ISG Provider Lens™

Cybersecurity – Solutions and Services

A research report evaluating cybersecurity provider and solution vendor strengths, challenges, and competitive differentiators

Customized report courtesy of:

pwc

QUADRANT REPORT | JULY 2022 | U.S.

Report Author:
Gowtham Kumar Sampath

Becoming cyber resilient; not only cyber secure

The cybersecurity market in the U.S., witnessed exceptional growth in spending against the backdrop of a multitude of reasons threatening to impact businesses and economy. The U.S. market is reflective of global trends; U.S. is recognized for its high maturity in IT and security adoption and as the hub for centralized business decision making for several enterprises. The post-COVID-19 phase witnessed an unprecedent acceleration in digital transformation investments, uptake of remote and hybrid work models, incidents of sophisticated attacks and data leaks across enterprises of all sizes, and the (ongoing) Ukraine-Russia conflict. These reasons, combined with the surge in insider threats, lack of cybersecurity awareness with misguided perceptions and false sense of complete protection, have created further complexities, necessitating innovative, real-time and advanced security capabilities.

Here are some of the key factors disrupting the market dynamics and creating headlines:

- Identify and access management (IAM) gaining a strong foothold across enterprises, as the starting point for security investments, to stop breaches and data losses
- The accelerated shift to cloud leading to misconfigurations, security gaps, outages and control challenges
- Strong thought leadership, R&D and investments being made on sovereign cloud architectures with trusted security capabilities to meet strict compliance requirements

- Extended managed detection and response (XMDR) solutions experiencing significant growth in the market due to their advanced threat intelligence and remediation capabilities
- IoT growth further accelerating the convergence of IT/OT security, with endpoint solutions gaining significant traction

Enterprises in the U.S. are rethinking their security strategy with investments directed toward advanced and innovative security solutions, including identity management, endpoint protection and advanced data leakage and protection solutions. C-suite executives are seeking cybersecurity provider partners that offer holistic, end-to-end services, with delivery capabilities designed to suit the dynamic and agile needs of their enterprise.

Concurrently, the market is undergoing aggressive consolidation, with several acquisitions targeted at improving portfolio attractiveness and competitive strength. In addition, there is intense collaboration among providers and vendors to create a robust ecosystem of partners, addressing specialized industry needs and compliance requirements, and future-proof solutions.

Cybercriminals Commercializing Threats Into a Business Model:

Cyber criminals are relentlessly uncovering vulnerabilities, using sophisticated phishing techniques and attacking with complex ransomware and malware. Comparable to state-sponsored adversaries in funding and structure, hacker groups are also gaining notoriety for executing complex attacks, at scale. The success of these attacks and their ability to exploit the combined intelligence of several threat actors have resulted in the availability of As-a-Service models for ransomware, malware and other exploits. Consequently, not only have the number of attacks and attackers increased, but also the needed skills among adversaries to execute such complex attacks have become less significant. Enterprises in the U.S. are perplexed with ransomware attacks because extortion is now not the only reason – exposing data or other critical vulnerabilities, stealing intellectual property and misleading/misdirection to hide advanced persistent threats are now some of the prevalent motivations.

A Shift to Cyber Resiliency from Cyber Security Technology:

Business leaders and enterprises are beginning to understand that attacks, threats and data losses are to a certain extent inevitable due to the sophistication of attacks, lack of visibility, awareness and human error. There is also an apparent and significant shift in mindset, especially among business leaders of small and midsize enterprises in the U.S. – a realization that attacks and breaches are not restricted to large, financially stable organizations with strong knowledge assets. Such attacks and breaches can happen to any organization and to some extent have already happened in their environment, however, many enterprises have no visibility to the extent and root cause.

Cyber resiliency is gaining prominence and mind share — the way forward to institutionalize a flexible and dynamic response together with recovery capabilities to ensure business continuity. While the premise of cyber resiliency is to ensure business and operational continuity with minimal losses and impact, the market lacks a standardized approach or methodology to measure cyber

resilience. The cybersecurity market needs to prioritize the design and launch of a framework or reference working model to assess the maturity of cyber resilience across businesses.

Renewed Interest in Frameworks, Security Assessment Certifications and More:

Service providers and vendors are scrambling to invest to gain certifications from NIST, ISO 27001, MITRE ATTACK, SANS and other institutions. Several vendors such as CyberArk and ForgeRock have gained SOC 2 Type II certifications for their solutions, thereby indicating their commitment to assuring enterprise-grade security, availability, confidentiality and privacy for customer data. A significant portion of the Leaders and other providers ISG evaluated have aligned their cyber strategies to reflect the NIST Framework of Identify, Protect, Detect, Respond & Recover, to create security awareness among enterprises and to reflect these extensive measures and capabilities within their respective portfolios. Maturity assessment models, operations models and capability models utilize these frameworks. These models also necessitate strong human intervention across the framework to effectively secure enterprise assets.

Integrating Human Intelligence with Automation:

U.S. enterprises have realized that investment in advanced security tools and solutions alone will not offer enhanced levels of resilience – cybersecurity specialists are needed to drive these technologies. This realization has helped in creating an integrated process that allows for human-intelligent decisions based on machine-automated analysis. Solutions that support the correlation between intuition, intelligence, analytics and automation, driving synergies between human expertise and machine capabilities, are on the rise. Service providers and vendors have started investing in human-centric solutions, where seasoned cybersecurity specialists work with advanced AI and machine learning to drive real-time threat detection, isolation and response capabilities. Advanced security operations centers are being built with capabilities that integrate machine learning algorithms with human analysis for automated detection of unknown threats from network log files and other data collected across an IT environment.

Lack of Talent Necessitates Investments in Training and Upskilling:

The plethora of products and services available in the cybersecurity sector is in stark contrast to the human resource available to harness their benefits; there is a deep gap between the supply and demand of cybersecurity professionals in the U.S. market. According to industry estimates, the U.S. cybersecurity workforce has more than 1 million workers, with approximately 600,000 positions yet to be filled. Service providers and vendors are also actively investing in training and upskilling initiatives to replenish talent and fill these gaps to ensure a secure business environment. For example, Microsoft has a national campaign with community colleges in the U.S., to help place 250,000 people into the cybersecurity workforce by 2025, Google is training 100,000 people for vital jobs in data privacy and security in the U.S., IBM has plans to train 150,000 people in cybersecurity skills over the next three years — several other companies are launching similar initiatives.

In this environment, enterprises are increasingly buying tools and solutions ad-hoc, resulting in point solutions that are effective for specific threats but do not address holistic security needs. Challenges arising from this situation, such as operational inefficiencies, lack of centralized ownership and inconsistent visibility can only be solved by specialized human expertise.

Data-Centric Approaches Drive Context- and Content-Aware Threat Detection Solutions:

Cyber analytics is witnessing increased traction to enhance threat hunting and detection capabilities. Through threat and data classification analytics helps identify unknown and advanced persistent threats. There is an increasing shift to leverage data-centric analytics to identify malicious behavior by users, files, software, endpoints, cloud and web applications.

Vendors and providers are relying on innovative approaches to determine the nature of threats within their network — using contextual awareness and content-based approaches to identify malicious behavior. These approaches enable increased visibility, thereby allowing isolation and further remediation.

Notes on quadrant positioning

In this study, several security services and solution providers that offer fairly similar portfolio attractiveness in most quadrants are assessed. This reflects the relative maturity of the market, providers and offerings. It is a given that not all are equal in circumstances. The vertical axis positioning in each quadrant reflects ISG's analysis of how well the offerings align with the full scope of public sector organizations' needs.

Readers will also note similarities in portfolio axis (vertical axis) positioning with providers included in ISG's Provider Lens™ U.S. Public Sector Cyber Security Solutions and Services study.

Human expertise and context-aware machine intelligence to enhance security

Provider Positioning

Page 1 of 10

	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
AT&T Cybersecurity	Not In	Not In	Not In	Not In	Not In	Product Challenger	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

Provider Positioning

Page 2 of 10

	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
Blackberry (Cylance)	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Blue Voyant	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
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	Market Challenger	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	Product Challenger	Product Challenger	Market Challenger	Not In
Comodo	Not In	Contender	Product Challenger	Not In	Not In	Not In	Not In

Provider Positioning

Page 3 of 10

	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
Computacenter	Not In	Not In	Not In	Contender	Contender	Not In	Product Challenger
CoSoSys	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Critical Start	Not In	Not In	Not In	Not In	Not In	Not In	Leader
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	Not In
CyberProof	Not In	Not In	Not In	Not In	Not In	Leader	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader	Not In
DriveLock	Not In	Contender	Not In	Not In	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger	Not In

Provider Positioning

Page 4 of 10

	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
EmpowerID	Product Challenger	Not In	Not In	Not In	Not In	Not In	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
Fischer Identity	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Not In	Not In	Not In	Not In
ForgeRock	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Fortinet	Market Challenger	Not In	Leader	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Product Challenger	Product Challenger	Contender	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	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
Google	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
GTB Technologies	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Happiest Minds	Not In	Not In	Not In	Contender	Contender	Not In	Product Challenger
HCL	Not In	Not In	Not In	Leader	Leader	Leader	Not In
HelpSystems	Product Challenger	Leader	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	Product Challenger	Leader	Leader	Leader	Not In
Ilantus Products	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Imperva	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Leader	Leader	Product Challenger	Not In

Provider Positioning

	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
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
KPMG	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
Kudelski Security	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger
LTI	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
Lumen	Not In	Not In	Not In	Market Challenger	Not In	Not In	Leader
ManageEngine	Product Challenger	Contender	Not In	Not In	Not In	Not In	Not In
Matrix42	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Micro Focus	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Microland	Not In	Not In	Not In	Product Challenger	Contender	Not In	Product Challenger

Provider Positioning

Page 7 of 10

	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
Microsoft	Leader	Market Challenger	Leader	Not In	Not In	Not In	Not In
Mindtree	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Mphasis	Not In	Not In	Not In	Not In	Not In	Contender	Product Challenger
Netskope	Not In	Rising Star ★	Product Challenger	Not In	Not In	Not In	Not In
NTT	Not In	Not In	Not In	Rising Star ★	Leader	Leader	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Omada	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Leader	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Market Challenger	Market Challenger	Not In	Not In	Not In	Not In
Optiv	Not In	Not In	Not In	Not In	Not In	Not In	Leader

Provider Positioning

	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
Palo Alto Networks	Not In	Product Challenger	Leader	Not In	Not In	Not In	Not In
Persistent Systems	Not In	Not In	Not In	Contender	Product Challenger	Contender	Product Challenger
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Proficio	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★
Proofpoint	Not In	Leader	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
Rackspace Technology	Not In	Not In	Not In	Not In	Not In	Not In	Leader
Rapid7	Not In	Not In	Leader	Not In	Not In	Not In	Not In
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

