ISG Provider Lens™

Cybersecurity – Services and Solutions

Next-Gen SOC Services

A research report comparing provider strengths, challenges and competitive differentiators

Customized report courtesy of:

Capgemini

QUADRANT REPORT | JULY 2025 | FRANCE, GLOBAL

Table of Contents

Executive Summary 03

Provider Positioning 21

Introduction

Definition 35
Scope of Report 37
Provider Classifications 38

Appendix

Methodology & Team 47
Author & Editor Biographies 48
About Our Company & Research 52

Next-Gen SOC Services 39 – 45

Who Should Read This Section 40
Quadrant 41
Definition & Eligibility Criteria 42
Observations 43
Provider Profile 45

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Report Author: Benoît Scheuber

Security teams in France need service providers' expert support to face regulatory demands and cyber threats.

The security teams of French companies face many challenges, including increasing regulatory requirements and advanced cyberthreats. They must also adapt to digital transformation and cloud migration. These difficulties are worsened by a shortage of skilled workers and the need to change work practices. In the fast-growing cybersecurity market, with frequent acquisitions of security vendors, service providers must offer clear support to help these teams navigate the complexities of merging operations and technologies.

ISG has observed a shift in clients' purchasing behavior for security services driven by the proliferation of security tools. Clients now prefer integrated services that enhance their confidence and visibility in the threat landscape without excessive spending on individual tools. As security budgets grow, clients increasingly seek guidance and actionable insights to help them prioritize and address their security concerns effectively.

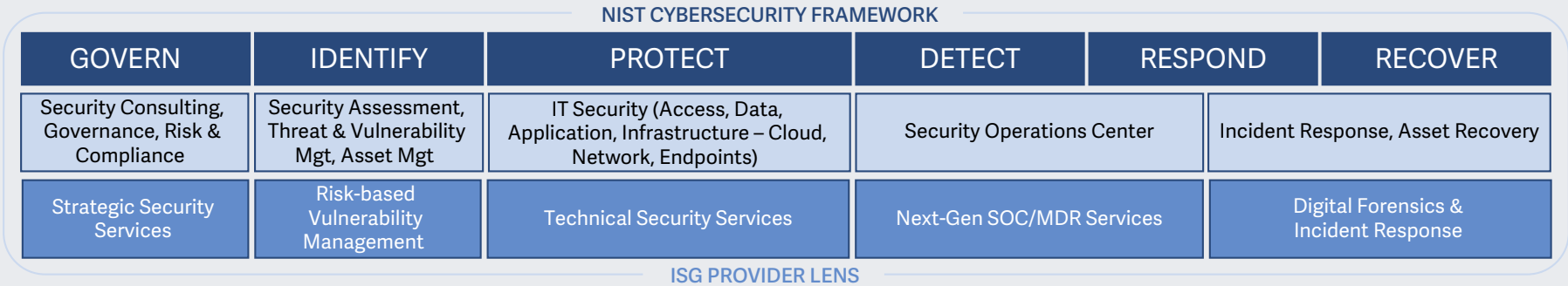
Cybersecurity services

The cybersecurity market is valued at $215 billion in 2025 and is projected to sustain a steady annual growth rate of 10 percent. The market in France is ranked sixth globally, with an estimated worth of approximately $6 to $7 billion.

France's regulations have specific features, with ANSSI (Agence nationale de la sécurité des systèmes d'information) acting as the main market regulator. ANSSI offers guidance, regulates certain activities, such as the protection of sensitive information and critical information infrastructures, and certifies software products, including identity authentication tools. The agency enables users to select a qualified product or service, ensuring access to reliable solutions utilized by the French administration, vital operators and companies in sensitive industries. For service providers, such a qualification opens doors

The regulator **ANSSI recommends top providers** to clients through its qualification process.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.



to regulated French and European markets, offering a competitive edge in the cybersecurity landscape. Currently, ANSSI has qualified 120 cybersecurity services: five for advisory, 99 for audits, nine for detection and seven for response. ISG has considered these factors in its evaluations, with further details provided in the respective quadrants.

To comprehensively cover the main cybersecurity services in the French market, ISG used the NIST Cybersecurity Framework to analyze all providers' offerings for this study. The following illustration shows how the study is structured.

Governance services are evaluated within the Strategic Security Services (SSS) quadrant, while identification services fall under the Risk-based Vulnerability Management quadrant. Protection services are analyzed in the Technical Security Services (TSS) quadrant, and detection services are categorized within the Next-Gen SOC Services and Managed Detection and Response (MDR) Services quadrants. Finally, response and recovery services are assessed in the Digital Forensics and Incident Response (DFIR) quadrant.

From the 145 companies assessed for this study, 67 qualified for at least one quadrant, with 16 being Leaders and four Rising Stars.

Technical Security Services (TSS)

AI is a central topic in almost all business discussions today. It presents both risks and opportunities for security teams. While malicious actors can leverage AI to execute fast and precise attacks, challenging detection and response efforts, security service providers can harness Generative AI (GenAI) and ML in their transformation services to bolster security measures and enhance overall protection.

Security vulnerabilities in OT systems are on the rise, making the convergence of IT and OT indispensable. For example, security issues in the SCADA systems of companies such as Mitsubishi Electric and Iconics can result in severe consequences, including unauthorized access and the introduction of malicious code. These vulnerabilities can directly impact critical industries such as utilities. As a result, IT security teams are now required to also protect OT systems, underscoring the importance of integrating OT security with IT and achieving IT-OT convergence.

With an increasing number of companies adopting Zero Trust principles, there is a growing demand for Identity Access Management (IAM) and Secure Access Service Edge (SASE) solutions. Many security service providers are now adding Security Service

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Edge (SSE) to their offerings and collaborating with partners to deliver comprehensive SASE solutions.

With many companies embracing cloud migration, managing security across different cloud and on-premises environments has become increasingly complex due to integration and visibility challenges. The shift toward cloud and multicloud environments calls for support to protect applications and data by ensuring security tools are correctly configured and managed. Consequently, security teams actively seek improved interoperability with solutions such as SASE and Extended Detection and Response (XDR) while adhering to the principles of cybersecurity mesh architecture, which promotes tech rationalization. Clients also seek integrated security platforms that enhance visibility and maximize their current tool investments. In response to the fragmented cybersecurity landscape, TSS providers offer centralized platforms that connect various security tools, delivering a comprehensive view of potential threats.

Clients recognize the ongoing talent shortage and the necessity for automation, but many remain reluctant to change their practices and utilize shared resources. As a result, the struggle for talent and associated costs is unlikely to end soon. Organizations are grappling with challenges such as a lack of personnel, financial pressures and the need for greater efficiency, prompting them to seek support from TSS providers.

As highlighted earlier, key trends include AI, OT security, IAM, SASE, integrated platforms and workforce shortages. TSS providers that can offer solutions addressing these trends are well-positioned for success in the market.

Strategic Security Services (SSS)

Governance, risk and compliance (GRC) now include cybersecurity, as data breaches and ransomware attacks can lead to substantial financial and reputational loss. Security risks have become a major business threat, prompting CEOs and board members to become more involved in cybersecurity and compliance to meet increased privacy and regulatory demands.

Surviving the compliance wave is becoming increasingly challenging for companies as data privacy laws and regulations, such as DORA, NIS2 and the AI Act, grow worldwide. Compliance experts will need advanced tools and knowledge to manage these evolving requirements and ensure adherence. They must focus on continuous compliance efforts rather than one-off tests and fixes, as relying on and maintaining occasional assessments will be challenging. For example, the NIS2 directive, now a part of French law, affects 15,000 strategic entities and introduces new requirements such as incident reporting and strengthened controls, along with financial penalties for non-compliance. The costs associated with regulatory compliance pose a major challenge, especially for SMEs. To navigate this complex landscape, organizations must adopt unified strategies for managing multiregulatory compliance, ensuring continuous adherence to standards such as GDPR and ISO.

The cybersecurity market is becoming more focused on AI, with numerous companies leveraging the technology to bolster security measures, implement AI-driven threat detection and response and ensure security compliance. Many providers are now integrating AI into their platforms to achieve consolidation and operational efficiency.

Awareness and training are essential because the human factor remains the leading cause of cyber incidents. Declared cyberattacks have increased by 6 percent year on year, with phishing becoming the main threat and rising by 65 percent. Despite this surge in attacks, many companies remain sluggish in implementing adequate security measures and effectively training their employees. Investing in comprehensive training programs can help significantly reduce the risk of these incidents and improve overall security.

Clients are strengthening cloud security and hybrid infrastructure by transitioning to SASE, using solutions such as Cloud Native Application Protection Platform (CNAPP) and embracing methods such as adaptive

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

authentication. They are shifting their focus from mere security to building resilience in IT, OT and critical infrastructure environments. Resilience is emerging as a key concept in cybersecurity.

