ISG Provider Lens®

Cybersecurity – Services and Solutions

An analysis of the cybersecurity market that compares the attractiveness of portfolios and the competitive strength of providers

Customized report courtesy of:

sure[secure]

QUADRANT REPORT | JULY 2025 | GERMANY, GLOBAL

Table of Contents

Report Author: Frank Heuer

Technological revolution and skills shortage drive the cybersecurity market in Germany

In increasingly challenging circumstances, cyber threats to companies in Germany are growing as cyberattacks become increasingly sophisticated, frequent, complex and adaptable. The shortage of qualified cybersecurity professionals is exacerbating the situation and driving demand for external services. New technologies favor cyber threats and also offer new business opportunities for service providers. Service providers that understand the requirements of different target groups and are proficient in both technical, business and regulatory aspects can also benefit here.

Those responsible in German companies are currently facing various challenges. The increased cyber threats in the context of political tensions, such as the war in Ukraine, and the trend toward remote working — along with the long-term trend of digitalization — have led to increased attack surfaces for cyber attacks in Germany, which require appropriate countermeasures. On the other hand, the weak economy is leading to financial challenges.

Business processes are increasingly being shifted to IT as part of digitalization. Intellectual property is also increasingly being represented digitally. As a result, the growing need to protect IT and communication systems has transformed IT security into corporate security. The increased use of home offices in Germany — and the resulting external connection of employees — has made IT systems more vulnerable to attack.

In addition to digitalization and increased remote working, the increasing provision of resources from the cloud has made IT systems more vulnerable and has led to the growing relevance of the zero trust approach and a loss of importance of perimeter security. The principle of *never trust, always verify* means, among other things, mutual authentication and continuous network monitoring.

Cyber criminals are implementing new, more sophisticated and more complex methods to overcome the cyber defense systems of

Multiple challenges are driving demand for external security services.

companies and authorities at ever shorter intervals. There have been a number of spectacular cyberattacks in the recent past, but less prominent attacks, such as ransomware, are also causing increasing problems for companies. Accordingly, cybersecurity measures must be completely up to date. Not least due to the shortage of IT specialists, especially in the cybersecurity market, companies and authorities are increasingly overwhelmed by this, and IT managers are increasingly using external services, such as security operations centers. These providers, as well as many IT security product providers, are increasingly relying on proactive rather than reactive methods based on AI, for example, to keep up with the threats themselves.

Not only companies' own protection, but also legal regulations such as the General Data Protection Regulation (GDPR) in the EU are forcing companies to implement stronger security measures to prevent cyberattacks. This continues to be a major challenge, especially for SMEs. In addition, many SMEs from certain sectors are currently being classified as infrastructure requiring special protection. Among other things, this will result in increased protection requirements and measures with regard to cybersecurity. The underlying EU Directive NIS-2 is expected to be transposed into national law in 2025.

SMEs are an interesting market segment for cybersecurity providers in Germany. Overall, SMEs have less mature IT security systems than large companies, but are forced to upgrade them due to the factors described above. As a result, they have significant progress to make and are, therefore, experiencing above-average growth in demand for cybersecurity solutions. A balanced customer structure of large and midsize companies is even more advantageous for security providers in order to benefit from the extensive budgets of large accounts. The current weak economy in Germany is not leaving the demand for cybersecurity solutions untouched, so that SMEs, with their above-average growth in demand, are becoming an increasingly attractive market segment that also needs to be adequately addressed. It is not enough to simply offer midsize customers a service for large customers. Rather, the entire go-to-market (GTM) approach — products, prices and communication — must be adapted to these customers. Communication and cultural aspects are particularly important in order to be accepted by SMEs as a provider that takes this segment seriously.

Despite the great importance of cybersecurity, IT managers are once again increasingly struggling with the task of legitimizing investments in cybersecurity vis-à-vis company stakeholders, especially the CFO. Unlike with other IT projects, it is not always possible to prove the profitability of cybersecurity investments; it is also not easy to quantify threat risks. On the other hand, more and more managers are recognizing that cyberattacks can lead to massive — and possibly existential — financial and reputational damage. As a result, IT security is becoming increasingly important in German companies, and senior management is becoming more involved in cyber risk management.

It is still the case that the cause of cybersecurity incidents is often not (solely) on the technical side. Rather, many attacks are facilitated by careless user behavior, such as phishing and Trojan attacks. In addition to up-to-date IT security equipment, user training and advice, therefore, continue to play an important role.

Advice is also increasingly in demand with regard to technical threats. In addition to cyber attacks and solutions based on AI, the need for advice is also increasing with regard to quantum-based attacks. These represent a new quality in attacks on the encryption of confidential data, which has now become much more urgent. While it was previously assumed that technical developments would leave time for concrete countermeasures until the end of the decade, this has changed due to new criminal strategies. With the *harvest now - decrypt later* approach, it has now become clear that the protection of data in the form of encryption needs to be reviewed and, if necessary, strengthened more urgently than previously assumed. As a result, the number of service providers that have adapted their consulting services to this new type of threat and opened up a new area of business has increased significantly over the last two years. These consulting services are currently still being used primarily by banks and insurance companies, as their assets consist of virtual

assets and are, therefore, potentially particularly at risk. Due to the dynamic development described above, demand is also rising sharply in other sectors of the economy.

Data leakage/loss prevention and data security (Products)

Interest in DLP solutions has increased significantly again in Germany in recent years. This is due to various factors that affect the security of data in companies. Data and intellectual property have become increasingly important and, in some cases, existentially significant corporate assets.

In addition, the increasing business use of private end devices poses a particular challenge in terms of protection against unwanted data leaks, as they are often beyond the configuration and control of the company's administration. Increasing regulatory requirements drive the demand for DLP solutions. AI supports manufacturers in offering powerful solutions.

Technical security services

Due to increasingly sophisticated cyberattacks and the pressing shortage of skilled workers, companies and authorities in Germany are increasingly reliant on external cybersecurity services to keep their IT security systems up to date.

Service providers that can offer a broad range of technical security services from a single source have a particular advantage in this market, as IT security projects are often complex and multifaceted.

Strategic security services

German companies are being called upon to protect their IT systems from damage in the face of increasingly frequent, intensive and sophisticated cyberattacks. It is no longer just the well-known large companies and public authorities that are affected, but increasingly also small and midsize companies. The shortage of IT specialists continues to make this situation more difficult.

Among other things, service providers that can offer their customers seamless end-to-end services and the integration of IT and security solutions from a single source have an advantage. In addition, in-depth knowledge of regulatory requirements is increasingly in demand, and advice on post-quantum encryption is becoming more important than previously expected.

Next-gen SOC/MDR services

The increasingly sophisticated cyberattacks are also driving demand for services from security operations centers (SOCs) and managed detection and response (MDR) services in particular. The shortage of qualified experts and the need for specialist knowledge that is always up to date make these services even more interesting for German companies.

Large and especially midsize customers appreciate SOCs with a German or EU location due to the increasingly important aspect of data protection (digital sovereignty). Integrated solutions comprising IT and associated security solutions, end-to-end security services and a high level of innovation are also important for both target groups in order to stay ahead in the race against cyber criminals.

Managed security service providers are increasingly turning to automation and AI to combat cyber threats. The ideal solution is to combine machine efficiency with comprehensive human expertise.

Quantum technology is becoming a threat to users faster than expected, but like AI, it also offers new opportunities for cybersecurity service providers. Service providers that address a balanced target group and master both technical and regulatory aspects have an advantage.

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**.

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

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.

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**.

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.

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**.

- **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.

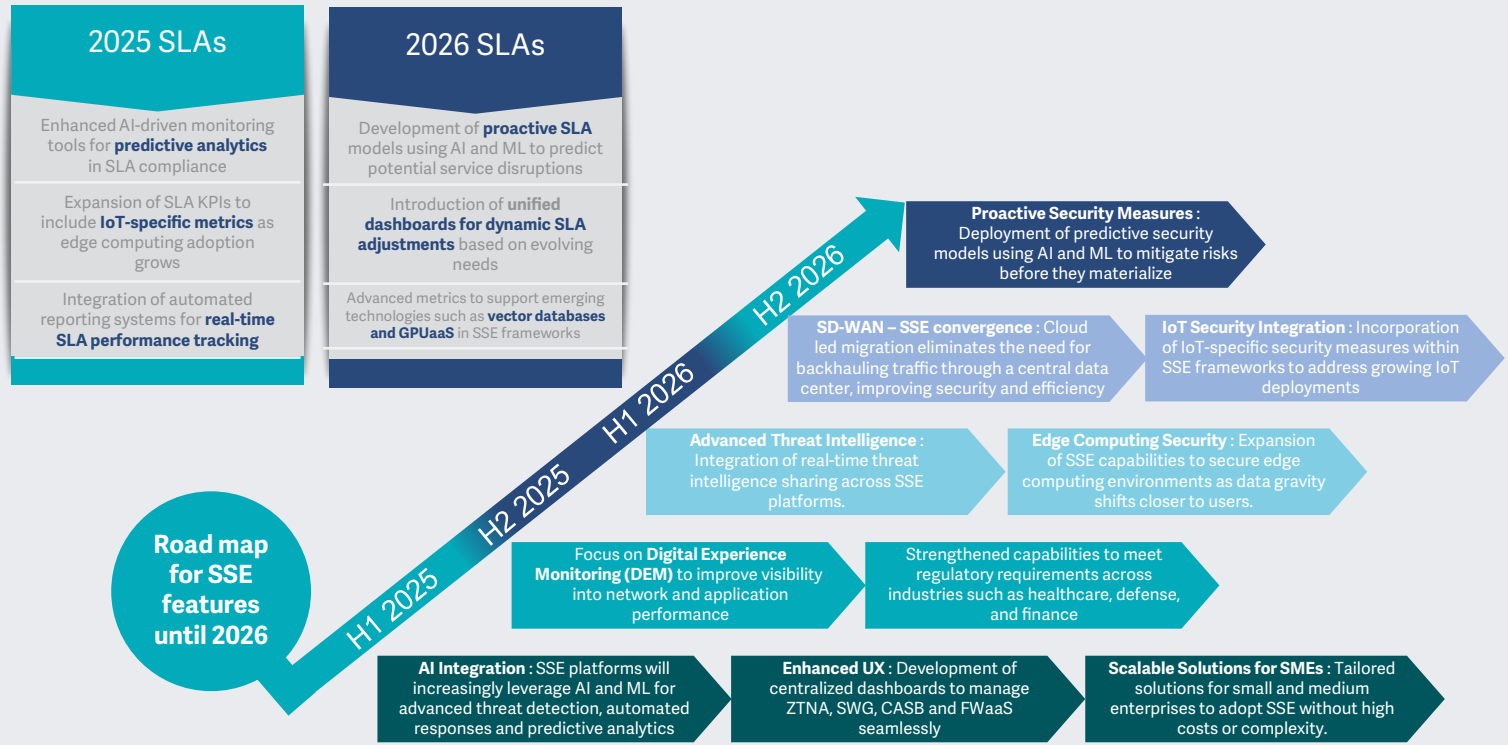
SSE provides the cloud-delivered security stack to implement zero trust principles at scale across distributed environments. It replaces traditional perimeter security with a flexible, identity-centric approach to secure remote work, cloud adoption and mobile access scenarios without sacrificing protection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



Source: ISG, 2025

- 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.

- 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

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.

Provider Positioning

Page 1 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Absolute Software	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Accenture	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Acronis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
All for One Group	Not In	Not In	Not In	Not In	Contender	Contender	Not In	Not In
Aryaka	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Atos	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Axians	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
Bechtle	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader	Leader
Beta Systems	Contender	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

Provider Positioning

Page 2 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Bitdefender	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
BlackBerry (Arctic Wolf)	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Brainloop	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In
CANCOM	Not In	Not In	Not In	Not In	Leader	Market Challenger	Leader	Leader
Capgemini	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Not In
Cato Networks	Not In	Not In	Not In	Leader	Not In	Not In	Not In	Not In
CGI	Not In	Not In	Not In	Not In	Not In	Product Challenger	Contender	Contender
Check Point Software	Not In	Not In	Product Challenger	Leader	Not In	Not In	Not In	Not In
Cisco	Not In	Not In	Market Challenger	Leader	Not In	Not In	Not In	Not In

Provider Positioning

Page 3 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Cloudflare	Not In	Not In	Not In	Market Challenger	Not In	Not In	Not In	Not In
Computacenter	Not In	Not In	Not In	Not In	Leader	Leader	Product Challenger	Contender
Controlware	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
CoSoSys (Netwrix)	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Not In	Leader	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
Cybereason	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
DATAGROUP	Not In	Not In	Not In	Not In	Not In	Not In	Market Challenger	Leader
Deloitte	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In

Provider Positioning

Page 4 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Deutsche Telekom	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Leader
DIGITALL	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
DriveLock	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
DXC Technology	Not In	Not In	Not In	Not In	Leader	Product Challenger	Contender	Not In
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Ericom Software	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
ESET	Not In	Not In	Contender	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
EY	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Fidelis Cybersecurity	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Fischer Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Leader	Not In	Leader	Not In	Not In	Not In	Not In
Fortinet	Market Challenger	Not In	Leader	Leader	Not In	Not In	Not In	Not In
Fortra	Market Challenger	Leader	Not In	Not In	Not In	Not In	Not In	Not In
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
GBS	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Getronics	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Product Challenger
glueckkanja	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
Google	Not In	Contender	Not In	Not In	Not In	Not In	Not In	Not In
Gopher Security	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In

Provider Positioning

Page 6 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
HCLTech	Not In	Not In	Not In	Not In	Leader	Leader	Leader	Product Challenger
HiSolutions	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
HPE (Aruba)	Not In	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In
IBM	Leader	Leader	Leader	Not In	Leader	Leader	Leader	Not In
iboss	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
iC Consult	Not In	Not In	Not In	Not In	Contender	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
indevis	Not In	Not In	Not In	Not In	Rising Star ★	Not In	Market Challenger	Market Challenger
InfoGuard	Not In	Not In	Not In	Not In	Not In	Not In	Rising Star ★	Leader
Infosys	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In

Provider Positioning

Page 7 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
itWatch	Not In	Product Challenger	Not In	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
Kaspersky	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Not In	Leader	Not In	Not In
Kyndryl	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Contender	Not In
LMNTRIX	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Logicalis	Not In	Not In	Not In	Not In	Contender	Contender	Product Challenger	Product Challenger
Lookout	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In
LTIMindtree	Not In	Not In	Not In	Not In	Contender	Not In	Product Challenger	Product Challenger
ManageEngine	Leader	Rising Star ★	Not In	Contender	Not In	Not In	Not In	Not In

Provider Positioning

Page 8 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Materna	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★	Not In	Not In
Matrix42	Not In	Leader	Not In	Not In	Not In	Not In	Not In	Not In
Menlo Security	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Microsoft	Leader	Leader	Leader	Market Challenger	Not In	Not In	Not In	Not In
Mimecast	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Netskope	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger
Okta	Leader	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
Open Systems	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In

Provider Positioning

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
OpenText	Product Challenger	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Orange Cyberdefense	Not In	Not In	Not In	Not In	Market Challenger	Product Challenger	Leader	Not In
ORBIT	Not In	Not In	Not In	Not In	Contender	Contender	Not In	Not In
Palo Alto Networks	Not In	Not In	Leader	Leader	Not In	Not In	Not In	Not In
pco	Not In	Not In	Not In	Not In	Not In	Contender	Contender	Contender
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Market Challenger	Not In	Contender	Not In	Not In	Not In	Not In
Rapid7	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
RSA	Market Challenger	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

Provider Positioning

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In	Not In	Not In
SenseOn	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
SentinelOne	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Seqrite	Not In	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Sequretek	Contender	Not In	Contender	Not In	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Product Challenger	Not In	Product Challenger	Not In	Not In	Not In	Not In
SonicWall (Banyan Security)	Not In	Not In	Not In	Contender	Not In	Not In	Not In	Not In
Sophos	Not In	Not In	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Sopra Steria	Not In	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger

Provider Positioning

Page 11 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
suresecure	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Leader
SVA	Not In	Not In	Not In	Not In	Not In	Not In	Product Challenger	Rising Star ★
Syntax	Not In	Not In	Not In	Not In	Product Challenger	Not In	Contender	Product Challenger
TCS	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader	Not In
Tech Mahindra	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger	Product Challenger
TEHTRIS	Not In	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In	Not In
Trellix	Not In	Leader	Leader	Not In	Not In	Not In	Not In	Not In
Trend Micro	Not In	Not In	Leader	Not In	Not In	Not In	Not In	Not In
Unisys	Not In	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger	Not In

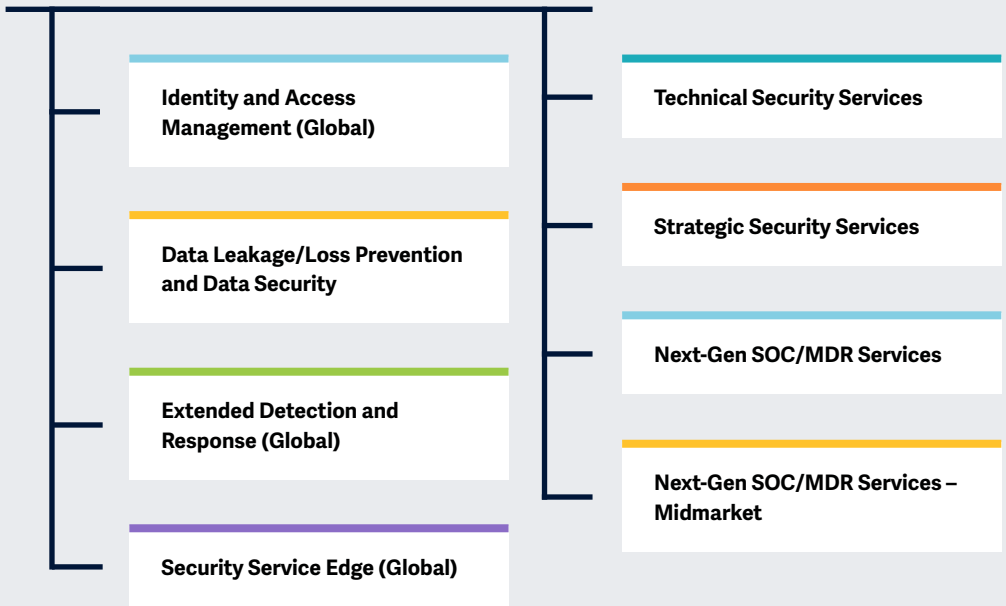
Provider Positioning

Page 12 of 12

	Identity and Access Management (Global)	Data Leakage/Loss Prevention and Data Security	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/ MDR Services	Next-Gen SOC/ MDR Services – Midmarket
Varonis	Not In	Product Challenger	Not In	Not In	Not In	Not In	Not In	Not In
Verizon Business	Not In	Not In	Not In	Not In	Not In	Contender	Product Challenger	Not In
Versa Networks	Not In	Not In	Not In	Leader	Not In	Not In	Not In	Not In
Wavestone	Not In	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In
Wipro	Not In	Not In	Not In	Not In	Product Challenger	Leader	Product Challenger	Not In
Xantaro	Not In	Not In	Not In	Not In	Product Challenger	Not In	Not In	Not In
Zscaler	Not In	Product Challenger	Not In	Leader	Not In	Not In	Not In	Not In

Key areas covered in the **"Cybersecurity – Services and Solutions 2025"** study.

Simplified Illustration Source: ISG 2025



Definition

Cybersecurity in the Age of AI and Upcoming Disruptive Technology

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 operational technology (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.

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.

Scope of the Report

This ISG Provider Lens® quadrant report covers the following eight quadrants for services/solutions: Identity and Access Management (Global), Data Leakage/Loss Prevention and Data Security, Extended Detection and Response (Global), Security Service Edge (Global), Technical Security Services, Strategic Security Services, Next-Gen SOC/MDR Services and Next-Gen SOC/MDR Services – Midmarket.

This ISG Provider Lens® study offers IT decision makers:

- Transparency about the strengths and weaknesses of the respective providers and software manufacturers
- differentiated positioning of providers according to segments (quadrants)
- Focus on the regional market

The study thus provides an essential decision-making basis for positioning, relationship and go-to-market considerations. ISG Advisors and enterprise clients also use information from these reports to evaluate their current and potential new vendor relationships.

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).

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.

Identity and Access Management (Global)

Who Should Read This Section

This report is valuable for vendors offering **identity and access management (IAM)** solutions **globally** to understand their market position and for enterprises looking to evaluate these vendors. In this quadrant, ISG highlights the current market positioning of these vendors based on the depth of their capabilities and market presence. The report outlines the key IAM challenges, including securing identities in hybrid IT environments, enabling seamless access and combating advanced threats, emphasizing the need for adaptive authentication, zero trust and unified identity solutions for agility.

