1,626 clients. Its security services comprise IAM, GRC, data privacy and protection, vulnerability management, cloud security, infrastructure security, threat detection and response, and emerging technologies.

Strengths

Powerful foundational platform: Infosys Cyber Next Platform is a comprehensive package of security products and associated services that offer pre-built, ready-to-use solutions and services for security monitoring, security analytics, threat intelligence and advanced security controls such as EDR, deception technology and malware analysis. These services are also offered with a subscription based and outcome-oriented pricing model.

Strong IP and technology stack: Infosys leverages technologies that are enhanced with proprietary content gained from vast research and rich experience. These come from use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture. This modern stack of commercial suite is complemented by the Infosys Innovation Hub, bringing the power of technology and cybersecurity excellence to secure client environments.

Next-generation intelligence capabilities: Infosys leverages its innovation hubs that house R&D labs and enable collaboration with various teams such as Infosys Center for Emerging Technology Solutions (iCETS) and Information Security Group – a leading industry partner ecosystem that helps Infosys diagnose and defend against advanced cyber threats. The company also has academic collaborations with Purdue University and the Mysore center of excellence to provide intensive cybersecurity training to upskill and reskill.

Caution

Infosys' technical security capabilities are often seen to be riding on other complementary portfolio offerings. This diminishes the visibility and mindshare among executives and stakeholders in the market.

2021 ISG Provider Lens™ Leader

With its capability to deliver holistic offerings, enhanced by its proprietary technology stack, and continuous investments to increase innovation within internal and external networks, Infosys has sustained its leadership position in the U.S.

© 2021 Information Services Group, Inc. All Rights Reserved.

ENTERPRISE CONTEXT

Strategic Security Services

This report is relevant to enterprises across all industries in the U.S. and evaluates providers of cybersecurity strategic security services.

In this quadrant report, ISG defines the current market positioning of cybersecurity strategic security service providers in the U.S, and how each provider addresses the key challenges faced in the region. Strategic services help enterprises transform security programs that are relevant, sustainable and actionable through program assessment and development services. Instead of reacting to incidents, the most efficient strategies emphasize the prevention of cyberattacks. Hence, large enterprise customers tend to engage with service providers with a large and highly skilled workforce, advanced capabilities and portfolios and a global presence.

The COVID-19 pandemic forced many enterprise clients to operate remotely. However, the quick turnaround with the right cybersecurity strategy helped customers to swiftly shift to a work-from-anywhere (WFA) model.

In the U.S., which is one of the mature markets compared with other regions and countries, the complexity of an enterprise's underlying security is proportional to its size. As a result, in most cases, large enterprises prefer providers that have strong consulting capabilities and are operating at a global level on their own without having to rely on the partners.

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

Marketing and sales leaders should read this report to understand the relative positioning and capabilities of service partners that can help them effectively develop and define a cybersecurity strategy, with the necessary assessments to related systems.

Chief strategy officers should read this report to understand the relative positioning and capabilities of service partners to collaborate with and develop an effective cybersecurity strategy.