In a nutshell, key trends include security services for the C-suite, growing regulatory requirements, AI, awareness and training, SASE and resilience. SSS providers that can deliver solutions that embrace these trends are in a strong position to thrive in the market.

Differentiating Next-Gen SOC and MDR Services

As many providers compete in the next-gen security operations center (SOC) and MDR services market, ISG decided to divide it into two quadrants for the France region. Unlike last year, there will not be one quadrant for large accounts and one for midmarket this year. However, the distinction still holds true based on the selected approach.

The first quadrant focuses on Next-Gen SOC Services, encompassing comprehensive supervision of the entire IT infrastructure and security systems and requiring significant internal involvement in setting up and managing security tools and technologies. Large accounts typically seek this type of service, as they need human expertise to support their security teams and offer additional services focused on security operations (such as XDR, firewalls, multifactor authentication [MFA]), threat intelligence, threat hunting, use case factory, vulnerability management, digital forensics and incident response.

The second quadrant focuses on Managed Detection and Response (MDR) Services, an outsourced service that detects, monitors and responds to cyberthreats with minimal involvement from the client's team. This service is best suited for midmarket enterprises that cannot afford a full SOC with expensive tool licenses and need to rely on managed security service providers (MSSPs) to offer packaged services that include both tools and support.

We differentiate the Next-Gen SOC services and MDR services quadrants in the France report due to the distinct operational frameworks and resource requirements each service entails, catering to different client needs—Next-Gen SOC Services requiring significant internal involvement and MDR Services being an outsourced solution. Additionally, the distinction between large accounts and midmarket in France is nuanced; the ISG definition of midmarket encompasses some of the country's largest firms, and with leading MSSPs increasingly targeting these midmarket companies, the competitive landscape diverges from other regions where these segments may be more clearly defined

Next-Gen SOC Services

Managed security services (MSS) are evolving beyond traditional SOCs, transforming themselves into advanced, AI-driven cyber defense entities to address the increasing complexity of cybersecurity threats. SOCs have typically focused on monitoring alerts from various security tools such as firewalls and anti-malware software. Developments such as expanding attack surface, increasing diversity of IT landscapes including OT and IoT, and the rise of remote work further complicate security efforts. SOCs remain essential despite these growing challenges. As companies strive to protect their operations across a broad risk landscape, the demand for Next-Gen SOC Services that can address these evolving needs is increasing.

The scope of SOCs is broadening to include service platformization that combines core detection and response with various cybersecurity operations services such as vulnerability management, OT security, cloud security and exposure management. SOCs are now integrating threat exposure management and breach and attack simulation (BAS), enabling a shift from reactive responses to proactive prevention strategies. This approach incorporates advanced visibility techniques for monitoring the deep and dark web and addresses new vulnerabilities stemming from AI integration. Moreover, SOCs are enhancing incident response capabilities and developing predefined action plans that involve coordination between security and IT teams. They are also implementing new data lake models to improve data management costs and coverage.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

AI-powered SOCs are beginning to incorporate viable GenAI features that enhance analysis and service engineering, focusing on queries and playbooks rather than fully autonomous detection. There is a strong demand for these GenAI features to improve UX and boost security productivity. Key use cases include explaining, summarizing and automating incident response, as well as the adoption of ML for predictive security, which helps organizations anticipate and address potential threats effectively.

Clients are seeking to augment their existing security capabilities by partnering with MSSPs for the expertise and additional workforce support, opting for co-management over full outsourcing or insourcing. Many organizations prefer a more integrated approach to incident management rather than services solely focused on detection. They want to understand the processes and have the option to manage certain aspects of security operations themselves. This demand for self-service or co-managed capabilities is increasing, especially with clients aiming to gradually improve their security operations. Clients align their security strategies with overall enterprise modernization goals by optimizing the effectiveness of their existing technology and enhancing protection, visibility and monitoring.

Ransomware also remains a top concern for organizations. Attackers are leveraging AI to execute rapid and targeted strikes in complex multicloud and hybrid environments, complicating detection and response efforts. To counter these evolving threats, Security Operations Centers (SOCs) are adopting AI-driven threat detection tools, advanced behavioral analytics, and automated response systems. These capabilities enable SOCs to identify anomalies in real time, correlate threat intelligence across environments, and accelerate incident response to contain ransomware outbreaks before they escalate.

As many organizations struggle to effectively manage cybersecurity due to a lack of expertise, the demand for SOC services is expected to remain strong in 2025. Consequently, there is a rising demand for MSSPs, particularly in countries such as France, where businesses commonly rely on external partners for IT services. SOC providers that can offer the comprehensive range of additional services sought by clients are well-positioned to thrive in this quadrant.

Managed Detection and Response (MDR) Services

Midsize businesses, unable to compete with sophisticated SOCs, are turning to MSSPs for essential services such as monitoring, response and threat hunting. The primary challenge for these enterprises is retaining cybersecurity experts, and MSSPs address this issue by offering access to highly skilled practitioners through MDR services. MSSPs typically assign four analysts to each client to ensure 24/7 coverage, but scaling this service remains challenging.

Many MSSPs continue to prioritize larger clients over midsize businesses, although automation and AI can improve effectiveness for both market segments. They are also increasingly competing with XDR solution vendors such as CrowdStrike and Palo Alto Networks, especially in the U.S., while the trend is less common in France. The MDR Services quadrant in this study evaluates only MSSPs that are not solely focused on their proprietary solutions. To remain competitive, MSSPs must either partner with vendors for top-quality products or develop their own advanced platforms. This is particularly important as the midmarket seeks higher-value services, evolving from initial MDR services adoption to the decision of whether to renew those services.

Risk-based Vulnerability Management

Given the increasing demand for continuous threat exposure management (CTEM) solutions, ISG has introduced a new quadrant this year. Risk-based vulnerability management combines vulnerability management and attack simulation to bolster system security. This approach allows for detecting and responding to threats before they can materialize.

Cybersecurity services providers use CTEM solutions to deliver risk-based vulnerability management. This includes both traditional vulnerability management, which focuses on identifying and fixing internal vulnerabilities, and attack surface management (ASM), which

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

offers a broad view, especially regarding external assets. Providers combine the advantages of both approaches by offering continuous monitoring, threat validation, attack simulations, penetration testing and prioritization based on business impact.

For chief information security officers (CISOs), prioritizing security efforts based on business impact is crucial. Risk-based vulnerability management seeks to strike a balance between risks and costs by identifying and prioritizing the most critical threats. A company's risk appetite determines the level of risk it is ready to accept. With risk-based vulnerability management services, the organization can manage threats based on its specific risk tolerance.

Clients increasingly require contextualized risk matrices to help prioritize the remediation of organizational risks. Regulatory-driven security testing, such as TIBER and Threat-Led Penetration Testing (TLPT), is expanding to comply with mandates such as NIS2 and DORA. As customers move from black box testing to collaborative testing, they aim to better understand the risks in their environments. The shift from on-premises to cloud and web solutions exposes organizations to new risks, as many tools struggle to accurately identify risks in shared cloud ecosystems. To tackle these challenges, automation and AI-driven Vulnerability Assessment and Penetration Testing (VAPT) enhance efficiency, scalability and real-time risk prioritization. Continuous vulnerability management, primarily encompassing automated processes to support real-time visibility of risks and vulnerabilities, now increasingly integrates CNAPP, risk-based vulnerability management, breach and attack simulation (BAS) and attack surface management (ASM) to provide a comprehensive security approach.

Digital Forensics and Incident Response (DFIR)

DFIR is a rapidly expanding field focused on identifying, managing and investigating cybersecurity incidents. It involves gathering, preserving and analyzing evidence to contain and mitigate cyberattacks. DFIR requires a mix of soft and technical skills, such as analytical thinking and effective communication, alongside technical expertise in areas such as file system forensics, memory forensics, network forensics, malware triage and log analysis. Given the challenges of finding qualified candidates, many organizations opt to use third-party DFIR services due to limited internal resources.

Organizations usually seek digital forensics services to confirm cyberattacks, understand their impact, identify their sources and gather evidence. Specialized forensics tools help accelerate the processes of remediation, restoration and recovery. With the rise in cyberthreats and the increasing number of endpoints, DFIR is essential for modern security strategies, especially as companies adopt cloud solutions and remote work arrangements. Although DFIR is often reactive, it increasingly leverages advanced technologies such as ML and AI to enable quick analysis and response. The network of technology and insurance partners is also growing strong, enhancing the quality and speed of DFIR services. For example, many cyber insurers now collaborate directly with DFIR firms to offer pre-approved response teams and 24/7 hotlines. Technology partners contribute real-time threat intelligence, automated response capabilities, and forensic tools—reducing average breach detection and containment times.