Provider Positioning

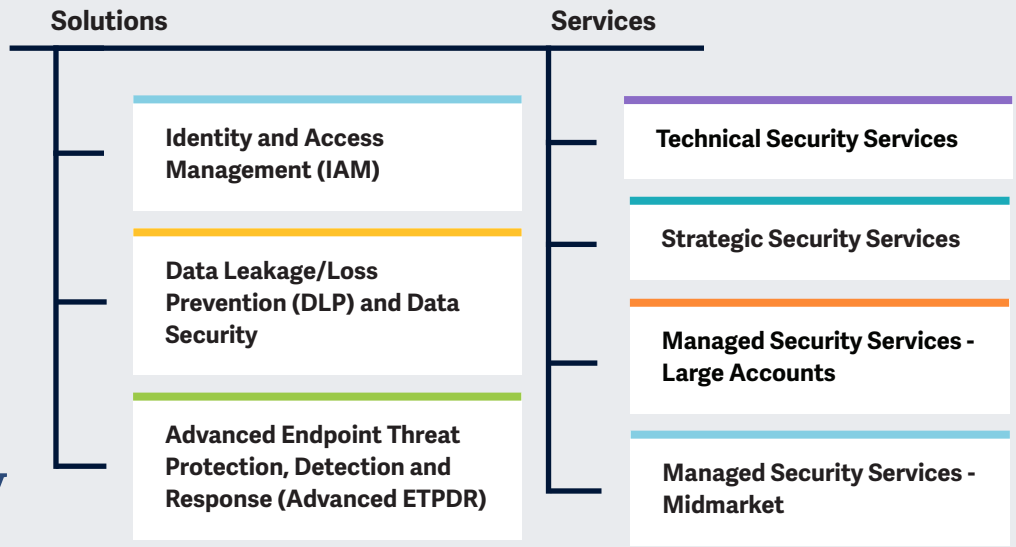
Page 9 of 10

	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
Saviynt	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
SecureAuth	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Not In	Product Challenger	Leader	Not In	Not In
SentinelOne	Not In	Not In	Leader	Not In	Not In	Not In	Not In
SLK Group	Not In	Not In	Not In	Not In	Not In	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	Not In
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Trellix	Not In	Leader	Leader	Not In	Not In	Not In	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	Rising Star ★	Not In

Provider Positioning

	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	Market Challenger	Not In	Not In	Leader	Product Challenger	Product Challenger	Leader
ValueLabs	Not In	Not In	Not In	Not In	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	Leader	Product Challenger	Leader	Not In
VMWare Carbon Black	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
WatchGuard	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Zecurion	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Zensar	Not In	Not In	Not In	Contender	Product Challenger	Contender	Contender
Zscaler	Not In	Leader	Not In	Not In	Not In	Not In	Not In

The study focuses on what is most critical in 2022 for **Cybersecurity**



Simplified Illustration Source: ISG 2022

Definition

Enterprises are adopting emerging technologies to embark on their digital transformation journey to stay competitive and align with ever-evolving end-user needs. This was further exacerbated with the COVID-19 pandemic accelerating enterprise adoption of remote work, cloud applications and other digital technologies to survive and thrive. The growing adoption of these technologies, along with new tools to deliver efficiency and speed, has led to an increase in the threat attack surface. Ransomware, advanced persistent threats and phishing attacks have emerged as some of the leading cyber threats in 2022. As the nature and complexity of cyberattacks continue to increase, cybersecurity has become a priority not just for enterprises, but for government agencies as well to protect their economies, industries and citizens.

With the ever-changing threat landscape, enterprises need to 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 identity and access management (IAM), data leakage/loss prevention (DLP) and managed security services (MSS) to achieve a robust, secure framework to reduce risk exposure.

In addition to the need for self-protection, regulations such as HIPAA, Gramm-Leach-Bliley Act, and the Homeland Security Act have compelled businesses to implement robust safeguard measures to counter cyberattacks. The Cybersecurity Enhancement Act (2014), The Cybersecurity Act of 2015 and the much expected "Strengthening American Cybersecurity Act of 2022" will further accelerate educating enterprises and strengthen the overall security posture.

Although, cybersecurity has become an important practice area for enterprise CISOs, IT executives often struggle to justify security investments, as it is not always possible to measure and demonstrate the ROI or to quantify threat-related risks. The sophistication of available technologies, difficulties in identifying and fixing vulnerabilities and the lack of awareness among end users continue to taunt enterprises and its executives.

Another challenge is that deploying adequate security tools does not imply that an enterprise will be immune to vulnerabilities; the human factor continues to remain the weakest link in the security wall, which is continuously exploited by attackers through cyber threats such as Trojan Horse and phishing attacks. A lack of awareness among end users may result in targeted attacks such as advanced persistent threats (APTs) and ransomware, impacting brand reputation, causing data and financial loss and precipitating operational outages. Therefore, user training, risk assessment and advisory services will continue to play a key role in keeping enterprise information and communications technology (ICT) infrastructure secure.

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following seven quadrants: Technical Security Services (TSS); Strategic Security Services (SSS); Managed Security Services (MSS) for Large Accounts; Managed Security Services (MSS) for the Midmarket; Identity and Access Management (IAM); Data Leakage/Loss Prevention (DLP) and Data Security; Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR).

This ISG Provider Lens™ study offers IT-decision makers:

- Transparency on the strengths and weaknesses of relevant providers/ software vendors
- A differentiated positioning of providers by segments
- Focus on regional market

Our study serves as the basis for important decision-making in terms of positioning, key relationships and go-to-market considerations. ISG advisors and enterprise clients also use information from these reports to evaluate their existing vendor relationships and potential engagements.

Provider Classifications

The provider position reflects the suitability of IT providers/ software vendors 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.

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. 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).

Provider Classifications: Quadrant Key

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.

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.

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 products/services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

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.

★ **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 means 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.

Identity and Access Management (IAM)

Who Should Read This

This report is relevant to enterprises across industries in the U.S. for evaluating providers that offer solutions that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalization.

In this quadrant report, ISG highlights the current market positioning of providers of identity and access management solutions that reduce security threats for enterprises in the U.S., and how each provider addresses the key challenges in the market.

The increased focus on identity and access management (IAM) aims to improve risk management, threat detection and regulatory compliance. The number of enterprises adopting cloud-based IAM solutions has been increasing over years. Also, investments in hybrid cloud services are high.

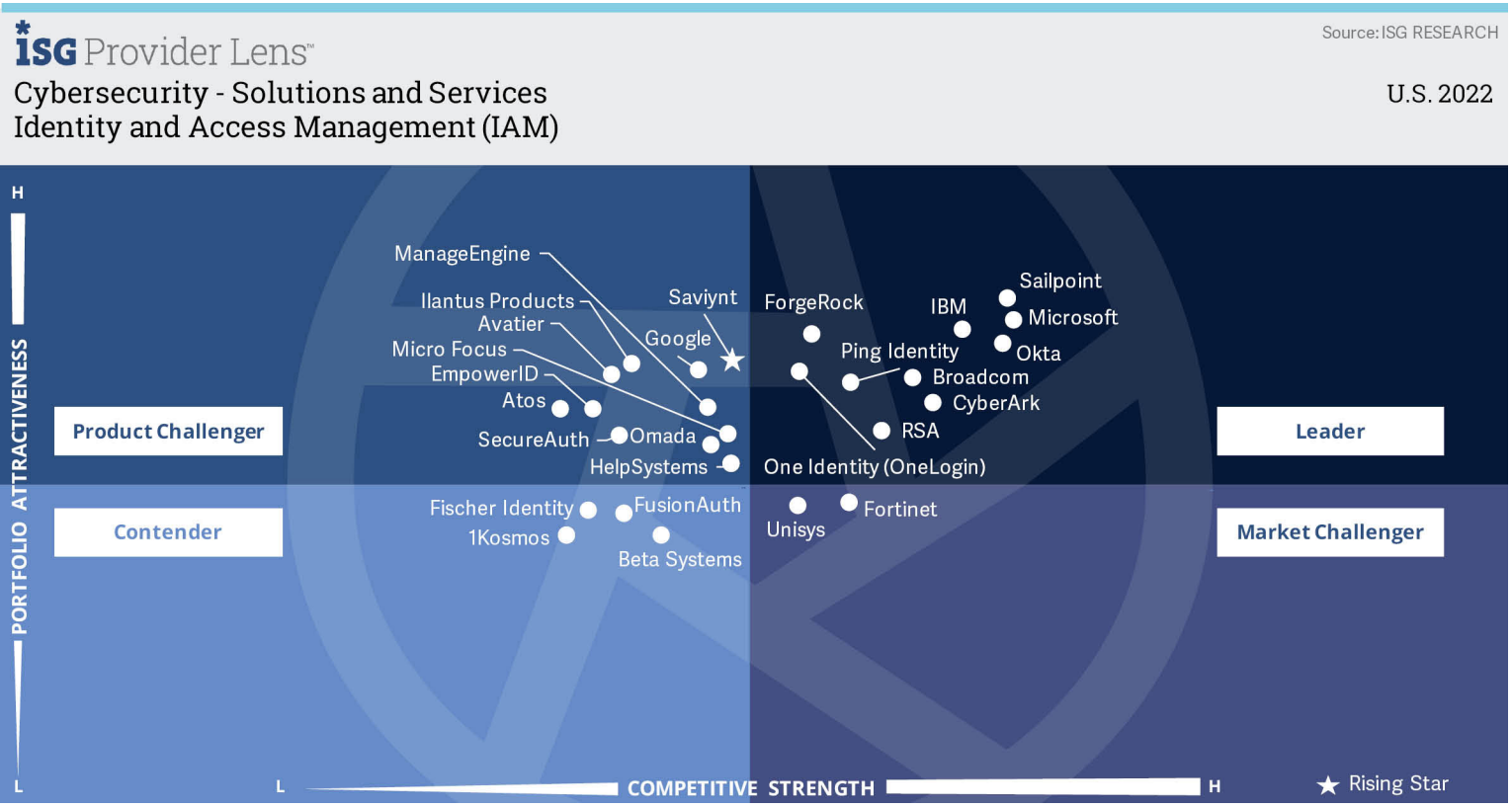
In U.S., the adoption of IAM solutions is increasing in tandem with digital transformation among enterprises and in keeping with growing regulatory guidelines and security concerns. Large enterprises are looking for IAM solutions integrated with AI and machine learning and with an easy login experience. End-users now expect authentication services on their phones to be as easy as unlocking their phones.

Enterprises prefer providers that offer combined comprehensive IAM solutions that combine single sign-on (SSO) and privileged access management (PAM).

Chief information security officers should read this report to understand how IAM solution providers address the significant challenges of compliance and security while maintaining a seamless experience for enterprise clients.

Chief data officers and data privacy officers should read this report to understand how the providers offer information protection and privacy, information governance, data quality and data lifecycle management.

Chief strategy officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.