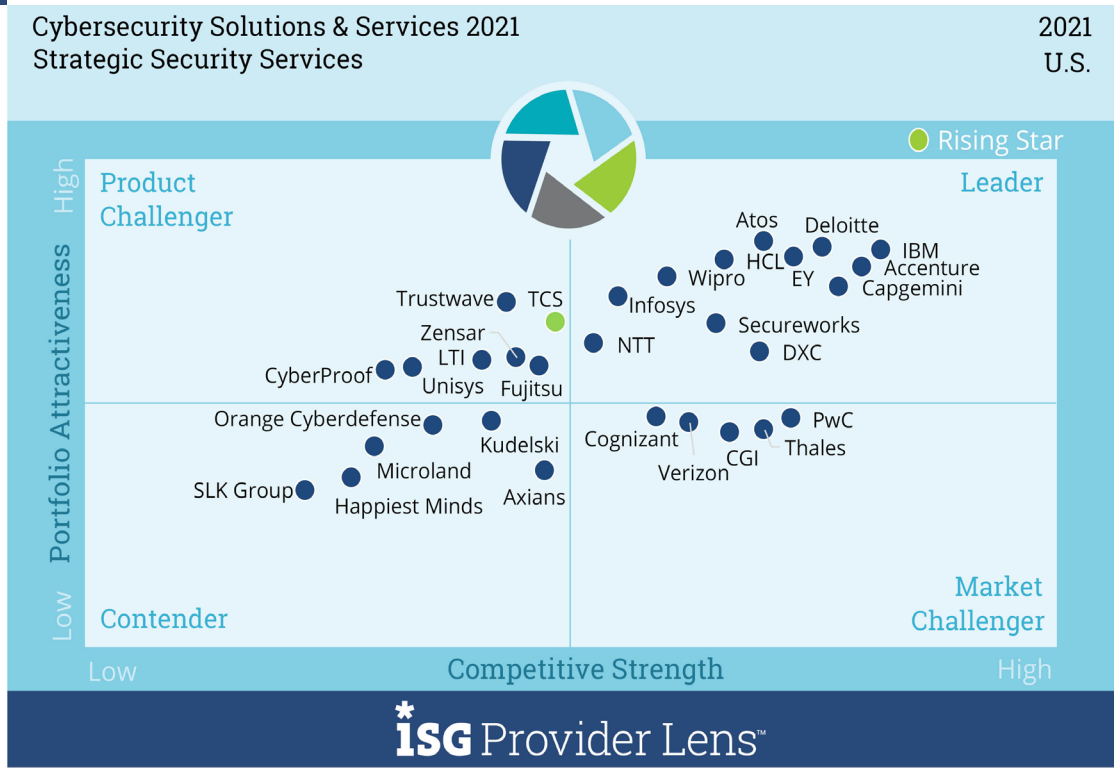
Security and data professionals should read this report to understand how providers comply with the security and data protection laws in the U.S.

© 2021 Information Services Group, Inc. All Rights Reserved.

STRATEGIC SECURITY SERVICES

Definition

Strategic security services primarily cover consulting for IT security. Some of the services covered in this quadrant include security audits, compliance and risk advisory services, security solution architecture consulting, and awareness and training. These are used to assess security maturity, risk posture, and define cybersecurity strategy for enterprises. This quadrant examines service providers that do not have an exclusive focus on proprietary products or solutions. The services analyzed here cover all security technologies.



Source: ISG Research 2021

© 2021 Information Services Group, Inc. All Rights Reserved.

STRATEGIC SECURITY SERVICES

Eligibility Criteria

- Service provider should demonstrate abilities in strategic security service areas such as evaluation, assessments, vendor selection, architecture consulting and risk advisory.
- It should offer at least one of the above services in the respective country.
- Execution of security consulting services using frameworks will be an advantage.
- The provider should not have an exclusive focus on proprietary products or solutions.

Observations

Enterprises are looking for service providers that have in-depth technical expertise, backed by dedicated internal cybersecurity resources and an extensive network of technology partners, academia and external security researchers. The knowledge generated by such functional and operational teams allow for innovation and application of advanced analytics and automated intelligence to security for application, cloud, digital identity, risk and threat operations services, as well as post-breach forensic investigation in each client engagement.

It is becoming highly important to support hundreds of different vendor technologies with the capability to handle complex use cases, such as data correlation and notification rules, for specific business requirements. In addition, these partnerships are converged to innovation hubs consisting of R&D labs and enable collaboration with global technical and advisory teams to solidify their partner ecosystem. This helps both experienced and newer consultants to better assess enterprise security capabilities and their maturity against industry best practices. They offer planning, designing and development of security operations centers with strong foundational capabilities.

Service providers are investing in building security frameworks, backed by competent services delivery models that combine the domain and technical expertise of teams in terms of knowledge and experience as well as the ability for clients to readily use these frameworks.

© 2021 Information Services Group, Inc. All Rights Reserved.

STRATEGIC SECURITY SERVICES

Observations (cont.)

From the 85 companies assessed for this study, 30 have qualified for this quadrant with 12 being Leaders and one a Rising star.