Threat intelligence has become essential for understanding information leaks, especially as threats have shifted from more visible attacks such as ransomware to quieter data leaks. As adversaries increasingly use valid accounts to gain access — seen in nearly 40 percent of IBM X-Force incident response cases — having accurate threat intelligence is crucial. Data theft and leaks accounted for 54 percent of incidents in 2024, highlighting the importance of monitoring both the deep and dark web. The sale of stolen credentials on the dark web demonstrates the need for organizations to stay informed to protect their information effectively.

While DFIR services initially focused only on reactive support, they have now evolved to offer proactive options such as threat hunting, vulnerability testing and security education. DFIR retainer services now include tabletop exercises, crisis simulations, red teaming and

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

compromise assessments. These prepaid subscription plans enable organizations to use unused consulting hours for proactive services if they experience fewer security incidents during a given period. This allows organizations to prepare for potential security incidents by conducting exercises with their leaders and executives.

In a fragmented cybersecurity market, French clients expect service providers to integrate the best products into a unified platform that addresses all potential threats to their businesses.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Report Author:
Bhuvaneshwari Mohan (Global - IAM)

AI-driven capabilities, zero trust and seamless UX are integral to IAM

The need for robust identity and access management (IAM) has become critical due to escalating cyberthreats, the expansion of hybrid work models and the widespread adoption of cloud technologies. IAM provides the foundation for secure operations, enabling organizations to innovate while meeting rigorous regulatory requirements.

Strategic importance of IAM for enterprises: IAM is foundational to building a resilient security posture that adapts to evolving threats and business demands and significantly strengthens security by reducing the risks of unauthorized access and data breaches. Key security measures such as adaptive and context-aware access controls, continuous identity risk assessments and zero trust architectures form the backbone of these efforts. Adaptive access controls leverage real-time analytics to identify and address unusual behavior effectively. Adopting zero trust frameworks within IAM systems is becoming a standard for securing access, regardless of the user's location or device. The cornerstone of zero trust is rigorous identity verification and access control; therefore, enterprises need robust authentication mechanisms.

In addition to enhancing security, IAM facilitates compliance with regulatory standards such as GDPR, HIPAA, CCPA, SOX and PCI DSS through real-time audit trails and automated user access provisioning. These capabilities prevent unauthorized access by providing visibility into user activity and safeguarding sensitive data. IAM also simplifies the adherence to complex regulations, allowing enterprises to focus on their core operations.

The IAM landscape is transforming significantly, driven by the need for secure, seamless identity solutions and evolving organizational needs. Below are the key IAM-related trends that ISG observed:

As an identity-centric approach taking **centre stage**, IAM has become a **strategic necessity**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Emergence of decentralized identities: One of the most promising developments is the rise of decentralized identity models, which leverage blockchain technology to empower users to control their digital identities, enabling consent-driven authentication and privacy. Both verifiable credentials and decentralized identifiers are essential standards for decentralized identities. Customer identity and access management (CIAM) is gaining increased relevance with the rise of decentralized identities due to the evolving focus on privacy, security and user-centric control over personal data.

Growth of identity as a service (IDaaS): The rapid growth of IDaaS underscores the broad enterprise shift toward cloud-first architectures. IAM vendors are enhancing their IDaaS platforms to integrate seamlessly with SaaS applications and multicloud and hybrid cloud infrastructures. This trend enables organizations to achieve greater agility, scalability and security while adapting quickly to dynamic business and workforce demands.

Market consolidation and strategic acquisitions: The ongoing consolidation in the IAM market reflects a strategic effort by vendors to integrate advanced technologies and expand their product capabilities. For instance, Microsoft's sustained investments in this space reshape the competitive landscape. While these developments drive innovation, they also increase dependency on a few dominant players.

Adoption of biometric authentication and passwordless access: Enterprises are increasingly adopting biometric authentication and passwordless access to enhance security and UX. These methods, including facial recognition, fingerprint scanning and FIDO2-based keys, reduce dependency on passwords, mitigate phishing risks and align with zero trust principles for strong identity assurance.

Industry-specific IAM solutions: The unique requirements of different industries necessitate tailored IAM solutions. Healthcare organizations must comply with HIPAA while securing electronic health records (EHRs), utilizing granular access controls and secure telemedicine platforms. Financial services need to adhere to SOX and PCI DSS standards by implementing robust measures, such as behavioral analytics and multifactor authentication (MFA), to prevent fraud and ensure data integrity. Retailers require scalable IAM solutions to protect customer data and manage workforce access efficiently during peak periods.

Technological advancements and product innovations: The IAM market continues to evolve, with innovations such as AI-driven identity analytics, context-aware authentication and deep integrations with cloud platforms. AI and ML play a vital role in IAM solutions, analyzing and detecting unusual user behavior and automatically adjusting access controls based on real-time information. These advancements enhance the ability of IAM systems to detect anomalies, adjust access decisions dynamically, and support hybrid cloud and multicloud environments. Identity and threat detection and response (ITDR) solutions are emerging as an important aspect of IAM as they focus on proactive threat detection, real-time monitoring and anomaly detection to address identity-centric attacks effectively.

Challenges in implementing IAM

Integration complexities often arise when organizations attempt to align IAM with legacy systems, cloud platforms and third-party applications. These technical hurdles frequently demand specialized expertise and extended implementation timelines. The rapidly evolving threat landscape and the need for enhanced UX without compromising security further complicate IAM implementation.

Enterprises must thoroughly evaluate criteria such as the ability to provide seamless integration, enhanced end UX, product effectiveness, and improved cost and licensing models to ensure the selected IAM vendor aligns with their security needs, business goals and compliance requirements.

As AI is increasingly incorporated into identity security, it also poses many threats, such as AI model poisoning, model theft and synthetic identities. Therefore, AI-enhanced IAM systems should consider following zero trust principles, strengthening IAM configurations, regularly auditing and testing AI models, and maintaining a hybrid approach using AI for

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

assistance while maintaining human oversight in decision-making.

The IAM market is set for growth driven by rising cyberthreats, regulatory pressures and digital transformation. Investment in decentralized identity models, IDaaS and AI-driven solutions will likely accelerate. Opportunities lie in developing industry-specific solutions that address unique regulatory and operational requirements. Evolving real-time adaptive security measures, identity governance and compliance management will prioritize UX.

IAM serves as a strategic enabler that supports compliance, drives innovation and enhances UX. As the digital landscape evolves, investment in advanced IAM solutions will be crucial for organizations aiming to secure their operations and grow in an interconnected world.

This report examines the strategic significance of IAM for organizations across all sizes, highlights key IAM vendors and their capabilities from a global perspective and offers a detailed overview of the market landscape.

Identity solutions of hyperscalers such as AWS and Google Cloud are excluded from this assessment as they are designed primarily for securing their own cloud ecosystems and are not sold as standalone offerings.

At the core of zero trust lies rigorous identity verification and strict access control, emphasizing continuous, risk-based authentication. Enterprises must go beyond traditional methods by adopting passwordless solutions, biometric authentication and behavioral analytics. Real-time, context-aware risk assessments ensure dynamic access, making identity security proactive rather than reactive, which is critical in today's evolving threat landscape.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Report Author: Gowtham Sampath (Global - XDR)

XDR addresses complex IT environments and talent shortages with enhanced visibility and automation

The extended detection and response (XDR) market is rapidly maturing, driven by enterprise demand for consolidated, intelligence-led security operations. In response to the increasing sophistication of cyberthreats, organizations are shifting from siloed detection tools to unified platforms that deliver comprehensive visibility, automation and contextual analytics across endpoints, networks, cloud workloads and identities. XDR has evolved from a niche extension of endpoint detection and response (EDR) into a core component of modern security operations center strategies, enabling proactive threat hunting, rapid containment and coordinated response across the attack surface.

At the core of this transformation is the pervasive adoption of AI, ML and behavioral analytics, which now power many detection, correlation and prioritization engines within XDR platforms. These technologies reduce false positives and allow for early-stage anomaly detection and advanced threat modeling. The growing integration of cloud-native security and zero trust frameworks reflects the market's recognition that security perimeters are dynamic and identity-driven. XDR platforms increasingly align with MITRE ATT&CK and support Continuous Threat Exposure Management (CTEM) and automation-first response models.

Key trends and developments

- **Emergence of agentic AI:** The integration of agentic AI (autonomous, goal-driven systems) is revolutionizing XDR platforms. These AI agents can independently detect, investigate and respond to threats, reducing reliance on human intervention and enhancing response times.
- **Shift toward open and modular architectures:** Organizations are demanding XDR solutions that offer open architectures, allowing seamless integration with existing

XDR's evolution **unifies defenses**, driving **proactive, intelligent** cyber **resilience**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

security tools and third-party applications. This modular approach enhances flexibility and ensures comprehensive threat visibility across diverse environments.