This quadrant **assesses vendors with commercially available products and excludes providers with no proprietary software** offering. The **key areas of focus include single-sign-on (SSO), zero trust access and multifactor authentication, with passwordless authentication** gaining mindshare.

Gowtham Kumar Sampath

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services 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 and/or cloud) based on proprietary software are not included here. Depending on organizational requirements, these solutions could be deployed in several ways such as on premises or in the cloud (managed by the customer) or as an as-a-service model, or a combination thereof.

IAM solutions are aimed at collecting, recording and administering user identities and related access rights, as well as specialized access to critical assets, including privileged access management (PAM). They ensure that access rights are granted based on defined policies. To handle existing and new application requirements, IAM 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 functionalities related to social media and mobile use to address their specific security needs that go beyond traditional web and context-related rights management. Machine identity management is also included here.

Eligibility Criteria

1. The solution should be capable of being **deployed** in combination with **on-premises, cloud, identity as a service (IDaaS)** and a managed third-party model.
2. The solution should be capable of supporting authentication by a combination of single-sign on **(SSO), multifactor authentication (MFA), risk-based and context-based** models.
3. 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.
4. The solution should be capable of supporting one or more legacy and newer IAM standards, including, but not limited to, **SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM**.
5. To support through 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).

Observations

IAM has undergone significant developments with enterprises shifting to remote, hybrid work models and investing in cloud transformation. IAM is being prioritized as the foundation to secure businesses from external adversaries and insider threats. The IAM market has undergone major consolidation, driven by the need to improve portfolio strength and competitiveness: One Identity acquired OneLogin, Thoma Bravo acquired SailPoint, SentinelOne acquired Attivo Networks and Avast acquired SecureKey Technologies.

Compared to our 2021 assessment, ISG excluded vendors with IAM solutions that support only their own environments (SAP and Oracle), and public key infrastructure (PKI) vendors due to their larger focus on machine identities and IoT devices in the industrial sector.

- Customer identity and access management (CIAM) has gained prominence across B2B and B2C engagements. Consistent **customer engagement and experience** and **improved privacy and enhanced compliance** are driving enterprise demand for these solutions.
- As zero trust begins to gain mindshare, privileged access tools are being integrated with dedicated functionalities to **remove default privileges, apply least privileges and continuously monitor privileged accounts.** Moreover, the integration of behavioral analytics, multi-factor authentication (MFA) and digital identities will enhance dynamic access and authentication.
- Cloud IAM gains traction with an **increase in remote employees and the growth in public and private cloud adoption.** Hyperscalers are industrializing cloud IAM solutions for optimally serving the unique requirements of verticals such as banking and finance, healthcare and education.

From more than 95 companies assessed for this study, 27 have qualified for this quadrant with ten being Leaders and one a Rising Star.

Broadcom

Broadcom continues to rely on the assets it gained from CA Technologies and Symantec to bolster its productized focus, and leverages their brand presence for expanding its revenue base and partnerships with service providers.

CyberArk

CyberArk takes an AI-based, security-first approach that is adaptive, and leverages context awareness for managing identities. It is a part of the C3 Alliance that has more than 100 technology partners and industry-leading product integrations.

ForgeRock

ForgeRock invests in offering new enhancements that enable centralized visibility and control. Other commitments include its SOC 2 certifications that are aimed at instilling confidence in its capabilities. Forge Autonomous Access offers increased threat protection using AI, machine learning and advanced pattern matching to analyze threat signals and behavior.

IBM

IBM offers a diverse portfolio of offerings that encompass IAM, cloud access management and authentication, IGA, privileged access management (PAM), CIAM and hybrid access management system. IBM's cloud-native approach ensures automated risk protection and continuous user authentication across multicloud environments.

Microsoft

Microsoft is creating a true zero-trust mindset to ensure effective protection and organizational resilience. Microsoft Azure AD offers traditional features such as SSO, Lightweight Directory services, rights management, certificate services and federation services.

Okta

Okta, with more than 7,000 integrations and products, has gained significant appeal among several corporate executives. The solutions have enabled enterprise workforces to rely on SSO across multiple cloud service providers.

One Identity

One Identity's acquisition of OneLogin has helped expand a portfolio that serves as a one-stop-shop for clients. The company is addressing a wider audience and aggressively expanding its partner network to promote sales.

Ping Identity

Ping Identity offers integration kits, a variety of bundled adapters, authentication selectors and data stores to other identity and service providers, which helps in extending access management systems and in enabling authentication, authorization and data synchronization.

RSA

RSA helps enterprises speed time-to-deployment and time-to-value by launching best practices and blueprints around implementation, and creating a set of use cases, partner product integrations and recommendations. RSA's recent initiatives and investments are expected to put it back on track with identity at the center of its brand strategy and business focus.

SailPoint

SailPoint's latest enhancements deliver a multi-tenant SaaS offering and leverage AI and machine learning to offer context-based relationships and better classification of users. Thoma Bravo acquiring SailPoint would provide enhanced presence and collaboration opportunities with other security acquisitions of the former.

Saviynt

Saviynt (Rising Star), has witnessed significant growth, over the past quarters, with its cloud-based identity, and the launch of compliant, healthcare-specific identity solutions. Saviynt is also creating niche capabilities with the launch of Healthcare Identity Cloud, targeting the healthcare industry and associated compliances.

Data Leakage/Loss Prevention (DLP) and Data Security

Who Should Read This

This report is relevant to enterprises across industries in the U.S. or evaluating providers that offer solutions integrating multiple cybersecurity features, addressing security concerns arising from changes in work patterns and increased digitalization.

In this quadrant report, ISG highlights the current market positioning of providers of data leakage/loss prevention (DLP) and data security solution providers that help enterprises in the U.S., and how each provider addresses the key challenges.

The pandemic triggered remote work and accelerated enterprise adoption of cloud services worldwide as executives scrambled to fulfil the new needs of their distributed workforce. Organizations of all sizes are increasingly investing in DLP solutions to secure data and ensure compliance.

Enterprises are using a cloud access security broker (CASB) to avoid data breaches on hosted apps, cloud security posture management (CSPM) solutions for cloud infrastructure and API-driven technologies for office suites such as Microsoft Office 365.

Chief information security officers should read this report to understand how DLP solution providers address the significant challenges of compliance and security while maintaining a seamless experience for enterprise clients.

Chief data officers and data privacy officer should read this report to understand how the providers offer information protection and privacy, information governance, data quality and data lifecycle management.

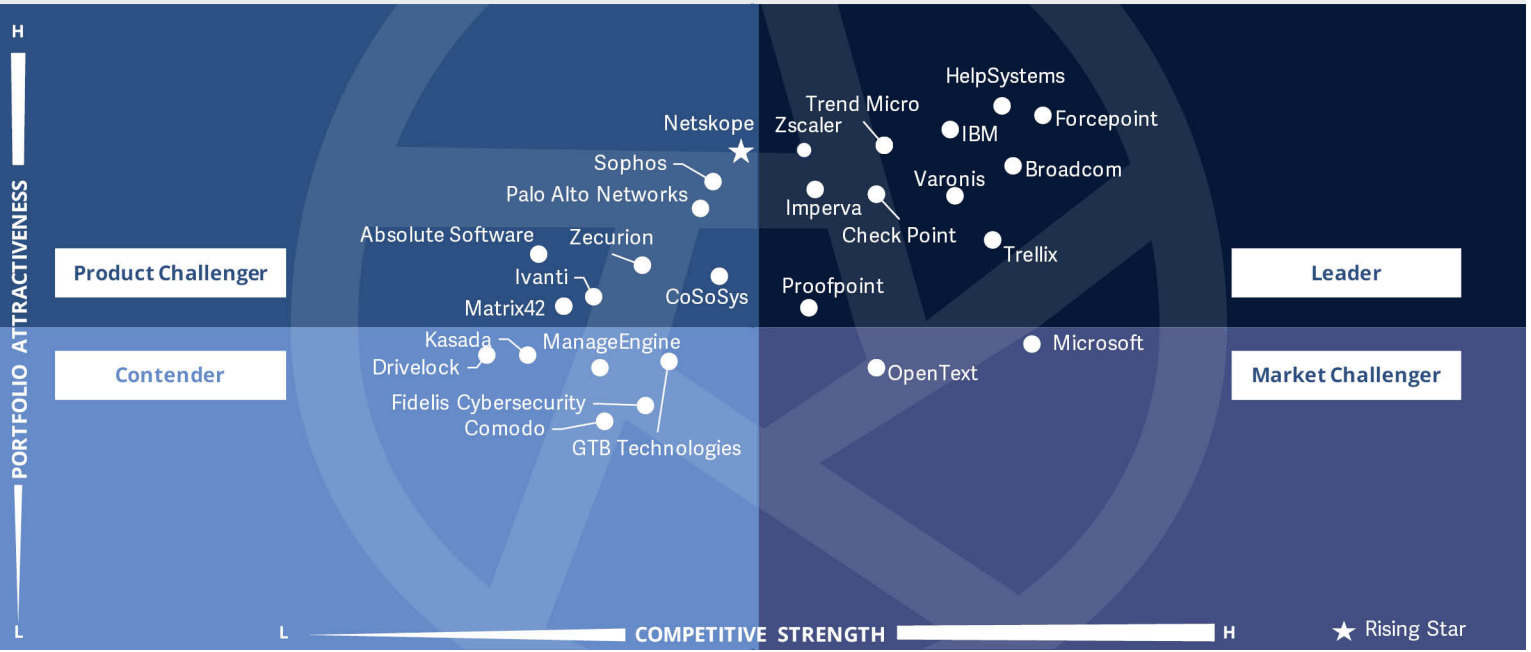
Chief executive officers should read this report to understand the vast potential of solution providers to differentiate themselves by better meeting evolving customer demands.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity - Solutions and Services
Data Leakage/Loss Prevention (DLP) and Data Security

U.S. 2022



This quadrant **assesses vendors with commercially available products and excludes providers with no proprietary software offering**. There has been a reduction of mainstream products as these functionalities are increasingly integrated with other security solutions and platforms.

Gowtham Kumar Sampath

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 proprietary software are not included here. DLP solutions are offerings that 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 capable of providing visibility and control over sensitive data residing in cloud applications, endpoint, network and other devices.

These solutions are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile devices, that are being used to store data is increasing in companies. These are mostly equipped with an internet connection and can send and receive data without passing it through a central internet gateway. Data security solutions protect data from unauthorized access, disclosure or theft.

Eligibility Criteria

1. The DLP offering should be based on **proprietary software** and not on a third-party software.
2. The solution should be capable of supporting DLP across any architecture such as the **cloud, network, storage or endpoint**.
3. The solution should be capable of handling sensitive data protection across structured or unstructured data, text or binary data.
4. The solution should be offered with a basic management support, including, but not limited to, **reporting, policy controls, installation and maintenance and advanced threat detection functionalities**.
5. The solution should be able to **identify sensitive data, enforce policies, monitor traffic** and improve data compliance.