- **Accenture's** competitive advantage stems from their significant technical expertise and extensive technology network of partners, academia and external security researchers and combining with dedicated internal cybersecurity resources.
- **Atos** has made multiple consulting-based acquisitions including In Fidem and SEC Consult Group specifically to enhance their advisory portfolio offering vertical-specific capabilities and in addressing cyber resilience efforts.
- **Capgemini's** Applied Innovation Exchange (AIE) network helps drive innovation and collaboration with clients, to enable enterprises in discovering relevant innovations as well as contextualizing and experimenting within their specific industry.
- **Deloitte** relies on conducting data discovery before assessing it from both value and cost perspectives and offers advisory services to assist enterprises with the technically and strategically hybrid practice of data management.
- **DXC Technology's** experts leverage Advanced Compromise Assessment (ACA) to conduct signature sweeps of clients' network to ensure a proper working condition of defenses as well as to search for adversaries.
- **EY's** consulting portfolio is complemented by their next-generation security operations and response services to help enterprises build a transformation strategy and roadmap to implement the next generation of security operations.
- **HCL** uses a 360-degree security framework and consulting approach, backed by a competent services delivery model, to provide superior levels of security to its clients.
- **IBM's** security intelligence operations and consulting services are aimed at helping clients to develop maturity in intelligence-driven operations across their IT environments.

© 2021 Information Services Group, Inc. All Rights Reserved.

STRATEGIC SECURITY SERVICES

Observations (cont.)

- **Infosys** leverages technologies that are enhanced with proprietary content gained from vast research and rich experience from use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture.
- **NTT** relies on powerful risk management capabilities, pulling security information and event management (SIEM) and IT system data directly into a proprietary application to quantify risk exposure. The company supports more than 200 different vendor technologies and can handle complex use cases.
- **Secureworks** has more than 400 security consultants to assist clients with challenges related to technical, operational and strategic cybersecurity as well as compliance. The company also offers consulting solutions to review and assess client deployments for major hyperscaler services such as AWS, Azure and Office 365.
- **Wipro's** clients are offered a combination of innovative platform-based security solutions, a unique risk-based approach, and the experience of over 6,000 security experts to improve their security posture.
- **TCS'** (Rising Star) team has deep domain and industry experience to contextualize cybersecurity programs as per specific client business needs and their risk appetite. The company's focus areas include OT/IoT, cloud, forensics, incident response professional services, development, integrations, and cyber risk and resiliency.

© 2021 Information Services Group, Inc. All Rights Reserved.

INFOSYS

Overview

Headquartered in Bangalore, India, Infosys is a multinational IT company that provides business consulting, information technology and outsourcing services. It has a global presence in 46 countries and posted revenues of US$14 billion in fiscal year 2021 with more than 250,000 employees and 1,625 clients. Its security services comprise IAM, GRC, data privacy and protection, vulnerability management, cloud security, infrastructure security, threat detection and response, and emerging technologies.

Strengths

Expertise from vast experience: Infosys leverages technologies that are enhanced with proprietary content gained from vast research and rich experience. These come from use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture. This modern stack of commercial suite is complemented by the Infosys Innovation Hub, bringing the power of technology and cybersecurity excellence to secure client environments.

Investments for innovation and knowledge: Infosys leverages its innovation hubs that house R&D labs and enable collaboration with various teams such as Infosys Center for Emerging Technology Solutions (iCETS) and Information Security Group – a leading industry partner ecosystem that helps Infosys diagnose and defend against advanced cyber threats. The company also has academic collaborations with Purdue University and the Mysore center of excellence to provide intensive cybersecurity training to upskill and reskill.

Dedicated defense centers: Infosys augments its commitment to the U.S. security market through the Cyber Defense Center in Indianapolis. The center monitors client environments round the clock, adopting a follow-the-sun model to deliver services such as 24-by-7 security monitoring, management and remediation, threat hunting, security analytics, incident discovery and response, compliance reporting and malware analysis.