- **Integration of behavioral analytics for insider threat detection:** Advanced behavioral analytics are being employed to detect insider threats by monitoring deviations from typical user behavior. This proactive approach enables early identification of potential security breaches originating from within the organization.
- **Adoption of CTEM:** XDR platforms are incorporating CTEM to provide real-time assessments of an organization's security posture. Organizations can prioritize remediation efforts by evaluating vulnerabilities and potential attack vectors.
- **Expansion into operational technology (OT):** XDR solutions are extending their capabilities to secure OT environments, addressing the unique challenges of industrial systems and critical infrastructure. This expansion ensures comprehensive protection across both IT and OT domains.
- **Integration of knowledge graphs:** XDR platforms are leveraging knowledge graphs to map relationships between various entities within an organization. This integration provides context-rich threat intelligence, improving the accuracy of threat detection and response strategies.
- **AI-driven insider risk management (IRM):** Advanced IRM systems powered by AI are being integrated into XDR platforms to proactively identify and mitigate insider threats. These systems utilize adaptive scoring and real-time policy enforcement to enhance organizational security.
- **Focus on proactive defense mechanisms:** The XDR market is experiencing a shift from reactive to proactive defense strategies. By anticipating potential threats and vulnerabilities, organizations can implement measures to prevent security incidents before they occur.

These trends underscore the dynamic evolution of the XDR landscape, highlighting the importance of adaptability, integration and proactive strategies in modern cybersecurity frameworks.

Looking forward, in the second half of 2025, vendors in the XDR market are expected to deepen their focus on open architectures, third-party integrations and AI-assisted analyst augmentation. Future-ready XDR platforms will detect and respond to known threats and act as decision-support engines capable of autonomous investigation, real-time risk scoring and adaptive policy enforcement. As cyberattacks become increasingly dynamic and multistage, XDR is poised to become the operational nerve center of enterprise cybersecurity.

XDR is fundamentally transforming cyber defense by shifting from reactive to proactive security. This profound evolution is powered by advanced AI and ML, enabling predictive capabilities to anticipate and block attacks before they escalate. XDR moves beyond mere detection to prevent breaches by integrating identity data and comprehensive threat intelligence.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Report Author: Yash Jethani (Global - SSE)

Zero trust SSE architecture uses AI to evolve, with continuous authentication and strict access controls

Why you need zero trust principles

In today's digital landscape, traditional security perimeters are obsolete. Zero trust architecture provides continuous authentication and strict access controls essential for secure remote work and cloud environments. Verifying every user and device before granting access, organizations can significantly reduce breach risks and protect sensitive data from external attackers and insider threats.

Zero trust architecture operates on the *never trust, always verify* principle, requiring continuous authentication regardless of location. Modern cybersecurity measures strengthen this approach by:

- **AI and ML:** Enhances zero trust by continuously monitoring user behavior patterns and automatically identifying anomalies that suggest compromised credentials
- **Ransomware defense:** Supports zero trust by isolating potential threats and preventing lateral movement within networks, limiting damage scope
- **Cloud security:** Extends zero trust principles to distributed environments through CASB tools that enforce consistent access policies across all applications
- **IoT protection:** Applies zero trust microsegmentation to connected devices, preventing compromised devices from accessing critical systems
- **Critical infrastructure security:** Implements zero trust measures to create secure operational zones with strict verification for accessing control systems
- **Data privacy:** Aligns with zero trust's least-privilege access controls to ensure regulatory compliance and protect sensitive information

Providers are aligning SSE with enterprise needs for **agility, integration** and **a unified SASE**.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- **Emerging technologies:** Strengthens zero trust authentication through quantum-resistant encryption and blockchain-verified identity management.

A robust cybersecurity strategy integrates these elements within a zero trust framework, creating multiple verification layers that protect against sophisticated threats.

Security service edge (SSE) is a fundamental component that enables zero trust principles in modern network environments. SSE delivers cloud-based security functions that enforce zero trust by:

- **Identity-based access control:** SSE validates user identity before granting access to applications, aligning with zero trust's *never trust, always verify* principle.
- **Continuous verification:** SSE continuously monitors sessions after initial authentication, detecting behavioral anomalies that might indicate a security compromise.
- **Policy enforcement point:** SSE serves as a cloud-delivered control point where zero trust policies are consistently applied across all users, locations and devices. Legacy VPN replacement reduces the attack surface with a more secure remote access solution.
- **Application-level controls:** Rather than securing network segments, SSE secures access to specific applications, supporting zero trust's focus on protecting resources rather than networks. ZTNA provides zero trust access to private applications, replacing VPNs while CASB secures connectivity to SaaS apps, preventing data loss and cyberattacks, and secure collaboration enables the safe sharing of confidential information.
- **Inspection and threat prevention:** SSE provides deep inspection of encrypted traffic, detecting and blocking threats that might exploit trusted connections. Secure web gateway (SWG) enables secure internet access with advanced threat prevention while DEM monitors device, application and network performance for rapid issue resolution.
- **Data protection integration:** SSE incorporates data loss prevention (DLP) and cloud access security broker (CASB) capabilities to prevent sensitive data exfiltration, supporting zero trust data security requirements. GenAI DLP prevents sensitive data sharing with GenAI, while AI-enabled DLP uses intelligent policies to control and protect sensitive data.
- **Sensitive information management:** SSE discovers, assesses and protects sensitive data in real time, while continuous zero trust access consistently authorizes user and device access.

SSE provides the cloud-delivered security stack to implement zero trust principles at scale across distributed environments. It replaces traditional perimeter security with a flexible, identity-centric approach to secure remote work, cloud adoption and mobile access scenarios without sacrificing protection or visibility.

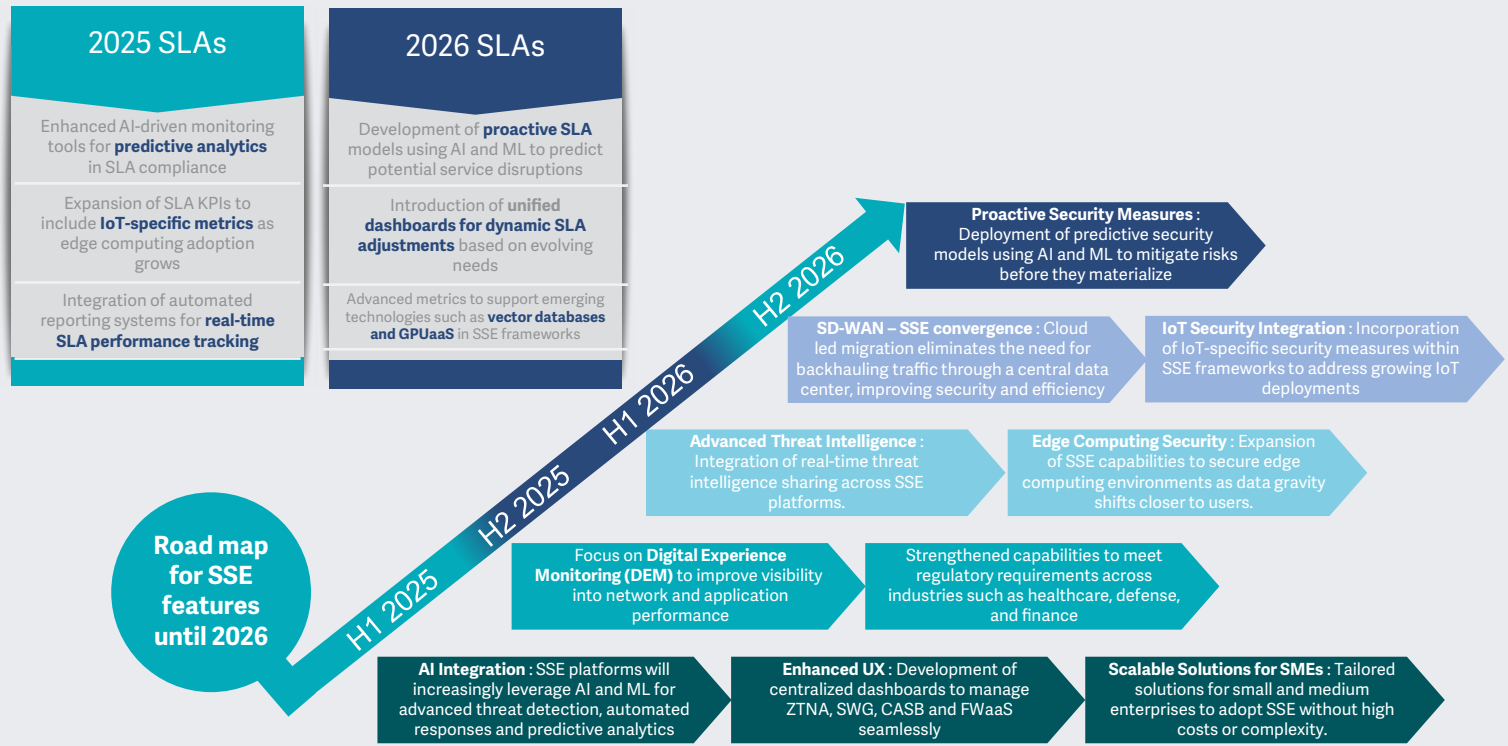
SSE serves a diverse range of customers, including end enterprises, cloud service providers (CSPs) delivering cloud services, network service providers (NSPs) offering network connectivity, and managed service providers (MSPs) providing outsourced IT and security. Large enterprises, characterized by extensive IT teams and infrastructure and small and midsize businesses (SMBs), often constrained by resources, also represent key customer segments. Understanding these distinct profiles is crucial for SSE vendors and organizations alike in tailoring solutions and adoption strategies.

Components and functions of SSE, SLA compliance expansion and road map for 2025 and 2026:

SSE components can be broken into four major buckets:

- CNAPP: Combines cloud security tools (CSPM, CIEM, CWP) for streamlined, scalable cloud protection — a key part of SSE
- Digital ecosystem exposure management: Identifies and mitigates risks across interconnected digital assets (cloud, IoT, BYOD), which is crucial for expanding digital footprints and being a differentiator for SSE vendors

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.



Source: ISG, 2025

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- Next-generation deep packet inspection (DPI): Uses advanced techniques such as ML to analyze encrypted traffic and detect sophisticated threats in cloud environments, enhancing visibility for CASB, SWG and ZTNA within SSE
- UEBA: Employs analytics and ML to detect abnormal user and entity behavior indicative of insider threats or attacks, increasingly integrated into SSE for advanced threat detection

Increasingly, SSE vendors offer platforms that integrate multiple functions and components. This platform offers comprehensive cloud-native security through a single architecture. It provides the ability to inspect encrypted traffic at scale and features an inline proxy for cloud and web traffic. Core security functions include a full-port firewall with intrusion protection (FWaaS), API-based data security for cloud services (CASB) and continuous security assessment for public cloud infrastructure (CSPM). Advanced data loss protection is usually included for data in transit and at rest, alongside advanced threat protection (ATP) leveraging AI and ML, UEBA and sandboxing. The platform integrates threat intelligence with other security tools (EPP/EDR, SIEM, SOAR), provides data loss from GenAI systems and offers zero trust network access (ZTNA) to replace legacy VPNs and finally enables secure collaboration via email and collaboration tools. It can also feature a software-defined perimeter with zero trust access (SD-WAN/SDP) and a global, scalable network infrastructure with optimizations for SaaS performance.

By 2026, as per the figure above, ISG expects the SSE components and functions to evolve to include IoT security, proactive edge healing and solutions tailored for SMEs.

Technology trends in SSE:

- SSE solutions increasingly adopt zero trust principles, moving away from VPN-based remote access to identity-driven security. ZTNA remains foundational to SSE, ensuring that only authorized users and devices access resources, driven by the need to secure remote work and cloud environments.
- Providers and product vendors are embedding ML and AI-driven threat detection for anomaly detection, automated remediation and real-time policy enforcement.
- As enterprises prefer cloud-native SSE over legacy appliance-based security, full cloud-native architecture now supports distributed workforces and multicloud adoption. Cloud-native SSE platforms are scaling to handle massive traffic volumes, supporting digital transformation with flexible, scalable security for hybrid IT environments.
- SSE solutions prioritize low latency and minimal downtime to match consumer-grade application experiences, addressing the demands of a distributed workforce without compromising security.
- SSE platforms are deeply integrated with Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) for better threat visibility and response. On the other hand, Autonomous Digital Experience Management/Monitoring (ADEM) is being integrated into SSE to monitor end-user performance and security, using AI for predictive analytics and troubleshooting.
- DLP, encryption and adaptive access controls are becoming standard features that address increasing compliance needs.
- Integration with IAM and SSE (SSO/MFA) is now seen as commonplace to enforce stronger authentication policies.

Business trends in SSE:

- Many enterprises adopt SSE first and integrate SD-WAN later for a complete SASE deployment. However, this is likely a two-way trend as many enterprises adopt networking solutions and then migrate to SASE by layering on SSE features. Hence, the line between SSE and secure access service edge (SASE) continues to blur as providers offer unified platforms combining networking (SD-WAN) and security (ZTNA, SWG, CASB, FWaaS) features, catering to hybrid and distributed workforces.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

- With VPN limitations, SSE is replacing traditional remote access solutions as remote and hybrid work drives SSE demand. Enterprises are increasingly adopting secure browsers as a critical first line of defense against browser-based threats, driven by the shift to cloud-based work and remote access. Given the growing reliance on web applications, this is seen as a necessity.
- SSE platforms are leveraging AI and ML for real-time threat detection, behavioral monitoring and automated responses, reducing manual intervention and enhancing proactive security.
- Enterprises are moving toward OpEx models instead of traditional CapEx-heavy hardware investments, thus favoring a shift to subscription-based security (Security-as-a-service).
- Enterprises prefer fewer providers that provide end-to-end SSE solutions instead of managing multiple security tools. This drives the consolidation of the vendor landscape, favoring single-vendor strategies, particularly for small and midsize enterprises.
- Industries such as finance, healthcare and government are embracing SSE to meet strict data protection and access control regulations.

Recent acquisitions in the zero trust or SSE space:

- **Cloudflare:** In February 2025, Cloudfare acquired BastionZero to enhance its zero trust infrastructure access controls, expanding the capabilities of Cloudflare One, its SASE platform. It also acquired Area 1 Security in 2022, enhancing email security within its SSE offering.
- **Zscaler:** In October 2024, Zscaler acquired network segmentation startup Airgap Networks to strengthen its zero trust security offerings. In March 2024, it purchased Israeli data security startup Avalor to enhance its AI-driven data protection capabilities. In February 2024, Zscaler acquired another Israeli application security company Canonic Security, to bolster its defenses against SaaS-based threats. In May 2021, it had acquired Smokescreen to add deception technology and enhance threat detection.
- **Hewlett Packard Enterprise (HPE):** In March 2023, HPE acquired Axis Security, a cloud-native SSE vendor. This acquisition bolstered HPE's edge-to-cloud security capabilities by integrating Axis Security into its Aruba networking platform, creating a unified SASE solution.
- **Netskope:** In June 2022, Netskope acquired WootCloud, an innovator in applying zero trust principles to IoT security, extending its zero trust capabilities to enterprise IoT. It also acquired Infiot in 2022, strengthening its zero trust and SD-WAN capabilities.
- **Palo Alto Networks:** The company acquired CloudGenix in 2020, integrating SD-WAN and SSE to create a full SASE stack. The move highlights the trend among enterprises toward single-vendor SSE/SASE platforms, which simplify deployment and management while avoiding the complexities associated with multivendor setups.
- **Check Point:** In September 2023, it completed its acquisition of Perimeter 81 to strengthen its SASE capabilities. Managed through a user-friendly cloud console, Perimeter 81's capabilities ensure reliable connectivity via a global backbone network, while its SWG protects against web-borne threats.
- **SonicWall:** In January 2024, SonicWall acquired Banyan Security, a cloud platform focused on identity-centric SSE, to extend its security capabilities to cloud and hybrid environments, remote workers and BYOD scenarios. Banyan Security's framework assessed device posture to guarantee secure access and included a SWG to defend against internet-based threats. Additionally, it offered VPN as a service (VPNaaS) for modern, secure network access.

SSE provides cloud-based security services such as SWG and ZTNA, making it easier for distributed workforces to interact securely from a distance. Enterprises must also adhere to changing legal standards, which calls for strong security measures to protect corporate and personal data. Various industries are adopting SSE solutions because they facilitate compliance efforts through centralized security policies, real-time threat monitoring and data loss prevention. The blurred lines between

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

SSE and Secure Access Service Edge (SASE) indicate a compelling trend where enterprises can seamlessly adopt comprehensive security and networking solutions tailored for hybrid and distributed workforces. As organizations continue to navigate a landscape shaped by remote operations and stringent compliance requirements, the SSE market is poised for growth, becoming an essential component of organizational strategy and operational resilience in the digital era.

For effective SSE deployment, organizations should adopt several key strategies. This includes minimizing reliance on legacy security hardware by leveraging SSE's integrated features and implementing zero trust principles through ZTNA for robust access control. Consolidating disparate security tools onto a unified SSE platform streamlines management while embracing hybrid and cloud-ready SSE architectures ensures flexibility. A phased rollout, starting with critical areas such as ZTNA, allows for gradual and strategic adoption. Furthermore, prioritizing the security of remote work environments and ensuring a positive UX with DEM is vital. Ultimately, strategic budget allocation toward SSE investments that address key risks will drive the most impactful security outcomes, and the CIOs and line of business heads need to converge on their own security budgets.

Enterprises seek scalable, high-performance solutions with seamless integration, unified management and a clear path to full SASE for future-ready security. While providers indicate a shift toward agile, unified and performance-oriented security frameworks, the ultimate aim is to deliver a truly frictionless and comprehensive security experience across any user, device, and location.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

Page 1 of 14

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Accenture	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader	Leader
Advens	Not In	Not In	Not In	Not In	Product Challenger	Leader	Leader	Leader	Not In
Airbus Protect	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Product Challenger	Product Challenger
Aizoon	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger
AlmavivA	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Almond	Not In	Not In	Not In	Product Challenger	Rising Star ★	Product Challenger	Product Challenger	Product Challenger	Rising Star ★
Alten	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Aryaka	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Atos	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader	Leader

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

Page 2 of 14

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Axians	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Contender	Not In
Bechtle/Apixit	Not In	Not In	Not In	Contender	Not In	Contender	Contender	Not In	Not In
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
BlackBerry (Arctic Wolf)	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
BT	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Contender
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Market Challenger	Leader

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Market Challenger	Contender	Not In	Not In	Not In
Check Point Software	Not In	Product Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Cognizant	Not In	Not In	Not In	Contender	Not In	Not In	Product Challenger	Not In	Contender
Computacenter	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Consort Group	Not In	Not In	Not In	Not In	Contender	Not In	Contender	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CyberArk	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CyberProof	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger
Deloitte	Not In	Not In	Not In	Market Challenger	Leader	Contender	Not In	Market Challenger	Not In
Devoteam	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Contender
DXC Technology	Not In	Not In	Not In	Contender	Contender	Contender	Not In	Contender	Not In
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Evidian IAM (Eviden)	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Not In	Market Challenger	Market Challenger
Fischer Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Formind	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Product Challenger	Rising Star ★
Fortinet	Market Challenger	Leader	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Fortra	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Fujitsu	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Gopher Security	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
HCLTech	Not In	Not In	Not In	Leader	Market Challenger	Leader	Leader	Not In	Market Challenger
Headmind Partners	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Holiseum	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In
HubOne (SysDream)	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Contender	Not In
IBM	Leader	Leader	Not In	Leader	Market Challenger	Leader	Leader	Leader	Market Challenger

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Inetum	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In
Infosys	Not In	Not In	Not In	Rising Star ★	Not In	Product Challenger	Not In	Not In	Not In
Intrinsec	Not In	Not In	Not In	Not In	Leader	Leader	Product Challenger	Leader	Product Challenger
ITS Group	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
JumpCloud	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	Contender	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

Page 8 of 14

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Kudelski Security	Not In	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger	Contender	Product Challenger
Kyndryl	Not In	Not In	Not In	Market Challenger	Contender	Contender	Not In	Contender	Not In
Lexfo	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★	Product Challenger
LMNTRIX	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Lookout	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Product Challenger	Contender	Not In	Contender	Not In	Not In
ManageEngine	Leader	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Menlo Security	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Metsys	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Contender

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Neverhack	Not In	Not In	Not In	Contender	Product Challenger	Not In	Not In	Product Challenger	Contender
Niji	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Nomios	Not In	Not In	Not In	Product Challenger	Not In	Not In	Contender	Not In	Not In
NTT DATA	Not In	Not In	Not In	Product Challenger	Not In	Contender	Not In	Not In	Not In
NXO	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Okta	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
OpenText	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Leader	Leader	Leader	Leader	Leader	Leader
Ornisec	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Not In	Leader	Product Challenger	Not In	Leader	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

Page 11 of 14

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
RSA	Market Challenger	Not In	Not In	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	Not In	Not In
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SCC	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Secureworks	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Contender	Contender
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Seqrite	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Sequretek	Contender	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SFR	Not In	Not In	Not In	Contender	Not In	Contender	Contender	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
SNS Security	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
SonicWall (Banyan Security)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Sophos	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Leader	Leader	Leader	Not In	Leader	Leader
Spie ICS	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Contender
Squad	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Provider Positioning

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
Synacktiv	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Synetis	Not In	Not In	Not In	Product Challenger	Contender	Product Challenger	Not In	Product Challenger	Product Challenger
TCS	Not In	Not In	Not In	Leader	Contender	Product Challenger	Not In	Not In	Leader
Tech Mahindra	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Telefonica Tech	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
Thales	Product Challenger	Not In	Not In	Leader	Leader	Leader	Leader	Leader	Leader
Trellix	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

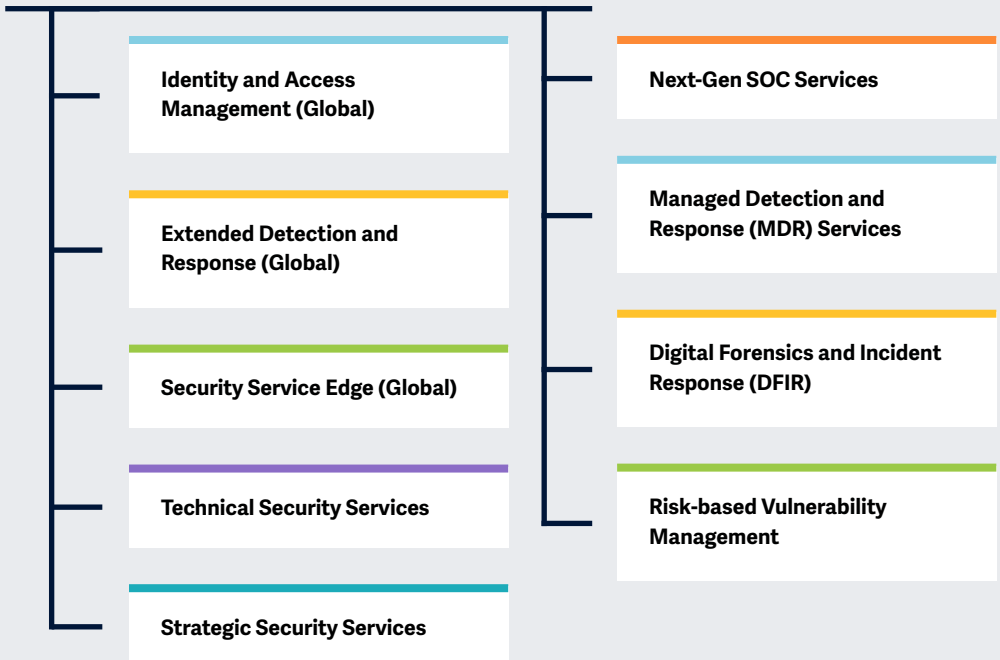
Provider Positioning

Page 14 of 14

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC Services	Managed Detection and Response (MDR) Services	Digital Forensics and Incident Response (DFIR)	Risk-based Vulnerability Management
T-Systems	Not In	Not In	Not In	Contender	Not In	Not In	Product Challenger	Not In	Not In
Unisys	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Not In	Contender
Verizon Business	Not In	Not In	Not In	Not In	Not In	Not In	Contender	Contender	Not In
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Leader	Not In	Not In	Leader	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In	Not In	Not In	Not In
Xmco	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Key focus areas for Cybersecurity – Services and Solutions 2025



Simplified Illustration Source: ISG 2025

Definition

In the era of rapid technological advancements and AI integration into daily operations, the cybersecurity landscape has become increasingly complex and multifaceted. Regulatory requirements such as the Network and Information Security (NIS) 2 Directive in the European Union are elevating the demand for robust cybersecurity measures, compelling organizations to reassess their security frameworks amidst emerging threats. Simultaneously, the commoditization of hacking tools has significantly reduced entry barriers for malicious actors, resulting in a surge of cybercriminal activities and a corresponding escalation of risks.

The proliferation of technology has expanded the attack surface, posing critical challenges for organizations as they navigate between OT and IT. The scarcity of skilled cybersecurity personnel has amplified this complexity, spurring accelerated demand for managed security services as companies seek external expertise to fortify their defenses.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Introduction

Continued AI development presents risks and opportunities in the cybersecurity space. Security service providers help clients navigate the cybersecurity landscape, where vigilance is crucial in identifying and mitigating emerging threats and understanding the transformative impact of new technologies such as quantum computing. In response to these challenges, businesses are increasingly investing in solutions such as identity and access management (IAM), data loss prevention (DLP), extended detection and response (XDR), and security service edge (SSE), combining advanced tools and human expertise with behavioral and contextual intelligence to enhance their security posture.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Scope of the Report

In this ISG Provider Lens™ quadrant study, ISG includes the following nine quadrants: Identity and Access Management (Global), Extended Detection and Response (Global), Security Service Edge (Global), Technical Security Services, Strategic Security Services, Next-Gen SOC Services, Managed Detection and Response (MDR) Services, Digital Forensics and Incident Response (DFIR), and Risk-based Vulnerability Management.