Observations

DLP is a mature market, and is expected to undergo disruptive changes as ISG believes that DLP vendors have not kept pace with advances in technology.

Compared with the 2021 assessment, this year ISG has noted vendors showing a higher inclination toward integrating DLP with endpoints, secure access service edge (SASE) and cloud. Concurrently, ISG has reduced the significance of vendors that have moved away from DLP as an offering to DLP as a function of other technologies.

- DLP has become a functionality that needs to be applied where the data reside. The increased adoption of cloud services, SaaS apps, API-driven services and IoT have necessitated the use of inherent data protection within their environments such as cloud access security broker (CASB), cloud security posture management and other solutions.
- Insider threats have become more complex to handle due to the lack of visibility or intent of insiders – whether malicious, stolen credential or just carelessness. Moreover, remote working models have blurred the lines between insiders accessing data through authorized devices and personal devices. Organizations are yet to place strong policies and controls in communication and collaboration platforms to prevent both intentional and unintended data loss.
- Adaptive and content aware DLP technologies are gaining traction in the market, especially due to challenges arising from differentiating the intent of malicious insiders and external adversaries. DLP solutions incorporating behavioral analytics, data classification engines and content classifiers are preferred over traditional DLP solutions.
- For long, DLP solutions have dealt with outbound traffic, however, sophisticated phishing campaigns and social engineering tactics have changed the DLP landscape. Outbound traffic has become a top priority, especially with the increased usage of SaaS collaboration suites such as OneDrive, Google Drive, Teams and more, to protect against malicious URLs and infected files.

From more than 95 companies assessed for this study, 27 have qualified for this quadrant with 11 being Leaders and 1 a Rising Star.

Broadcom

Broadcom showcases extensive capabilities in identifying threats across different file types. Its pre-built policy templates have helped create a coordinated approach to threat protection, detection and response.

Check Point Software

Check Point Software leverages advanced functionalities from several AI engines that combine behavioral and contextual intelligence to offer layered analysis across different stages of protection.

Forcepoint

Forcepoint's Dynamic Data Protection gathers information from user and data activity, from monitoring and enforcement points across endpoint networks and cloud, allowing it to gain more context from behavior.

Help Systems

Help Systems (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, along with the risk areas. The platform adopts a use case-based-approach toward known data types or user groups.

IBM

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 an enterprise.

Imperva

Imperva's extensive partner ecosystem enable it with an extensive suite of pre-built integrations. The acquisition of CloudVector has enhanced its data protection capabilities.

Proofpoint

Proofpoint's acquisition of Dathena has strengthened its AI-based data classification capabilities to mitigate insider threats by enabling it to identify user intent, context and threat telemetry.

Trellix

Trellix (McAfee) leverages third-party technology partners to help in maximizing intelligence sharing, thus offering a unified management of DLP through a centralized console. The Raw DLP event data is shared with the McAfee Behavioral Analytics platform to detect risky user behavior.

Trend Micro

Trend Micro's Integrated DLP creates contextual awareness using an exhaustive list of identifiers to determine specific data by patterns, formulas, positioning and other metrics. The DLP solutions also provide advanced fingerprinting to secure unstructured data and IP that resides on or off the network.

Varonis

Varonis has invested in creating platform and cloud partnerships that have improved data classification, availability, confidentiality and privacy. It has also enhanced its data classification matching capabilities.

zscaler

Zscaler's 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.

Netskope

Netskope (Rising Star) showcases thousands of built-in data identifiers and data file types, and uses a machine learning-based engine for data classification. Netskope has also invested in major cloud-based partnerships to improve protection for data-in-motion.

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

Who Should Read This

This report is relevant to enterprises across all industries in the U.S. for evaluating providers that offer solutions that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalization.

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

With the proliferation of bring your own device (BYOD) strategies, end point security has become a priority. Endpoint devices are a point of vulnerability, compromising the security of networks. With advanced endpoint security, enterprises can seal off attack points, giving organizations valuable protection.

Endpoint threat detection combines real-time monitoring, automated responses and analytical capabilities to prevent attacks. Technologies such as AI, machine learning, security analytics and real-time threat intelligence go a step further to identify potential or complex threats.

In the U.S., cybersecurity is critical and a top priority at all levels of the government and among private enterprises. The government has enforced regulations to boost the adoption of advanced endpoint security solutions, across sectors, primarily to deal with ransomware.

Chief information security officers should read this report because it presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats, the capabilities needed to combat them, and assists in making the related strategic business decisions.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security service providers in the U.S. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to comprehend the changing security landscape. In addition to setting strategic objectives and adopting security platforms in accordance with their needs.

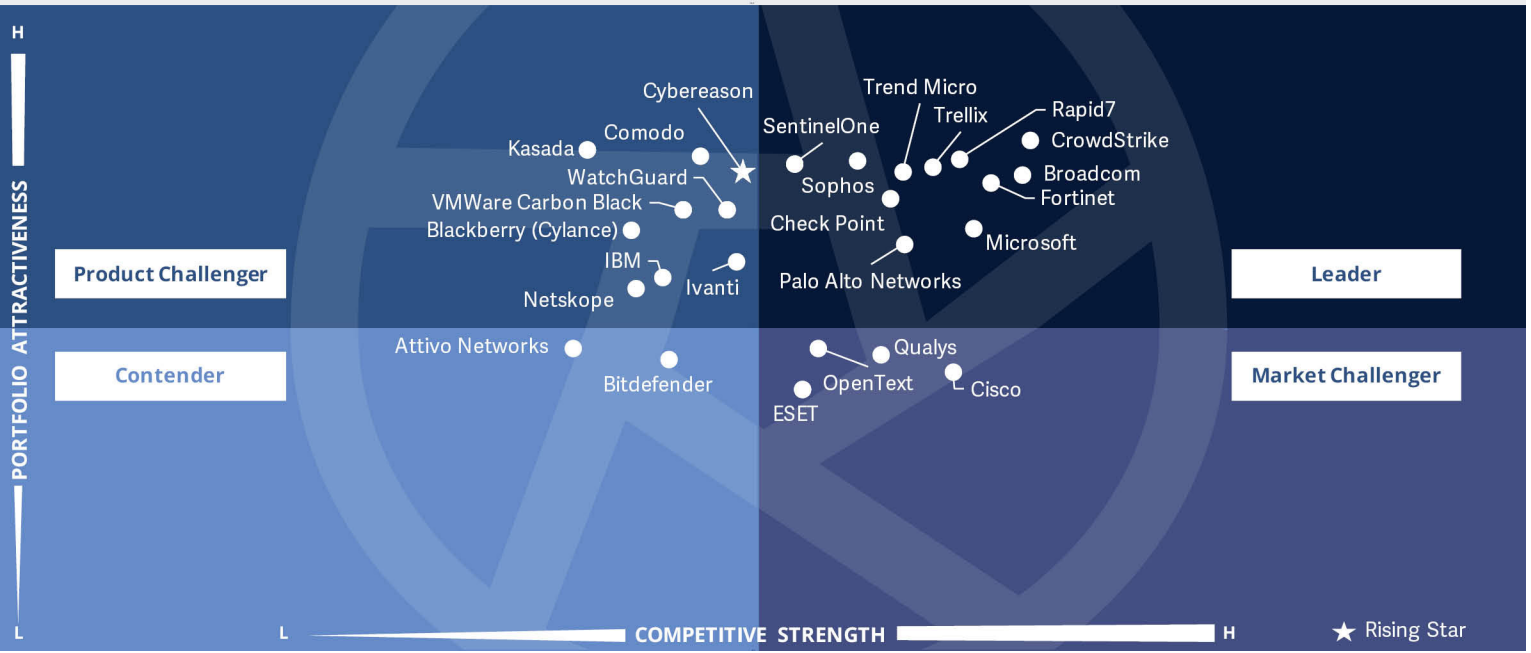
ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity - Solutions and Services

U.S. 2022

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



This quadrant **assesses vendors with commercially available products, excluding providers without proprietary software.** Providers are increasingly relying on behavioral, contextual, AI and machine learning-based intelligence and automation to enhance threat detection, remediation and response capabilities.

Gowtham Kumar Sampath

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

Definition

Advanced ETPDR 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 an advanced ETPDR product (on-premises or cloud based) based on proprietary software are not included here.

This quadrant evaluates providers offering products that can provide continuous monitoring and complete visibility of all endpoints, and can analyze, prevent and respond to advanced threats. Endpoint security solutions that integrate Secure Access Service Edge (SASE) are also included here. In our consideration, endpoint security also includes the corresponding protection of operational technology (OT) solutions.

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

Eligibility Criteria

1. The solution provides comprehensive and **total coverage and visibility of all endpoints** in a network.
2. The solution demonstrates effectiveness in **blocking sophisticated threats such as advanced persistent threats,** ransomware and malware.
3. The solution leverages threat intelligence, analyzes and offers **real-time insights on threats** emanating across endpoints.
4. The solution should include **automated response features** that include, but are not limited to, deleting malicious files, sandboxing, ending suspicious processes, **isolating infected endpoint and blocking suspicious accounts**.

Observations

AETDPR solutions underwent a meteoric growth in the cybersecurity market. Aside from platforms, vendors have also started offering managed services through security operations centers. The market has undergone consolidation with large vendors acquiring niche players to improve functionalities. For example, IBM acquired Reaqta and SentinelOne acquired Attivo Networks. Some of the other developments in this space are:

- Endpoint telemetry gains prominence and is added with other solutions and especially marketed as extended detection and response (XDR) solutions.
- Several vendors have participated in MITRE ATTACK test evaluations to showcase their capabilities and commitment to providing defense against specific advanced persistent threats (APTs) and common behaviors across multiple threat actors. Check Point Software, Rapid7 and SentinelOne took part and showcased their scores to improve visibility for their portfolios.
- Vendors have launched Graph techniques that integrate behavior-based pattern matching with AI and machine learning algorithms to correlate and analyze cybersecurity events and automatically prevent threats in real-time.
- Vendors are leveraging pre-emptive threat identification based on context and content awareness to increase visibility across the threat landscape. AI- and machine learning-based data classification and behavior analysis are used to identify the context and intent of malicious actors to isolate and remediate threats.
- Several vendors are offering a single-pane-of-glass view or a unified platform to analyze and provide centralized control and visibility.
- Vendors are combining human intelligence with machine learning and automation to better drive behavior-based and context-driven threat hunting, detection and response capabilities.

From more than 95 companies assessed for this study, 26 have qualified for this quadrant with 11 being Leaders and one as a Rising Star.

Broadcom

Broadcom provides real-time threat visibility and management options across on-premises, cloud or hybrid infrastructures, using a single agent for attack surface reduction, attack prevention, breach prevention and endpoint detection and response (EDR) with a single console.