Caution

Infosys should further differentiate its consulting capabilities to gain a stronger foothold in the U.S. It should enhance and create a powerful storyline that is centered on solving complex security challenges for clients.

2021 ISG Provider Lens™ Leader

With its continuous investments to build a comprehensive portfolio and a specialized team of experts with rich intellectual propertyand playbooks, Infosys is continuing its growth trajectory in the U.S.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

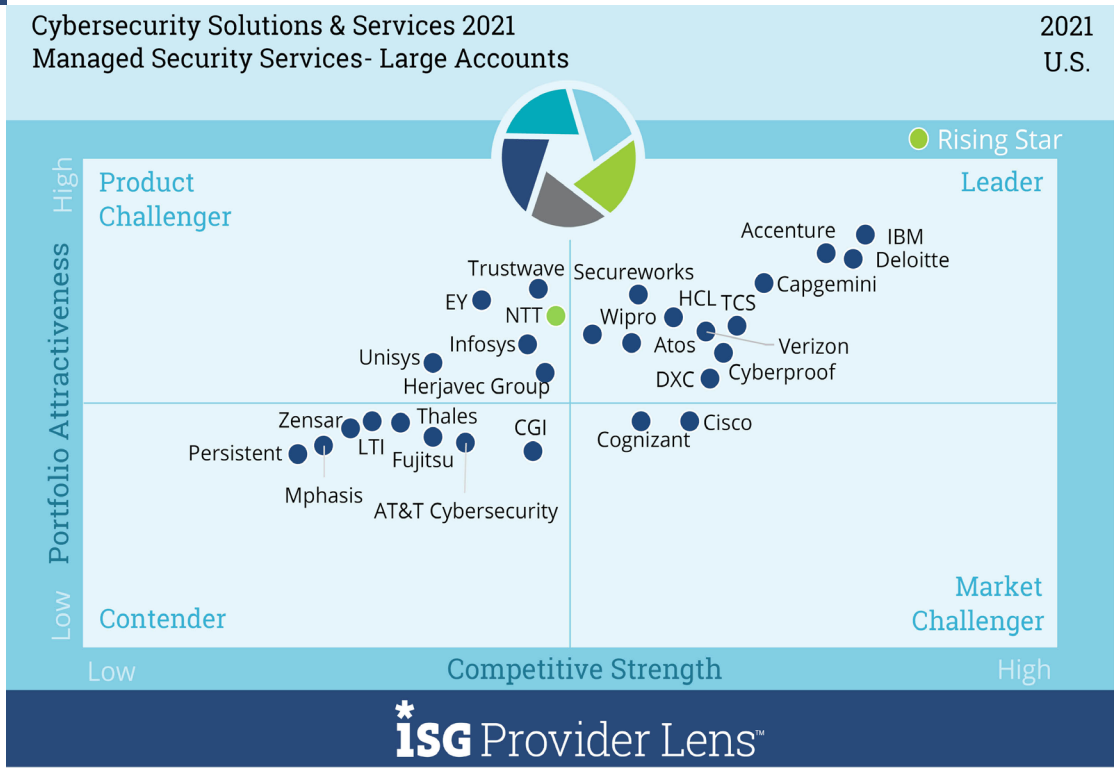
Security leaders should read this report to understand the relative positioning and capabilities of MSSPs. The report also compares the technical capabilities of various service providers in the market.

© 2021 Information Services Group, Inc. All Rights Reserved.

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

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

ENTERPRISE CONTEXT

Managed Security Services - Midmarket

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.