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

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

Our study serves as the basis for important decision-making by covering providers' 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 providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the service requirements from enterprise customers differ and the spectrum of providers operating in the local market is sufficiently wide, a further differentiation of the 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 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 $20 million and $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 $1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product & Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include a service provider(s) which ISG believes has strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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 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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Next-Gen SOC Services

Who Should Read This Section

This report is valuable for providers offering **next-gen SOC services** in **France** to understand their market position and for enterprises looking to evaluate these providers. In this quadrant, ISG highlights the current market positioning of these providers based on the depth of their service offerings and market presence.

Cybersecurity professionals

Should read this report to understand emerging trends and immediate threats. It aids in strategic decision-making, enhances productivity and reduces security complexity.

Technology professionals

Should read this report to know emerging trends and gain insights into tailored security platforms and strategic objectives necessary to adapt to the evolving security landscape.

Business professionals

Should read this report to gain valuable insights into streamlining security operations. It offers practical solutions to reduce complexity and enhance efficiency.

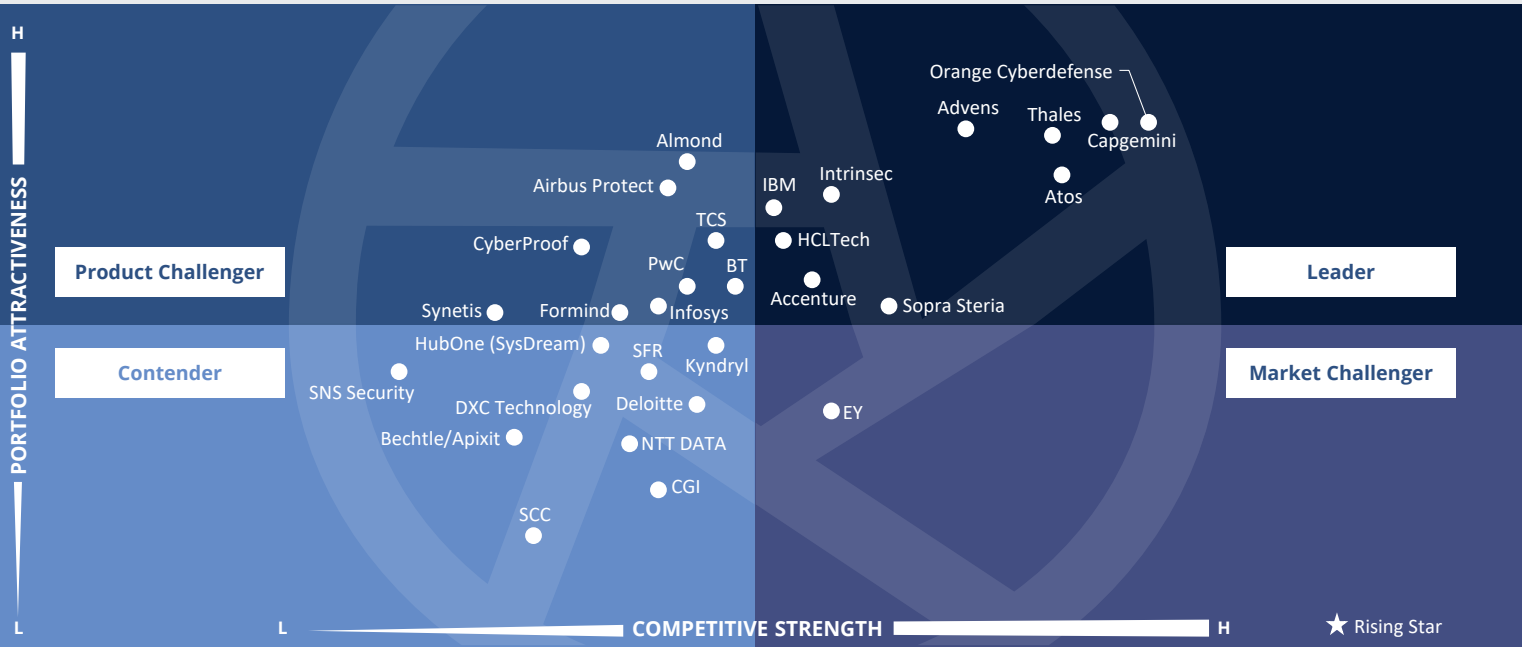
© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC Services

France 2025



This quadrant examines **SOC providers** that are not exclusively focused on their proprietary products but can manage and operate best-of-breed security tools. These providers can handle **the entire incident lifecycle**, from identification to response.

Benoît Scheuber

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Definition

Providers assessed in this quadrant offer services related to the continuous monitoring of IT and OT infrastructures by a security operations center (SOC). This quadrant examines service providers that are not exclusively focused on proprietary products but can manage and operate best-of-breed security tools. These service providers can handle the entire security incident lifecycle from identification to response and remediation.

Next-Gen SOC providers are in demand to strengthen enterprises' security posture and improve the effectiveness of security programs. They blend traditional managed security services with innovation to deliver integrated cyber defense and managed detection and response (MDR) services. These providers also invest in threat detection and hunting, threat intelligence, modeling and forensics, incident management and advanced technologies, such as automation, big data, AI and ML, to offer a holistic approach to proactive threat mitigation and advanced security.

Eligibility Criteria

1. Offer standard services, including **security monitoring, behavior analysis, unauthorized access detection, advisory on prevention measures, penetration testing** and all other operating services, to provide ongoing, real-time protection without compromising business performance
2. Provide security services, such as prevention and **detection, security information and event management (SIEM) services,** security advisors and auditing support, either remotely or at clients' site
3. MDR-specific capabilities, including **advanced threat intelligence** and **behavior-based and human**-led threat hunting, delivering **offensive and defensive** security capabilities with a unified view for reporting and metrics
4. Possess **accreditations** from security tools vendors
5. **Manage own SOCs**
6. Maintain **staff** with certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) and Global Information Assurance Certification (GIAC)
7. Offer a variety of **tiered** pricing models

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Observations

The Next-Gen SOC Services quadrant assesses service providers based on their SOC capabilities in France. ISG considered several parameters for rating, including continuous monitoring, detection and response, advanced analytics and other in-demand services such as threat intelligence, vulnerability management, digital forensics and red teaming. Advanced features such as a user portal, deception techniques and OT coverage were a plus.

France has unique regulatory requirements, and the ANSSI offers guidance to help with compliance. While several large companies and government agencies may require ANSSI-qualified PDIS, only eight of the assessed companies have this qualification: Airbus Protect, Atos Group, BT, Capgemini, HubOne, Orange Cyberdefense, Sopra Steria and Thales. Advens and I-TRACING are in the process of obtaining this qualification. It has been considered in the ratings because it shows good compliance with French regulations. Pure play providers such as Intrinsec, Almond and Formind are increasingly gaining market share.

A local presence is important to support clients who are increasingly seeking co-management instead of full SOC outsourcing. Service providers that do not have offices in France and those solely focused on detection and response, without covering threat and vulnerability management, are placed in the MDR Services quadrant instead of the Next-Gen SOC Services quadrant.

Some large companies offer managed IT services to their customers and incorporate security alongside IT services. While this is advantageous, providers lacking a separate SOC received lower scores in this study.

From the 126 companies assessed for this study, 30 qualified for this quadrant, with ten being Leaders.

accenture

Accenture enhances its offerings through strategic partnerships with industry leaders. Its modular SOC approach integrates seamlessly with platforms. It combines global reach with local insights to deliver innovative, outcome-focused solutions.

Advens

Advens offers next-gen SOC services through its mySOC platform, providing 24/7 visibility and AI-driven threat detection. Tailored client-focused solutions and a strong partner ecosystem enhance its cybersecurity offerings.

Atos

Atos Group enhances security with its proprietary security analytics platform, integrating tools for predictive intelligence. The company's cybersecurity mesh architecture fosters real-time threat responses, backed by the expertise and strategic partnerships with leading security vendors.

Capgemini

Capgemini ensures robust cybersecurity with localized support and tailored solutions. Its innovation-driven approach, industry recognition and strong partnerships enhance SOC efficiency and foster client trust.

HCLTech

HCLTech delivers tailored cybersecurity solutions powered by 7,500 professionals and more than 60 innovation labs, enhancing cloud security and identity management. Its proactive Next-Gen SOC services ensure enterprise resilience against evolving threats.

IBM

IBM is a leader in SOC services, leveraging global expertise and patented technologies for effective threat management. Its AI-driven approach processes more than 100 billion events daily, ensuring streamlined detection and response.

Intrinsec

Intrinsec offers advanced threat defense with specialized training and flexible SOC services tailored for organizations of any size. Its expert team ensures effective incident response and forensic analysis, enhancing the overall security posture.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Cyberdefense

Orange Cyberdefense combines localized expertise with a multivendor approach, enhancing services through partnerships and proprietary AI capabilities. Its proactive threat management ensures 24/7 monitoring, enabling robust cyber protection.

Sopra Steria

Sopra Steria's Next-Gen SOC Services integrate consulting and managed services to mitigate business risks and build a security culture for its clients. Its innovation lab enhances solutions, while its acquisitions strengthen its position in the cybersecurity landscape.

Thales

Thales commits to cyber sovereignty, offering secure data storage in France and tailored detection and response services. Its sector-specific solutions and sovereign cybersecurity center enhance national defense capabilities.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Leader

"The Capgemini Defend services portfolio offers clients comprehensive threat detection, response and mitigation capabilities across the full range of potential threats."

Benoît Scheuber

Capgemini

Overview

Capgemini is headquartered in Paris, France, and has more than 341,100 employees worldwide. In FY24, the company generated €22.1 billion in revenue, with Applications and Technology as its largest segment. Its cybersecurity portfolio accounts for three percent of its total revenue. Capgemini offers a broad range of Next-Gen SOC services, including managed security operations, threat intelligence, vulnerability management and endpoint security. Its advanced Cyber Defense Platform supports dynamic detection and automated response, leveraging AI and ML to enhance security measures across client environments.

Strengths

Robust global presence: With a significant workforce and a presence in numerous locations in France, Capgemini provides localized support while ensuring comprehensive coverage. Its experienced team helps clients navigate the cybersecurity landscape through tailored solutions that strengthen security performance and resilience.

Innovation and automation: Capgemini places a strong emphasis on innovation, with ongoing investments in automation and emerging technologies. Its Integrated Cyber Defense platform features global playbook automation and seamless integration of client-owned SIEMs, enhancing SOC efficiency and response capabilities.

Industry recognition and partnerships: Recognized as a leader in the cybersecurity space, Capgemini holds the PDIS qualification from ANSSI and collaborates with top vendors such as Microsoft, Palo Alto Networks and ServiceNow. This extensive partner ecosystem empowers Capgemini to deliver advanced, tailored and effective security solutions across various industries.

Client-centric approach: Capgemini is dedicated to providing exceptional client service by offering customized solutions backed by a strong foundation of cybersecurity best practices. It focuses on developing innovative strategies that align with clients' specific needs, fostering long-term relationships and trust in its cybersecurity services.

Caution

While Capgemini has limited thought leadership on SOC and marketing focused on DFIR and has a smaller partner ecosystem than other SOC leaders, it can leverage its network of 17 Cyber Defense Centers to strengthen its market position.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Appendix

Methodology & Team

The ISG Provider Lens 2025 – Cybersecurity – Services and Solutions study analyzes the relevant software vendors/service providers in the French, Global markets based on a multi-phased research and analysis process, and positions these providers based on the ISG Research methodology.

Study Sponsor:
Heiko Henkes

Lead Authors:
Benoît Scheuber, Bhuvaneshwari Mohan (Global - IAM), Gowtham Sampath (Global - XDR), and Yash Jethani (Global - SSE)

Editors:
Radhika Venkatachalam and Ritu Sharma

Research Analysts:
Monika K and Sandya Kattimani

Data Analysts:
Rajesh Chillappagari and Laxmi Kadve

Consultant Advisor:
Christophe de Boisset

Project Manager:
Shreemadhu Rai B

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 study will include data from the ISG Provider Lens™ program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. The data collected for this report represent information that ISG believes to be current as of May 2025 for providers that actively participated and for providers that did not. ISG recognizes that many mergers and acquisitions may have occurred since then, but this report does not reflect these changes.

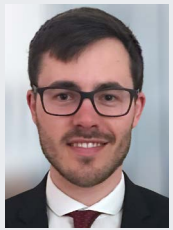
All revenue references are in U.S. dollars ($US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Services and Solutions 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

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Lead Author



Benoît Scheuber

Principal Consultant and Security Analyst

Senior and highly respected consultant in the fields of IT and security operations across all industries with a particular focus on the BFSI sector, Benoit has conducted many projects for large clients, including benchmark and sourcing projects, 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.

Author (Global - IAM)

Bhuvaneshwari Mohan

Author and Research Analyst

Bhuvaneshwari is a Senior Research Analyst at ISG and is responsible for driving and co-authoring ISG Provider Lens™ studies on Digital Business Enablement, Supply Chain, ESG Services and Cybersecurity. She contributes to the research process with necessary data and market analysis, develops content from an enterprise perspective, and authors Global Summary reports. She comes with 8 years of hands-on experience and has delivered insightful custom reports across verticals.

She is a versatile research professional having experience in Competitive Benchmarking, Social Media Analytics, and Talent Intelligence. Prior to ISG, she honed her research expertise in Sales Enablement roles with IT & Digital Services Providers and was predominantly part of Sales Enablement teams.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Author (Global - XDR)

Gowtham Sampath

Assistant Director and Principal Analyst, ISG Provider Lens™

Gowtham Sampath is a Prinicipal Analyst with ISG Research, responsible for authoring ISG Provider LensTM quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices.

In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries. He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.

Author (Global - SSE)

Yash Jethani

Senior Manager and Principal Analyst

Yash has over 14 years of professional experience, primarily in the technology, media and telecom (TMT) vertical. He has contributed to thought leadership, market and competitive research, consulting, business development, and due diligence as well as account management cutting across corporate marketing, risk, strategy, and sales functions.

Prior to ISG, Yash worked with KPMG in India supporting their national TMT practice in advisory, thought leadership as well as strategic pursuits. While at IDC, he was responsible for delivering custom as well as syndicated research for Telco & IoT Asia Pacific clients.

He has also had stints with CGI and TCS in supporting their corporate and account marketing initiatives with a focus on next-gen IT delivery within Telco/ Comms verticals. He currently contributes to ISG Provider Lens global research studies as a lead analyst for software defined networks, managed network services as well as telecom and media managed services studies across regions.

Yash holds a PGDM in Telecom & IT supported by an engineering degree in computers. He is also TM Forum certified and actively contributes as a member to the Bangalore Software Process Improvement Network, a non-profit.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Research Analyst (Global)

Sandya Kattimani

Senior Research Analyst

Sandya Kattimani is a senior research analyst at ISG and is responsible for supporting and co-authoring ISG Provider Lens™ studies on Contact Center, Life Sciences, Mainframes. Sandya has over 6 years of experience in the technology research industry and in her prior role, she carried out research delivery for both primary and secondary research capabilities. Her area of expertise lies in Competitive Intelligence, Customer Journey Analysis, Battle Cards, Market analysis and digital transformation.

She is responsible for authoring the enterprise content and the global summary report, highlighting regional as well as global market trends and insights. Prior to this role she has worked as technology research analyst, where she was responsible for project work which includes detail technology scouting, competitive intelligence, company analysis, technologies study and other Ad hoc business research assignments

Enterprise Context and Global Overview

Monica K

Assistant Manager and Lead Research Specialist

Monica K is an Assistant Manager and Lead Research Specialist at ISG, where she also serves as a digital expert. She co-authors Provider Lens™ studies, the global summary report, and the enterprise perspective for the cybersecurity, ESG, and sustainability markets. Her responsibilities include managing comprehensive research projects and collaborating with internal stakeholders on diverse consulting initiatives.

With over a decade of experience in technology, business, and market research, Monica brings valuable expertise to ISG clients. Previously, she worked at a research firm specializing in IoT, product engineering, vendor profiling, and talent intelligence.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

Study Sponsor

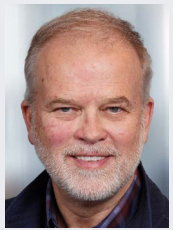
Heiko Henkes

Director & Principal Analyst, Global IPL Content Lead

Heiko Henkes serves as Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens™ (IPL) Program for all IT Outsourcing (ITO) studies alongside his pivotal role in the global IPL division as a strategic program manager and thought leader for IPL lead analysts.

Henkes heads Star of Excellence, ISG's global customer experience initiative, steering program design and its integration with IPL and ISG's sourcing practice. His expertise lies in guiding companies through IT-based business model transformations, leveraging his deep understanding of continuous transformation, IT competencies, sustainable business strategies and change management in a cloud-AI-driven business landscape. Henkes is known for his contributions as a keynote speaker on digital innovation, sharing insights on using technology for business growth and transformation.

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.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

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.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: Public Sector.

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 (Nasdaq: III) is a global AI-centered technology research and advisory firm. A trusted partner to more than 900 clients, including 75 of the world's top 100 enterprises, ISG is a long-time leader in technology and business services sourcing that is now at the forefront of leveraging AI to help organizations achieve operational excellence and faster growth.

The firm, founded in 2006, is known for its proprietary market data, in-depth knowledge of provider ecosystems, and the expertise of its 1,600 professionals worldwide working together to help clients maximize the value of their technology investments.

For more information, visit isg-one.com.

© 2025 INFORMATION SERVICES GROUP, INC. ALL RIGHTS RESERVED.

ISG Provider Lens™

JULY, 2025

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS

© 2025 Information Services Group, Inc.
All Rights Reserved