Check Point Software

Check Point Software's security teams leverage its security operations center to filter out high volumes of alerts and reduce network blind spots to identify and stop cyberattacks with speed and precision.

CrowdStrike

CrowdStrike's cloud-native and AI-powered platform uses a combination of AI and behavioral pattern-matching techniques to analyze cybersecurity events and prevent threats in real time. Third-party integrations help customers verify users' device posture before granting access to internal or external applications.

Fortinet

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. FortiXDR has capabilities such as automated analytics, incident investigation and predefined responses, offered out of the box.

Microsoft

Microsoft has gained significant ground and mindshare in the market, due to ease of use and advanced capabilities that are offered by its endpoint suite of offerings. Microsoft's vast presence in the market has also enabled it to offer support to legacy products.

Palo Alto Network

Palo Alto Networks' Cortex XDR agent provides a comprehensive prevention stack that leverages AI-based local analysis, using a local machine learning model with data sets from global sources. Cortex XDR Forensics gives customers access to the forensic investigation tool used by the Palo Alto Networks Unit 42 security consulting group.

Rapid7

Rapid7 has been acquiring cloud-based firms such as Alcide.IO (for Kubernetes security) and DivvyCloud (CSPM), to improve its cloud-native security platform and enable continuous management of risk and compliance across cloud environments.

SentinelOne

SentinelOne acquired Attivo Networks, allowing it to extend the Singularity XDR platform's capabilities to mitigate threats across endpoints, cloud workloads, IoT devices, mobile and data. SentinelOne has scored the highest among analytic detections with the MITRE evaluations for three consecutive years.

Sophos

Sophos EDR leverages a deep learning neural network to offer on-demand access to threat intelligence focused on millions of samples to look for threat indicators. Sophos Central's adaptive cybersecurity ecosystem offers a centralized data lake and open APIs for its ecosystem.

Trellix

Trellix (McAfee) identifies attacks and behavior to prevent sophisticated threats, using a broad set of capabilities such as advanced detection, response, proactive and adaptive investigation and real-time threat intelligence. Trellix XDR uses AI-guided threat investigation to rapidly prioritize threats and minimize potential disruption.

Trend Micro

Trend Micro's Apex One™ is a critical component of its endpoint offering, allowing users to add security and investigation capabilities, and offers threat detection, response and investigation within a single agent.

Cybereason (Rising Star) integrates endpoint telemetry with behavioral analytics to detect and end cyberattacks anywhere on enterprise networks across IT environments.

Technical Security Services

Who Should Read This

This report is designed to help companies in the U.S., across industries, evaluate providers that are not exclusively focused on their proprietary products but can implement and integrate other vendors' products or solutions. The report covers integration of IT security products or solutions.

In this quadrant, ISG defines the current market positioning of providers of technical security services, offering implementation and integration services. The report highlights how each provider addresses the key challenges in the U.S. It also evaluates providers' ability to respond to emerging threats, using the latest attack techniques. The solutions offered by providers allow organizations to defend themselves against attacks and respond swiftly to any malicious intent to access and misuse their sensitive data.

The key implementation or integration tasks include secure access service edge (SASE) and zero-trust networks. Considering the post-pandemic volatile security landscape, technical security services are in high demand in the U.S. According to ISG research, the skilled technical workforce and advanced technologies available in the market are additional benefits.

To ensure adoption throughout the organization, enterprises are looking for solutions that integrate with their existing systems. Large enterprises, in particular, have partnerships with large providers that can offer enterprise-wide implementation services.

Chief information security officers should read this report because, with digital transformation at the forefront of businesses today, they need to find a balance between data security, customer experience and privacy. To achieve the same, they need to have a thorough understanding of the leading service providers in the market that assist with integrating IT security services, and they need deep insight about provider capabilities.

Chief strategy officers should read this report to understand the relative positioning and capabilities of service providers and collaborate with them to develop an effective cybersecurity service. This report contains information that can be used to implement a security solution.

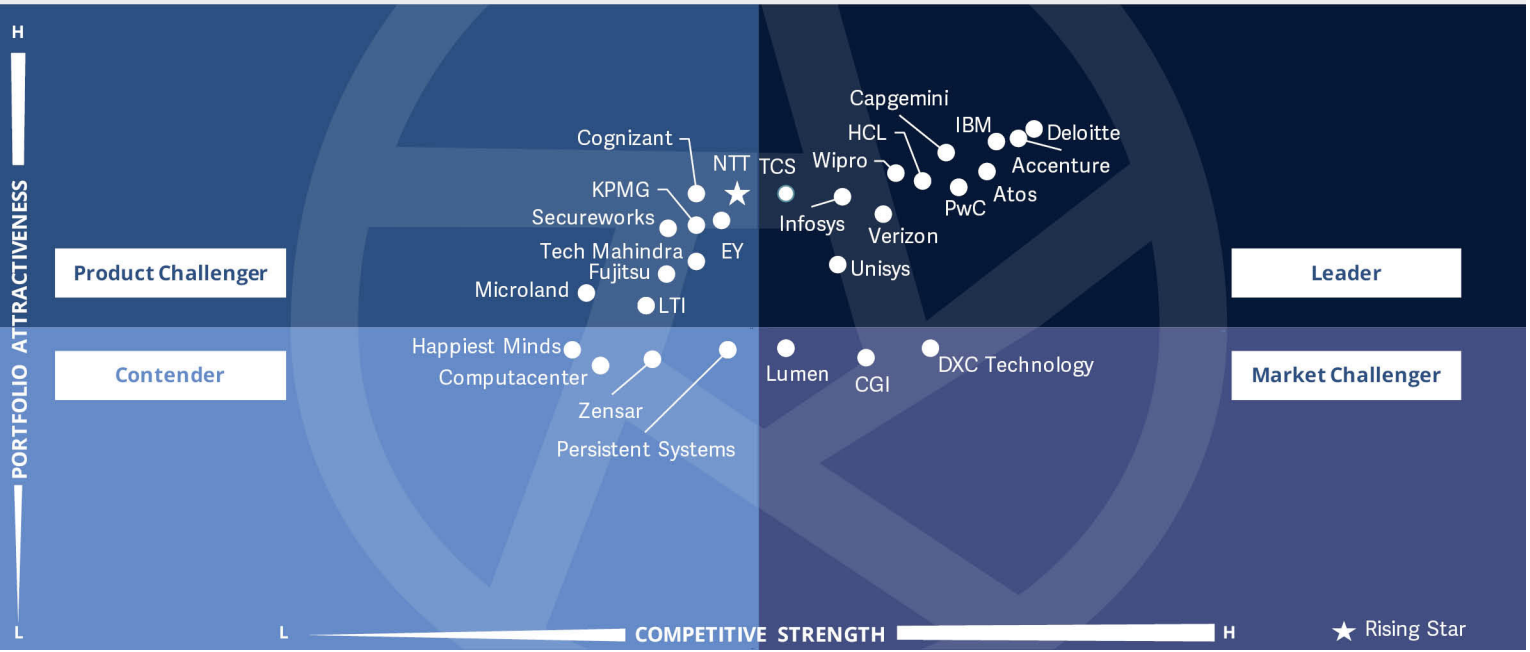
Security analysts should read this report to understand how providers adhere to the security and data protection laws in the U.S., to stay abreast with market trends and to prepare themselves to utilize all available services.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Technical Security Services

Source: ISG RESEARCH

U.S. 2022



This quadrant assesses **providers capable of integrating and implementing partner and technology vendor products and solutions**. These offerings are increasingly becoming a part of strategic and managed services and will lose mainstream focus in the future.

Gowtham Kumar Sampath

Definition

TSS covers integration, maintenance and support for both IT and operational technology (OT) security products or solutions. DevSecOps services are also included here. TSS addresses all security products, including antivirus, cloud and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM), OT security, SASE and others. This quadrant assesses service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate other vendor products or solutions.

Eligibility Criteria

1. Demonstrate experience in **implementing cybersecurity solutions** for companies in the respective country.
2. Authorized by security technology vendors (hardware and software) to **distribute and support security solutions**.
3. Providers should employ **certified experts** (vendor-sponsored, association- and organization-led credentials, government agencies) capable of supporting security technologies.

Observations

Traditional technical security services (TSS) are being increasingly integrated with consulting or managed services – leaving very few pure-play service providers in the market.

Compared with the 2021 assessments, ISG this year has excluded service providers that have already integrated their TSS with other services. Some of the other developments in this space are:

- Service providers are showing high dependency on playbooks and templatized delivery to reduce costs and increase efficiency. Providers are investing on building strong reusable artefacts and other intellectual property.
- Providers are industrializing their TSS offerings to suit the unique requirements of specific verticals such as manufacturing and automotive to enable standardized delivery. Services are also designed to be flexible to accommodate existing technologies and transform to emerging technologies.
- Providers are investing to establish a large ecosystem to showcase a vendor-agnostic approach and best-of-breed capabilities. Providers are fostering a network of partners and alliances to gain access to a wide range of technologies, implementation options and best practices.
- With the increased convergence of IT/OT environments, providers are investing to gain OT capabilities. They are continuously extending IT service management (ITSM) capabilities toward operations technology areas, enabling integration, convergence and standardization of infrastructure and security services.
- Providers are applying automated security controls and tests early in the development cycle; DevSecOps teams can minimize human errors, downtime and vulnerabilities. They are also investing to develop proprietary tools and leveraging third-party security tools to support the development of the integration pipeline.

From more than 95 companies assessed for this study, 28 have qualified for this quadrant with 12 being Leaders and one as a Rising Star.

accenture

Accenture continues its investments to combine human intelligence with applied intelligence and digital technologies to drive intelligent operations. Its services also leverage analytics to collect and analyze the vulnerabilities of more than 71,000 products from over 1,000 vendors. Atos has more than 6,000 cybersecurity specialists and has invested in a large ecosystem of technology partners. Atos also takes part in several working groups and is a thought leader across industry organizations within the cybersecurity community.

Capgemini

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. Capgemini's "Factory design and setup" offers an industrialized factory approach to serve customers in specific industries.

Deloitte

Deloitte's more than 8,600 dedicated cyber risk service practitioners support customization of solution packages for clients based on size, industry and business needs. These services are combined with a function-leading toolset from its partner network and proprietary solutions.

HCL

HCL relies on its large set of skilled experts in multiple security technologies, delivering its transformation and integration services through seasoned subject matter experts placed across the globe. HCL's cybersecurity fusion platform solutions and deep domain knowledge, along with Microsoft's range of security products creates a compelling suite.

IBM

IBM showcases a strong portfolio with its integrated security services aimed at protecting critical assets. It offers quick response and recovery from disruptions and manages the complete threat lifecycle. IBM offers assessment libraries and maturity models that are customized based on client industry, segment and geography.

Infosys

Infosys relies on its comprehensive portfolio that 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

PwC leverages a multidisciplinary team of specialists in the areas of digital technologies, people and organization, business resilience, forensics, financial crime and human-centric design. PwC's deep knowledge across industries helps clients build a robust cybersecurity and privacy program.

