ISG Provider Lens™

Cybersecurity – Solutions and Services

Identity and Access Management (IAM)

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

Atos

QUADRANT REPORT | JULY 2022 | FRANCE

Table of Contents

Report Author: Benoît Scheuber, Dr Maxime Martelli

Cybersecurity – an ongoing challenge for sovereignty

General Trends

Unlike in other European countries (for example, DACH, the U.K. and the Nordics), large global security players have a limited presence in France. Local customers expect security services to be delivered locally and in French, and they are not usually accepting of offshore nor nearshore delivery.

The importance given to service in French places France-based managed security service providers (MSSPs) in the best position to be selected by French customers.

In addition to the new ways of working, driven by the COVID-19 pandemic, ISG has observed changes in the purchase of security services in France. Many are now focused on digital transformation to meet their changing business needs — cloud adoption, hybrid environments and other emerging technologies. The consequent expansion of the IT landscape to new environments is also increasing attack surfaces, compelling clients to seek next-generation security services such as advanced cloud security.

While security expenditure continues to increase, the pandemic has forced some French companies to renegotiate security contracts in parallel to reduce their spending. At the same time, because of the compliance requirements of stringent data-related regulations, among other security areas, some companies have

French Security Market is growing at a fast rate.

chosen to outsource their compliance needs. MSSPs that offer such services are therefore popular in France.

With the increasing complexity of cyberattacks and the evolving global threat landscape, organizations of all types and sizes are compelled to make conscious efforts to protect their critical data and infrastructure. They are asking for next-generation security services, such as Zero Trust Network Access (ZTNA), full or partial secure access service edge (SASE), or resilience.

In addition to the standard evolution of IT, local industries are now even more actively pushing for MSSPs to secure their operations technology (OT) and Internet of Things (IoT) with companies such as EDF. The largest multinational electric utility company in France, EDF partners with providers to increase OT and IoT protection for critical infrastructure.

In the cybersecurity space, SASE is the new buzzword — a service that needs to be tailored specifically to a client, encompassing hybrid environment, cloud-first workloads and regional requirements, among other aspects. It includes many technical solutions such as data leakage/loss prevention (DLP), ZTNA and cloud access security broker (CASB).

Even though some players are rebranding their existing solutions as SASE, many others are adopting a new agile approach in integrating Zero Trust at the heart of their security architecture. At the same time, they are embracing cloud environment protection at the core, and not only as a copy and paste of on-premises solutions and services.

ISG has clearly observed this evolution in the cybersecurity market in France as providers have had to adapt their security posture and solution architecture to best answer clients' needs for next-generation security.

Identity and Access Management (IAM) Market Trends

Directly linked to the Zero Trust Model, the main evolution for IAM this year is to expand identity not only to people but to infrastructure as well. A Zero Trust Model is only as robust as the least robust element of the chain, and machines, in addition to people, need an identity to help CISOs and security teams tackle risks. IAM is now not only about protecting and monitoring people's identity, but also about protecting systems, applications, and even the ever-growing number of robots, like the ones used for robotic process automation (RPA).

Here, the solutions of providers without automated processes and management at scale will be seen as cumbersome. On the other hand, providers that enable an agile, decentralized and easily maintained architecture will stand out from the crowd.

The overall shift in focus of security from technology to business also highlights the importance of a smooth user experience for IAM users. Tools that blend transparently with the standard user interaction are more successful and are perceived as more attractive by decision-makers keen to reinforce security, while simplifying user connectivity.

Two of the trends from last year, namely, cloud IAM and identity as a service (IDaaS), continue to be relevant, with multi-tenancy remaining a regular ask from clients wanting to avoid vendor lock-in.

Data Leakage/Loss Prevention Market Trends

DLP solutions, whether they are deployed on-premises or are cloud-based, fall into three categories: network, endpoint and data center/storage.