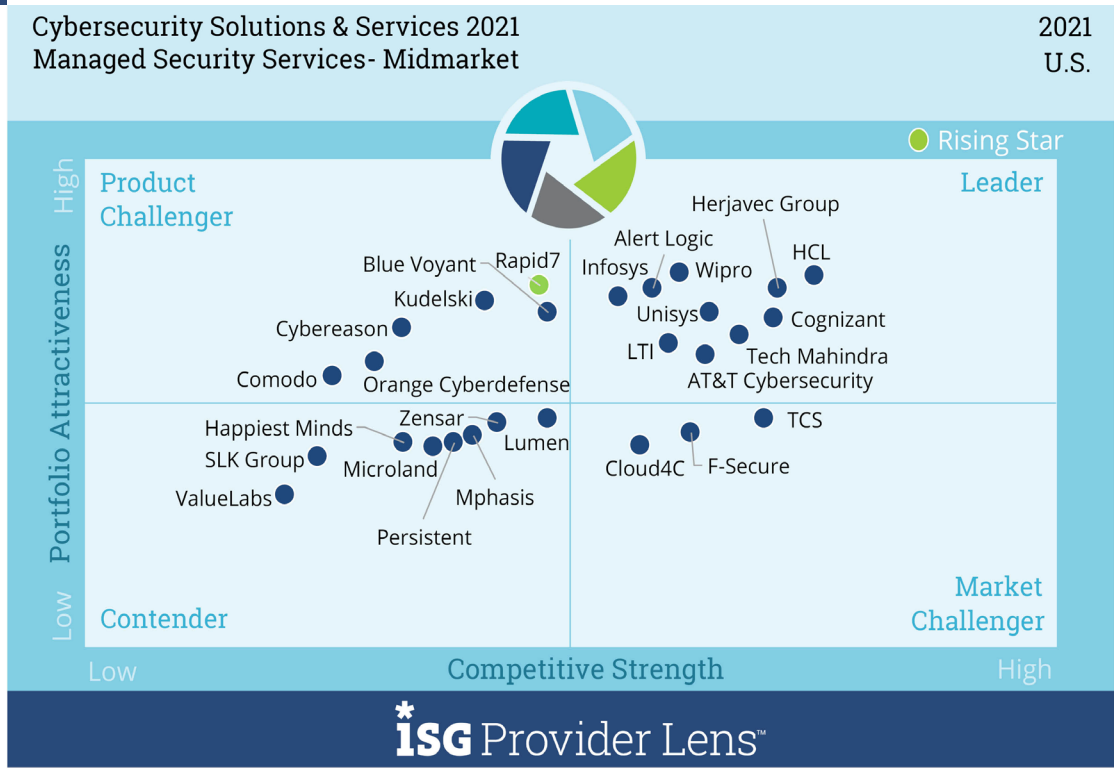
Security leaders should read this report to understand the relative positioning and capabilities of MSSPs. The report also compares the technical capabilities of various service providers in the market.

© 2021 Information Services Group, Inc. All Rights Reserved.

MANAGED SECURITY SERVICES - MIDMARKET

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

© 2021 Information Services Group, Inc. All Rights Reserved.

MANAGED SECURITY SERVICES - MIDMARKET

Eligibility Criteria

- The service provider should be able to provide security services such as detection and prevention, security incident and event management (SIEM), and security advisor and auditing support remotely or at the client site.
- The provider should hold relevance (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 centers should be ideally owned and managed by the provider and not predominantly by partners.
- 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 when conditions are outside of expectations. Increasingly, clients are engaging 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 and 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 MSSPs on a hybrid basis to supplement some existing in-house capacity or skillset with services that fill the gaps or enhance vigilance.

© 2021 Information Services Group, Inc. All Rights Reserved.

MANAGED SECURITY SERVICES - MIDMARKET

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, 27 have qualified for this quadrant with 11 being Leaders and one as a Rising star.