TCS

TCS invests heavily in alliances with technology vendors for service development and a go-to-market strategy, and positions them collectively within its service model. TCS' cyber vigilance operations allow for proactive scanning for any security vulnerabilities and responding quickly to data breaches.

Unisys

Unisys uses its understanding of how clients are targeted to create a security architecture to address these areas, with a strong focus on providing an ecosystem of solutions addressing specific threats.

Wipro

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. Wipro optimally combines home-grown intellectual properties and also leverages IP from various strategic partners.

verizon

Verizon 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. Verizon is enhancing offerings in SASE, network security, cloud security and MDR and is developing new offerings to meet customer needs.

NTT

NTT (Rising Star) provides customized offerings to suit the specific needs of enterprises across different industry verticals. Decades experience in handling complex industry challenges and localized expertise creates a compelling offering.

Leader

"PwC shows wide technical capabilities, experience, skillsets and exceptional delivery capabilities."

Gowtham Kumar Sampath

PwC

Overview

PwC is headquartered in London and operates in 156 countries. As a service provider, it has over 295,370 employees across 719 global offices. In FY21 the company generated $45.1 billion in revenue (+4.9 percent YoY), with assurance as its largest segment. Its cybersecurity practice offers security strategy and governance, security architecture, active defense services, security implementation, threat and vulnerability management, risk and compliance, incident management, managed services and IAM.

Strengths

Extensive technical capabilities: PwC has gained deep knowledge across industries, addressing business, technical and regulatory issues to help clients build a robust cybersecurity and privacy program. This program is complemented by strong alliances with cybersecurity and privacy vendors, allowing PwC to build enhanced accelerators that can help maximize ROI on cybersecurity and privacy technologies.

Experienced talent and skillset: PwC's multidisciplinary team of specialists has in-depth expertise in multiple digital technologies, people and organizational areas, and in business resilience, forensics, financial crime and human-centric design. This expertise is complemented by a network of more than 3,300 practitioners, 60 labs and operations centers and domain experts from a global crisis center.

Investments for service enhancement and upskilling: PwC teams have created more than 7,500 assets, included in the digital lab and the Connect suite of collaboration tools. The suite helps 700,000 users to efficiently collaborate and exchange information with clients and audit teams across a network.

Caution

PwC's offerings are attuned to large enterprise needs and are exemplified by revenue contribution. The company should strengthen its focus on SMBs.

Strategic Security Services

Who Should Read This

This report is relevant to enterprises across all industries in the U.S. for evaluating providers offering services that integrate multiple features that address cybersecurity concerns arising from changes in work patterns and increased digitalization.

In this quadrant, ISG focuses on the current market positioning of strategic security service providers that reduce security threats for enterprises in the U.S., and how each provider addresses the key challenges in the market.

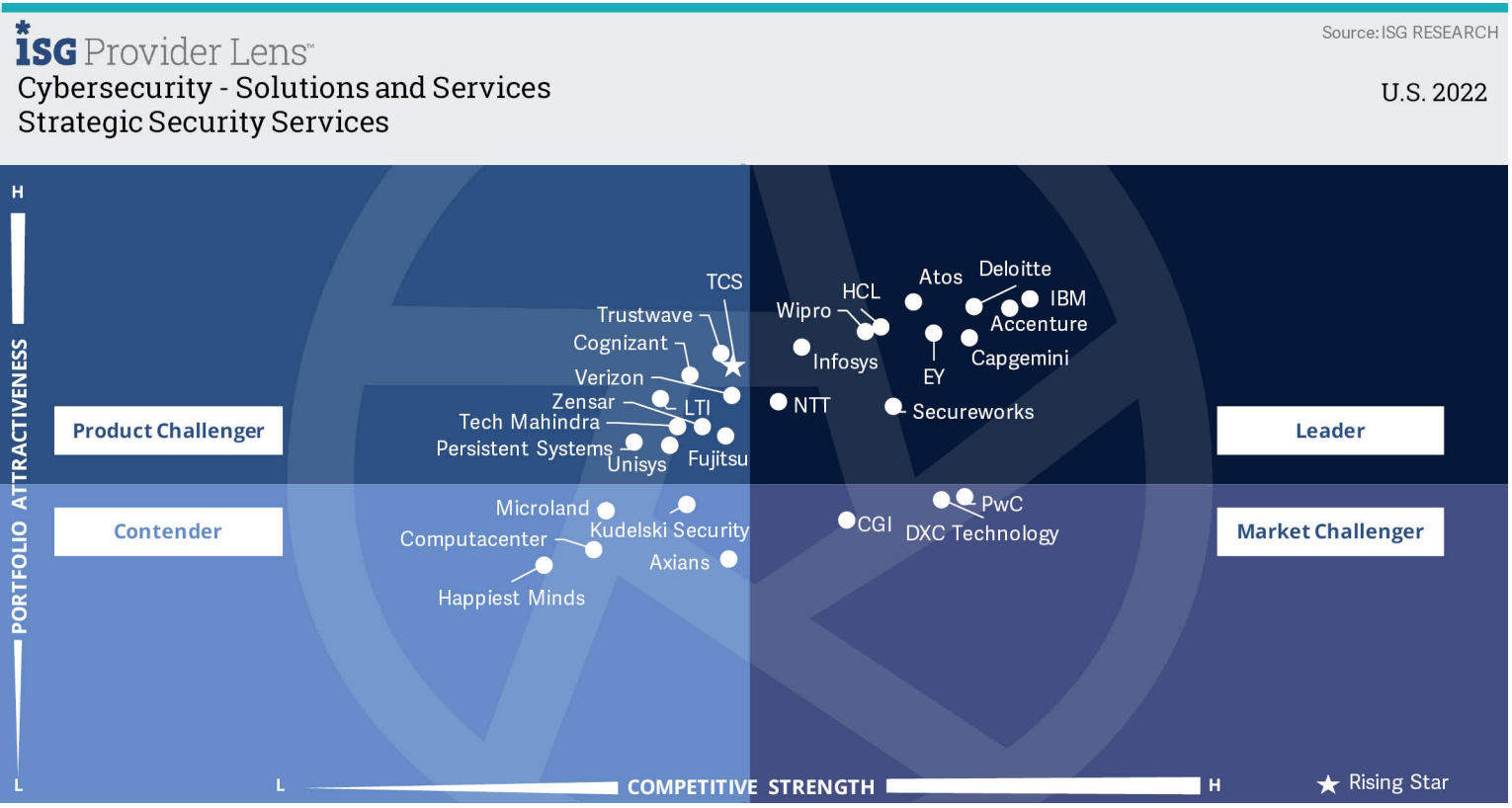
Security issues are taking a toll on enterprises, with the consistent emergence of new threats, requiring the implementation of smarter ways to manage security concerns. Strategic security services help organizations build security programs that are relevant to the needs of their business and have a lasting impact.

Most enterprises seek security services that can prevent attacks rather than simply respond to them. Therefore, strategic security services (SSS) also include audits, assessments, and awareness. U.S. enterprises tend to engage service providers that have a broad base of security capabilities and skilled resources.

Chief information security officers should read this report because it presents a broad view of latest trends in the security landscape. It also provides a comprehensive understanding of immediate threats and the capabilities needed to combat them, and it assists in making strategic business decisions. This report provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.

Chief technology officers should read this report because it highlights the latest trends, enabling CTOs to stay apace with the changing security landscape. In addition to setting strategic objectives and developing security platforms in accordance with marketing needs.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of strategic security service providers in the U.S. It helps the company determine its vision and strategy for security. Also, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.



This quadrant assesses **providers with advisory capabilities that strengthen security posture** across an enterprise attack surface. Providers are relying on frameworks, maturity assessments for implementing zero trust, SASE and supply chain security, and the convergence of IT and OT.

Gowtham Kumar Sampath

Definition

Strategic security services (SSS) primarily cover consulting for IT and OT security. Services covered in this quadrant include security audits, compliance and risk advisory services, security assessments, security solution architecture consulting and awareness and training. These services are used to assess security maturity and risk posture and define cybersecurity strategy for enterprises (tailored to specific requirements). This quadrant examines service providers that are not exclusively focused on proprietary products or solutions. The services analyzed here cover all security technologies, especially OT security and SASE.

Eligibility Criteria

1. Service providers should demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, architecture consulting and risk advisory.**
2. Service providers should offer at least one of the above services in the respective country.
3. Execution of security consulting services using **frameworks** will be an advantage.
4. No exclusive focus on proprietary products or solutions.

Observations

Advisory and consulting offerings continue to remain as the entry and foundational phase of most engagements in the cybersecurity market. Accelerated digital transformation and compliance initiatives have especially necessitated the need to employ strategic partners with cybersecurity experience to navigate the technology, infrastructure and process challenges to establish a robust and secure business environment. Some of the other developments in this space are:

Transformational advisory: SSS have generated significant demand in the backdrop of enterprise IT transformation initiatives. Many enterprises are struggling with their existing security infrastructure due to the vast number of tools, solutions and systems put in place to address ad-hoc and siloed challenges.

Demand for next-generation technologies: In addition to typical advisory services, providers are witnessing demand for their offerings that address areas such as cloud security, IAM, SASE, zero trust and IT/OT security. Other issues, including supply chain security and user training, also are undergoing growth in the enterprise market.

Strategic CISO-level services: Providers are gaining traction for their virtual chief information security officer (vCISO) services, specifically for addressing the gap and enabling the connect between security posture and business operations. Providers are also developing standardized training such as tabletop and cyber crisis exercises with red/blue/purple teaming, threat management, incident response and other services.

IP-led frameworks, solutions and delivery: Service providers are also relying on creating exceptional frameworks that include a clear strategy and roadmap for assessment, design, deployment and management.

From more than 95 companies assessed for this study, 29 have qualified for this quadrant with 11 being Leaders and one as a Rising Star.

accenture

Accenture's competitive advantage stems from its significant technical expertise and extensive technology network of partners, academia and external security researchers, combined with dedicated internal cyber security resources.

Atos

Atos has made multiple consulting-based acquisitions, including that of Fidem and SEC Consult Group, specifically to enhance its advisory portfolio, offering vertical-specific capabilities, and to address cyber resilience efforts among enterprises.

Capgemini

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

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.

EY's

EY's consulting portfolio is complemented by its next-generation security operations and response services that help enterprises build a transformation strategy and roadmap to implement 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

IBM's security intelligence operations and consulting services are aimed at helping clients to develop maturity in intelligence-driven operations across their IT environments.

Infosys leverages technologies that are enhanced with proprietary content, gained from vast research and rich experience obtained through use cases, playbooks, standard operating procedures (SOPs), security metrics and architecture.

NTT

NTT relies on powerful risk management capability, 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

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 hyperscalers such as AWS and Microsoft (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 more than 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.