Although the DLP and data security market in France is mature because of strict data regulations, such as the General Data Protection Regulation (GDPR), some new customers in France are increasingly adopting DLP.

One key growing industry for DLP in France is healthcare, where IT investment and digital transformation has not been a top priority until very recently. Because of growing breaches and cybersecurity incidents, and the core importance of the healthcare data, regulators had to increase the mandatory protection for both IT infrastructure and health-related data.

This growth brings many challenges, such as securing the vast landscape of medical devices from malicious attacks.

But this also makes securing sensitive data transparently a sought-after component for a successful Cloud Adoption Framework, that will reassure companies hesitant to embrace it.

The focus on digital transformation is enabling many small to midsize companies to embrace DLP as the new norm to protect their data efficiently.

With ever-increasing data sources, visibility into data flow and data lakes is of the highest importance, but this requires efficient data categorization to know the value and implement appropriate DLP strategies.

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

The main driver for market growth is the inability of employees to perceive the inherent risks of an unsecured Internet connection. In addition, the technical complexity of interfacing legacy infrastructure with the Internet is a challenge, but companies are investing in next-generation IT to alleviate some of those challenges.

Because advanced ETPDR and DLP are interdependent, their growth is often correlated, and companies will often demand both solutions to improve their security postures.

Technical Security Services Market Trends

The principal trend is the growing number of security solutions in France. 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, and ISG notes a trend where CISOs wish to decrease complexity and the attack surface by reducing the number of security solutions.

Strategic Security Services Market Trends

Trust, data protection and privacy considerations are now included in all conversations and business decisions. As a result, strategic consulting firms are increasingly focusing on cybersecurity by acquiring expertise around related technologies and architecture, and they are conducting vulnerability assessments as a part of their risk and compliance consulting practice. These companies are hiring specialists and announcing new service offerings.

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

Enterprise security spend per user increased by more than 10 percent between 2020 and 2021, and it is likely to increase further in 2022. Budget rationalization will soon be needed, together with management asks for maturity assessments to justify investments. For cost optimization, some enterprises are looking at a global delivery model for managed security services, IAM and GRC.

Managed Security Services for Large Accounts Market Trends

The shortage of security-related skills worldwide is creating a significant opportunities for MSSPs. ISG expects an increasing use of managed security services over the next 12 months. This trend is even more visible in France, where customers are used to relying on external partners for IT services.

The pandemic has amplified existing enterprise challenges such as alert overload and the lack of threat management capabilities. MSSPs are in the best position to respond to these issues. Their next-generation security services focus on threat investigation based on advanced analytics, threat detection powered by AI and machine learning, contextualized threat intelligence, and automated incident responses — all of which can help thwart the ever-growing attacks. MSSPs have also gained traction because of their ability to provide agility, scale and resilience. Enterprises are partnering with them for intelligence-led threat hunting and detection, orchestration, and automation of alerts that are underpinned by modular platform-led operations, reduced incident response times and cyber forensics.

Managed Security Services for the Midmarket Trends

Midsize businesses are unable to compete for or even afford sophisticated security operations centers to keep their security postures updated, and they are reaching out to MSSPs to help with everything, including monitoring, response and hunting. The service providers that focus on the midmarket generate significant revenue and leverage high-scale automation and AI threat intelligence to provide monitoring and protection services at competitive prices. Others have a deep specialization that 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.

Managed detection and response (MDR) has become a buzzword in the midmarket because of its modular service architecture and the ease with which clients can deploy it without forgoing their investments in security tools.

Executive Summary

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. Because 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 take advantage of highly skilled practitioners.

MSSPs without French offices or skills have a low chance of winning deals.