- **AT&T Cybersecurity** leverages its rich ecosystem of cybersecurity technologies and strategic alliances to offer global oversight and threat intelligence with eight security operations centers worldwide. Their Alien Labs™ delivers tactical threat intelligence, enabling resilient threat detection and response.
- **Alert Logic** uses its engineering and security experts to offer insights from the proprietary platform and third-party feeds to define and develop new detection methods. This also helps in implementing new techniques improving threat research and intelligence platform.
- **Cognizant** offers end-to-end security services combining deep domain and industry expertise with advisory, transformation and managed services. The partnership with IBM and its global presence offer a rich source of extensive library use cases that are pre-built in the CT Cyber Threat Defense (CTD) platform.
- **HCL** invests significantly in partnerships with leading industry vendors, including niche security products from original equipment manufacturers (OEM) which supports security technology management across the security ecosystem.
- **Herjavec Group** derives its strength from combining aspects of technology, AI and automation with intelligence to build its managed security offering to enhance IT security monitoring, incident detection and incident response times.
- **Infosys** leverages its innovation hubs that house R&D labs and enable collaboration with various teams such as Infosys Center for Emerging Technology Solutions (iCETS) and Information Security Group, helping it to diagnose and defend against advanced cyber threats.
- **LTI** relies on a comprehensive managed security services portfolio is designed with a cybersecurity framework that cover cyber threat defense, advanced threat and vulnerability management, identity governance and digital security.

© 2021 Information Services Group, Inc. All Rights Reserved.

MANAGED SECURITY SERVICES - MIDMARKET

Observations (cont.)

- **Tech Mahindra's** AI-powered Predictive Cyber Risk Platform and Global Data Privacy ecosystem deliver advanced threat management capabilities through file-less, memory attack prevention that enables real-time detection without false positives.
- **Unisys** leverages its network of global delivery centers, providing a set of flexible support options based on client needs. It also delivers a methodology based on IT infrastructure library (ITIL), with annual ISO and SSAE audits, helping clients to meet compliance requirements.
- **Wipro's** managed security services business caters to client needs, spanning across intelligence, protection, detection, remediation, response and recovery. It offers integrated, automated and comprehensive capabilities improving visibility into a client's entire data center and cloud environment.
- **Rapid7** (Rising Star) leverages its Insight cloud to collect data from client environments and manage vulnerabilities, monitor for malicious behavior, investigate and stop attacks, and automate operations.

© 2021 Information Services Group, Inc. All Rights Reserved.

INFOSYS

Overview

Headquartered in Bangalore, India, Infosys is a multinational IT company that provides business consulting, information technology and outsourcing services. It has a global presence in 46 countries and posted revenues of US$14 billion in fiscal year 2021 with more than 250,000 employees and 1,625 clients. Infosys offers managed identity security services, managed threat detection and response services, managed vulnerability management services, cyber threat intelligence, managed infrastructure security service, managed cloud security services and managed emerging technologies services as part of its managed security portfolio.

Strengths

Broad and advanced portfolio: As part of its managed security portfolio, Infosys provides comprehensive cybersecurity solutions to enterprises through the Cyber Next platform. The platform provides deep visibility into security events, capability for automated response to contain and remediate security anomalies, intelligence on latest threats that could damage business, proactive vulnerability management, and the ability to manage security and architecture compliance.

Dedicated defense centers: Infosys augments its commitment to the U.S. security market through the Cyber Defense Center in Indianapolis. The center monitors client environments round the clock, adopting a follow-the-sun model to deliver services such as 24-by-7 security monitoring, management and remediation, threat hunting, security analytics, incident discovery and response, compliance reporting and malware analysis.

Next-generation intelligence capabilities: Infosys leverages its innovation hubs that house R&D labs and enable collaboration with various teams such as Infosys Center for Emerging Technology Solutions (iCETS) and Information Security Group – a leading industry partner ecosystem that helps Infosys diagnose and defend against advanced cyber threats. The company also has academic collaborations with Purdue University and the Mysore center of excellence (COE) to provide intensive cybersecurity training to upskill and reskill.

Caution

Infosys is growing its security capabilities through continuous investments in the U.S. However, the company should still improve its visibility among large enterprises to grow market and mind share.

2021 ISG Provider Lens™ Leader

Infosys offers advanced competencies across technologies, enabling a holistic threat coverage with a comprehensive portfolio. With a commitment to investing in next-generation capabilities in people and processes, the company has achieved leadership in the U.S. midmarket.

© 2021 Information Services Group, Inc. All Rights Reserved.

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

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

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.

© 2021 Information Services Group, Inc. All Rights Reserved.

ISG Provider Lens™ | Quadrant Report
August 2021

© 2021 Information Services Group, Inc. All Rights Reserved

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.