Market Challenger

"PwC's multifaceted team of experts, extensive knowledge and partnerships create a compelling service."

Gowtham Kumar Sampath

PwC

Overview

PwC is headquartered in London and operates in 156 countries. As a service provider, it has over 295,370 employees across 719 global offices. In FY21, the company generated $45.1 billion in revenue (+4.9 percent YoY), with assurance as its largest segment. Its cybersecurity practice offers security strategy and governance, security architecture, active defense services, security implementation, threat and vulnerability management, risk and compliance, incident management, managed services and IAM.

Strengths

Focus on cyber resilience: PwC's Cyber Risk Assessment offerings create a snapshot of the effectiveness of current cybersecurity measures and preparedness in managing cyber risks across several dimensions. Its cyber capability library helps in visualizing a security posture and in identifying hidden gaps to be investigated and mitigated.

Insights from simulated platform: PwC's Cyber Security Simulation platform provides a hyper realistic, controlled environment to mirror real-world networks, security technologies and cyberattacks. These help in assessing, auditing and in augmenting existing security capabilities to better detect, protect and respond to threats.

Recognized thought leadership: PwC is recognized for its actionable insights, publications and annual survey based reports. It also has deep knowledge of business, technical and regulatory dynamics to provide multifaceted solutions, designed to meet unique requirements. PwC's CISO Support as a Service is designed to enable enterprise CISOs develop and implement programs to enhance cybersecurity strategies.

Caution

PwC's cybersecurity advisory and strategic capabilities in the U.S. are overshadowed by its overall risk and technology consulting offerings. The company should focus on improving its portfolio and on showcasing its recent references and use cases from a cybersecurity perspective.

Managed Security Services - Large Accounts

Who Should Read This

This report is relevant to enterprises across industries in the U.S. for evaluating providers offering services that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalization.

In this quadrant, ISG focuses on the current market positioning of managed security service providers that help mitigate security threats for enterprises in the U.S., and how each provider addresses the key challenges in the market.

Security issues are taking a toll on enterprises, with the continuous emergence of new threats, requiring smarter ways to manage security concerns. Enterprises are currently leveraging the latest developments in security to drive efficiency, while intercepting all risks.

The managed security services market in the U.S. is driven by the growing adoption of secure access service edge (SASE) and zero-trust access to protect data and control access to information. Over the last year, the demand for cloud security, data security, and IoT/OT security have increased among enterprises in an effort to respond immediately to security threats.

Chief information security officers should read this report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of the immediate threats and the security capabilities needed to combat them, and it assists in taking strategic business decisions to address the current security concerns. This report provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.

Chief technology officers should read this report because it highlights the latest trends to enable CTOs to stay apace with the changing security landscape. In addition to setting strategic objectives and adopting security platforms in accordance with their needs.

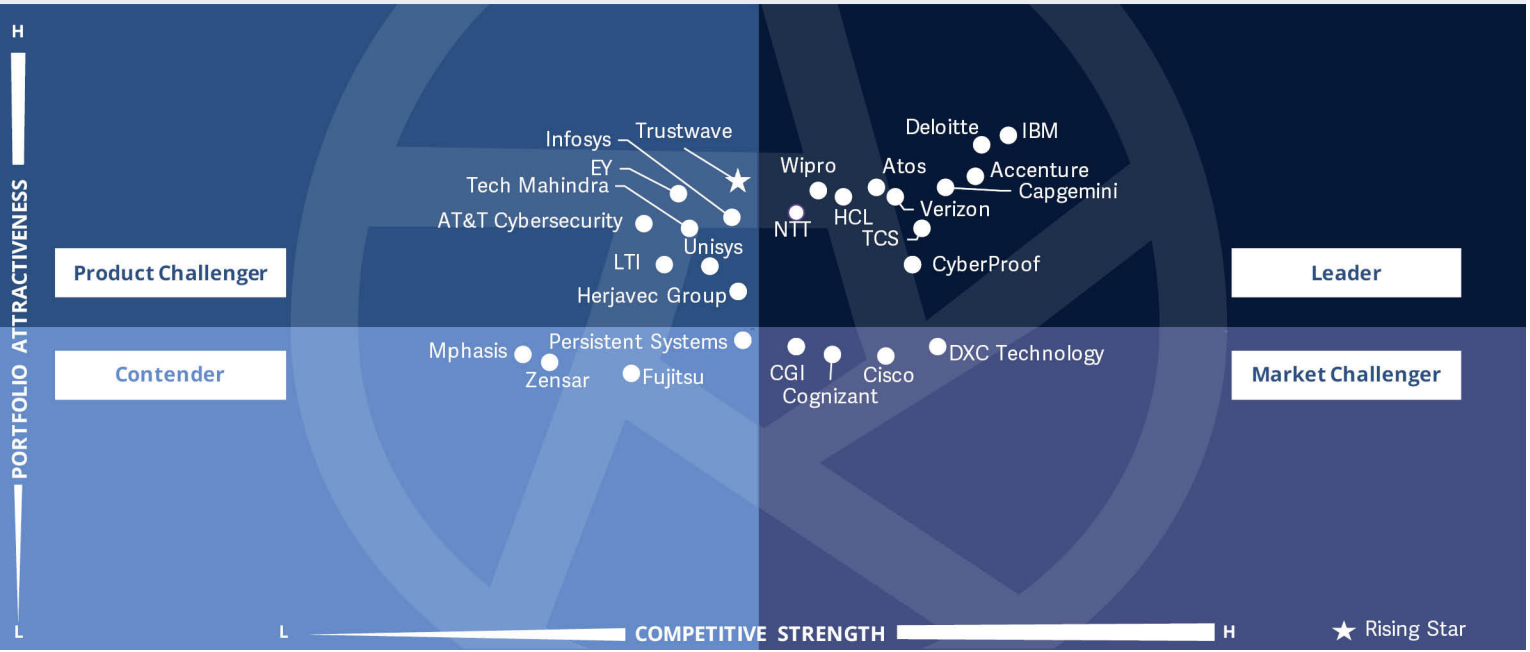
Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security services providers in the U.S It helps a company determine its vision and strategy for security. Additionally, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.

ISG Provider Lens™

Cybersecurity - Solutions and Services
Managed Security Services - Large Accounts

Source: ISG RESEARCH

U.S. 2022



This quadrant **assesses managed security providers, where more than 40 percent revenue is generated from large enterprises.** Key areas of focus include cloud security, intelligent security operations centers, managed detection and response (MDR), and investigative cyber analytics.

Gowtham Kumar Sampath

Definition

Managed security services comprises the operations and management of IT and OT security infrastructures for one or several customers by a security operations center. This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.

Eligibility Criteria

1. Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, anti-virus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations and all other operating services to provide **ongoing, real-time protection, without compromising business performance**. In particular, Secure Access Service Edge (SASE) is also included.
2. Ability 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.
3. Possesses **accreditations** from vendors of security tools.
4. SOCs ideally owned and managed by the provider and not predominantly by partners.
5. Maintains certified staff, for example, in **Certified Information** Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

Observations

Managed security services (MSS) continue to grow in demand and has matured as a delivery model, but there continues to room for the adoption of technology and service capabilities.

Compared with 2021, ISG, for this quadrant, has excluded providers that have less than 40 percent revenue contributed by large enterprises (more than $5 billion in revenue). Some of the other developments in this space are:

- **Growth of MDR and XDR:** Most providers have integrated their offerings with managed detection and response (MDR) and extended detection and response (XDR) services and partnering with MDR platform providers. These offerings include advanced technologies such as AI, machine learning and behavior analytics for enabling proactive security monitoring, alarm validation, security orchestration and automation.
- **Innovative and sophisticated offerings:** As remote working has become the new normal, MSS focus on helping clients with governance, risk and compliance (GRC); next-gen identity and access controls, remote access, threat management and endpoint protection.
- **Demand for skills and talent:** One of the key factors impacting the MSS market is the lack of talented specialists that are capable of managing the current challenging requirements. Enterprises and providers realize that technology alone might not solve the problem; they require human-led expertise to address sophisticated threats.
- **Intelligence-led cyber centers:** Providers are investing in innovating their cyber centers or defense centers with superior and next-generation capabilities in threat intelligence, adversary simulations, incident response services and behavior analytics.

From more than 95 companies assessed for this study, 27 have qualified for this quadrant with 11 being Leaders and one as a Rising Star.

accenture

Accenture has a 7,000-member strong cybersecurity team that applies strategy and transformational processes to client engagements. It is complemented by a network of global fusion and operation centers specializing in more than a dozen industry verticals.

Atos

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

Capgemini's global network of Cyber Defense Centers (CDCs) provides advanced, analytics-driven security information event management (SIEM) services that combine incident detection and response and monitoring. Capgemini has developed a highly automated and scalable global cyber insurance offer to bolster trust and security.

CyberProof

CyberProof approaches its client by way of use cases that aims to identify and map business risks against the most likely attack scenarios. These gaps improve detection and response capabilities against the MITRE ATT&CK matrix.

Deloitte

Deloitte is heavily focused on MDR 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 a cyber data lake.

HCL

HCL takes a structured approach to its key offerings that includes 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 operation.

IBM

IBM has invested in a new advisory and managed services offering, Cloud Native Security Services, aimed at reducing the risk of cloud misconfiguration and offering insights into potential threats. IBM's managed security offerings are based on the QRadar platform and backed by hundreds of security experts.

NTT

NTT has integrated a zero-trust framework into its consulting services. extending it to integration and managed services. NTT's threat intelligence, machine learning, advanced analytics and threat behavior modelling detect both known and unknown threats that manage to evade standard detection techniques.

TCS

TCS leverages its more than 12 threat management centers and over 200 security operations centers, most of which are client specific. It has invested in developing platforms for most of the managed security services that can integrate with existing technology stacks.

verizon

Verizon's advanced SOC solutions are fully customizable cyber security event-monitoring offerings designed for enterprises to maximize their SIEM and related security investments. Verizon enables its customers to monitor and manage all IT assets via a single interface and dashboard.

Wipro leverages its security operations centers with a 24/7/365 service delivery window to analyze system-prioritized alerts in near real time. Its managed security services business caters to customer needs, spanning intelligence, protection, detection, remediation, response and recovery.

Trustwave

Trustwave's (Rising Star) experts and security operations centers provide a combination of automated analysis by a cloud engine with human analysis for advanced threat triage, threat hunting, reverse engineering and other activities. The investment in SpiderLabs helps in gathering and utilizing global threat intelligence.

Managed Security Services - Midmarket

Who Should Read This

This report is relevant to enterprises across industries in the U.S. for evaluating providers offering services that integrate multiple features that address security concerns arising from changes in work patterns and increased digitalization.

In this quadrant, ISG focuses on the current market positioning of managed security service providers that help combat security threats for midmarket enterprises in the U.S., and how each provider addresses the key challenges in the market.

