ISG Provider Lens™

Cybersecurity - Solutions & Services

France 2021

Quadrant Report

A research report comparing provider strengths, challenges and competitive differentiators

September 2021

Customized report courtesy of:

orange™ Business Services

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 September 2021, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The lead author for this report is Benoît Scheuber. The editor is Ipshita Sengupta. The research analyst is Srinivasan and the data analyst is Rajesh C. The quality and consistency advisor is Roger Albrecht.

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

For some time now in France, security investments have been driven by compliance requirements, breaches and audit failures. With the rising importance of cybersecurity, enterprises are changing their approach to procuring security services. Top executives are now frequently involved in decision making, and are seeking a better understanding of the topic to handle cyberattacks.

Security is moving from a static to a dynamic posture to support digitalization and new business models. Enterprises need to protect information and identity everywhere. The use of multiple cloud brings more complexity and numerous controls are deployed for data in use, in motion and at rest. Ransomware continues to be the biggest threat for enterprises, with cybercriminals exploiting vulnerabilities in remote access protocols.

In addition to the boom in connected devices, the exponential increase in financial scams and the rush to the cloud, ISG has observed changes driven by the COVID-19 pandemic. Companies have prioritized remote access, collaboration services, anti-phishing and business continuity. Company budgets will now expand to secure end users, data and brand before approaching the next topics in the trend such as Zero Trust and Secure Access Service Edge (SASE).

Enterprises have never been this exposed, with internal applications being accessed remotely, increasing reliance on third parties and the use of open-source software. DevSecOps has therefore become essential, and enterprises have integrated and automated security processes and tooling across the entire software development life cycle (SDLC).

ISG Provider Lens™

Identity and Access Management Software Market Trends

Identity and access management (IAM) and identity management (IdM) are often used interchangeably. In this study, IAM refers to all access authentication, controls, and governance of identity throughout its lifecycle, with less emphasis on the authentication methods.

IAM remains in strong demand in France as perimeters continue to fade with customers adopting more of a zero-trust approach to security. With remote work at scale, accelerated migration to the cloud and more sophisticated attacks, zero trust is not just a buzzword but the new normal. “Never trust, always verify” has become more important in mitigating insider threats, data loss and reputation damage.

The adoption of cloud is driving two trends that are changing the competitive landscape. Vendors are moving IAM from on-premises to the cloud, while clients are demanding pay-as-you-go (PAYG) models or IAM as a Service that some vendors refer to as Identity as a Service (IDaaS). The impact on established vendors is somewhat conflicting. Porting products that are designed for on-premises to the cloud demands new investments and produce few differentiations because the functionality stays the same. At the same time, changing from traditional licensing, paid in full before use, to a pay-per-month model affects a company’s cash flow, reducing its capacity to invest in product development. Therefore, established vendors are observing a rapid growth of cloud-native IAM products that are offered at competitive prices and as an as-a-Service business model.

It is early to say that multi-tenant IAM will prevail as a service. However, some vendors believe it is the way forward. By enabling scalable multi-tenant, cloud-hosted IAM as a service, vendors envision the possibility to become global providers of identity services. In this visionary future, an individual would have a single digital identity across companies and systems.

Among the 83 companies assessed in this study, 22 qualified for this quadrant. Seven are Leaders and one is a Rising Star.

Data Loss Prevention Software Market Trends

Data loss prevention (DLP) and data security are mature markets in France. Strict privacy regulations, including the General Data Protection Regulation (GDPR), have pushed France-based corporations to adopt data classification and protection measures. The country has advanced privacy and security standards, putting individual rights before corporate interests. However, software vendors in the country have not taken the lead in developing data protection software. Leading DLP solutions have been developed in other countries, including countries in Europe.

In addition to data theft, data manipulation prevails as cybercriminals hack core systems, instead of stealing data, manipulate the information, leading to catastrophic consequences such as altered financial records. Data security is critical in a data-driven world. One of the biggest sources of competitive differentiation comes from the way businesses use data and insights. Data privacy controls must adapt to the increasing reliance on data stored and processed for analytics, automation and insights.

Among the 83 companies assessed in this study, 20 qualified for this quadrant. Seven are Leaders and one is a Rising Star.

Advanced Endpoint Threat Protection, Detection And Response Market Trends

With an increasing number of employees working remotely from unsecure networks, the adoption of advanced endpoint threat protection, detection and response (ETPDR) solutions has increased significantly in France. Not only are external threats driving the high demand for security solutions and services, but also the combination of legacy technology and explosion of Internet-facing endpoints and services is generating technical complexity and leading to configuration errors, becoming one of the leading causes for breaches.

Enterprises need continuous monitoring and total visibility of all endpoints, and a tool that can analyze, prevent, and respond to advanced threats by isolating the compromised endpoint.

Among the 83 companies assessed in this study, 16 qualified for this quadrant. Eight are Leaders and one is a Rising Star.

Technical Services Trends

The principal trend is the growing number of security solutions in the french market. Leading service providers have developed proprietary platforms that integrate many security solutions, while covering the gaps with specific functionalities that are developed as per need.

Some enterprises have more than 25 different security solutions, several of them focused on security operations center analysts. ISG notes a trend where CISOs wish to reduce complexity and attack surface by reducing the number of security solutions.

Among the 83 companies assessed in this study, 21 are classified for this quadrant. Eight are Leaders and one is a Rising Star.

Strategic Services Trends

As trust, data protection and privacy considerations are included in all conversations and business decisions, strategic consulting firms increasingly focus on cybersecurity by acquiring expertise around cyber technology architecture and conducting vulnerability assessments as a part of the risk and compliance consulting practice. These companies are hiring specialists and announcing new service offerings.

Governance, risk and compliance (GRC), which were once strictly focused on business factors, now cover cybersecurity because of the cost and brand credibility implications of a data breach or a ransomware attack.

The pandemic has forced security managers (CISOs) to reevaluate their capabilities to weather future systemic risk events. CISOs are broadening the aperture of external events within a risk management plan. Risk quantification has become a way for CISOs to prioritize what to do and where to invest to manage risks and protect an enterprise.

Enterprise security spending, per user, has increased by more than 20 percent between 2019 and 2020, and is likely to increase further in 2021. Budget rationalization will soon be needed, and management asks for maturity assessments to justify investments. As an example of cost optimization, some enterprises are looking at global delivery model for managed security services, IAM and GRC.

Among the 83 companies assessed in this study, 25 are classified for this quadrant. Nine are Leaders and one is a Rising Star.

Managed Security Services For Large Accounts Market Trends

The shortage of security skills worldwide is creating a booming business for managed security service providers (MSSPs). ISG expects an increasing use of security consulting services over next 24 months, with a focus on new pricing/delivery models such as intellectual property and value-based and consulting as a service. The security services market is responding. Some by organically building next-generation cyber services, and some by acquiring the same. Recently, Atos acquired Motiv ICT and In Fidem, Deloitte acquired R9B and Wipro acquired Ampion. ISG expects to see many more M&A in 2021.

Managed security services (MSS) are evolving from security operations centers (SOCs) to complex, AI-powered cyber defense army-like organizations. Security operations center (SOC) services typically include monitoring the alerts generated by security appliances such as firewalls, endpoint security tools, network routers, anti-malware software and other event monitoring tools. Companies cannot lower their defenses and SOCs continue to have a role in the cybersecurity scene. However, they provide basic security that is not adequate to circumvent more sophisticated threats.

Enterprises need to adopt more sophisticated tools to defend themselves. Cyber defense centers (CDCs) have emerged, not to replace SOCs but to expand security operations. These CDCs leverage advanced machine learning (ML) tools that can handle large volumes of data and use smart analytics to understand how threats are morphing, moving and

spreading. They share information dynamically with other CDCs to keep pace with the rise in cybercrime. New tools, such as micro segmentation that can isolate hackers or bots when they break into an enterprise network, have emerged. Managed cybersecurity services have become essential for enterprises.

Among the 83 companies assessed in this study for large accounts, 27 have qualified for this quadrant. Nine are Leaders and one is a Rising Star.

Managed Security Services For The Midmarket Trends

Midsize businesses are unable to compete or even afford sophisticated SOCs to keep up their security posture, and are reaching out to MSSPs to help with everything, including, monitoring, response and hunting. Some service providers that focus on the midmarket generate significant revenues and leverage high-scale automation and AI threat intelligence to provide monitoring and protection services at competitive prices. Others have a deep specialization, which compensates for scale and is in proximity to clients. ISG expects an increase in hybrid delivery models and a local presence to help address local challenges.

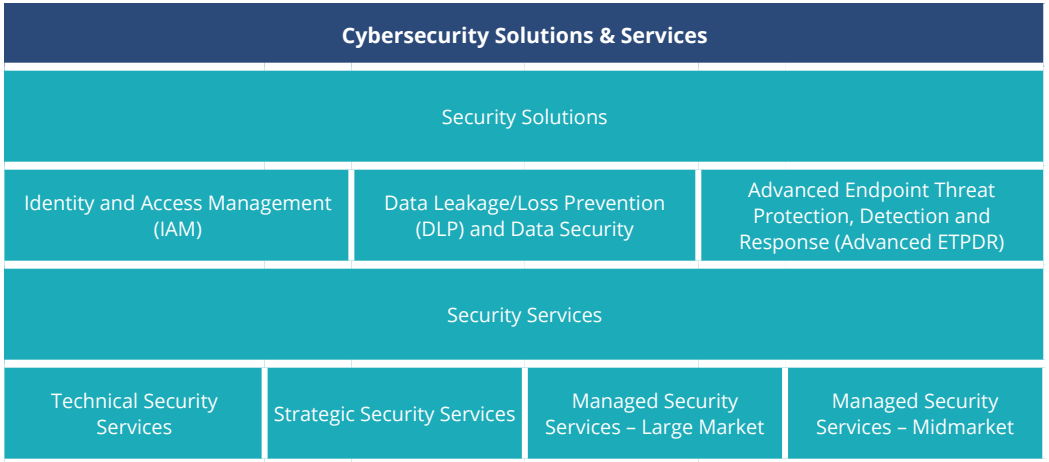
"Security by design" is a recurring theme. The term was coined for software development, referring to best practices of software engineering to avoid constructions that allow hackers to exploit the code and access the database. Many service providers like to emphasize the need to adequately secure the enterprise network and its integration to the public cloud and the users' access to SaaS solutions. In practical terms, it means replacing security tools. Service providers offer a bypass, claiming their managed security platform is ready to use, thus eliminating the need for expensive technology upgrades. The compelling "security by design" focus is more secure than the tools it is replacing. However, these tools still require considerable analyst expertise to block cyberattacks. For most companies ranked in this study, the technology behind the service provides market differentiation, but clients should recognize that people are still essential to provide security.

As security requires significant expertise, staff shortage is a concern for most enterprises. It is difficult for a midsize enterprise to retain cybersecurity experts. Service providers address this concern by allowing midmarket clients to leverage highly skilled practitioners.

Among the 83 companies assessed in this study, 19 are classified for this quadrant. Six are Leaders and one is a Rising Star.

Introduction

Simplified illustration



Source: ISG 2021

Definition

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

Definition (cont.)

Scope of the Report

As part of the ISG Provider Lens™ Quadrant Study, we are introducing the following six quadrants (market) research on Cybersecurity – Solutions & Services 2021 by region:

Scope of the Study – Quadrant and Geography Coverage

	U.S.	U.K.	Nordics	Germany	Switzerland	France	Brazil	Australia
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 (TSS)	✓	✓	✓	✓	✓	✓	✓	✓
Strategic Security Services (SSS)	✓	✓	✓	✓	✓	✓	✓	✓
Managed Security Services (MSS)	✓	✓	✓	✓	✓	✓	✓	✓

Provider Classifications

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

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

Provider Classifications

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

Leader

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

Product Challenger

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

Market Challenger

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

Contender

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

Provider Classifications (cont.)

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

Rising Star

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

Not In

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

Cybersecurity - Solutions & Services - Quadrant Provider Listing 1 of 7

	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
Absolute Software	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Accenture	Not in	Not in	Not in	Not in	Leader	Leader	Not in
Airbus CyberSecurity	Not in	Not in	Not in	Not in	Not in	Product Challenger	Not in
Atos	Leader	Not in	Not in	Leader	Leader	Leader	Not in
Axians	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger	Not in
Beta Systems	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Bitdefender	Not in	Not in	Product Challenger	Not in	Not in	Not in	Not in
Brainloop	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Broadcom	Market Challenger	Leader	Leader	Not in	Not in	Not in	Not in
Capgemini	Not in	Not in	Not in	Leader	Leader	Leader	Leader
CGI	Not in	Not in	Not in	Contender	Contender	Contender	Contender
Check Point	Not in	Not in	Leader	Not in	Not in	Not in	Not in

Cybersecurity - Solutions & Services - Quadrant Provider Listing 2 of 7

	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
Cisco	Not in	Not in	Contender	Not in	Not in	Not in	Not in
Clearswift	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Cognizant	Not in	Not in	Not in	Contender	Not in	Contender	Not in
Computacenter	Not in	Not in	Not in	Market Challenger	Not in	Not in	Leader
CoSoSys	Not in	Contender	Not in	Not in	Not in	Not in	Not in
CrowdStrike	Not in	Not in	Leader	Not in	Not in	Not in	Not in
CyberArk	Product Challenger	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	Rising Star	Rising Star	Rising Star
Cylance	Not in	Not in	Market Challenger	Not in	Not in	Not in	Not in
Dell/RSA	Market Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Deloitte	Not in	Not in	Not in	Rising Star	Leader	Product Challenger	Not in

Cybersecurity - Solutions & Services - Quadrant Provider Listing 3 of 7

	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
Digital Guardian	Not in	Rising Star	Not in	Not in	Not in	Not in	Not in
DXC	Not in	Not in	Not in	Product Challenger	Contender	Market Challenger	Not in
ESET	Not in	Not in	Contender	Not in	Not in	Not in	Not in
EY	Not in	Not in	Not in	Not in	Leader	Not in	Not in
FireEye	Not in	Not in	Product Challenger	Not in	Not in	Not in	Not in
Forcepoint	Not in	Leader	Not in	Not in	Not in	Not in	Not in
Forgerock	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Fortinet	Contender	Not in	Not in	Not in	Not in	Not in	Not in
GBS	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Getronics	Not in	Not in	Not in	Not in	Not in	Not in	Product Challenger
Google DLP	Not in	Contender	Not in	Not in	Not in	Not in	Not in
HCL	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger	Product Challenger

Cybersecurity - Solutions & Services - Quadrant Provider Listing 4 of 7

	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
IBM	Leader	Leader	Not in	Leader	Leader	Leader	Not in
IN Groupe (Nexus)	Rising Star	Not in	Not in	Not in	Not in	Not in	Not in
Infosys	Not in	Not in	Not in	Product Challenger	Product Challenger	Contender	Not in
Intrinsec	Not in	Not in	Not in	Not in	Not in	Not in	Leader
Kaspersky	Not in	Not in	Leader	Not in	Not in	Not in	Not in
KPMG	Not in	Not in	Not in	Not in	Product Challenger	Not in	Not in
Kudelski Security	Not in	Not in	Not in	Leader	Contender	Product Challenger	Product Challenger
Linkbynet	Not in	Not in	Not in	Contender	Not in	Not in	Product Challenger
LTI	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger	Product Challenger
Lumen	Not in	Not in	Not in	Not in	Not in	Product Challenger	Contender
Matrix42	Not in	Product Challenger	Not in	Not in	Not in	Not in	Not in
McAfee	Not in	Leader	Product Challenger	Not in	Not in	Not in	Not in

Cybersecurity - Solutions & Services - Quadrant Provider Listing 5 of 7

	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
Micro Focus	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Microsoft	Leader	Market Challenger	Leader	Not in	Not in	Not in	Not in
Netskope	Not in	Contender	Not in	Not in	Not in	Not in	Not in
NTT	Not in	Not in	Not in	Leader	Leader	Leader	Leader
NXO	Not in	Not in	Not in	Product Challenger	Market Challenger	Not in	Not in
Okta	Leader	Not in	Not in	Not in	Not in	Not in	Not in
One Identity	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
OneLogin	Product Challenger	Not in	Not in	Not in	Not in	Not in	Not in
OpenText	Not in	Leader	Not in	Not in	Not in	Not in	Not in
Oracle	Market Challenger	Not in	Not in	Not in	Not in	Not in	Not in
Orange Cyberdefense	Not in	Not in	Not in	Leader	Leader	Leader	Leader
Palo Alto Networks	Not in	Not in	Contender	Not in	Not in	Not in	Not in

Cybersecurity - Solutions & Services - Quadrant Provider Listing 6 of 7

	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
Ping Identity	Leader	Not in	Not in	Not in	Not in	Not in	Not in
PwC	Not in	Not in	Not in	Not in	Leader	Not in	Not in
SailPoint	Leader	Not in	Not in	Not in	Not in	Not in	Not in
SAP	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Saviynt	Contender	Not in	Not in	Not in	Not in	Not in	Not in
Secureworks	Not in	Not in	Not in	Not in	Contender	Contender	Contender
Sophos	Not in	Not in	Leader	Not in	Not in	Not in	Not in
Sopra Steria	Not in	Not in	Not in	Not in	Market Challenger	Leader	Market Challenger
Systancia	Contender	Not in	Not in	Not in	Not in	Not in	Not in
TCS	Not in	Not in	Not in	Product Challenger	Product Challenger	Product Challenger	Product Challenger
Tech Mahindra	Not in	Not in	Not in	Not in	Not in	Contender	Contender
Thales	Market Challenger	Not in	Not in	Leader	Market Challenger	Leader	Not in

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

	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
Titus	Not in	Contender	Not in	Not in	Not in	Not in	Not in
Trend Micro	Not in	Leader	Leader	Not in	Not in	Not in	Not in
T-Systems	Not in	Not in	Not in	Contender	Not in	Contender	Contender
Unisys	Not in	Not in	Not in	Not in	Not in	Product Challenger	Not in
Varonis	Not in	Leader	Not in	Not in	Not in	Not in	Not in
Verizon	Not in	Not in	Not in	Not in	Not in	Product Challenger	Leader
VMware Carbon Black	Not in	Not in	Leader	Not in	Not in	Not in	Not in
WALLIX	Leader	Not in	Not in	Not in	Not in	Not in	Not in
Watchguard	Not in	Market Challenger	Not in	Not in	Not in	Not in	Not in
Wipro	Not in	Not in	Not in	Leader	Product Challenger	Leader	Not in
Zscaler	Not in	Contender	Not in	Not in	Not in	Not in	Not in

Cybersecurity - Solutions & Services Quadrants

ENTERPRISE CONTEXT

Identity and Access Management (IAM)

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

In this quadrant report, ISG highlights the current market positioning of IAM providers in France, and how each provider addresses the key challenges faced in the region. Enterprises in France are increasingly adopting cloud-based authentication systems for IAM. In France, enterprises are recommended to store information in the eurozone. Enterprises consider this as a key criterion when selecting an IAM provider for implementation though federated secure sign-on of the cloud provider offers enhanced security as all the data are encrypted.

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

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

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

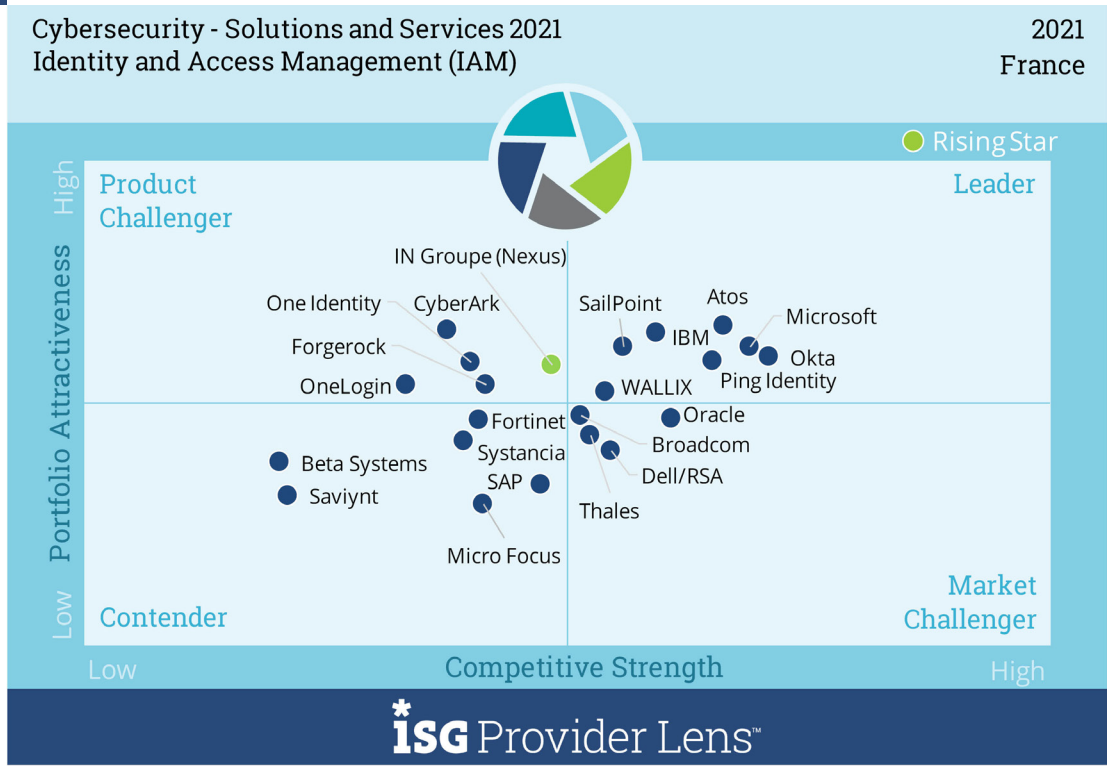
Compliance and governance leaders should read this report to understand the landscape of IAM as it directly affects compliance with region's data and privacy related legislations.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software and associated services to meet unique demands for securely managing enterprise user identities and devices. This quadrant also includes SaaS based on proprietary software. Pure service providers that do not offer an IAM product (on-premises or in the cloud) based on self-developed 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 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 and include 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 features related to social media and mobile users to address their security needs that go beyond traditional web and context-related rights management.



Source: ISG Research 2021

IDENTITY AND ACCESS MANAGEMENT (IAM)

Eligibility Criteria

- The provider should be relevant, in terms of revenue and number of customers, as an IAM product vendor in the respective country.
- IAM offerings should be based on proprietary software and not on third-party software.
- The solution should be capable of being deployed individually or as a combination of on-premises, cloud, identity as a service (IDaaS) and a managed (third-party) model.
- The solution should be capable of supporting authentication individually or by a combination of single-sign on (SSO), multifactor authentication (MFA), risk-based and context-based models.
- The solution should be capable of supporting role-based access and privileged access management.
- The IAM solution provider should be able to provide access management for one or more enterprise needs such as cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.
- The solution should be capable of supporting one or more legacy and newer IAM standards, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIM.
- 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).

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations

IAM tools have long been available for managing access credentials and passwords, including encryption and self-service for password reset. Poor password practices can significantly impact protection systems. Password management has evolved into identity management (IdM). Other methods include user authentication such as two-factor authentication (2FA) and self-service passwords resets with security questions. IdM has the means to verify identity and now includes biometrics such as face recognition. The concept of identity lifecycle management has emerged recently, together with access management controls. Access refers to listing all systems and services that an individual can access and the functions that can be used in the accessed system. IAM covers IdM; the terms often used interchangeably confuse clients. In this study, we consider IAM to have all access controls, with less emphasis on the identity authentication methods.

IAM remains in strong demand as perimeters continue to fade with customers adopting more of a zero-trust approach to security. With remote work at scale, accelerated migration to the cloud and more sophisticated attacks, zero trust is not just a buzzword but the new normal. “Never trust, always verify” has become more important in mitigating insider threats, data loss and reputation damage.

The adoption of cloud is driving two trends that are changing the competitive landscape. Vendors are moving IAM from on-premises to the cloud, while clients are demanding pay-as-you-go (PAYG) models or IAM-as-a-Service that some vendors refer to as Identity-as-a-Service (IDaaS). The impact on established vendors is somewhat conflicting. Porting products that are designed for on-premises to the cloud demands new investments and produce few differentiations because the functionality stays the same. At the same time, changing from traditional licensing, paid in full before use, to a pay-per-month model affects a company’s cash flow, reducing its capacity to invest in product development. Therefore, established vendors are observing a rapid growth of cloud-native IAM products that are offered at competitive prices and as an as-a-Service business model.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations (cont.)

France-based clients that are less hesitant to move to the cloud should understand the benefits of cloud-based IAM when providing an SSO to for SaaS solutions such as Microsoft Office 365, Google G Suit and Salesforce, and many other SaaS options such as enterprise resource management (ERP) and human capital management (HCM). The cloud-based federated SSO provides secure identification for all the requested private data in one place. The cloud IAM solution, which works as a proxy to all other applications, eliminates the distribution of private data to multiple applications, thus reducing the risk of data breaches.

European enterprises concerned with GDPR compliance should understand that federated SSO in the cloud provides better security as it encrypts all sensitive data. However, they must check where the data resides physically. All IAM solutions, qualified for this quadrant, store data in the Eurozone. However, few vendors do not store data in France.

Two-factor authentication is a common feature in IAM, while social authentication is not typically offered (using Google, LinkedIn, or another social network ID for authentication to access a corporate network). Customer IAM (CIAM) is gaining traction, pushed by compliance requests. Blockchain identity is undergoing testing by at least two vendors, but no real cases in production were identified for inclusion in this study.

Enterprises procuring IAM solutions should take their unique needs into consideration to make the right decision. Vendor support, partner network and product development roadmap should be strictly assessed, as the technology is still changing rapidly due to the evolving identification technologies, novel SaaS offerings and the growing demand to include the IAM functionality in DevOps and containers as well for secure IoT devices.

Among the 83 companies assessed in this study, 22 qualified for this quadrant. Seven are Leaders and one is a Rising Star.

- **Atos Evidian** is a full-featured solution, providing France-based clients a robust option for IAM.
- **IBM** offers a robust portfolio of IAM products that integrate well with its other cybersecurity software, including analytics and AI, thus making it a Leader in this quadrant.

IDENTITY AND ACCESS MANAGEMENT (IAM)

Observations (cont.)

- **Microsoft** Azure Active Directory services (Azure AD) offers ready-to-use IAM and integrates easily with cloud applications making it a Leader.
- **Okta** offers a simplified approach to managing complex integrations involving different directory solutions and strengthens it with identity security and regulatory compliance.
- **Ping Identity's** positioning as an identity specialist, combined with a technical partner network and flexible hybrid model delivery makes it a Leader.
- **SailPoint** has a solid presence in France, with a strong base of resellers and channel partners. It has a strong partnership network with major consultancies and security implementation specialists.
- **WALLIX** is a prominent vendor of advanced IAM, enabling full compliance, with sensitive data stored in France.
- **IN Groupe,** the Rising Star, acquired the IdM software company Nexus Group in 2020, and it brings in a world-class investment capacity to take Nexus' identity technology to a superior competitive level.

ENTERPRISE CONTEXT

Data Leakage/Loss Prevention (DLP) and Data Security

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

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

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

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

The French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés) supervises the enforcement of the Personal Data Protection (DPA) regulations and frequently issues decisions and guidelines on the DPA.

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

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

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

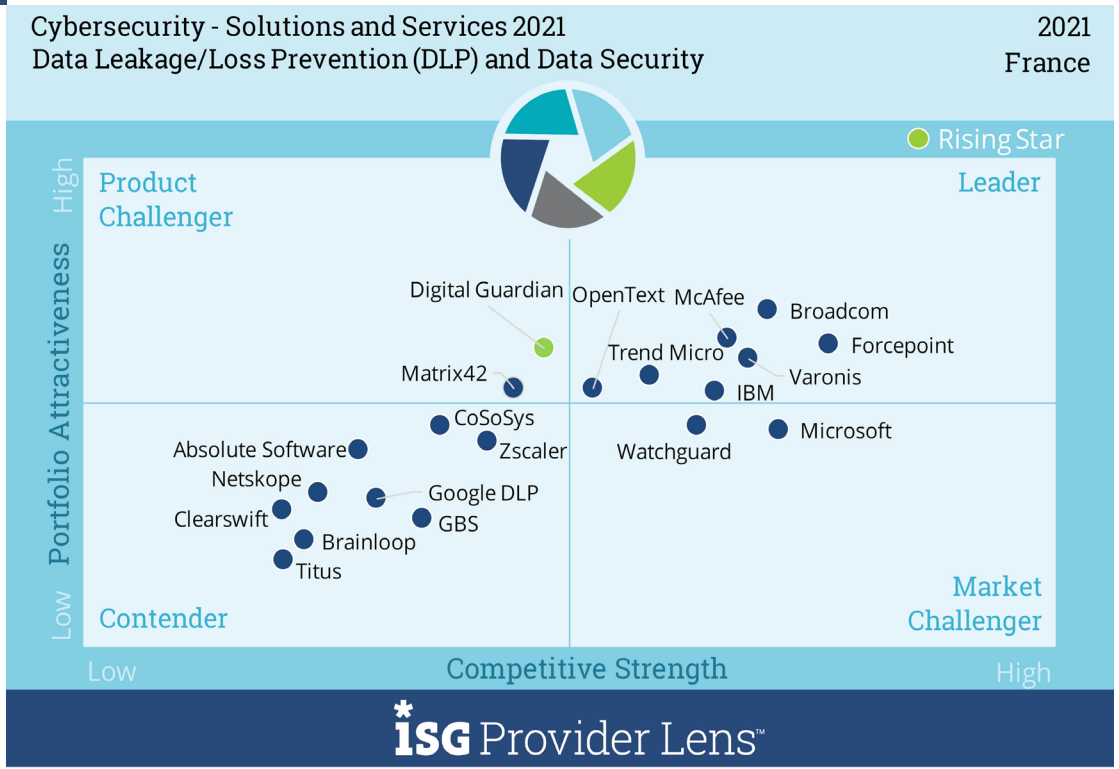
Security architects should read this report to understand how providers of DLP solutions fit their initiatives and needs compared with each other.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Definition

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

These solutions should be able to identify sensitive data, enforce policies, monitor traffic and improve data compliance. They are gaining considerable importance as it has become increasingly difficult for companies to control data movements and transfers. The number of devices, including mobile, that are 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. The devices are supplied with a multitude of interfaces, such as USB ports, Bluetooth, wireless local area network (WLAN) and near-field communication (NFC) that enable data sharing. Data security solutions protect data from unauthorized access, disclosure or theft.



Source: ISG Research 2021

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Eligibility Criteria

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

Observations

Advanced DLP tools can scan files and databases in search of privacy data, tag those assets and alert for intervention. Client companies can define rules to process those assets, decide on deleting the privacy information, obfuscating, replacing, encrypting or moving files to safe storage. With DLP tools, clients can fix past data to comply with new business processes.

Data loss prevention (DLP) and data security are mature markets in France. Strict privacy regulations, including the General Data Protection Regulation (GDPR), have pushed France-based corporations to adopt data classification and protection measures. The country has advanced privacy and security standards, putting individual rights before corporate interests. However, software vendors in the country have not taken the lead in developing data protection software. Leading DLP solutions have been developed in other countries, including countries in Europe.

In addition to data theft, data manipulation prevails as cybercriminals hack core systems, instead of stealing data, manipulate the information, leading to catastrophic consequences such as altered financial records. Data security is critical in a data-driven world. One of the biggest sources of competitive differentiation comes from the way businesses use data and insights. Data privacy controls must adapt to the increasing reliance on data stored and processed for analytics, automation and insights.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Observations (cont.)

Enterprises should be aware that some solutions are highly efficient and sophisticated, for instance, the ones designed to support high volume transactions in large financial institutions. The first factor to consider when procuring a DLP solution relies on how frequent private and confidential data changes. Changing business processes to segregate private and sensitive data reduces the complexity and cost of DLP solutions.

The CIO, CTO, CISO and chief compliance officer are the main decision makers when it comes to purchasing DLP solutions. Clients procuring DLP solutions should look for local partners with strong implementation capabilities, after-sales support and licensing model. If compliance is the major concern, they should focus on tools that scan and obfuscate data. Those concerned about malware, ransomware, data breaches and intellectual property protection can consider tools that provide real-time data access monitoring and automated access blocking. Few vendors offer real-time blocking, and its effectiveness varies according to configuration and context. Traffic inspection tools that provide micro-segmentation may be necessary for blocking data access and ransomware.

This study has identified three types of DLP solutions. Some allow users or applications to tag private and confidential information before saving. These more straightforward solutions can inspect a file, form, email or message before sending or saving it, which helps in identifying and preventing non-compliance. The second type can inspect existing files, databases and documents to tag and fix non-compliance only after it happens in the next scan cycle. The last type can inspect data moving in the network, monitor user access and check context (for example, source, destiny, credential, location and sensibility of the data) to block or allow access and change. All combinations of these methods exist, providing the market with numerous alternatives.

Among the 83 companies assessed in this study, 20 qualified for this quadrant. Seven are Leaders and one is a Rising Star.

- **Broadcom's** established DLP portfolio covers most aspects of data identification, classification and asset protection and is aligned with GDPR requirements.
- **Forcepoint** offers a broad, integrated proactive suite of user and data protection products for governance, analytics, risk management and compliance. This makes the company a promising player in DLP.
- **IBM** offers a robust and highly scalable DLP solution that is particularly suitable for large enterprises, making the company a Leader in data security.

DATA LEAKAGE/LOSS PREVENTION (DLP) AND DATA SECURITY

Observations (cont.)

- **McAfee** with its capabilities around data discover, content aware protect and unified centralized reporting offers adequate DLP functionalities.
- **OpenText** has fortified its market position by acquiring companies, such as XMedius in2020 and Carbonite in 2019, and remains a solid security solutions provider.
- **Trend Micro** takes an integrated approach to DLP. The company offers strong threat research expertise and an integrated approach to data security. This makes the company a good choice for DLP offering.
- **Varonis**' end-to-end DLP solution, combined with its GDPR compliance-led focus and context-aware approach, makes it a Leader in this quadrant.
- **Digital Guardian** provides a single, data protection platform that combines DLP and EDR. Its offerings protect against both insider and external threats, making the company a Rising Star in the DLP market.

ENTERPRISE CONTEXT

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

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

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

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

Enterprises in France have seen an increase in attack volumes and sophistication. They are responding to the rise in cybercrime by increasing cyberdefense spending and implementing advanced threat protection solutions.

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

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

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

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

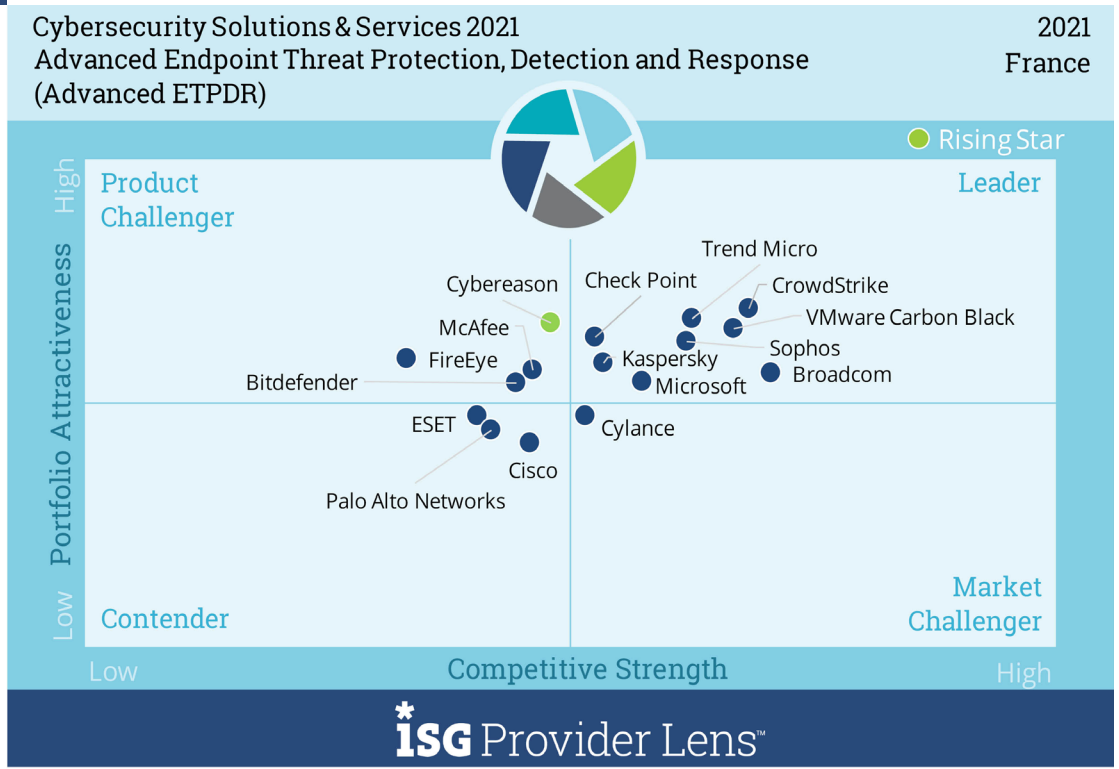
Security architects should read this report to understand how providers of advanced endpoint solution fit their initiatives and needs compared with each other.

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 SaaS based on proprietary software. Pure service providers that do not offer an advanced ETPDR product (on-premises or cloud-based) based on self-developed software are not included here. This quadrant evaluates providers offering solutions that enable continuous monitoring and total visibility of all endpoints, and can analyze, prevent, and respond to advanced threats.

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



Source: ISG Research 2021

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

Eligibility Criteria

- The provider should be relevant, in terms of revenue and number of customers, as an advanced ETPDR product vendor in the respective country.
- The advanced ETPDR offering should be based on proprietary software and not on a third-party software.
- The providers' solutions should provide comprehensive and total coverage and visibility of all endpoints in the network.
- The solution should demonstrate effectiveness in blocking sophisticated threats such as APTs, ransomware and malware.
- The solution should leverage threat intelligence, analyze, and offer real-time insights on threats across endpoints.

Observations

With an increasing number of employees working remotely from unsecure networks, the adoption of advanced endpoint threat protection, detection and response (ETPDR) solutions has increased significantly. Not only are external threats driving the high demand for security solutions and services, but also the combination of legacy technology and explosion of internet-facing endpoints and services is generating technical complexity and leading to configuration errors, becoming one of the leading causes for breaches.

Enterprises need continuous monitoring and total visibility of all endpoints, and a tool that can analyze, prevent, and respond to advanced threats by isolating the compromised endpoint. The platforms may also integrate with other security tools to provide a consolidated view of a threat landscape and events to increase visibility on the prevailing risks. Another key tenet addressed by the ETPDR solutions pertain to continuous monitoring and analysis of the parameters gathered from the data around endpoints by these solutions.

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

Observations (cont.)

Many enterprises are already using an endpoint protection solution, but advanced ETPDR solutions offer automation and orchestration of multiple threat protection, detection and response capabilities into a single product. The best advanced ETPDR solutions include behavioral detection with automatic response. Furthermore, to cover all enterprise endpoint landscape, the solution should offer threat protection and detection capabilities across all operating systems. Finally, the most mature solutions use risk-based approaches to policy architecture and enforcement to help support a zero-trust device posture.

Among the 83 companies assessed in this study, 16 qualified for this quadrant. Eight are Leaders and one is a Rising Star.

- **Broadcom** offerings are backed by strong intelligence support and a simplified management console. It is supported by broad network of partners. This makes it a Leader.
- **Carbon Black** differentiates itself through continuous and centralized recording, behavior led malware detection and large base of use cases.
- **Check Point's** portfolio is led by strong research focused workforce and partner network, making it suitable for a variety of enterprise needs.
- **CrowdStrike's** Falcon Platform modules are flexible and scalable and deliver granular visibility through cloud-based consoles. This makes the company a Leader.
- **Kaspersky's** flexible deployment models, varied enterprise coverage and threat prevention and detection features make it a promising player in the country.
- **Microsoft's** capabilities in endpoint detection, protection and response behavioral analytics and threat intelligence expertise, coupled with integration with other offerings, makes it a leader.
- **Sophos'** endpoint detection and response offering leverages deep learning and addresses key security threats such as ransomware, making the company a Leader.
- **Trend Micro's** automation-led advanced ETPDR capabilities backed by threat-detection techniques differentiates it in the ETPDR market.
- **Cybereason's** ability to offer instant remediation, end processes with the use of an intuitive interface and AI-led behavioral analysis make it a Rising Star.

ENTERPRISE CONTEXT

Technical Security Services

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

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

Providers that offer high technological expertise in advanced technologies such as AI, analytics, data and threat intelligence, and automation, along with domain expertise in these areas, are highly considered by enterprise customers for wide implementation of cybersecurity solutions in France. Enterprises also look for providers that offer service improvement programs, flexible pricing models, and volume discounts with sustainable innovation and customer satisfaction on a regular basis when choosing a provider for integration of the systems.

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

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

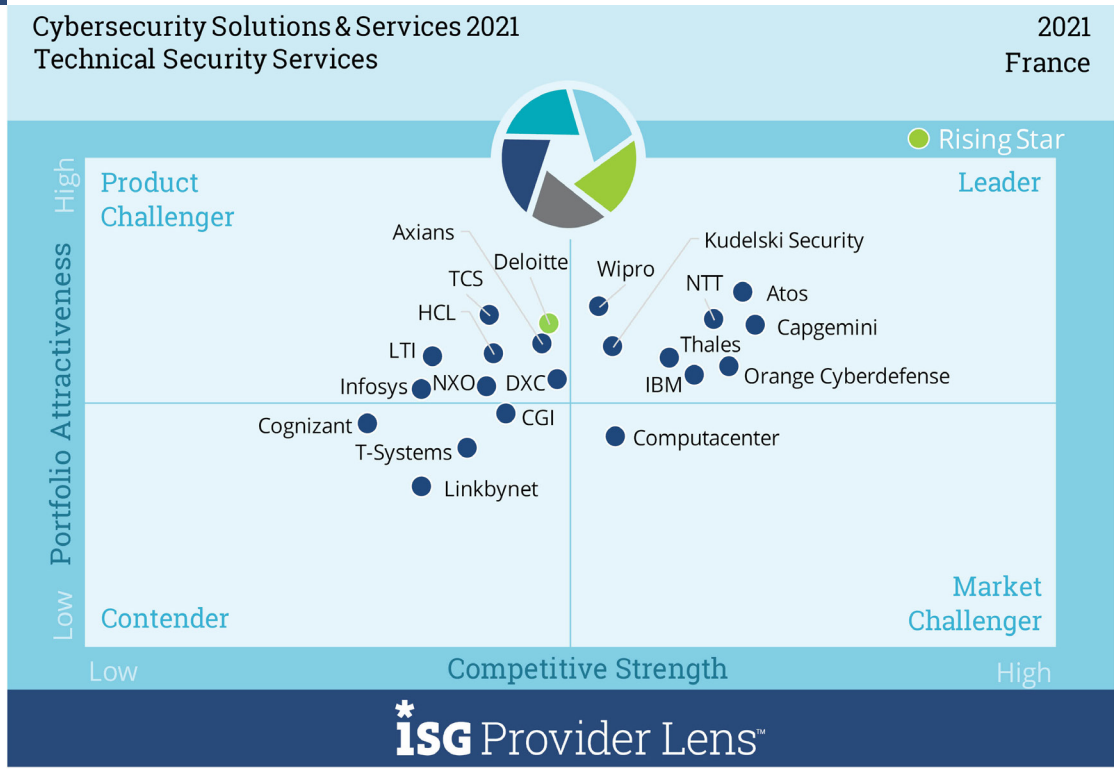
Chief strategy officers should read this report to understand the relative positioning and capabilities of service partners to collaborate with and develop an effective cybersecurity strategy.

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

TECHNICAL SECURITY SERVICES

Definition

This quadrant examines service providers that are not exclusively focused on their respective proprietary products, and can implement and integrate other vendor products or solutions. TSS covers integration, maintenance and support for IT security products or solutions, and encompasses all security products, including anti-virus, cloud, and data center security, IAM, DLP, network security, endpoint security, unified threat management (UTM) and others.



Source: ISG Research 2021

TECHNICAL SECURITY SERVICES

Eligibility Criteria

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

Observations

Software vendors rely on service partners to install, configure and integrate their solutions. It is often the service partner that closes the sale, using the pre-sales team of a vendor to provide product information. Service partners retain client relationships and have trusted consultants to estimate capacity and system requirements. Security products require high-performing appliances and complex cloud and network configurations. The service partners' consultants design the implementation architecture and project plan, and choose the appliance models and software versions to match client requirements.

Clients procuring security solutions should check if service partners are available locally to provide the requisite engineering, architecture and integration. The procurement process must bundle software, hardware and service partners in a balanced manner to ensure long-term service support. They may require immediate support from a robust service partner to address a data breach or a cyberattack.

TECHNICAL SECURITY SERVICES

Observations (cont.)

France has strict data protection regulations other than the GDPR. Clients seeking security software and partners in the country should first understand the regulations that apply to them to include the necessary certifications.

This quadrant evaluates the service providers with respect to their vendor partnerships. More than 200 security software vendors were identified. The top 10 vendors that have a strong ecosystem are Cisco, Palo Alto Networks, Broadcom, CheckPoint, F5 Networks, Fortinet, Microsoft, Cyberark, IBM and McAfee.

A service partner in France typically associates with 25 security vendors. This diversity enables its technical security experts to advice clients on the best solution configuration. For an unbiased and broad solution design, clients should note that the organizations assessed in the Strategic Security Services quadrant are vendor independent.

Among the 83 participants in this study, 21 have qualified for this quadrant. Eight are Leaders and one is a Rising Star.

- **Atos** leverages Alsaac, its proprietary cloud ready AI platform for deep detection and faster time response. The company has a strong partner base for integration services, making it a Leader in TSS.
- **Capgemini's** diverse TSS portfolio; tools; expertise in integration, maintenance and support; and ability manage scale across implementation and integration engagement are some of its strengths.
- **IBM's** global presence, partner ecosystem, ability to offer scalable integration and technological leadership makes the company a Leader.
- **Kudelski Security** is a security specialist that provides technology services, including assessments, architecture and design, rationalization, solution implementation, automation and orchestration, security tuning and optimization.
- **NTT** has robust operations in Europe and a broad cybersecurity portfolio. It has consolidated its technology expertise, including the acquired companies, namely, Everis, Capside, Itelligence, Arkadin, Transatel and Dimension Data, making it a Leader in MSS.

TECHNICAL SECURITY SERVICES

Observations (cont.)

- **Orange Cyberdefense** takes an intelligence-led approach to cybersecurity. The company has invested in innovation and has a large set of certifications and partnerships. This makes the company a player to watch out for in TSS.
- **Thales** leverages its national security expertise to enable high security standards for companies in all industry verticals.
- **Wipro** has developed in-house frameworks for identity, data privacy, risk governance and vulnerability management. The company focuses on strengthening its ties with partners and offers a spectrum of TSS that makes it a Leader.
- **Deloitte** offers comprehensive customized solutions, thought leadership in cybersecurity and has a large partner base, making the company the Rising Star in this quadrant.

ORANGE CYBERDEFENSE

Overview

Orange has extensive experience in providing TSS. In 2019, it acquired SecureData (U.K.) and SecureLink (US). Orange Cyberdefense has 2,500 security experts, 11 cyber SOCs, 18 SOCs and four computer emergency response teams (CERTs). It operates in 20 countries, supporting 8,000 customers worldwide (including many midmarket clients). Orange Cyberdefense has 43 technology partners, and a large client base is in France.

Strengths

The highest accreditations: Orange Cyberdefense is the only Cisco Master Security Partner in France. It has the highest accreditation from nine other security vendors, and a partner network of 43 technology vendors. It is a founding partner of the Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA). Orange Cyberdefense holds a security visa issued by ANSSI, qualifying it as an Information Systems Security Audit Service Provider (PASSI). Its engineers have 400 certifications. With its reseller authorizations, Orange Cybersecurity has over 1,000 technical and commercial accreditations.

Superior execution capacity in France: Orange Cyberdefense delivers more than 500 projects, each year. In France, it has over 500 security engineers and project managers, and more than 1,500 customers of all sizes. With a deep understanding of the peculiarities of this market and a vast technology portfolio, its experts provide clients with a variety of options for their security requirements and ensure an efficient delivery.

Extensive portfolio: Orange Cyberdefense provides all IT security implementation services, including advanced threat intelligence and SIEM integration. Security integration includes data center, hybrid and private cloud, networks, workstations, email/collaboration and mobile. It also covers IIoT and operations technology (OT) security. It has more than 100 operational technology/IIoT experts to support industry 4.0.

Caution

Orange Cyberdefense can improve its portfolio attractiveness in the areas of integration handover to enterprise clients that operate its security technology.

2021 ISG Provider Lens™ Leader

With a wide network of security technology partners, Orange Cyberdefense is well positioned to serve enterprise clients of any size across France.

ENTERPRISE CONTEXT

Strategic Security Services

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

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

COVID-19 forced many enterprise clients to operate remotely, but the quick turnaround with the right cybersecurity strategy helped customers to swiftly shift the operating model to working from anywhere (WFA).

With rising privacy regulations, GDPR laws and breaches, the need for strategic services has increased with service providers and enterprises securing more expertise around the frameworks, assessments and architectures. With additional regulations required by the French government, the service providers strive to improve their portfolio by hiring new talent, expanding their offerings and acquiring niche boutique firms, thereby helping enterprise customers to stay compliant.

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

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

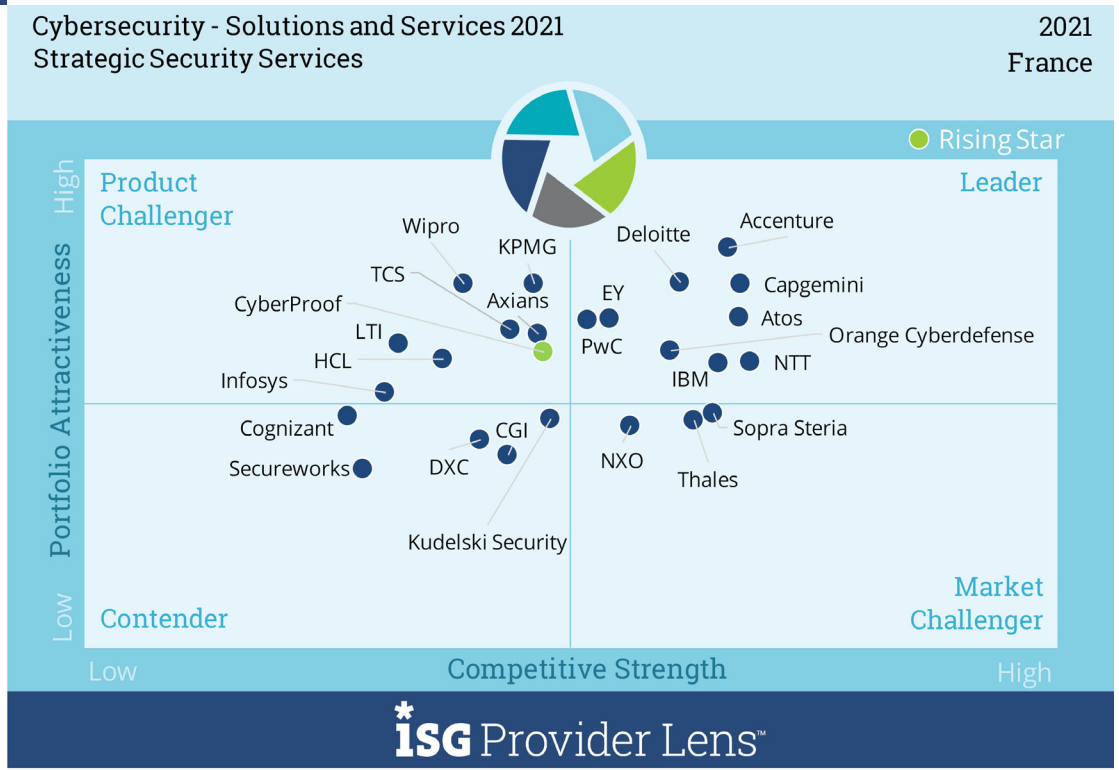
Chief strategy officers should read this report to understand the relative positioning and capabilities of service partners to collaborate with and develop an effective cybersecurity strategy.

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

STRATEGIC SECURITY SERVICES

Definition

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



Source: ISG Research 2021

STRATEGIC SECURITY SERVICES

Eligibility Criteria

- The provider should demonstrate abilities in the areas of strategic security services such as evaluation, assessments, vendor selection, architecture consulting and risk advisory.
- The provider should offer at least one of the strategic security services in the respective country.
- The provider should have the ability to offer security consulting services using frameworks will be an advantage.
- The provider shouldn't be exclusively focused on proprietary products or solutions.

Observations

As trust, data protection and privacy considerations are included in all conversations and business decisions, strategic consulting firms increasingly focus on cybersecurity by acquiring expertise around cyber technology architecture and conducting vulnerability assessments as a part of the risk and compliance consulting practice. These companies are hiring specialists and announcing new service offerings.

Governance, risk and compliance (GRC), which were once strictly focused on business factors, now cover cybersecurity because of the cost and brand credibility implications of a data breach or a ransomware attack.

France's regulations have additional particularities. ANSSI (Agence nationale de la sécurité des systèmes d'information) is the principal market regulator. It provides guidance, regulates certain activities such as auditing, and certifies software products such as identity authentication tools. Under the strictly regulated environment, consulting firms in the country have developed additional expertise to help clients stay compliant.

The pandemic has forced security managers (CISOs) to reevaluate their capabilities to weather future systemic risk events. CISOs are broadening the aperture of external events within a risk management plan. Risk quantification has become a way for CISOs to prioritize what to do and where to invest to manage risks and protect an enterprise.

STRATEGIC SECURITY SERVICES

Observations (cont.)

Enterprise security spending, per user, has increased by more than 20 percent between 2019 and 2020, and is likely to increase further in 2021. Budget rationalization will soon be needed, and management asks for maturity assessments to justify investments. As an example of cost optimization, some enterprises are looking at global delivery model for managed security services, IAM and GRC.

Among the 83 service providers assessed in this study, 25 qualified for this quadrant. Nine are Leaders and one is a Rising Star.

- **Accenture's** market presence in the security led strategy, risk and advisory services resonates well with enterprises, making it a Leader in SSS.
- **Atos** is known for its broad services portfolio and sound understanding of emerging technologies. The company has a large ecosystem of partners and, combined with its services, is one of the leading companies in the region for SSS.
- **Capgemini's** base of skilled resources, coupled with strong consulting expertise and strategic security advisory focus make it a Leader.
- **Deloitte** offers a balanced mix of technical, strategic and risk-based Cybersecurity solutions, which is backed by its extensive strategic consulting and risk advisory expertise.
- **EY's** vast range of Cybersecurity services, combined with strong GRC and audit capabilities, make it a Leader in France. .
- **IBM** leads in the security and related strategy areas based on its technical proficiency in AI, services-led framework and innovative technologies.
- **NTT** leverages innovative, proprietary tools, threat-intelligence driven approach and platforms alongside its strong partner network to deliver strategic transformation to clients.
- **Orange Cyberdefense** offers a good mix of innovation-led design, implementation approach, and a broad base of services.
- **PwC's** established advisory and consulting practice, extensive expertise in M&A and network of cybersecurity facilities make it a Leader.
- **CyberProof,** the Rising Star, is a subsidiary of UST Global and leverages its global footprint with a pragmatic approach, applying sophisticated technologies, including AI, to rapidly deploy cybersecurity measures.

ORANGE CYBERDEFENSE

Overview

Orange Cyberdefense has 2,500 security experts, 11 cyber SOCs, 18 SOCs and four computer emergency response teams (CERTs). The company's CERT offers services such as cybercrime prevention and threat intelligence. Its proprietary threat intelligence services use more than 500 public and private sources, including partnerships with governments and intelligence agencies such as the Europol. It provides vulnerability assessments and consulting around protection, defense and compliance.

Strengths

Superior capacity in France: Orange Cyberdefense has its largest footprint in France, in terms of number of security experts and enterprise clients. Its privileged market position enables it to identify new security threats well in advance. SensePost is its cyber consulting arm, with a renowned ethical hacking team dedicated to uncovering vulnerabilities. It has helped governments and enterprises review their security measures to stay ahead of evolving threats. In 2020, Orange announced a €1.5 billion investment in skills development and the launch of the Centre de Formation d'Apprentis (CFA). In 2019, its work-study training included more 3,500 apprentices.

Fit for clients of all sizes: Orange Cyberdefense has a sophisticated cybersecurity practice to assess multinational enterprises and validate their security strategies. It also has structured approaches, based on consistent methodologies, to offer cybersecurity. Its flexibility is unique compared with leading providers of SSS in France.

Comprehensive portfolio: The company's cybersecurity practice covers business risk and compliance, mobile, digital workplace security and network security, and is extending this expertise to IIoT and operational technology security. It has more than 100 OT/IIoT experts dedicated to industry 4.0. The company can design new solutions in response to new threats, such as the ones revolving around OT security, and provide vulnerability assessment and resolution. Orange Cyberdefense's CERT supplements its strategic service offerings.

Caution

Orange Cyberdefense may need more time to consolidate the organizational changes expected following mergers. In the meanwhile, clients should be clear about contractual clauses to prevent key consultants from being transferred to other projects or locations before they fully execute delivery.

2021 ISG Provider Lens™ Leader

Orange Cyberdefense provides clients with multiple alternatives in cybersecurity solutions to cover all aspects of protection, defense and compliance.

ENTERPRISE CONTEXT

Managed Security Services Large Accounts

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

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

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

Managed security service providers (MSSPs) established their own, dedicated, comanaged or virtual SOCs within the region to serve the enterprises. The managed security services (MSS) market in France is mainly driven by the growing need for security solutions across various end-user industries. Additionally, increased spending by the government on security solutions and growing concerns over breach of intelligence data are further expected to foster the market growth. Regulation and compliance pressure will increase the demand for MSS in the region.

France is an established market for security service providers. MSS is becoming increasingly popular in the country. Enterprises in France evaluate providers based on their ability to provide specialized and highly skilled resources locally as part of their service engagements.

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

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

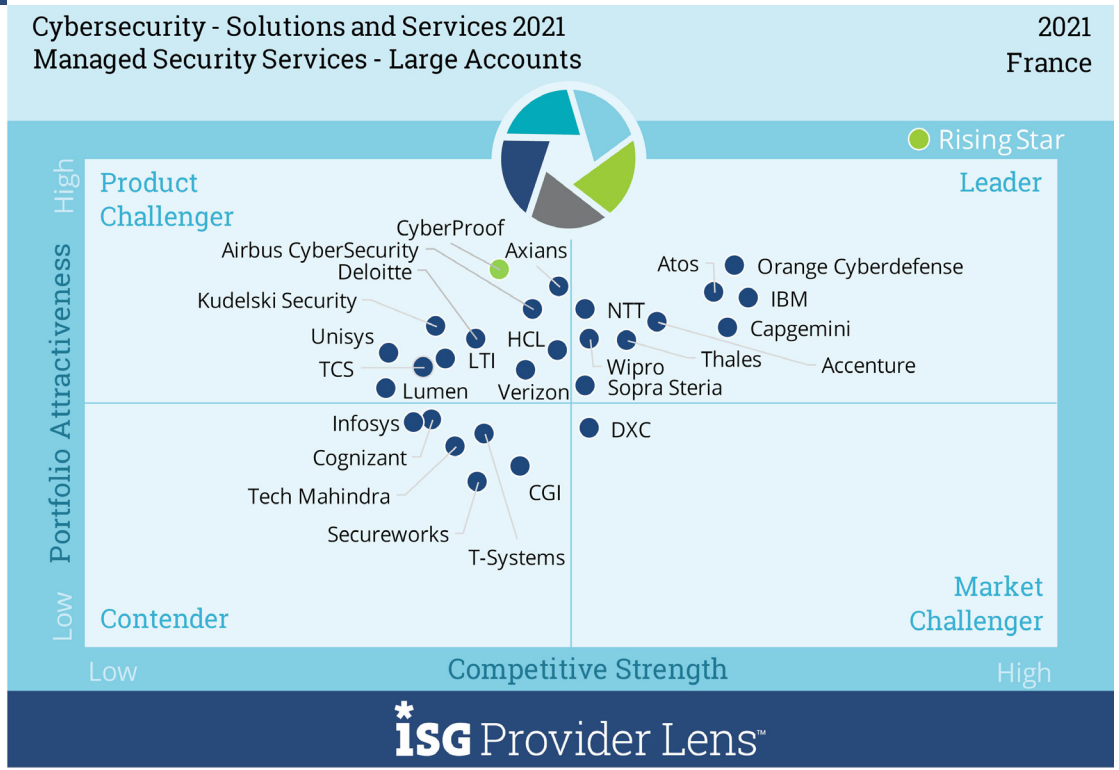
Chief technology officers (CTOs) handling operations and services should read this report to acquire in-depth knowledge on emerging technologies and solutions to gain strategic directions as well as partnership options with relevant service providers. CTOs can also ensure the deployment of appropriate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

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

MANAGED SECURITY SERVICES LARGE ACCOUNTS

Definition

MSS comprises the operations and management of IT security infrastructures for one or several customers by a security operations center. Typical services include security monitoring, behavior analysis, unauthorized access detection, advisory on preventive measures, penetration testing, firewall operations, antivirus operations, IAM operation services, DLP operations and all other operating services to provide ongoing, real-time protection, without compromising business performance. 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.



Source: ISG Research 2021

MANAGED SECURITY SERVICES LARGE ACCOUNTS

Definition (cont.)

This quadrant assesses a service provider's ability to offer management services to large enterprise clients. These clients usually run operations in many countries, with a broad network with a large number of secure endpoints. They are the preferred targets of hackers and data breaches because of the value of their assets and their financial capacity to pay off ransomware. This group also includes banking, financial services, insurance, healthcare organizations and other enterprises that must comply with strict regulations. To support these companies, service providers in this space provide many security tools and superior threat identification technologies.

Eligibility Criteria

- The provider should have the ability to provide security services such as detection and prevention; SIEM; and security advisor and auditing support, remotely or at a client's site.
- The provider should be relevant, in terms of revenue and number of customers, as an MSS provider in the respective country.
- The provider should not be exclusively focused on proprietary products but can manage and operate best-of-breed security tools.
- The provider should possess accreditations from vendors of security tools.
- The provider's SOCs are ideally owned and managed by the provider and not predominantly by partners.
- The provider should maintain certified staff, for example, with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC).

MANAGED SECURITY SERVICES LARGE ACCOUNTS

Observations (cont.)

The shortage of security skills worldwide is creating a booming business for managed security service providers (MSSPs). ISG expects an increasing use of security consulting services over next 24 months, with a focus on new pricing and delivery models such as intellectual property/value-based and consulting as a service. The security services market is responding. Some by organically building next-generation cyber services, and some by acquiring the same. Recently, Atos acquired Motiv ICT and In Fidem, Deloitte acquired R9B and Wipro acquired Ampion. ISG expects to see many more M&A in 2021.

Managed security services are evolving from security operations centers (SOCs) to complex, AI-powered cyber defense army-like organizations. SOC services typically include monitoring the alerts generated by security appliances such as firewalls, endpoint security tools, network routers, anti-malware software and other event monitoring tools. Companies cannot lower their defenses, and SOCs continue to have a role in the cybersecurity scene. However, they provide basic security that is not adequate to circumvent more sophisticated threats.

Cyber criminals around the world are using AI tools to automate threat creation, for web scanning and for malware distribution. They sell their expertise and tools through cyber commerce in the dark web. Sophisticated criminal organizations are continuously improving their capabilities around fraud, subversive schemes, espionage and theft of valuable information.

Enterprises need to adopt more sophisticated tools to defend themselves. Cyber defense centers (CDCs) have emerged, not to replace SOCs but to expand security operations. These CDCs leverage advanced machine learning (ML) tools that can handle large volumes of data and use smart analytics to understand how threats are morphing, moving and spreading. They share information dynamically with other CDCs to keep pace with the rise in cybercrime. New tools, such as micro segmentation that can isolate hackers or bots when they break into an enterprise network, have emerged. Extended detection and response (XDR) platforms use analytics and automation to accelerate and simplify detection and response. Services around identity management (IdM) governance and data protection that help clients audit access, manage segregation of duties, and produce evidence of implementing protection measures prior to a data breach, help in reducing the consequences and any subsequent penalties. Managed cybersecurity services have become essential for enterprises.

MANAGED SECURITY SERVICES LARGE ACCOUNTS

Observations (cont.)

Companies procuring MSS should look into the tools their proponents have in place. The integration with threat intelligence sources is of increasing importance. Organizations should pay attention to service-level agreements (SLA). A typical security service SLA involves 15 minutes of response time (to start working on the incident) and four hours of resolution (eliminating the problem). These measures are sufficient to tackle internal incidents such as patching a desktop, changing a firewall rule or fixing an AWS S3 bucket misconfiguration. However, in the event of a cyberattack, 15 minutes to react is enough time for a ransomware cyber bot to reach an unrecoverable point. Enterprises need to rethink their service expectations and focus on building innovative deals. Service providers should immediately allocate the necessary resources without considering the risk of not getting paid or being penalized for not meeting SLAs. Timed SLAs are meaningless in the provision of security services. New deals should impose penalties for the lack of available skills, malfunctioning tools, indolent behavior and not acting on attacks. Quick decision making is crucial to stop an attack. As an attack evolves, more resources are required, and costs go up. A balanced deal allows for additional resource allocation while sharing the risk with the provider that should not bill for overtime, tool usage, licenses and indirect costs.

France's regulations have additional specifics. Agence nationale de la sécurité des systèmes d'information (ANSSI) is the principal market regulator in the country. In this strictly regulated environment, some large enterprises and government agencies may require ANSSI certified prestataire de détection des incidents de sécurité (PDIS). So far, only the following five companies have this accreditation:

- Airbus Cybersecurity (Airbus CyberSecurity SOC PDIS)
- Capgemini Technology Services (SOC PDIS: Service de détection et de supervision de sécurité)
- Orange (Security Event Intelligence - PDIS)
- Sopra Steria Infrastructures and Security Services (SOC PDIS by Sopra Steria)
- Thales SIX GTS France (Thales CyberSecurité SOC PDIS)

MANAGED SECURITY SERVICES LARGE ACCOUNTS

Observations (cont.)

Among the 83 companies assessed in this study, 27 have qualified for this quadrant. Nine are Leaders and one is a Rising Star.

- **Accenture's** acquisition of Context Information Security, along with its management consulting background, research focused approach and partner ecosystem makes it a Leader.
- **Atos** differentiates itself with the proprietary AI-driven Alsaac platform, intelligence led SOCs and flexible delivery models for MSS.
- **Capgemini** is a large Paris-based global technology consultancy. The company's dedicated network of Cyber Defense Centers (CDCs), flexible delivery model and advanced threat hunting capabilities are some of its strengths.
- **IBM's** leadership in applications and infrastructure, coupled with acquisitions and research led strong cybersecurity portfolio services make it a Leader.
- **NTT** has robust operations in Europe and a broad cybersecurity portfolio. It has consolidated its technology expertise, including the acquired companies — Everis, Capside, Itelligence, Arkadin, Transatel and Dimension Data — making it a leader in MSS.
- **Orange Cyberdefense's** strength lies in its extensive base of proprietary assets, most of which are developed in-house. The company takes an intelligence led approach to security that is backed by a strong base of certified analysts. This makes Orange Cyberdefense a Leader in MSS.
- **Sopra Steria** has a good market footprint in France, leveraging its PDIS certified SOC.
- **Thales** leverages its national security expertise to enable high security standards for companies in all industry verticals.
- **Wipro's** broad MSS portfolio, HOLMES-led SOC automation, Cyber Defense Platform, wide industry presence and analytics leadership makes it a Leader in France.
- **CyberProof**, the Rising Star, proposes an innovative cloud-native cyber defense platform, providing a built-in virtual analyst, transparent automation, orchestration and centralized view of security operations.

ORANGE CYBERDEFENSE

Overview

Orange Cyberdefense has 2,500 security experts in 20 countries, supporting 3,700 large accounts and increasingly addressing midmarket clients. It acquired SecureData and SecureLink in 2019. It has a large client base in France, with revenue of around €770 million in 2020. Orange Cyberdefense has 11 CyberSOCs, 18 SOCs and four computer emergency response teams (CERTs) across the globe to provide sales and services support in 160 countries, via Orange Business Services.

Strengths

Large scale in France: Orange's network reaches 36,000 municipalities in France. Orange Cyberdefense monitors a global network, enabling it to identify new threats as soon as they appear. In France, it has one CERT, two SOCs to respond to incidents and two CyberSOCs to focus on the analysis and remediation of new threats. Two scrubbing centers provide response to distributed denial of service (DDoS) attacks. One scrubbing center in the U.S.; three CERTs in Canada, Poland and Singapore; 16 SOCs; and nine CyberSOCs supplement its global capacity.

Comprehensive portfolio: Orange Cyberdefense offers event monitoring (MDR), incident monitoring, incident response, threat intelligence, intrusion detection and defense services. Red teams discover and strengthen client security, and blue teams circumvent attacks. IAM, DLP, mobility and operational technology/IIoT are a part of its services. In 2019, the company contained 29,000 security incidents from 263,000 alerts detected.

Source of threats knowledge: Orange Cybersecurity threat research organization has more than 25 years of experience, and is supported by 250 researchers and analysts. The company's proprietary threat intelligence uses more than 500 public and private sources. Orange Cyberdefense is widely known and featured at industry conferences, including Infosec, Manchester DTX, RSA, Black Hat and DefCon.

Recognized through certifications: Orange Cybersecurity is one of five companies certified by the ANSSI for incident detection (Security Event Intelligence – PDIS).

Caution

Orange Cyberdefense plans to optimize processes to eliminate redundancies within the acquired companies, which may impact its organizational structure. Clients from the acquired companies, SecureData and SecureLink, may have to adapt to new service terms and service support channels.

2021 ISG Provider Lens™ Leader

Orange Cyberdefense offers global protection to large enterprises, while maintaining local support through its extensive presence in the French territory.

ENTERPRISE CONTEXT

Managed Security Services Midmarket

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

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

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

Managed security service providers (MSSPs) established their own, dedicated, comanaged or virtual SOCs within the region to serve the enterprises. The managed security services (MSS) market in France is mainly driven by the growing need for security solutions across various end-user industries. Additionally, increased spending by the government on security solutions and growing concerns over breach of intelligence data are further expected to foster the market growth. Regulation and compliance pressure will increase the demand for MSS in the region.

France is an established market for security service providers. MSS is becoming increasingly popular in the country. Enterprises in France evaluate providers based on their ability to provide specialized and highly skilled resources locally as part of their service engagements.

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

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

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

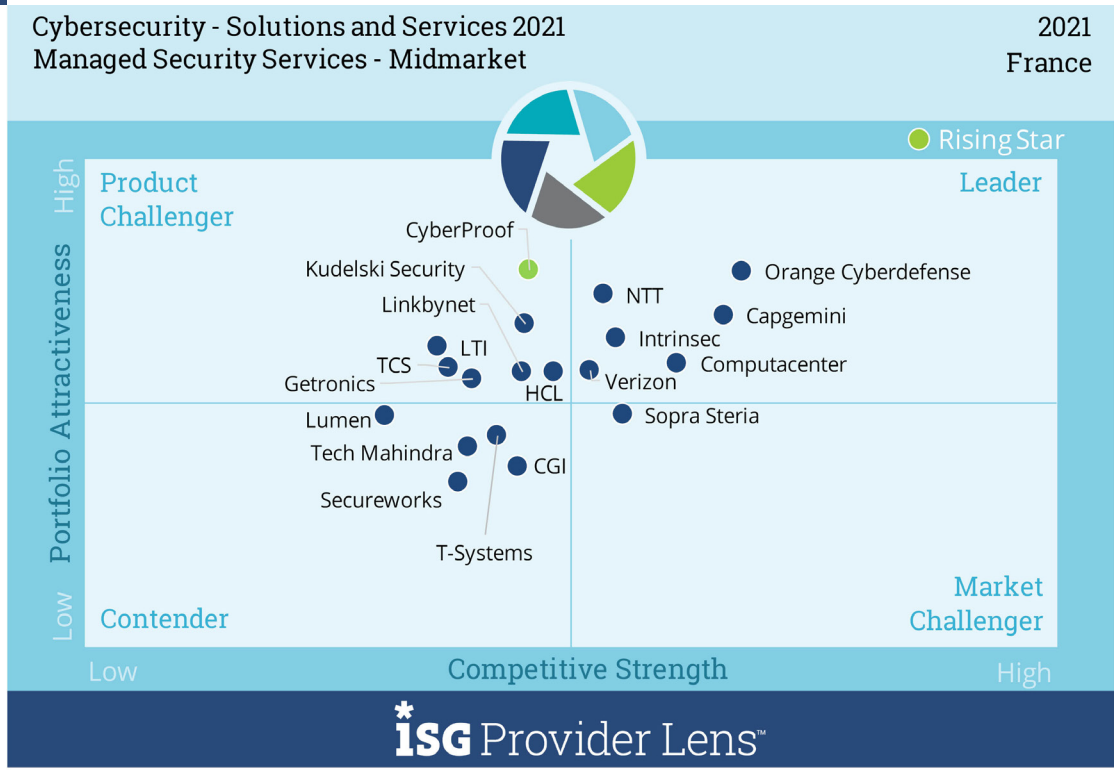
Security leaders should read this report to understand the relative positioning and capabilities of MSSPs. The report also compares the technical capabilities of various service providers in the market.

MANAGED SECURITY SERVICES MIDMARKET

Definition

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

The midmarket includes companies that are growing into large enterprises, but have not achieved the same size and complexity. Typically, these companies have less than 5,000 employees or make less than US$1 billion in revenue. Service providers in this market have a strong sales focus and suitable delivery structures to respond to midmarket needs.



Source: ISG Research 2021

MANAGED SECURITY SERVICES MIDMARKET

Eligibility Criteria

- The provider should have the ability to provide security services such as detection and prevention; SIEM; and security advisor and auditing support, remotely or at the client site.
- The provider should be relevant, in terms of revenue and number of customers, as an MSS provider in the respective country.
- The provider shouldn't be exclusively focused on proprietary products but can manage and operate best-of-breed security tools.
- The provider should possess accreditations from vendors of security tools.
- The provider's SOCs are ideally owned and managed by the provider and not predominantly by partners.
- The provider should maintain certified staff, for example, as CISSP, CISM and GIAC.

Observations

Midsize businesses are unable to compete or even afford sophisticated SOCs to keep up their security posture, and are reaching out to MSSPs to help with everything, including, monitoring, response and hunting. Some service providers that focus on the midmarket generate significant revenues and leverage high-scale automation and AI threat intelligence to provide monitoring and protection services at competitive prices. Others have a deep specialization, which compensates for scale and is in proximity to clients. ISG expects an increase in hybrid delivery models and a local presence to help address local challenges.

"Security by design" is a recurring theme. The term was coined for software development, referring to best practices of software engineering to avoid constructions that allow hackers to exploit the code and access the database. Many service providers like to emphasize the need to adequately secure the enterprise network and its integration to the public cloud and the users' access to SaaS solutions. In practical terms, it means replacing security tools. Service providers offer a bypass, claiming their managed security platform is ready to use, thus eliminating the need for expensive technology upgrades. The compelling "security by design" is more secure than the tools it is replacing. However, these tools still require considerable analyst expertise to block cyberattacks. For most companies ranked in this study, the technology behind the service provides market differentiation, but clients should recognize that people are still essential to provide security.

MANAGED SECURITY SERVICES MIDMARKET

Observations (cont.)

A typical MSS provider has four analysts for each client, which indicates the difficulty in scaling the security service. It involves a person watching a monitor throughout, on a rotation basis of three shifts to provide 24-by-7 services. Automation and AI provide effectiveness rather than scale. The exceptions to the rule are the network service providers, such as Orange, Verizon, CenturyLink and NTT, which leverage their network operations centers to capture threats and produce an automated response that is distributed throughout their centers around the globe.

As security requires significant expertise, staff shortage is a concern for most enterprises. It is difficult for a midsize enterprise to retain cybersecurity experts. Service providers address this concern by allowing midmarket clients to leverage highly skilled practitioners.

Among the 83 companies assessed in this study, 19 have classified for this quadrant. Six are Leaders and one is a Rising Star.

- **Capgemini** is a large Paris-based global technology consultancy. The company's dedicated network of CDCs, flexible delivery model and advanced threat hunting capabilities are some of its strengths.
- **Computacenter's** regional presence, coupled with its multi-tower IT expertise and strong MSS practice, comprising wide security and MDR coverage, makes it a Leader.
- **Intrinsec**, is well positioned in the midmarket in France, and provides managed services, vulnerability assessments, consulting and training on cybersecurity.
- **NTT** has robust operations in Europe and a broad cybersecurity portfolio. It has consolidated its technology expertise, including the acquired companies, namely, Everis, Capside, Itelligence, Arkadin, Transatel and Dimension Data, making it a Leader in MSS.
- **Orange Cyberdefense's** strength lies in its extensive base of proprietary assets most of which are developed in-house. The company takes an intelligence-led approach to security that is backed by a strong base of certified analysts. This makes Orange Cyberdefense a Leader in MSS.
- **Verizon's** large information and communications technology footprint and intelligence-led approach to security, make it a dominant MSS provider in Europe.
- **CyberProof,** the Rising Star, proposes an innovative cloud-native cyber defense platform, providing a built-in virtual analyst, transparent automation, orchestration and centralized view of security operations.

ORANGE CYBERDEFENSE

Overview

Orange Cyberdefense has 2,500 security experts, 11 CyberSOCs, 18 SOCs and four computer emergency response teams (CERTs). The company's four CERTs offer services such as cybercrime prevention and threat intelligence. Its proprietary threat intelligence services use more than 500 public and private sources, including partnerships with governments and intelligence agencies such as the Europol. The company has security experts in Paris, Rennes, Marseille, Lyon, Lille and Toulouse.

Strengths

Countrywide presence: Orange's network reaches 36,000 municipalities in France. The company monitors a global network, identifying new threats as soon as they appear. Two SOCs manage technology-focused ITIL processes and two CyberSOCs detect and respond to incidents. Two scrubbing centers provide response to DDoS attacks, whereas Orange's CERT/CSIRT provides additional intelligence to remediate attacks.

Client proximity and focus on people: Orange Cyberdefense is focused on advanced technologies with the belief that it empowers, along with focusing on experienced personnel as they have a deep understanding of the operating landscape. With this belief, the company has a special focus on attracting and retaining talent. It has partnerships with universities and vendors such as Microsoft to provide education and training. The strong focus on people enables it to address skills shortage, provide clients with access to knowledgeable professionals and enhance customer intimacy.

Comprehensive portfolio: Orange Cyberdefense offers event monitoring (MDR), incident monitoring, incident response, threat intelligence, intrusion detection and defense services. Red teams discover and strengthen clients' protection and blue teams circumvent attacks. IAM, DLP, mobility and operational technology/IIoT are included in its offerings, while CERTs and threat intelligence sources supplement its offering. In 2019, the company contained 29,000 incidents from 263,000 alerts detected.

Recognition by way of certifications: Orange Cyberdefense is one of the five companies certified by the ANSSI for incident detection (Security Event Intelligence – PDIS).

Caution

Orange Cyberdefense has many clients in the midmarket. However, its wide portfolio increasingly leverages AI incident detection and threat response services that are difficult to downscale for midsize companies. AI-services are available to midmarket clients on an ad-hoc basis.

2021 ISG Provider Lens™ Leader

Orange Cyberdefense provides advanced technologies and a robust threat response, offering world-class security to midmarket clients.

Methodology

METHODOLOGY

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

The study was divided into the following steps:

1. Definition of 2021 ISG Provider Lens™ Cybersecurity – Solutions & Services French 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

Benoît Scheuber, Author

Consulting Manager and Security Analyst

Senior and highly respected consultant in the fields IT and security operations, Benoit has conducted many projects for large clients including contract negotiations, IT assessments and security benchmarks where he was responsible for the content and quality of delivery of client-facing work. Benoît brings his experience in both the providers offerings and the market.

Srinivasan PN, Author

Senior Analyst

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

Authors and Editors

Jan Erik Aase, Editor

Director and Principal Analyst

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 advisor and analyst. Jan Erik has overall accountability for the ISG Provider Lens™ reports, including both the buyer-centric Archetype reports and the 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™ | Quadrant Report
September 2021

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