Provider Positioning

Page 1 of 13

	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	Leader	Leader	Leader	Not In
Advens	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger
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
Bechtle	Not In	Not In	Product Challenger	Not In	Not In	Not In	Contender

Provider Positioning

Page 2 of 13

	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
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
Blackberry (Cylance)	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Brainloop	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Broadcom	Product Challenger	Leader	Leader	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Not In	Not In	Contender	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader	Leader

Provider Positioning

Page 3 of 13

	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
CGI	Not In	Not In	Not In	Contender	Contender	Contender	Contender
Check Point	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Cisco	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Cognizant	Not In	Not In	Not In	Contender	Contender	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

Provider Positioning

Page 4 of 13

	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
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	Product Challenger	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★	Rising Star ★
Deloitte	Not In	Not In	Not In	Rising Star ★	Leader	Product Challenger	Not In
DXC Technology	Not In	Not In	Not In	Product Challenger	Contender	Contender	Not In
ESET	Not In	Not In	Contender	Not In	Not In	Not In	Not In

Provider Positioning

Page 5 of 13

	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
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	Contender	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	Contender

Provider Positioning

Page 6 of 13

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Google	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
HelpSystems	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Huge Networks	Not In	Not In	Contender	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader	Not In
Infosys	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Not In
Intrinsec	Not In	Not In	Not In	Not In	Not In	Not In	Leader

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
I-Tracing	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
ITrust	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Kaspersky	Not In	Not In	Product Challenger	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
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	Contender	Not In

Provider Positioning

Page 8 of 13

	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
Matrix42	Contender	Product Challenger	Not In	Not In	Not In	Not In	Not In
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
Mindtree	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Mphasis	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Netskope	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Nexus Group	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Nomios	Not In	Not In	Not In	Contender	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	Contender	Not In	Not In
Okta	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Leader	Leader	Leader	Leader

Provider Positioning

	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Palo Alto Networks	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In
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
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Saviynt	Contender	Not In	Not In	Not In	Not In	Not In	Not In
SCC	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In

Provider Positioning

Page 11 of 13

	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
Secureworks	Not In	Not In	Not In	Not In	Not In	Contender	Not In
senhasegura	Contender	Not In	Not In	Not In	Not In	Not In	Not In
SFR	Not In	Not In	Not In	Not In	Not In	Not In	Contender
Sophos	Not In	Contender	Leader	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Market Challenger	Leader	Leader
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

Provider Positioning

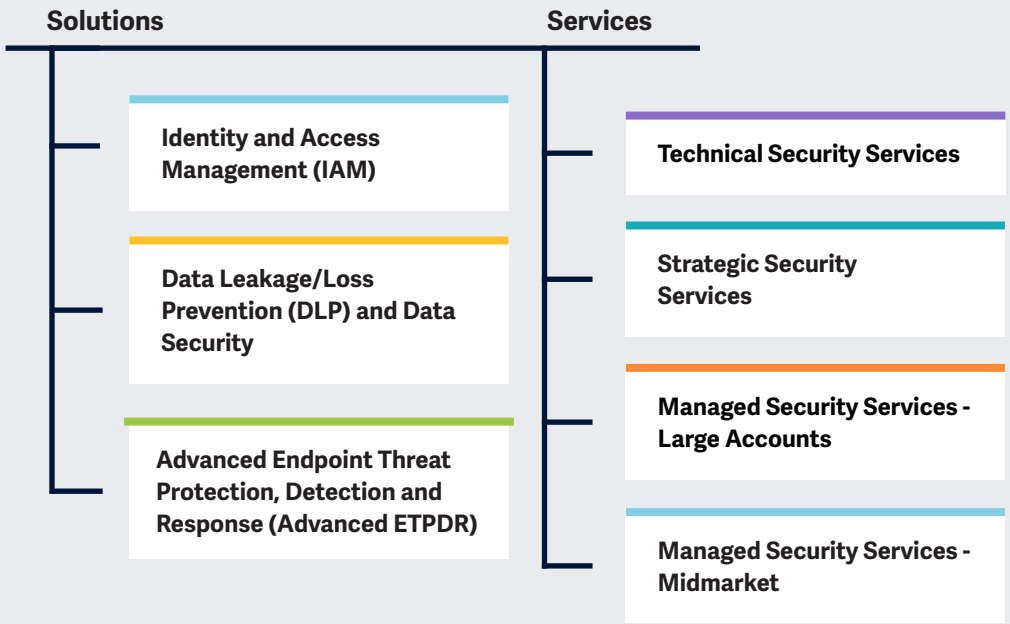
	Identity and Access Management (IAM)	Data Leakage/ Loss Prevention (DLP) and Data Security	Advanced Endpoint Threat Protection, Detection and Response (Advanced ETPDR)	Technical Security Services	Strategic Security Services	Managed Security Services - Large Accounts	Managed Security Services - Midmarket
Tech Mahindra	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Contender
Thales	Market Challenger	Not In	Not In	Leader	Market Challenger	Leader	Not In
Titus	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Product Challenger	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	Not In
Unisys	Market Challenger	Not In	Not In	Not In	Not In	Product Challenger	Not In

Provider Positioning

Page 13 of 13

	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
Varonis	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In
Verizon	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
VMware Carbon Black	Not In	Not In	Leader	Not In	Not In	Not In	Not In
WALLIX	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Contender	Not In	Not In
Wipro	Not In	Not In	Not In	Leader	Product Challenger	Leader	Not In
Zscaler	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In

This study focuses on what ISG perceives as **most critical in 2022** for Cybersecurity - Solutions and Services.



Simplified Illustration Source: ISG 2022

Definition

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

With the ever-changing threat landscape, enterprises need to take a detailed and inclusive approach to cybersecurity to safeguard their businesses by implementing a mix of security products and services across areas such as identity and access management (IAM), data leakage/loss prevention (DLP) and managed security services (MSS) to achieve a robust, secure framework to reduce risk exposure.

In addition to the need for self-protection, regulations such as the General Data Protection Regulation (GDPR) in Europe, and other regional compliances, have compelled businesses to implement robust safeguard measures to counter cyberattacks. Similar legislation exists in other countries such as Brazil and Australia to safeguard users from cyberthreats.

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

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

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following seven quadrants: 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) for Large Accounts; and Managed Security Services (MSS) for the Midmarket

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

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

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

Provider Classifications

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

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

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens quadrant may include a service provider 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).

(Continues on next page)

Provider Classifications: Quadrant Key

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

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

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

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

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

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

Identity and Access Management (IAM)

Who Should Read This

This report is relevant to enterprises across industries in France for evaluating providers' solutions that integrate multiple cybersecurity features, which address security concerns caused by changes in work patterns and increased digitalization.

In this quadrant report, ISG highlights the current market positioning of providers of identity and access management (IAM) solutions that can help reduce security threats for enterprises in France, and how each provider addresses the key challenges faced.