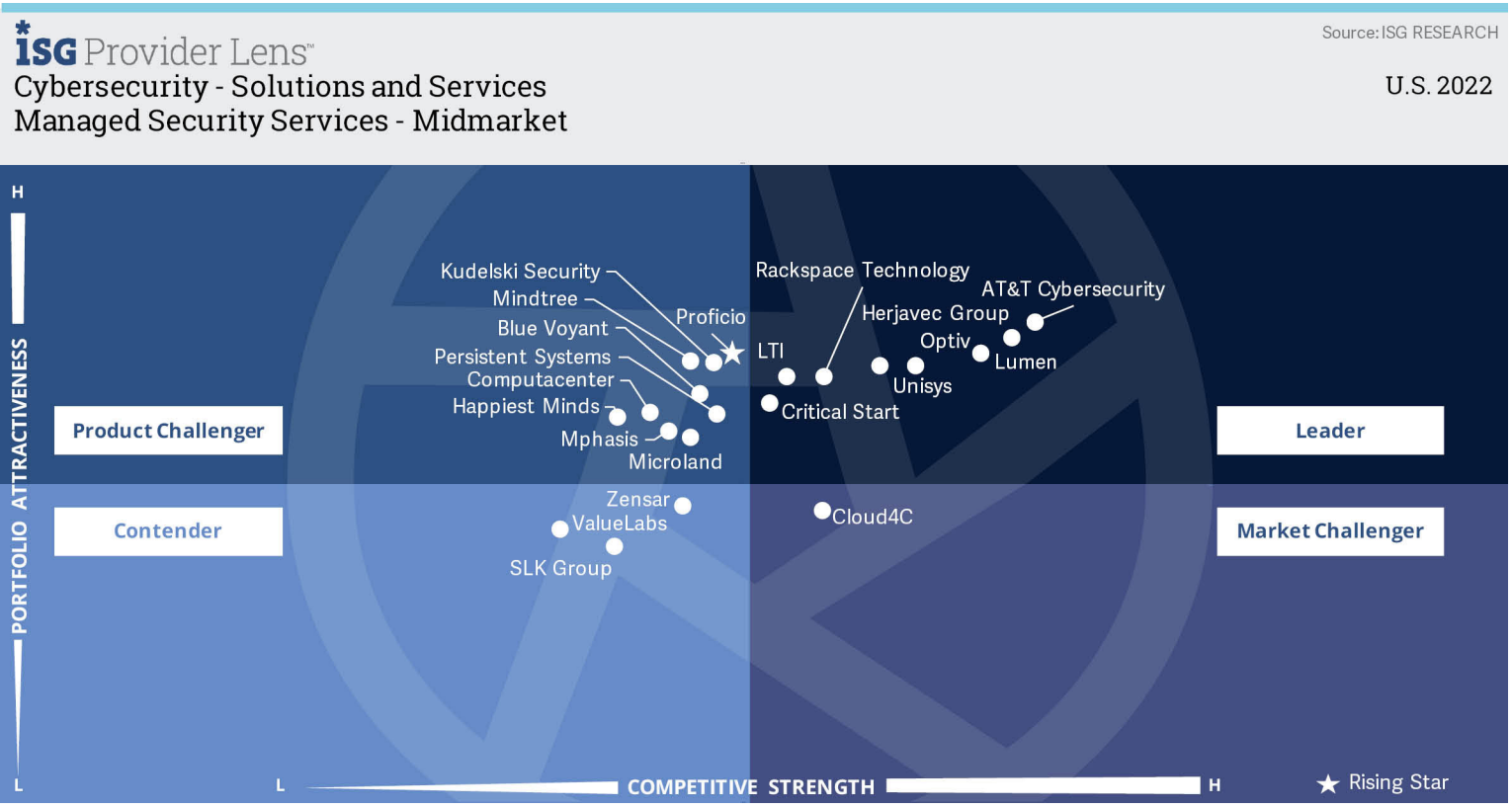
Unlike a few years ago, midmarket companies are increasingly taking measures to adapt and respond to cyberattacks because these security threats are more debilitating for them. Phishing and malware attacks were the primary attacks before the pandemic. In the last two years, with the acceleration of digital transformation, midsize companies are unable to protect themselves with their existing resources, budgets and expertise.

Midmarket companies are seeking security services that can deal with these attacks at low costs and provide real-time protection without compromising on business performance. Over the last year, enterprises have increased their demands for cloud security, data security and IoT/OT security to respond immediately to threats.

Chief information security officers should read this report because it presents a broad view of the latest trends in the security landscape. Also, it provides a comprehensive understanding of the immediate threats and the security capabilities needed to combat them, and it assists in taking strategic business decisions to address the current security concerns. This report provides valuable insights on enhancing productivity and reducing complexity in enterprise security operations.

Chief technology officers should read this report because it highlights the latest trends to enable CTOs to stay apace with the changing security landscape. In addition, it helps them in setting strategic objectives and adopting security platforms in accordance with their needs.

Chief strategy officers should read this report because it examines the relative positioning and capabilities of managed security services providers in the U.S. It helps a company determine its vision and strategy for security. Additionally, it supports decision-making on collaborations, partnerships and cost-reduction initiatives.



This quadrant **assesses providers offering managed security, where more than 40 percent of revenue is from the midmarket** enterprises. Key areas of focus include cloud security, intelligent SOCs, MDR, proactive threat hunting and deep investigative cyber analytics.

Gowtham Kumar Sampath

Definition

MSS comprises the operations and management of IT and OT security infrastructures for one or several customers by a security operations center (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle, starting from identification to resolution.

Eligibility Criteria

1. Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing, firewall operations, antivirus operations, identity and access management (IAM) operation services, data leakage/loss prevention (DLP) operations and all other operating services to provide **ongoing, real-time protection, without compromising business performance.** In particular, Secure Access Service Edge (SASE) is also included.
2. Ability 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.
3. Possesses **accreditations** from vendors of security tools.
4. SOCs ideally owned and managed by the provider and not predominantly by partners.
5. Maintains **certified staff,** for example, in Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

Observations

The demand for managed security services (MSS) for the midmarket have been growing significantly with the launch of managed detection and response (MDR) offerings, designed specifically to address the skillset challenges of SMEs.

Compared with 2021, ISG, for this quadrant analysis, has excluded providers that offer MDR services for their respective proprietary platforms. Moreover, ISG has excluded providers that have less than 40 percent of revenue from midmarket enterprises (less than $5 billion revenue). Some of the other developments in this space are:

- **Growth of MDR and XDR:** Most providers have integrated their offerings with MDR and XDR services and are partnering with MDR platform providers. These offerings include the use of advanced technologies such as AI, machine learning and behavior analytics; enabling proactive security monitoring; alarm validation; security orchestration; and automation.
- **Innovative and sophisticated offerings:** ISG's managed security services study focuses on services helping clients with governance, risk and compliance (GRC), next-gen identity and access controls, remote access, threat management and endpoint protection.
- **Demand for skillset and talent:** One of the key factors impacting the MSS market is the lack of talent with the capability to manage the current challenges of the business environment. Enterprises and providers realize that technology alone might not solve the problem; they require human-led expertise to address advanced threats.
- **Intelligence-led cyber centers:** Providers are investing on innovating their cyber centers or defense centers that offer advanced and next-generation capabilities in threat intelligence, adversary simulations, incident response services and behavior analytics.

From more than 95 companies assessed for this study, 21 have qualified for this quadrant with eight being Leaders and one as a Rising Star.

AT&T Cybersecurity

AT&T Cybersecurity leverages its rich ecosystem of cybersecurity technologies and strategic alliances to offer global insights and threat intelligence with eight security operations centers worldwide. Its Alien Labs™ delivers tactical threat intelligence, enabling resilient threat detection and response.

Critical Start

Critical Start's proprietary platform and third-party feeds define and develop new detection methods. This also helps in implementing new techniques and on improving threat research and intelligence platform.

Herjavec Group

Herjavec Group derives its strength from combining aspects of technology such as AI and automation, with intelligence to build its managed security offering and enhance IT security monitoring, incident detection and incident response times.

LTI
Let's Solve

LTI relies on a comprehensive managed security services portfolio that is designed with a cyber security framework to cover cyber threat defense, advanced threat and vulnerability management, identity governance and digital security.

LUMEN

Lumen Technologies' investment in its labs and a strong partner ecosystem enable it to offer enhanced intelligence that feeds into the AI-powered adaptive platform, resulting in advanced capabilities for threat detection and response. Lumen helps security specialists quickly neutralize threats before they attack.

Optiv

Optiv takes a consulting and advisory approach to its managed services, delivering strong capabilities with a comprehensive portfolio that identifies vulnerabilities and ensures a suitable threat response. Optiv's Advanced Fusion Center Operations leverage smart automation and data fusion to upgrade SOC maturity.

Rackspace Technology

Rackspace Technology leverages its inhouse R&D and proprietary security architecture with decades of experience in handling data center infrastructure to create a robust and integrated offering. Security platforms are integrated into management tools to give customers one view of their organization's vulnerability and threats.

Unisys

Unisys leverages its network of global delivery centers to provide flexible support based on client needs. It also delivers a methodology based on IT infrastructure library (ITIL), with annual ISO and SSAE audits, helping clients meet compliance requirements.

PROFICIO

Proficio, the Rising Star, offers MSS that cater to client needs, spanning intelligence, protection, detection, remediation, response and recovery. It offers integrated, automated and comprehensive capabilities to improve visibility into a client's entire data center and cloud environment.

Appendix

Methodology & Team

The ISG Provider Lens™ 2022 – Cybersecurity – Solutions & Services research study 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.

Lead Author:
Gowtham Kumar Sampath

Editors:
John Burnell, Ipshita Sengupta

Research Analyst:
Monica K

Data Analyst:
Rajesh Chillappagari

Consultant Advisor:
Doug Saylors

Project Manager:
Ridam Bhattacharjee

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 June 2022, 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 study was divided into the following steps:

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

Author

Gowtham Kumar Sampath
Principal Analyst

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/ Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years 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 thought leadership research, whitepapers, 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.

Research Analyst

Monica K
Research Specialist

Monica K is a research specialist and a digital expert at ISG. She supports and co-authoring Provider Lens™ studies on the Internet of Things (IoT), Digital Business Transformation, Blockchain, Enterprise Application as a Service, and Cybersecurity. She has created content for the aforementioned Provider Lens™ studies, as well as content from an enterprise perspective, and she is the author of the global summary report. Monica K brings over 8 years of experience and expertise in technology, business, and market research for ISG clients. Prior to ISG, Monica worked for a research firm specializing in technologies such as IoT and product engineering, as well as vendor profiling and talent intelligence. She has also been in charge of delivering end-to-end research projects and collaborating with internal stakeholders on various consulting projects.

IPL Product Owner

Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

ISG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens research, please visit this webpage.

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 +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the 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.

ISG Provider Lens™

JULY 2022

REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES