ISG Provider Lens™

Cyber Security - Solutions & Services

Technical Security Services

U.S. 2020

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

HCL

August 2020

About this Report

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

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of August 2020 for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The lead authors for this report are David Wilkinson and Karen Antons. The editor is Ambrosia Sabrina and Ipshita Sengupta. The research analyst is Monica K and the data analyst is Kankaiah Yasareni.

ISG Provider Lens™

ISG Provider Lens™

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

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

ISG Research™

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

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

EXECUTIVE SUMMARY

General Trends

Most business processes, which involve storing, processing and communicating information including valuable assets, personal information and corporate intellectual property (IP), have gone digital. With the growing frequency and sophistication of cyberattacks on enterprise infrastructures, security has become a crucial need for all firms. For public companies, the board directors must now be educated or trained in cyber security as they are now instrumental in the cyber risk management process. Cyber security continues to be a challenge due to several factors such as new regulatory requirements, stricter penalties for non-compliance, migration of many business components to the cloud, new application development, and merger and acquisition activities (M&A). Consequently, it now involves hardened security controls such as data encryption, multifactor authentication (MFA), arduous breach notification protocols, and the active use of data loss/leakage prevention (DLP) tools.

The confidentiality, integrity and availability (CIA) of data remain central to cyber security. Data protection has become increasingly important. Security control suites such as access to data and egress monitoring are both included in this report as identity and access management (IAM) and DLP respectively. Other security measures such as the effective encryption of all personal data at rest (DAR) are equally important. Three types of security service offerings are increasing in importance to enterprises pursuing the principles of CIA.

These are strategic security services, technical security services and managed security services. Strategic security services cover security assessment, gap analysis, security strategy development, mitigative selection, procurement support and the risk-based allocation of resources. Technical security services include deployment, setup and maintenance for procured security tooling. Managed security services represent a solution for the partial or complete outsourcing of security as a service. All three are growing practice areas as security continues to converge and software providers partner with service providers to broaden their access to the market. Providers of all three of these service types are evaluated in this report, and each type of security service has its own leadership quadrant.

From an organizational perspective, a combination of regulatory requirements and best practices has led to the creation of new executive positions such as CISO, chief risk officer (CRO) and chief compliance officer (CCO). Enterprise risk management (ERM) has emerged, integrating many corporate risk functions and providing a two-way communication channel to the board of directors via a governing risk committee. Cyber security and risk management are becoming increasingly integrated as a result. Revised security and risk management frameworks together with regulatory practices push enterprises to become more proactive in their security processes rather than simply relying on perimeter defense. This drives the need for better monitoring of suspicious cyber activity through

internal and external sources of intelligence. Machine learning (ML) and artificial intelligence (AI) are enabling better analytic processes to prioritize and alert enterprise security officers of potentially dangerous events. High-priority alerts need to be acted on quickly and effectively. As a result, critical event response teams (CERTs), automated escalation protocols and technical response teams have emerged to undertake the mitigation, containment and recovery from damaging events and potential attacks. In essence, digital security has evolved to become cyber risk management and resiliency as some degree of attacks and data loss is expected. Also, from an organizational perspective, the selection of a security solution provider is expected be a more rigorous procedure involving a broader range of influencers due to the risk management aspect discussed above.

The cyber security industry has been estimated to be worth $125 billion. Overall, it was growing around 8 percent per year until the rise of the COVID-19 pandemic and is now forecast to grow 2 to 3 percent in 2020. However, the different security domains within the overall industry are growing at different rates. Cloud services are forecast to grow closer to 30 percent in 2020, and IAM, DLP and security services are estimated to grow slightly faster than the larger security industry, thus raising their relative importance as part of an overall cyber security solution. It is anticipated that managed service providers will continue to take market share from legacy on-premise security service providers in the future as security solutions become more complicated and challenging to self-implement and third-party cloud-based solutions become increasingly cost effective. Technical partnerships between the two types of providers have enabled this.

The recent pandemic has led to a significant increase in the number of people working from home. This has put further pressure on enterprises to ensure that PC and mobile device endpoints as well as local (routers) and IoT connectivity are secure. Work-from-home (WFH) security practices also need to be integrated with screen locking, access protection (such as multi-factor authentication/MFA) and physical security (cable locks, locked filing cabinet for storage, etc.). In the event of loss or theft, hard drive encryption can provide additional security along with the data owner's ability to remotely wipe sensitive data and applications on devices. It is likely that the proportion of employees connecting to enterprise systems remotely will remain at a higher level even after the pandemic has passed, and these additional security controls and compliance with WFH policies will prevail.

IAM Software Market Trends

Enterprise IT systems are transforming rapidly to adapt to the growing threat and regulatory environments. The evolution of cyberattacks has had a significant impact on IAM providers and their customers. Legacy IT systems relied on in-house, on-premise software solutions such as lightweight directory access protocol (LDAP) and Microsoft AD. Many enterprises still have these systems today. The migration of services to the cloud has elevated the need for a different approach to IAM. With the rapid increase in external cyberattacks and internal threats (intentional and unintentional), the need for reliable, user-friendly IAM has grown to an unprecedented, new level. This has been fueled by newer, more restrictive privacy regulations such as CCPA, DFS 23 NYCRR 500 and GDPR, with

new and additional requirements and substantially higher fines in the event of breaches. These factors have driven the IAM market to continue evolving in both the product feature portfolio and the go-to-market strategies of service providers.

IAM is comprised of two functionally differentiated areas: identity governance and administration (IGA) and access control (AC). IGA is concerned with who has access to what and is primarily focused on governance and risk management. AC is primarily concerned with identity authentication and access provision, subject to the access rules and constraints of IGA. AC also controls what authorized users can do with data in the system. The two functional areas typically have different vendors providing solutions, though there are a few such as IBM that offer leading solutions in both areas. The frontrunners in each specialization are not necessarily the same as those vendors offering a strong combined functionality of both IGA and AC.

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

As a result, many established providers are witnessing a rapid growth of cloud-native IAM products at a competitive pricing through an as-a-service business model.

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

MFA is a legal requirement in some jurisdictions and is a best practice in IAM. Two factor authentication (2FA) is generally the default method where MFA is required. Customer IAM (CIAM) is also a growing trend, primarily driven by compliance requirements. Social authentication, which involves an end user signing in through Google, LinkedIn, or another social network ID, is typically not used for authentication into corporate environments.

Competitive positioning is changing significantly along with changes to IAM features being offered. It is likely that this will continue along both fronts into the foreseeable future. Legacy IAM software providers are adding cloud-based services or partnering with managed service providers to be a part of a cloud-based solution. IAM is converging and integrating with other security tools areas such as data protection and data encryption to present as a single, complete solution. Managed security service providers are the vehicles by which much of this is taking place.

In the future, IAM will be different than it is today. Managed service providers (MSPs) will increase their share in the IAM market. More authentication features, such as three-factor and even four-factor authentication, will become commonplace for some use cases. It is early to say whether multi-tenant IAM will prevail as a service, but some providers believe it will. By enabling scalable multi-tenant, cloud-hosted IDaaS, they envision becoming global providers of identity services that would allow everyone to have a single digital identity rather than multiple ones for different enterprise platforms and systems. Blockchain IAM is also being tested by some providers, but there are not yet any identified systems in production that have been identified. For these reasons, IAM has emerged as a highly dynamic security solution both now and for the foreseeable future.

DLP Software Market Trends

Enterprise IT systems, together with today's threat and regulatory environments, are undergoing rapid change. DLP providers are being forced to respond quickly to keep up. These combined changes have significant consequences for almost all enterprise information security programs. With the increasing threats from both external cyberattacks and internal threats (intentional and unintentional), the need for reliable, user-friendly DLP is gaining importance. New privacy regulations such as the California Consumer Privacy Act (CCPA) and others, are much more restrictive than in the past and come with substantially higher fines for non-compliance in the event of breaches. This has ensured DLP a place at the top of the list in data protection. DLP has become a required security control, according to some regulations and regulatory bodies. DLP is also an essential component of security frameworks (ISO, NIST, COBIT, etc.) and an important input to user and entity behavioral analysis (UEBA). Consequently, most enterprises consider DLP an essential element to their data protection programs. The DLP market not only continues to change from a product feature perspective but also in the way the protective solution is being acquired by customers and, therefore, the go-to-market strategies pursued by DLP providers.

The delivery landscape for DLP cloud computing is also changing. Firstly, many DLP providers must continue to offer solutions for legacy, on-premise systems. Secondly and simultaneously, they need to provide a separate solution for applications and services provided through the cloud. In some cases, this means a cloud-based DLP service or the use of cloud access security brokers (CASBs). DLP can be provided through a single cloud-based service depending on the enterprise's needs and risk tolerance. For this, they are demanding pay-as-you-go (PAYG) models (DLP as a service) as opposed to annual licensing commitments. This is significantly impacting providers from two sides. Products that are designed for on-premise usage that run in the cloud demand considerable investment by the provider while the functionality essentially stays the same. In addition, shifting from a traditional, licensing model that involves pre-payment to a pay-per-month model affects the provider's cash flow and potentially affects its ability to invest in product development. The result being many established providers are witnessing a rapid growth of cloud-native DLP products offered as-a-service with competitive pricing. DLP software providers are increasingly partnering with managed security service providers (MSSPs) as an essential part of their go-to-market (GTM) strategies to cover a wider market for their products.

DLP tools undertake three primary tasks: discovery, processing and action-taking. For a complete solution, these must be applied to data-in-use (DIU), data-in-motion (DIM), data-at-rest (DAR), and to data used or stored in cloud applications. Different challenges are presented for structured and unstructured data and each must be addressed. Unstructured data is by far the most difficult as it requires capabilities to discover or identify potentially confidential data in numerous formats (Microsoft Excel, Adobe PDF, JPEG, etc.). This creates many different data situations where the possibilities are multiplied together, and DLP tools differ substantially in their abilities to reliably undertake content inspection under all these conditions.

CIOs or CISOs typically make the final decision for DLP solutions purchases. However, information security committees or councils are also regularly involved in selecting a solution, as well as in the policies and standards guiding the overall DLP program. Their guidance is important to balance security and risk tolerance with the potential negative effects on the business when automated reporting or transaction blocking is implemented. These governance entities often have a broad membership with representatives from many corporate departments. The CTO, CRO, CCO and CFO may all be involved or, at least influence, the selection decision. Representatives from HR, Legal and the businesses are also often considered critical contributors. Finally, data owners typically have a significant voice as to how the DLP solution will be used.

Those selecting DLP solutions for their enterprises should view their needs from a wide perspective. Many factors determine the DLP solution or suite of solutions that is optimal for each enterprise. Such factors include the sensitivity of the data being protected, the velocity with which it changes, the need for a visibly compliant solution, tolerance for risk, investigative resource requirements and the net effect on productivity. Appetite for outsourcing, the need for vendor support, partner network, and a product development roadmap that looks to keep solutions current with the changing data security landscape should also be considered.

Strategic Services Trends

The U.S. strategic security services market is driven by companies looking to improve their cyber security programs. Evaluation of current enterprise programs typically generates a gap analysis that can be used as the foundation from which a new security strategy can be developed or an existing one be modified. Many consulting firms offer strategic security consulting in the form of program or security domain (for example, IAM) assessments, compliancy audits, and gap analyses for optimizing resource allocation. Assessments can also measure compliance by scoring a client's program and capabilities against specific regulations (for example, CCPA, NYDFS, and GDPR), or frameworks and industry standards (for example, CMMI, NIST CSF, and FFIEC CAT). Consultants may employ other methodologies to quantify program and function efficacy or efficiency. Compliancy audits compare the client's security program's structure, governance, processes and security and risk management controls against regulatory requirements that apply to the enterprise. These are often consulting firms with their roots in accounting and audit. Their abilities to provide more technical security services for security tool deployment, configuration and maintenance differ considerably.

Some, but not all, technology and managed security services providers offer strategic consulting services, and of those offering security strategy, not all have a robust consulting capability. Some traditional technology outsourcing companies have developed or are buying strategic consulting practices to evaluate programs and identify sales opportunities with existing or new potential clients. Some strategy consulting firms that have the expertise to assess security program maturity, find gaps and make recommendations are buying and building the technical capability to deliver further on their recommendations. In short, there is a lot of acquisition and expansionist activity taking place in the security services arena. Such activities include hiring specialists, entering new partnerships, opening cyber security labs for training, sandboxing experimentation, learning centers and other new service offerings

As part of program improvement initiatives, U.S. companies are evaluating which skills should remain in-house and whether it is possible to hire and retain qualified personnel to do cyber security work. Strategy consultants help customers answer common questions such as how much security should be outsourced to a managed security provider and what pieces should remain in-house. Strategic security consultants are also helping clients answer more difficult, less technical, questions such as what the enterprise's risk tolerance for adverse cyber events is. Now that boards of directors must both attest to their knowledge of risks the business faces and provide direction as to how risks should be managed, the role of strategic security consulting has expanded further. Their direct lead-in to the development of security and risk solutions for identified gaps against internal and external requirements includes supporting vendor selection and management and ensures their importance to software vendors and technical and managed security service providers alike. Small and medium-size businesses with less in-house capacity find an attractive overall solution in security providers that offer all three security services as a one-stop cohesive opportunity.

Cyberattacks, phishing campaigns and ransomware are also on the rise and driving the demand for strategic security services. Companies understand that manipulation of financial markets, social media or elections is cyber warfare with the goal of nation-states gaining economic advantage, and none wants to have their reputation damaged by being associated with such criminal activity. Despite their goals and objectives, clients still need to look for risk-balanced security solutions to satisfy their shareholders.

As a result of all these pressures, maturity and compliance assessments have become regular occurrences as companies endeavor to document readiness, demonstrate security program improvement and ensure regulatory compliance with ever more demanding privacy laws. A more mature security program can be positive business differentiator and provide an attractive selling point for companies when they negotiate with prospective customers of their core business. A third-party verification is preferable to an unvalidated self-assessment, and consequently, threat intelligence is used to inform security decisions. Also, systems failing vulnerability tests require technical patches, upgrades or replacements. Strategic security services are increasingly valuable for clients to satisfy their customers, regulators and shareholders.

Technical Services Trends

Many security solutions and technical security service providers compete in the U.S. market covering all aspects of IT and business. It falls to technical security service providers to determine how best to integrate all these vendor solutions with customer systems and business processes. Despite the considerable number of technical service providers in the U.S. market, gaps still exist. Leading service providers are developing proprietary platforms and interfaces to integrate the varied vendor solutions and plug security gaps.

The U.S. market is fragmented with hundreds of security providers offering services for integration, system stress-testing and training. However, most do not have adequate expertise, or delivery capacity for enterprise-level engagements. Some may operate only in a specific region of the country; others may focus on certain sectors, tools or systems. These local players are recognized referral resources for software solution vendors. They take a local slice of business where there is a targeted, ad hoc or small and some-what regular engagement with the end customer. Consequently, these smaller, niche players are not included in ISG's Provider Lens Report because they do not handle enterprise-wide implementations.

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

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

Managed Security Services Trends

Managed security services are changing from traditional monitor and react models to a more proactive one that includes both defensive and offensive capabilities. Managed detection and response (MDR) includes components of the traditional model where a service provider monitors for anomalies in networks, servers, firewalls, log activity, web traffic, etc., and generates alerts when conditions are outside of expectations. Increasingly, customers are engaging providers to coordinate the incident response team. Cyber security and fusion centers have emerged, not to replace SOCs, but to expand and extend security operations. These centers leverage advanced technologies such as artificial intelligence (AI), machine learning (ML), edge computing, blockchain and other tools that can ingest large volumes of data and produce smart analytics, deliver layered security, push back criminals and open lines of business communication and collaboration, while giving insights into how threats morph, move and multiply.

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

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

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

ISG Provider Lens™

Introduction

Scope of the Report

With the growth of digitalization and the connected world of things such as Industrial Internet of Things (IIoT), smart cities and connected cars, business processes are increasingly focused on the need to protect IT and communication systems to such an extent that IT security has now become synonymous with business security. In addition to the need to protect confidential and sensitive data within organizations, the enforcement of regulations such as GDPR in Europe and California Consumer Protection Act (CCPA) in the U.S., compels businesses to implement stronger safeguards to counter cyberattacks.

This study examines five subject areas of cyber security in the U.S. market and makes a distinction between security solutions and security services. In this study, security solutions cover software and cloud services, based on proprietary software, from product providers. The topics considered are identity and access management (IAM) and data leakage/loss prevention (DLP). Security services is a subsector of general IT services where specialists apply security-specific technologies and methodologies that comply with industry standards and regulations. This report focuses on strategic, technical and managed security services.

The ISG Provider Lens™ Cyber Security - Solutions & Services 2020 study aims to support decision-makers in optimizing their security budgets.

How the Study Can Help

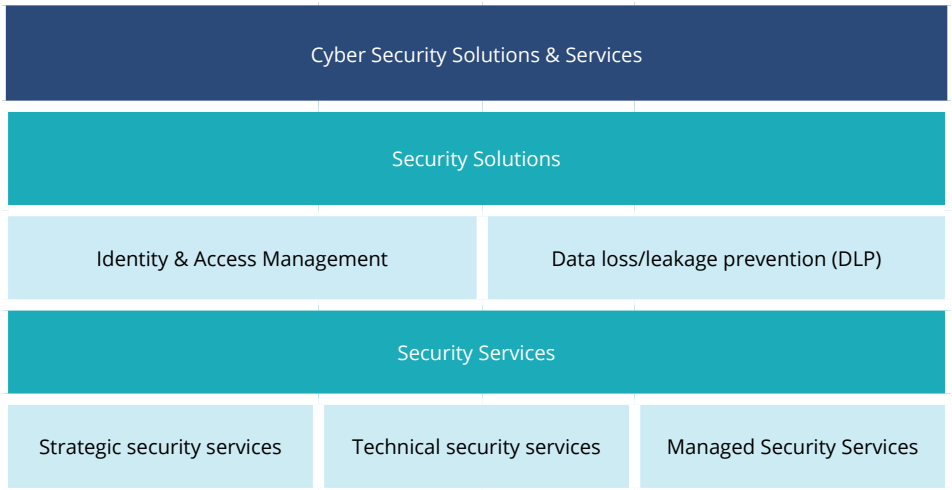
The ISG Provider Lens™ study offers the following to IT decision-makers:

- Transparency on the strengths and weaknesses of relevant providers;
- A differentiated positioning of providers by segments;
- Perspective on markets, including the U.S., the U.K., Germany, Switzerland, France, Brazil and Australia.

ISG market research studies serve as an important decision-making basis for positioning key relationships and go-to-market considerations. ISG advisors and enterprise clients use information from these reports to evaluate their current vendor relationships and potential engagements.

The study comprises multiple quadrants covering the spectrum of services that an enterprise client requires, as illustrated in the following figure:

Simplified illustration



Source: ISG 2020

The quadrant descriptions are as follows:

Identity and access management (IAM): This quadrant compares vendors of products that are used to collect, record and manage user identities and related access rights. It examines on-premise software licensing models, software-as-a-service (SaaS) and cloud-only service options.

Data loss/leakage prevention (DLP): This quadrant compares vendors of products that identify and monitor sensitive data, restrict access to only authorized users, and prevent data leakage. It includes appliances, on-premise software licensing, SaaS and cloud-only service options.

Strategic security services: This quadrant covers strategy consulting for IT security solutions, including governance, risk and compliance (GRC) elements. It examines service providers that do not have an exclusive focus on proprietary products or solutions.

Technical security services: This quadrant assesses service providers of integration, maintenance and support for IT security solutions. It examines service providers that do not have an exclusive focus on their respective proprietary products and can implement and integrate vendor solutions.

Managed security services: This quadrant comprises operations and management of IT security infrastructures for one or several customers through a security operations center (SOC). Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on preventive measures, penetration testing, firewall operations, anti-virus operations, IAM services, DLP operations and other operating services.

Provider Classifications

The ISG Provider Lens™ quadrants were created using an evaluation matrix containing four segments, where the providers are positioned accordingly.

Leader

The "Leaders" among the vendors/providers have a highly attractive product and service offering and a very strong market and competitive position; they fulfill all requirements for successful market cultivation. They can be regarded as opinion leaders, providing strategic impulses to the market. They also ensure innovative strength and stability.

Product Challenger

The "Product Challengers" offer a product and service portfolio that provides an above-average coverage of corporate requirements, but are not able to provide the same resources and strengths as the Leaders regarding the individual market cultivation categories. Often, this is due to the respective vendor's size or their weak footprint within the respective target segment.

Market Challenger

"Market Challengers" are also very competitive, but there is still significant portfolio potential and they clearly lag behind the Leaders. Often, the Market Challengers are established vendors that are somewhat slow to address new trends, due to their size and company structure, and therefore have some potential to optimize their portfolio and increase their attractiveness.

Contender

"Contenders" are still lacking mature products and services or sufficient depth and breadth of their offering, while also showing some strengths and improvement potentials in their market cultivation efforts. These vendors are often generalists or niche players.

Provider Classifications (cont.)

Each ISG Provider Lens™ quadrant may include a service provider(s) who ISG believes has a strong potential to move into the leader's quadrant.

Rising Star

"Rising Stars" are usually Product Challengers with high future potential. Companies that receive the Rising Star award have a promising portfolio, including the required roadmap and an adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market. This award is only given to vendors or service providers that have made extreme progress towards their goals within the last 12 months and are on a good way to reach the leader quadrant within the next 12 to 24 months, due to their above-average impact and innovative strength.

Not In

This service provider or vendor was not included in this quadrant as ISG could not obtain enough information to position them. This omission does not imply that the service provider or vendor does not provide this service. In dependence of the market ISG positions providers according to their business sweet spot, which can be the related midmarket or large accounts quadrant.

Cyber Security - Solutions & Services - Quadrant Provider Listing 1 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Accenture	Not In	Not In	Leader	Leader	Leader
AT&T	Not In	Not In	Not In	Not In	Market Challenger
Atos	Product Challenger	Not In	Leader	Leader	Leader
Axians	Not In	Not In	Not In	Contender	Not In
BAE Systems	Not In	Not In	Contender	Not In	Not In
Beta Systems	Contender	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Not In	Not In	Not In
Capgemini	Not In	Not In	Leader	Leader	Leader
Centurylink	Not In	Not In	Contender	Not In	Contender
CGI	Not In	Not In	Contender	Not In	Not In
Cigniti	Not In	Not In	Not In	Contender	Not In
Clearswift	Not In	Contender	Not In	Not In	Not In
Cognizant	Not In	Not In	Contender	Market Challenger	Market Challenger
Computacenter	Not In	Not In	Contender	Not In	Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 2 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
CoSoSys	Not In	Contender	Not In	Not In	Not In
Cyberproof	Not In	Not In	Not In	Not In	Contender
Deloitte	Not In	Not In	Leader	Leader	Leader
Digital Guardian	Not In	Leader	Not In	Not In	Not In
Drivelock	Not In	Product Challenger	Not In	Not In	Not In
DXC	Not In	Not In	Leader	Leader	Leader
EY	Not In	Not In	Product Challenger	Leader	Not In
Fidelis	Not In	Contender	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Not In	Not In
Forgerock	Product Challenger	Not In	Not In	Not In	Not In
Fortinet	Contender	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Product Challenger	Product Challenger	Contender
GBS	Not In	Contender	Not In	Not In	Not In
Google DLP	Not In	Contender	Not In	Not In	Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 3 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
HCL	Not In	Not In	Leader	Leader	Leader
Herjavec Group	Not In	Not In	Not In	Not In	Contender
IBM	Leader	Leader	Leader	Leader	Leader
Infosys	Not In	Not In	Product Challenger	Product Challenger	Contender
Kudelski	Not In	Not In	Contender	Contender	Contender
LTI	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Matrix 42	Not In	Contender	Not In	Not In	Not In
McAfee	Not In	Leader	Not In	Not In	Not In
Micro Focus	Market Challenger	Not In	Not In	Not In	Not In
Microsoft	Leader	Market Challenger	Not In	Not In	Not In
MobileIron	Not In	Product Challenger	Not In	Not In	Not In
Mphasis	Not In	Not In	Not In	Not In	Contender
Netskope	Not In	Rising Star	Not In	Not In	Not In
Nexus	Product Challenger	Not In	Not In	Not In	Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 4 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
NTT	Not In	Not In	Product Challenger	Leader	Rising Star
Okta	Leader	Not In	Not In	Not In	Not In
Omada	Market Challenger	Not In	Not In	Not In	Not In
One Identity	Rising Star	Not In	Not In	Not In	Not In
OneLogin	Product Challenger	Not In	Not In	Not In	Not In
Oracle	Leader	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Contender	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In
Proofpoint	Not In	Market Challenger	Not In	Not In	Not In
PWC	Not In	Not In	Not In	Market Challenger	Not In
RSA	Leader	Not In	Not In	Not In	Not In
SailPoint	Contender	Not In	Not In	Not In	Not In
SAP	Market Challenger	Not In	Not In	Not In	Not In
Saviynt	Contender	Not In	Not In	Not In	Not In

Cyber Security - Solutions & Services - Quadrant Provider Listing 5 of 5

	Identity & Access Management	Data Leakage/Loss Prevention (DLP)	Technical Security Services	Strategic Security Services	Managed Security Services
Secureworks	Not In	Not In	Product Challenger	Leader	Leader
TCS	Not In	Not In	Market Challenger	Not In	Contender
Tech Mahindra	Not In	Not In	Contender	Not In	Product Challenger
Thales	Market Challenger	Not In	Contender	Market Challenger	Not In
Trend Micro	Not In	Product Challenger	Not In	Not In	Not In
Trustwave	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Unisys	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Varonis	Not In	Leader	Not In	Not In	Not In
Verizon	Not In	Not In	Market Challenger	Leader	Leader
Watchguard	Not In	Product Challenger	Not In	Not In	Not In
Wipro	Not In	Not In	Leader	Leader	Leader
Yash Technologies	Not In	Not In	Not In	Contender	Not In
ZenSar	Not In	Not In	Contender	Contender	Contender
Zscaler	Not In	Product Challenger	Not In	Not In	Not In

Cyber Security - Solutions & Services Quadrants

ENTERPRISE CONTEXT

Technical Security Services

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

In this quadrant report, ISG highlights the current market positioning of providers of technical security services in the U.S. and the way they address the key challenges faced by enterprises in the country. With the growing number of vendors offering cyber security tools and a shortage of personnel with expertise, providers of technical security services are increasingly in demand to architect secure configurations and streamline customized implementation plans.

The U.S. is a mature market for security services. Large companies typically require extensive technical security services because of their complex architectures and requirement for a wide variety of tools. In ISG's experience, companies in the U.S. discern providers based on their ability to provide specialized and highly skilled resources locally as part of a service engagement.

IT and technology leaders should read this report to understand the capabilities of technical security services providers and the positioning of those companies compared herein relative to each other and the market.

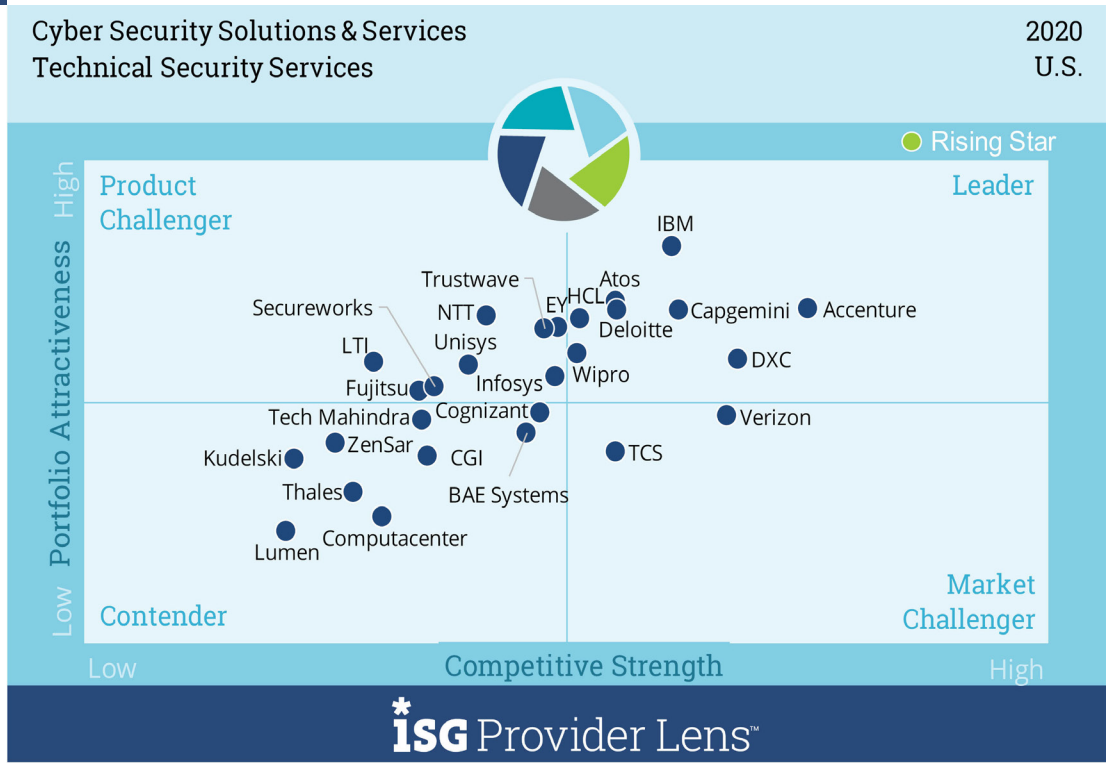
Information security and data professionals should read this report to understand how technical security service providers can be leveraged in the implementation and integration of security tools and platforms to create more secure information ecosystems and how TSS providers can be compared with each other.

Senior business executives, including those in the C-suite and directors, should read this report to understand how the application of technical security services directly affects the business environment and helps to reduce the potential for cyberattacks and the impact of attacks when they do happen.

TECHNICAL SECURITY SERVICES

Definition

Technical security services (TSS) cover integration, maintenance and support for IT security solutions. Providers in this space regularly select hardware and software versions to match requirements. They partner with multiple vendors and seek to achieve certification in each vendor's technologies so as to competently integrate tools and platforms with appliance and network configurations. Secure architecture designs are maintained after implementation to reflect changes in the client security ecosystem and risk posture. Training for client representatives (executives, engineers and analysts) is a common activity. This quadrant examines service providers that are not exclusively focused on their respective proprietary products and can implement and integrate vendor solutions.



Source: ISG Research 2020

TECHNICAL SECURITY SERVICES

Eligibility Criteria

- Demonstrate experience in implementing security solutions for companies in the U.S.;
- Authorized by vendors to distribute and support security solutions;
- Have certified experts to support security technologies;
- Ideally a member of security associations and certification agencies.

Observations

Technical security service providers work in concert with cyber security software vendors to install, configure and integrate their solutions. Service partners are often the party that closes the sale. They are trusted to accurately estimate capacity and system requirements. Furthermore, security service providers retain client relationships through seamless product implementation and on-going maintenance.

The complex solutions originating from many security products require elaborate configuration and customization for both network and cloud environments. Security engineers design the implementation architecture and plan and manage the delivery team and schedule. Solution architects must match the technical capability of appliance models and software versions to business risk tolerance, regulatory compliance requirements and industry standards. Technical security service providers train analysts and engineers, service and maintain both hardware and software, and stress the test functionality to identify security gaps. The required skills to successfully deliver new security technology to clients are substantial and a barrier to entry for some.

TECHNICAL SECURITY SERVICES

Observations (cont.)

Technical security service providers have a symbiotic relationship with solution providers as described above. Thus, the partner ecosystem is crucial for evaluating providers. With different risk tolerances, budgets, regulations and business goals, few security domains have a one-product-fits-all solution for customers. Among hundreds of solutions available, prospective customers should carefully consider the quality of the solution, balanced hardware and the skills needed to deploy and maintain the technology, as well as the remediation and support requirements in the event of a cyberattack or breach.

The U.S. market has a mix of federal and state as well as international regulations that are applicable to cyber security, cyber risk management and privacy. All three are closely connected. Unfortunately, there is no single overarching privacy or cyber security regulation that holds sway across all states and industries such as with EU members and GDPR. The alphabet soup of regulations varies greatly in their reach, scope, penalties and administrative burden. Customers typically create their own unique set of security standards by selecting from frameworks and regulations such as CCPA, ECPA, FCPA, FERPA, FINRA, FISMA, GLB, HIPAA, HITECH, HITRUST and SOX based on their product and service offerings and geographic and infrastructural footprints. Technical security service providers and their security partners must be fluent in all of them to support the needs of each customer.

Thousands of IT companies in the U.S. offer some level of integration and implementation capability. This quadrant is focused on the larger providers of that group with a local delivery capacity able to handle larger customer accounts.

From the 70 providers reviewed in this study, 25 have qualified for inclusion in this quadrant. Eight are Leaders and one is a Rising Star:

- **Accenture** is a large management consulting, technology and outsourcing service provider, employing more than 500,000 people globally and 50,000 in the U.S. It has a large cyber security practice called Accenture Security with 8,000 cyber security specialists delivering over 500 security projects each year. The company acquired six SOCs in January 2020 from Broadcom that had previously belonged Symantec.

TECHNICAL SECURITY SERVICES

Observations (cont.)

- **Atos** is a technology transformation and digital services company headquartered in Bezons, France with about 5 percent of its 110,000 employees based in the U.S. It offers hardware, software and security services backed by a network of PSOCs including two in the U.S. Atos is the Worldwide Information Technology Partner for the next Olympic and Paralympic Games.
- **Capgemini** is a large global technology consultancy based in Paris, with more than $6.5 billion in revenues from North America and around 20,000 employees in the U.S. Cyber security engineers and analysts comprise more than 4,500 of the company's global workforce and support 650 clients through 15 SOCs, 12 research labs (AIEs) and two client experience centers. The strategic acquisition of Leidos Cyber has expanded Capgemini's U.S. portfolio offering substantially.
- **Deloitte** is a large global consultancy network with member firms around the world and has more than 100,000 employees placed across 100 offices in the U.S. Its revenues from the region reached more than $24 billion in 2019, giving it the means to both organically develop and acquire additional security delivery capacity around the world. Recent acquisitions include SecurePath (security consultancy), Integrity Paahi Solutions (MSSP), and Converging Data (technical security services).
- **DXC Technology:** Four years after it was spun-out of Hewlett-Packard Enterprise (HPE) and merged with Computer Sciences Corporation (CSC), DXC generates an annual revenue of $21 billion and has 138,000 employees in over 70 countries, including 3,000 security professionals globally. The company has a network of 12 SOCs, including one in Delaware. It delivers cyber security services through its DXC Security Platform (DSP) and ensures continuous monitoring and management of incidents and vulnerabilities round the clock.

TECHNICAL SECURITY SERVICES

Observations (cont.)

- **HCL Technologies** is a large IT services company headquartered in Noida, India with $9.9 billion in revenue in 2019 and more than 150,000 employees in 46 countries. Its broad security portfolio builds on the company's six Cyber Security Fusion Centers (CSFCs), including one in the U.S. It has expanded its footprint to ensure both on-shore and near-shore delivery capabilities with more than 9,000 employees in the region. HCL maintains alliances with more than 120 global technology vendors, customers, and niche solution providers to ensure it can deliver a best-in-class solution for each customer engagement.
- **IBM** has more than 350,000 employees working in 85 percent of the world's countries. Its 8,000-member team of security experts addresses both strategic and operational elements of cyber security and offers security services and tools for data center, network, digital workplace, security access and cloud cyber security environments. IBM's network of global SOCs offers threat detection and investigation capabilities, as well as incident response training. Notable cyber security acquisitions include Resilient Systems (incident response platform), Iris Analytics (transaction fraud detection), Promontory Financial Group (risk management and compliance) in 2016, and Spanugo, (cloud security) in 2020.
- **Wipro** is an information systems, consulting and business process company with annual revenues of $8 billion. Based in Bengaluru, India, Wipro has 21 locations in the U.S. and 130 across the globe, housing 175,000 employees. Its cyber security practice, which accounts for about 10 percent of Wipro's global business, has 700 U.S.-based specialists amongst its 8,000-strong employee base. Wipro works with 200 U.S. customers on data governance, privacy, identity, intelligence, threat management, and cloud security. In 2018, it bought a minority stake in Texas-based Denim Group to leverage its capabilities in application security and secure development training services. This year, it invested in cloud security company CloudKnox to develop a collaborative offering across multiple public cloud service providers.

HCL

Overview

HCL Technologies is a $9.9 billion India-based IT service provider with 450 cyber security customers worldwide. It employs more than 150,000 people including over 9,000 in the U.S. The company offers managed, technical and strategic security services that are focused on bringing innovative security solutions to infrastructure, application, GRC, IAM, business continuity (BC) and disaster (DR), IoT and data security/privacy. HCL has six Cyber Security Fusion Centers (CSFCs) and offers clients both on-shore and near-shore delivery capabilities through its expanding global footprint.

Strengths

Best customer fit: HCL maintains a relationship with more than 40 partners to provide the technology agnostic solution and architecture that is best suited to each cyber security challenge. It works with companies to design cost-effective control solutions and implement and integrate proprietary techniques and partner solutions into customer ecosystems. Its consultants address compliance requirements and industry standards such as PCI, HIPAA, CFR and SOX, whether for on-premise or in the cloud.

Proactive threat mitigation: HCL's Security Intelligence & Analytic Solution (SecIntAI) leverages contextual information from assets, data classification and user identities. Its pattern library is continuously updated through more than 40 social media, dark web, IP/domain reputation and threat database sources. Real-time analytics correlate anomalies and behaviors against threat patterns to achieve the reaction speed that is needed to stop hackers and malware bots.

Comprehensive portfolio: HCL's services include SOC, SIEM, endpoint security, IoT, digital workplace and application protection to defend the customer's full attack surface. Identity as a service (IDaaS) accelerates compliance. SecIntAI inspects transactions. Pre-defined security incident response playbooks guide automated incident mitigation. HCL BigFix enables high success rates with first-pass server patching and fully automated endpoint discovery, management and remediation. HCL AppScan remediates application vulnerabilities throughout the development lifecycle.

Caution

HCL uses a follow-the-sun model to provide 24-by-7-by-365 services through its six CSFC locations. Its preferred delivery model is offshore. Recent investment in its U.S. footprint may begin to alleviate some concerns for U.S. based companies.

Impending changes to HCL's roadmap include some modifications to its cyber security services offering, which may result in existing U.S. clients being guided towards new or modified services as the portfolio evolves.

2020 ISG Provider Lens™ Leader

HCL's security engineers solve challenges faced by U.S. clients by leveraging innovation and technology-agnostic solutions that improve defensive posture and reduce response times.

Methodology

METHODOLOGY

The research study "2020 ISG Provider Lens™ Cyber Security - Solutions & Services" analyses the relevant software vendors/service providers in the U.S. market, based on a multi-phased research and analysis process and positions these providers based on the ISG Research methodology.

The study was divided into the following steps:

1. Definition of 2020 ISG Provider Lens™ Cyber Security - Solutions & Services, U.S. market
2. Use of questionnaire-based surveys of service providers/vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities and use cases
4. Use of ISG's internal databases and advisor knowledge and experience (wherever applicable)
5. Detailed analysis and evaluation of services and service documentation based on the facts and figures received from providers and other sources.
6. Use of the following key evaluation criteria:
   - Strategy & vision
   - Innovation
   - Brand awareness and presence in the market
   - Sales and partner landscape
   - Breadth and depth of portfolio of services offered
   - Technology advancements

Authors and Editors

David Wilkinson, Author

Lead Analyst, ISG Research

David Wilkinson is a Lead Analyst at ISG Research and Senior Managing Partner at the Bellwether Group. David has over 30 years of experience in cybersecurity, risk management, strategy development and executive management and was recently a Senior Director at Gartner Consulting where he headed up Security and Risk Management for the Financial Services Industry. He has undertaken security and risk management work with over 85 major corporations in more than 17 industries. He is an Adjunct Professor at Boston College where he teaches Cybersecurity Risk Management and Resiliency in the graduate program. Before Bellwether, David was at City Investing, The Boston Consulting Group (BCG) and Unilever, Ltd.

Karen Antons, Author

Lead Analyst, ISG Research

Co-author and Lead Analyst, Ms. Antons has over 20 years of business and consulting expertise and partnered in the establishment and growth of The Bellwether Group, a thought leadership practice focused on security and risk management. Karen works with and advises client companies to develop strategies, organizational and reporting structures, as well as policies and governance relative to information and cyber security, enterprise risk management and preparedness. In addition to Bellwether, Ms. Antons has held consulting positions at Gartner, Inc., TRG (now Deloitte), and independent engagements. At present she is also an adjunct professor at Boston College teaching a graduate level course in cyber resiliency and risk management.

Authors and Editors

Jan Erik Aase, Editor

Director

Jan Erik Aase is a director and principal analyst for ISG. He has more than 35 years of collective experience as an enterprise client, services provider, ISG adviser and analyst. Jan Erik has overall accountability for the ISG Provider Lens™ reports, including both the buyer-centric Archetype reports and the Brazilian-based Quadrant reports, focused on provider strengths and portfolio attractiveness. He sets the research agenda and ensures the quality and consistency of the Provider Lens™ team.

ISG Provider Lens™ Report: Cyber Security - Solutions & Services
August 2020

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including more than 75 of 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.