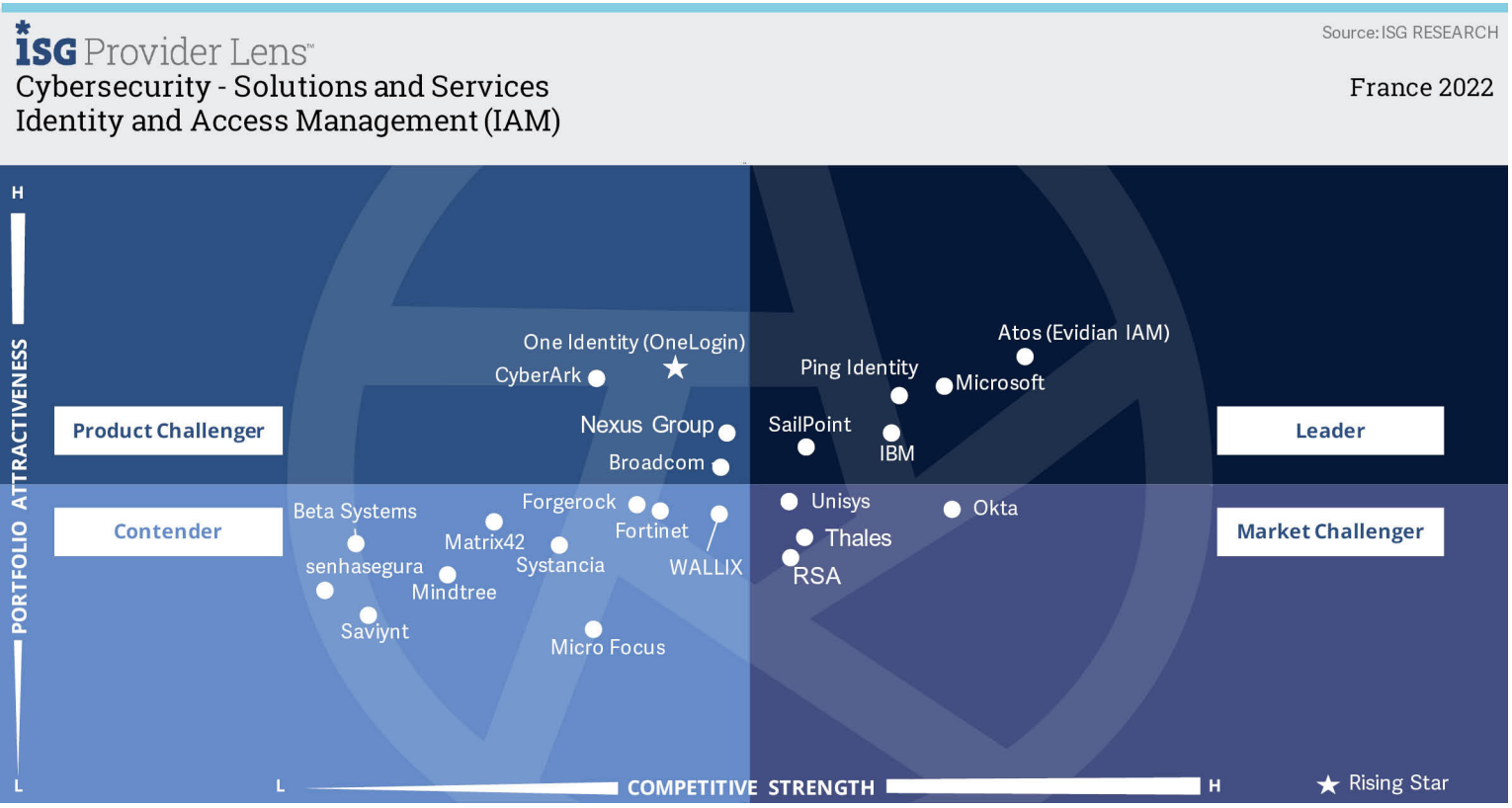
Enterprises leverage single sign-on (SSO) systems with multifactor authentication (MFA) to enable users to access networks, data, apps, the web and the cloud via a single set of credentials. The use of AI and machine learning by enterprises in IAM processes is expanding, allowing for additional improvements in user experience through automation and reduction of manual touchpoints across the whole IAM process chain.

It has become critical to implement secure digital strategies, including cloud-based user access management (UAM) software to provide benefits such as efficiency, scalability and flexibility.

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

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

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



This quadrant assesses IAM software providers for their ability to offer **proprietary software and associated services for securely managing enterprise user identities and devices.**

Dr Maxime Martelli

Definition

IAM vendors and solution providers are characterized by their ability to offer proprietary software (including Software as a Service) and associated services for securely managing enterprise user identities and devices. **Pure service providers that do not offer an IAM product based on proprietary software are not included here**. Depending on organizational requirements, these solutions could be deployed in several ways such as on-premises or in the cloud (managed by the customer) or as an as-a-Service model or a combination thereof.

IAM solutions collect, record and administer user identities and related access rights, as well as specialized access to critical assets, including privileged access management (PAM). They ensure that access rights are granted based on defined policies. To handle existing and new application requirements, IAM solutions are increasingly embedded with secure mechanisms, frameworks and automation (for example, risk analyses) within their management suites to provide real-time user and attack profiling functionalities. Solution providers are also expected to provide additional functionalities related to social media and mobile use to address their specific security needs that go beyond traditional web and context-related rights management. Machine identity management is also included here.

Eligibility Criteria

1. The solution should be capable of being deployed in combination with on-premises, cloud, Identity as a service (IDaaS) and a managed third-party model.
2. The solution should support authentication by a combination of single-sign on (SSO), multifactor authentication (MFA), risk-based and context-based models.
3. The solution should support role-based access and PAM.
4. The IAM vendor should be able to provide access management for one or more enterprise needs such as the cloud, endpoint, mobile devices, application programming interfaces (APIs) and web applications.
5. 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.
6. To support through secure access, the portfolio should offer one or more of the following: directory solutions, dashboard or self-service management, and lifecycle management (migration, sync and replication).

Observations

IAM tools are available for managing access credentials, including encryption and self-service for password reset. Password management has evolved into identity management (IdM). Other methods of user authentication include two-factor authentication and self-service passwords resets with security questions. The concept of identity lifecycle management has emerged recently, together with access management controls, where access refers to identifying systems and services that an individual can access and the functions that can be used in the accessed system. IAM covers IdM. The terms are often used interchangeably, which can confuse clients. In this study, we consider IAM to have all access controls, with less emphasis on the identity authentication methods.

The market is maturing, with multiple consolidations and expansion of capabilities. Some of the recent IAM market consolidations: Okta acquiring AuthO; One Identity acquiring OneLogin; Microsoft acquiring CloudKnox Security; and Ping Identity acquiring Singular Key. The adoption of the cloud model has triggered a fresh round of investments from IAM tool providers for establishing data centers and security operations centers. However, SaaS-delivered IAM solutions bring challenges related to scalability, availability and reliability.

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 critical to mitigating insider threats, data loss and reputation damage.

From the 91 companies assessed for this study, 23 have qualified for this quadrant, with five being identified as Leaders and one as a Rising Star.

Atos

Atos' full-featured Evidian solution provides France-based clients with a robust IAM that includes IA-based advanced analytics and is fully compliant with EU regulations.

IBM

IBM Security Verify, which is offered in on-premises, cloud and appliance models, is a robust solution aligned with the Zero Trust Model, integrates well with its other cybersecurity software, and includes analytics and AI.

Microsoft

Microsoft Azure Active Directory continues to bank on the bundling strategy. It expands its IAM capabilities by adding features such as FIDO2 support and an identity experience framework, as well as a ready-to-use features, integrating easily with cloud applications.

Ping Identity

Ping Identity offers cloud-based IAM solutions to large enterprises to secure access to APIs, networks, cloud/on-premises applications, and other corporate resources. The solutions use AI to track, detect and block malicious activities to ensure regulatory compliance. The company has a strong technical partner network and flexible hybrid delivery model.

SailPoint

SailPoint has a solid presence in France, with a strong base of resellers, channel partners, major consultancies and security implementation specialists. SailPoint Cloud Governance enables automating identity policies across multi-cloud environments.

One Identity

One Identity's IAM solution, One Identity Manager, has a competitive advantage in terms of pricing and has capabilities similar to best-in-breed IAM solutions in the market. Its recent acquisition of OneLogin has created an opportunity gain both visibility and market share in France.

Leader

"Atos' Evidian is a full-featured, robust IAM solution developed in compliance with EU regulations."

Dr Maxime Martelli

Atos

Overview

Atos is a global solution provider with 111,000 employees in 73 countries. Its portfolio includes super computers, commercial software products and managed services. Its Evidian IAM Suite includes Evidian Authentication Manager, Evidian Web Access Manager, Evidian Identity Governance and Administration (IGA), Evidian Enterprise SSO, and Evidian Analytics and Intelligence. In France, Atos has 10 delivery centers, five data centers and nine innovation labs, with more than 10,000 employees.

Strengths

Advanced analytics: Evidian data access analytics, using AI, provides insights on detecting suspicious events. Its drill-down functionality allows users to focus on a specific indicator. The audit analysis feature supports incident investigation with advanced filtering capabilities. Proofs of compliance reports are easily created by searching historical data. The access certification feature audits users' right to remediate in case of unauthorized access.

Convenient authentication: Evidian Identity as a Service (IDaaS) is integrated with MFA, identity federation and single sign-on (SSO) solutions. Designed with a hybrid infrastructure in mind, it helps manage access to all applications, on-premises or in the cloud. It supports an exhaustive list of authentication mechanisms such as Evidian Push Authentication (one-touch authentication), FIDO 2 framework (password-less) and security assertion markup language (SAML).

GDPR-compliant identity governance: Evidian combines the features of entitlement approval, robust authentication, events recording and advanced analytics to provide an end-to-end solution around security and compliance.

Caution

Clients are advised to ask for product demonstrations or proofs of concept to confirm if its features meet their requirements.

Considering Evidian's profound technical ramifications, implementation success depends heavily on the capabilities of the implementation partner.

Firms should focus on the right partnership to meet implementation deadlines.

Appendix

The ISG Provider Lens 2022 – Cybersecurity - Solutions and Services research study 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.

Lead Authors:
Benoît Scheuber, Dr Maxime Martelli

Editors:
Ipshita Sengupta, Jack Kirshbaum

Research Analyst:
Monica K

Data Analyst:
Rajesh Chillappagari

Consultant Advisors:
Roger Albrecht

Project Manager:
Ridam Bhattacharjee

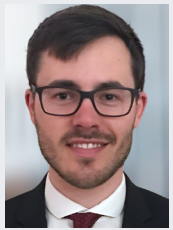
Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens program, ongoing ISG Research programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of June 2022, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

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

The study was divided into the following steps:

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

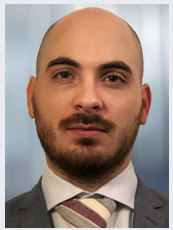


Lead Author

Benoît Scheuber

Consulting Manager and Security Analyst

Senior and highly respected consultant in the fields IT and security operations, Benoît 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. As a consultant, Benoît has been exposed to leading-edge concepts, technologies and clients and has worked on many engagements to contribute to improving operational performance of IT and Security operations.



Co-Lead Author

Dr Maxime Martelli

Consulting Manager and Security Analyst

Maxime Martelli is a Consulting Manager at ISG France. He takes part in ISG's "Digital & Strategy" solution for multinational firms and the public sector services, as well as applying his expertise around Information Security and Cloud Security projects. Author, teacher and lecturer in the field of IT, Maxime is passionate about technology and applies his knowledge of processes, digital strategy, and IT organization to satisfy his clients' requirements. As a Security Analyst, he conducts transformation and strategy projects for all kind of Security tools and solutions, with a strong focus on SOC/SIEM and SASE next-generation security transformations.

Research Analyst

Monica K
Research Specialist

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

IPL Product Owner

Jan Erik Aase
Partner and Global Head – ISG Provider Lens™

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

ISG Provider Lens™

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

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

ISG Research™

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

For more information about ISG Research subscriptions, please email contact@isg-one.com, call +1.203.454.3900, or visit research.isg-one.com.

ISG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 800 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For more information, visit www.isg-one.com.

ISG Provider Lens™

JULY 2022

REPORT: CYBERSECURITY — SOLUTIONS AND SERVICES