Technology professionals

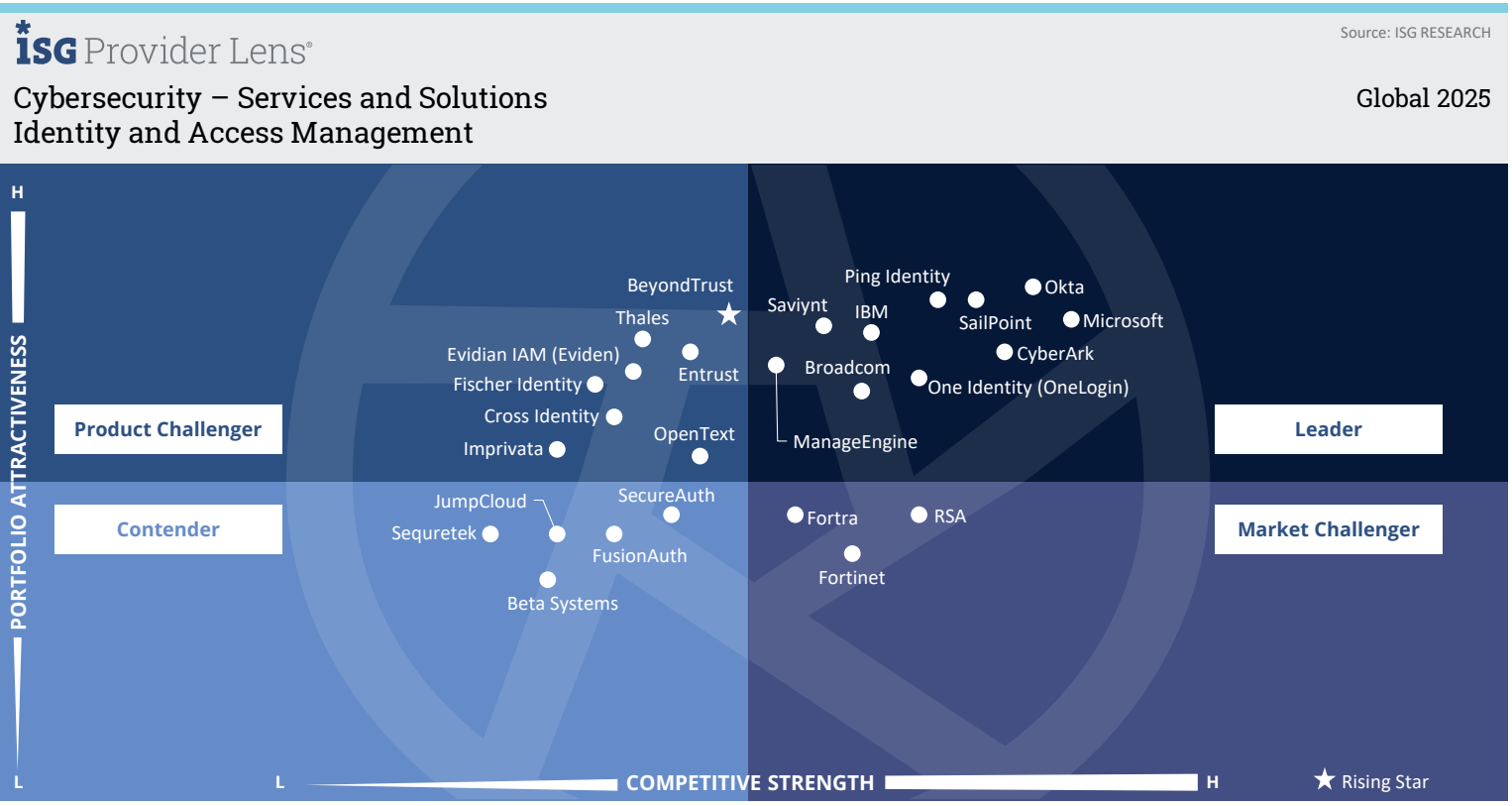
Should read this report to understand vendors' integration capabilities to reduce threat impact, where they use advanced technologies to transform legacy systems.

Security and data professionals

Should read this report to gain insights into the way vendors comply with security and data protection regulations and stay updated with market trends.

Business professionals

Should read this report to balance data security, CX and privacy in the current business environment, which prioritizes digital transformation.



The quadrant examines IAM vendors that excel in deploying **adaptive identity solutions**. Essential features include **real-time access controls** for **zero trust security**, along with a **user-friendly interface** and compliance with **regulatory requirements**.

Bhuvaneshwari Mohan

Definition

IAM solution providers assessed in this quadrant are distinguished by their proprietary software, including SaaS, and services for managing enterprise user identities. It excludes pure service providers that do not offer an IAM product, either on-premises or cloud-based, developed with proprietary software. Depending on organizational needs, these solutions can be deployed on-premises, in customer-managed clouds, as as-a-service models or as a combination of these options.

IAM solutions focus on managing user identities and access rights, including specialized access through privileged access management (PAM) governed by defined policies. IAM suites integrate secure mechanisms, frameworks and automation for real-time user and attack profiling to meet evolving application needs. Providers are also expected to include social media and mobile access functionalities, addressing security needs beyond traditional web rights management. This quadrant also encompasses machine identity management.

Eligibility Criteria

1. Offer solutions that can be **deployed on-premises**, in the **cloud**, as **identity-as-a-service** (IDaaS) or through a managed third-party model
2. Deliver solutions that can **support authentication** as a combination of **single sign-on (SSO), multifactor authentication (MFA)**, and risk-based and context-based models
3. Offer solutions that can **support role-based access** and PAM
4. Provide **access management** to address multiple enterprise needs such as **cloud, endpoint, mobile devices, APIs and web applications**
5. Propose solutions that can **support one or more legacy and new IAM standards**, including, but not limited to, SAML, OAuth, OpenID Connect, WS-Federation, WS-Trust and SCIMOffer a portfolio with one or more of the following solutions — **directory, dashboard or self-service management** and lifecycle management (migration, sync and replication) — to support secure access

Observations

In 2025, the IAM market will evolve rapidly, driven by AI-powered security, passwordless authentication and compliance needs. Vendors focus on identity-centric security, automation and UX to support enterprises in managing the digital identities of both human and non-human identities across dynamic and complex environments.

Identity threat detection and response (ITDR) has gained significant attention over the last 12-18 months. Vendors are integrating AI and ML for identity threat detection, automating governance and enforcing risk-based authentication. Security teams increasingly leverage intelligent identity analytics to detect and respond to threats in real time, minimizing the attack surface. Passwordless authentication, including passkeys, biometrics and FIDO2, is becoming standard, reducing phishing risks while ensuring seamless user access.

Zero trust models continue to shape IAM, as it is essential for robust identity management. Real-time capabilities such as dynamic access management are becoming critical to ensure better alignment with zero trust principles. Most IAM platforms are steadily evolving toward semi-autonomous access control by integrating predictive AI to enhance policy decisions and context-aware responses while maintaining operational oversight.

Cloud adoption accelerates IAM's shift toward scalable, interoperable IDaaS solutions, ensuring seamless authentication across hybrid and multicloud environments. Decentralized identity is also emerging, allowing users greater control over personal data. The demand for CIAM solutions is rising as businesses seek to provide secure, personalized and seamless digital experiences for their customers while ensuring robust fraud prevention and privacy protection.

From the 61 companies assessed for this study on a global level, 26 qualified for this quadrant, with ten being Leaders and one Rising Star.

Broadcom

Broadcom empowers enterprises to shift from fragmented IAM to a fully orchestrated one by combining technology, scale and domain expertise and identity-centric security model — ready for hybrid cloud, zero trust architectures and regulatory agility.

CyberArk

CyberArk is transforming into a full-scale identity security powerhouse, addressing modern attack surfaces while maintaining its PAM leadership augmented by its adaptive and zero trust-driven approach.

IBM

IBM's Security Verify enables enterprises to ensure frictionless and secure access control across on-premises, cloud and hybrid cloud environments. Its identity fabric and orchestration capabilities allow for highly customizable workflows.

ManageEngine

ManageEngine offers cost-effective, modular IAM tailored for Microsoft environments. Enterprises benefit from robust on-premises AD lifecycle automation, MFA and auditing without needing full cloud migration.

Microsoft

Microsoft Entra delivers a unified identity platform with deep integration across Microsoft 365, Azure and third-party applications. It is ideal for enterprises seeking scalable, cloud-native identity with native zero trust and conditional access controls.

Okta

Okta's cloud-native architecture ensures high availability and scalability, making it ideal for enterprises of all sizes. Its multicloud compatibility allows seamless integration with AWS, Google Cloud and Azure.

One Identity

One Identity unifies identity governance and administration (IGA) with PAM on a single platform, which is ideal for enterprises modernizing legacy IAM while controlling privileged access. Its deep AD/LDAP integration and robust governance automation simplify hybrid deployments.

Ping Identity excels with its flexible, hybrid-ready IAM platform, blending AI-driven risk analysis, no-code orchestration via DaVinci and deep standards support to empower secure, adaptive access across complex enterprise environments.

SailPoint

SailPoint is solidifying its position as a leader in identity security with cutting-edge AI-powered solutions and cloud-first innovation. Strategic acquisitions, including PAM, third-party risk management and healthcare-focused IGA, are broadening its capabilities, driving secure, scalable identity management for enterprises.

Saviynt

Saviynt empowers enterprises with cloud-native identity governance, unifying IGA, PAM and access to insights in a single platform. Its fine-grained entitlement management and risk-aware automation support complex compliance-driven environments.

BeyondTrust (Rising Star) stands out with enterprise-grade privileged access management, offering adaptive risk-based controls, session monitoring and endpoint privilege security, which are critical for minimizing attack surfaces across hybrid infrastructure.

Hidden Champions:

Entrust is recognised as a hidden champion for its strong capabilities in IAM, particularly in digital identity, PKI and authentication. Its offerings are well-suited to enterprises addressing hybrid work models, zero trust adoption and regulatory compliance requirements. Its ability to deliver scalable, secure and compliance-ready IAM solutions makes Entrust a valuable enabler of resilient access control and trust assurance, especially for financial and government clients.

Fischer Identity is recognised as a hidden champion for its policy-driven IGA automation, seamless Identity as a Service (IDaaS) delivery model, and purpose-built support for regulated sectors such as education and public sector. It excels in delivering configurable lifecycle governance, centralized identity data management, and compliance-aligned access controls. Its streamlined architecture reduces complexity and offers a strong value proposition for mid-sized enterprises needing rapid deployment.

Data Leakage/Loss Prevention and Data Security

Who Should Read This Section

This report is valuable for vendors offering **data leakage/loss prevention (DLP) and data security** solutions in **Germany** to understand their market position and for enterprises looking to evaluate these vendors. In this quadrant, ISG highlights the current market positioning of these vendors based on the depth of their solution offerings and market presence.

IT security professionals

Should read this report to gain insights into emerging trends, innovative features and best practices in the field.

Chief information security officers

Must read this report to gain insights into the evolving landscape of DLP strategies and solutions, enabling informed decision-making investments in cybersecurity technologies.

Compliance officers

Responsible for ensuring adherence to data protection regulations should read this report to learn how DLP solutions can help their organizations achieve and maintain compliance.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Data Leakage/Loss Prevention and Data Security

Germany 2025

This quadrant evaluates the **most relevant** DLP providers in Germany that offer or operate proprietary **software**. The protection of **intellectual property** and pressing **data protection concerns** contribute to the importance of the market.

Frank Heuer

Data Leakage/Loss Prevention and Data Security

Definition

DLP solution providers assessed in this quadrant are distinguished by their proprietary software, including SaaS, and associated services. It excludes pure service providers that do not offer a DLP product, either on-premises or cloud-based, developed with proprietary software. DLP solutions can identify and monitor sensitive data and provide access to authorized users. They include a mix of products offering visibility and control over sensitive data residing in cloud applications, endpoints, networks and various devices.

DLP solutions help companies face challenges in controlling data movements, with over one-third of data violations originating internally. The proliferation of mobile and other devices for data storage elevates these concerns, as they can exchange data without central gateways. Data security solutions protect against unauthorized access and theft by prioritizing, classifying and monitoring data at rest and in transit, enabling organizations to enhance data security.

Eligibility Criteria

1. Offer DLP solutions based on **proprietary software** and not third-party software
2. Demonstrate the capability to support DLP **across any architecture, such as the cloud, network, storage or endpoint**
3. Showcase the ability to **protect sensitive data**, whether **structured or unstructured**, in text or binary formats
4. Provide solutions with **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
5. Offer solutions capable of **identifying sensitive data, enforcing policies**, monitoring traffic and improving data compliance

Observations

Data and intellectual property have become increasingly important and, in some cases, existentially significant corporate assets, which has contributed to the growing interest in DLP solutions. The increasing business use of private end devices also poses a particular challenge in terms of protection against unwanted data outflows, as they are often beyond the configuration and control of the company administration and, in some cases, may not be comprehensively monitored by the company for legal reasons. DLP solutions must take these restrictions into account when monitoring without allowing operational security gaps. The GDPR and the NIS 2 Directive have further increased the importance of data protection in companies.

The enormous increase in company data requires powerful DLP solutions that can quickly detect and classify data and protect it from unauthorized actions according to its protection requirements. Cloud storage solutions and applications inherently carry the risk of data unintentionally leaking from the company network during processing. Social media and communication platforms open up communication channels through which data can flow; last but not least, there are risks associated with data transfers via email. However, the risks do not solely stem from unintentional data leaks caused by internal players; companies must also be able to protect themselves against unfaithful behavior on the part of internal participants. AI is increasingly helping to overcome these challenges.

Mimecast and ManageEngine are new to the quadrant. The latter provider is also the new Rising Star.

Of the 68 providers that were assessed specifically for the German market in this study, 24 qualified for this quadrant, with nine Leaders and one Rising Star.

Broadcom

Broadcom's solutions' performance and flexibility are an advantage for both the provider and its customers. Broadcom supports its customers through centralization and standardization.

DriveLock

DriveLock scores points with its trustworthiness and earns this trust in the market with the *Made in Germany* and *No Backdoor* credentials. DriveLock is also characterized by the consistent use of ML algorithms.

Forcepoint

Forcepoint helps users quickly with its range of advanced solutions and relieves them of data loss protection challenges.

Fortra

Fortra is able to comprehensively support its customers with proactive data classification, advanced analysis and reporting services and simple integration.

GBS

GBS's sophisticated technology, the dual control principle and DLP made in Germany contribute to its leading position.

IBM

IBM combines a strong market presence with a forward-looking DLP solution and scores points with the competent combination of DLP with AI and post-quantum encryption. IBM's solution also covers a universal range of applications.

Matrix42 offers an efficient DLP solution with a broad range of functions. Matrix42 enjoys a high level of acceptance among end users thanks to its user-friendly, low-impact approach, which also promotes the successful use of the solution.

Microsoft

Microsoft knows how to further expand its position in the German market for DLP solutions . The provider is increasingly establishing itself in this country with the help of integration and bundling and convincing performance features.

Trellix

Trellix is very versatile in terms of delivery due to its strong local and international presence. Trellix customers also benefit from the wide range of services offered by the DLP solution.

ManageEngine helps to make it easier to ensure data security through automation and simplify compliance with legal requirements. This makes ManageEngine a Rising Star in the DLP market.

Extended Detection and Response (Global)

Who Should Read This Section

This report is valuable for providers offering **extended detection and response (XDR)** services **globally** 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. It evaluates global XDR service providers for their enhanced visibility and unified threat detection capabilities that aid enterprises having limited resources with data-driven insights and integration.

Security professionals

Should read this report for a broad outlook on security trends and discern providers' capabilities in helping enterprises devise robust security strategies.

Technology professionals

Should read this report to gain insights into the emerging trends in the security landscape and providers' abilities to develop tailored security platforms.

Strategy professionals

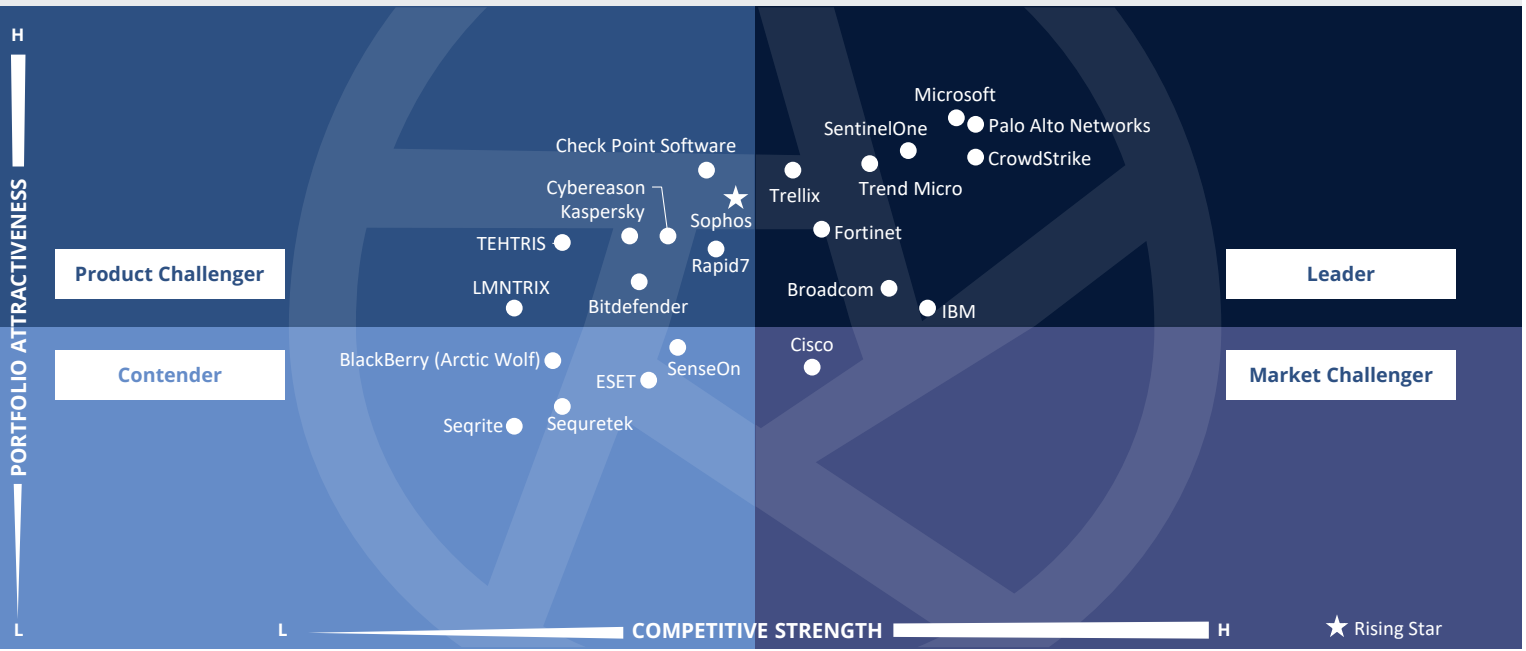
Should read this report to understand service providers' relative positioning and also capabilities in supporting decision-making on partnerships and cost-reduction initiatives.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Extended Detection and Response

Global 2025



This quadrant assesses XDR vendors' and their platforms' ability to provide **integrated threat detection, investigation and response capabilities that enhance visibility and threat context across multiple endpoints, networks and cloud** environments.

Gowtham Sampath

Definition

XDR solution providers assessed in this quadrant are distinguished by their platforms that integrate, correlate and contextualize data and alerts from multiple threat prevention, detection and response components. XDR is a cloud-based technology integrating multiple security solutions and using analytics to improve detection accuracy. It consolidates security products to enhance visibility and threat context across enterprise workspaces, networks and workloads.

XDR solutions use telemetry and contextual data for detection and response, integrating multiple products into a unified interface. They feature high automation and prioritize alerts based on severity to determine the needed tailored responses. This quadrant excludes pure service providers that do not offer an XDR solution based on proprietary software. XDR solutions aim to reduce product sprawl alert fatigue and address integration challenges. They help security operations teams manage or derive value from security information and event management (SIEM) or security orchestration, automation and response (SOAR) solutions.

Eligibility Criteria

1. Offer XDR solutions based on **proprietary software** and not on third-party software
2. Ensure that an XDR solution has two primary components: **XDR front end and XDR back end**
3. Offer front end with **three or more solutions or sensors**, including, but not limited to, **endpoint detection and response, endpoint protection platforms**, network protection (firewalls and IDPS), **network detection and response**, identity management, email security, mobile threat detection, cloud workload protection and deception identification
4. Provide solutions with **comprehensive and total coverage and visibility of all endpoints** in a network
5. Offer solutions capable of **blocking** sophisticated threats such as **advanced persistent threats, ransomware** and malware
6. Provide solutions using **threat intelligence** and **real-time insights on threats** emanating across endpoints
7. Deliver solutions with **automated response features**

Observations

The XDR market is undergoing rapid evolution, shaped by increasing enterprise demand for integrated threat detection, response automation and advanced analytics across endpoints, networks, cloud environments and identities. Vendors are aggressively embedding AI and ML across their platforms to reduce dwell times, accelerate threat triage and enable more predictive, behavior-based detection models. This has elevated XDR from a reactive tool into a proactive defense layer, particularly as threat actors become sophisticated and targeted in their approaches.

Native- and third-party solution integration continues to be a critical differentiator, with XDR platforms expanding telemetry ingestion capabilities to include third-party SIEMs, SOAR tools, threat intelligence feeds and adjacent security technologies. Many solutions now offer unified analyst workbenches, curated detections and automated playbooks designed to support lean security operations center (SOC) teams. This enhances visibility and enables faster correlation and contextualization of alerts, reducing false positives and analyst fatigue.

Vendors are actively acquiring competitors, accelerating innovation to enhance threat detection capabilities, expand into new customer segments, or embed managed detection and response (MDR) expertise.

As enterprises seek outcomes over tooling, XDR platforms are evolving to offer modular, cloud-delivered architectures with flexible deployment models. Vendors also focus on modular deployment options that cater to hybrid and multicloud environments, enabling organizations to extend security coverage without increasing complexity.

From the 61 companies assessed for this study on a global level, 23 qualified for this quadrant, with nine being Leaders and one Rising Star.

Broadcom

Broadcom's Symantec XDR solution delivers unified threat detection and response, integrating telemetry across multiple domains. The focus is on reducing alert fatigue through correlation, prioritization and automation within a broad ecosystem of Symantec solutions.

CrowdStrike

CrowdStrike's Falcon Insight XDR platform builds on its well-known EDR foundation and cloud-native architecture to deliver a scalable, high-performance detection and response solution that combines threat intelligence, AI and behavioral analytics.

Fortinet

Fortinet's FortiXDR delivers extended detection and response by tightly integrating across its native security fabric, including network, endpoint, email and cloud. The platform emphasizes automation-first response, AI-driven analytics and deep telemetry correlation.

IBM

IBM's XDR strategy is centered around QRadar Suite, combining threat detection, investigation, and response capabilities across hybrid environments. The platform emphasizes open integration, AI-driven automation and deep threat intelligence via IBM X-Force.

Microsoft

Microsoft Defender XDR's 100 percent protection in the MITRE Engenuity ATT&CK® Evaluations shows full visibility and defense across all attack stages, including Windows and Linux underscoring its robust multiplatform support.

Palo Alto Networks

Palo Alto Networks has completed its acquisition of IBM's QRadar SaaS assets. The company aims to provide its customers with advanced security solutions powered by next-gen security SOCs and AI.

SentinelOne

SentinelOne will retire its legacy deception product to focus on higher-growth segments and prioritize investments in AI-powered security and data. It is authorized to sell AI-powered security tools to the most security-conscious federal agencies.

Trellix

Trellix delivers an open and adaptive XDR platform to support dynamic defense strategies. Its emphasis is on integration, threat intelligence and ML to enable faster detection and autonomous response across enterprise environments.

Trend Micro

Trend Micro launched Trend Cybertron, a specialized cybersecurity large language model (LLM) integrated with its Trend Vision One platform. This innovative AI-powered cybersecurity agent is designed to shift enterprises toward a proactive security model.

Sophos

Sophos' (Rising Star) recent acquisition of SecureWorks' MDR business is expected to significantly expand Sophos' threat detection capabilities, service-led offerings and Intercept X platform with improved visibility and automation.

Security Service Edge (Global)

Who Should Read This Section

This report is valuable for providers offering services related to **security service edge (SSE) globally** 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. Enterprises should read this report for insights on security service edge (SSE) service providers, which is crucial for ensuring security across hybrid and multicloud environments.

Data management professionals

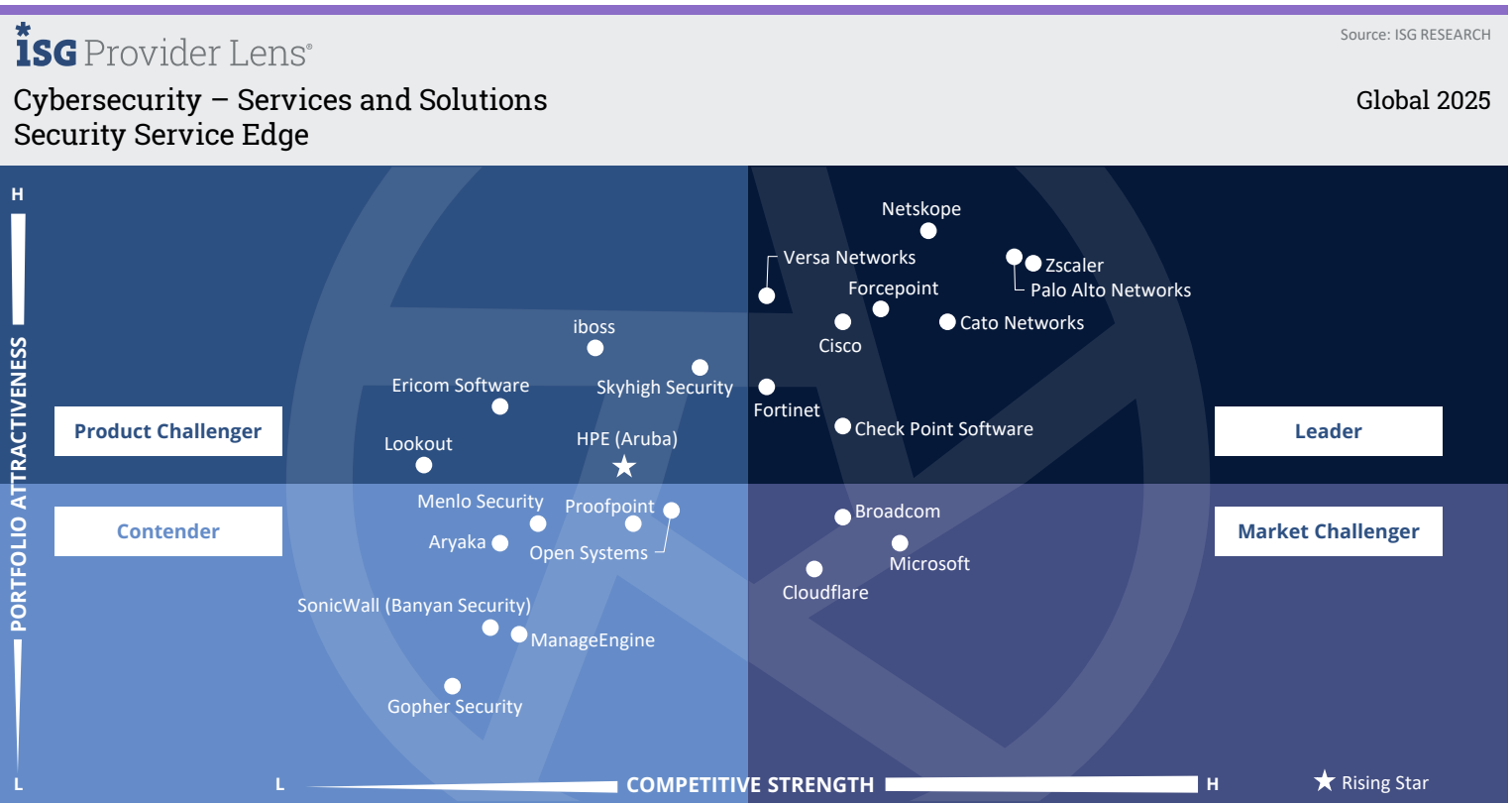
Should read this report to understand how SSE providers help enterprises overcome challenges related to data regulation mandates with enhanced policy controls and reporting.

Technology professionals

Should read this report to understand how SSE providers assist with adopting enterprisewide zero trust frameworks to improve their security posture.

Strategy professionals

Should read this report for insights on SSE providers' critical capabilities and their focus on user-centricity to deliver security at the edge or for devices through the cloud.



This quadrant, emphasizing UX, evaluates SSE vendors that deliver **cloud-centric solutions**, integrating various offerings to enable safe access to cloud, **SaaS, web services and private applications**.

Yash Jethani

Definition

SSE solution providers assessed in this quadrant offer cloud-centric solutions, combining proprietary software or hardware and associated services, enabling secure access to the cloud, SaaS, web services and private applications. Providers offer SSE solutions as an integrated security service through globally positioned points of presence with support for local data storage that combines individual solutions such as zero trust network access (ZTNA), cloud access security broker (CASB), secure web gateways (SWG) and firewall as a service (FWaaS). SSE can also include other security solutions such as DLP, browser isolation and next-generation firewall (NGFW) to secure access to cloud and on-premises applications.

Providers showcase expertise in complying with local, regional and domestic laws, such as data sovereignty, for global clients. This quadrant excludes the network components of secure access service edge (SASE), such as SD-WAN, which will be covered in the ISG Provider Lens® Network – Software Defined Solutions and Services 2025 study.

Eligibility Criteria

1. Provide SSE as an **integrated solution** with **ZTNA, CASB, SWG and FWaaS** components
2. Offer solutions **predominantly based on proprietary** software; these solutions may **partially rely on partner solutions** while avoiding **complete dependency on third-party** software
3. Maintain **globally located points of presence** to deliver solutions
4. Deliver **SSE functionalities to cloud and on-premises** environments (including hybrid environments)
5. Undertake **contextual and behavioral evaluations and analysis (user entity and behavior analytics [UEBA])** to detect and prevent malicious or suspicious intent
6. Offer **basic management support**, including, but not limited to, **reporting, policy controls**, installation and maintenance, and advanced threat detection functionalities
7. Ensure **availability of solutions globally**

Observations

Most companies prioritize SASE or SSE architectures with integrated security and networking. There is a growing shift toward cloud-native services for scalability and resilience, with AI increasingly enhancing threat defense and data protection. Zero trust is commonly emphasized for securing application and data access. Many providers are expanding globally and strengthening offerings through partnerships, with most focusing on cybersecurity, data protection and threat mitigation.

However, differentiated features of top providers include contextual policy enforcement, future-proof security and strategic growth partnerships. Many providers highlight advanced threat defense and data protection as core strengths, providing integrated or cloud-native solutions across diverse environments. Innovation in AI-driven security, intelligent service delivery for targeted markets, and foresight into emerging technologies such as secure browsers and quantum and AI applications stand out as differentiators.

Besides, the convergence of networking and security for high-performance environments necessitates providers to constantly adapt and expand their capabilities to address the complexities of modern security. UX and cloud-native scalability are key priorities, especially for HPE (Aruba) and Fortinet via global PoPs and partnerships. Single-vendor solutions from Versa and Netskope streamline deployment, while Palo Alto's Prisma SASE targets digital experience monitoring (DEM). Market growth is projected to be driven by a threefold to fivefold increase in AI applications set to reshape security.

From the 61 companies assessed for this study on a global level, 24 qualified for this quadrant, with nine being Leaders and one Rising Star.

Cato Networks

Cato Networks delivers the scalable, resilient Cato Single Pass Cloud Engine (Cato SPACE) architecture that powers a global cloud service with comprehensive contextual policy enforcement based on network, device, identity, application and data attributes.

Checkpoint

Checkpoint emphasizes Quantum SASE and Harmony Connect, focusing on cloud security and ZTNA. Partnerships, including Tata Communications, enhance its global reach and drive regional growth through industry recognition, consulting expertise, global R&D and AI-driven security innovations.

Cisco

Cisco highlighted its threat defense during the Mobile World Congress 2025, with AI assistant integrations announced for 2025.

Forcepoint

Forcepoint establishes itself as a leader in data protection and AI with its Forcepoint ONE™ platform, offering a comprehensive cloud-native SSE solution for cloud, web, private apps and endpoints.

Fortinet

Fortinet's FortiSASE leverages partnerships and FortiGuard AI services, targeting hybrid environments with a licensing model. Fortinet focuses on unified SASE enhancements, hybrid mesh firewall evolution, and OT security integration.

Netskope

Netskope promotes its intelligent SSE and NewEdge cloud, with a midmarket SASE launch in January 2024 tailored for MSPs, emphasizing zero trust telemetry.

Palo Alto Networks

Palo Alto Networks expects threefold to a fivefold growth in AI apps – providing a boost to adoption of its secure browser adoption – integrating AI into Prisma SASE while excelling in SSE with strong Zero Trust and threat prevention capabilities.

Versa Networks

Versa Networks highlights over 100 Gbps unified SASE gateways, focusing on consolidating networking and security for large enterprises via a robust partner ecosystem.

Zscaler emphasizes its zero trust SASE with new SD-WAN capabilities launched in January 2024, focusing on seamless UX and AI-driven security enhancements.

HPE (Aruba)

HPE (Aruba) (Rising Star) has integrated its SSE with SD-WAN following the acquisition of Axis Security in 2023. With the addition of AI enhancements and plans for acquiring Juniper Networks (pending for 2025), HPE (Aruba) is poised to expand its capabilities further.

Technical Security Services

Who Should Read This Section

This report is valuable for providers offering **technical security services (TSS)** in **Germany** 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.

Technology professionals

Should read this report to understand how providers' integration capabilities can reduce threat impact by transforming legacy systems and using advanced technologies.

Security and data professionals

Should read this report to gain insights into how providers comply with security and data protection laws and stay abreast with market trends.

Business professionals

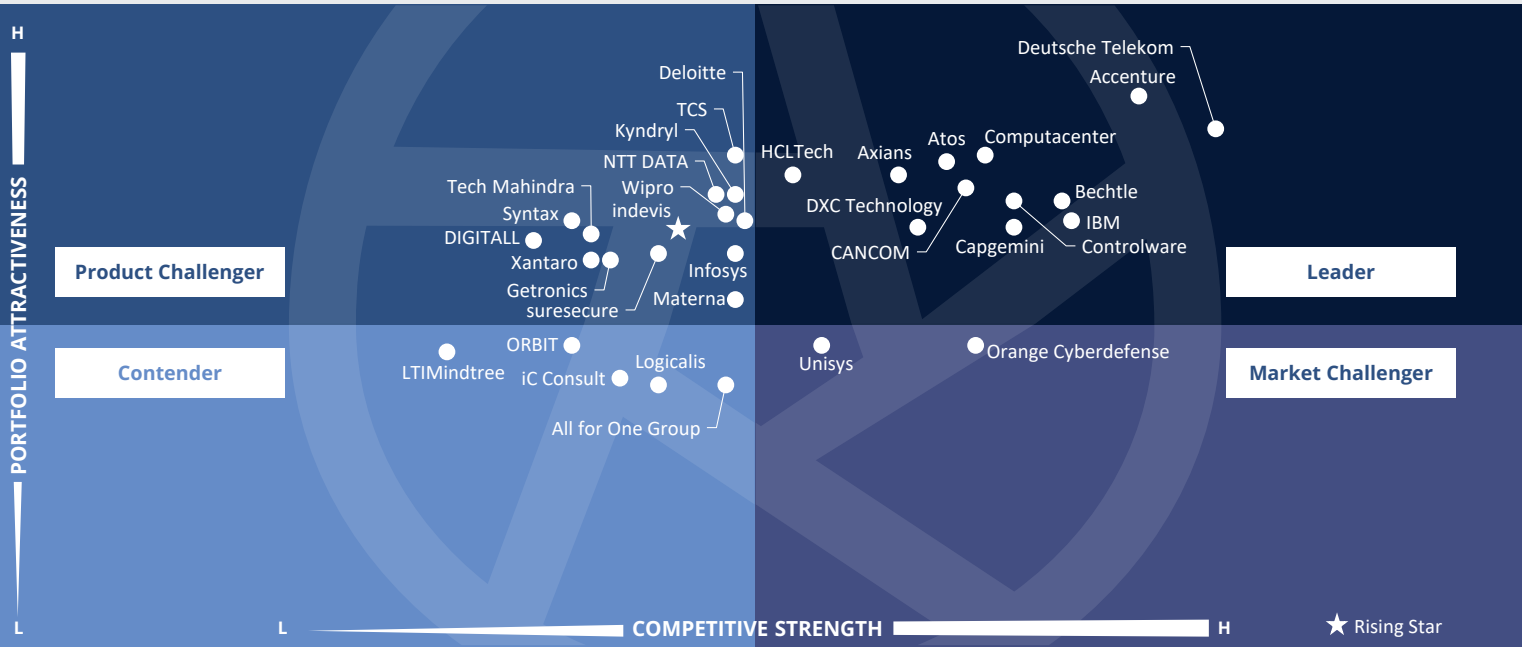
Should read this report to effectively balance data security, CX and privacy in the context of digital transformation, which is a priority for businesses today.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services

Germany 2025



This quadrant focuses on the **most relevant** providers of technical security services in Germany, whose services **extend beyond their own products.** Due to the shortage of specialists, **external providers** are playing an increasingly **important role**.

Frank Heuer

Definition

TSS providers assessed in this quadrant cover integration, maintenance and support for IT and OT security products or solutions. TSS encompasses a wide range of security products, including cloud and data center security, IAM, DLP, network security, endpoint security, OT security, SASE and others.

These providers offer playbooks and road maps to enhance security using best-of-breed tools, improving posture and reducing threats. Their portfolios support complete or individual security architecture transformations, alongside product or solution identification, assessment, design and implementation. They invest in establishing partnerships with security solutions and technology vendors to gain specialized accreditations and expand their portfolio.

This quadrant also includes classic managed security services provided without a security operations center. It examines service providers that are not exclusively focused on their proprietary products but are capable of implementing and integrating solutions from other solution vendors and service providers.

Eligibility Criteria

1. Demonstrate experience in designing and **implementing cybersecurity solutions** for companies in the respective country
2. Obtain **authorization from security technology vendors** (hardware and software) to distribute and support security solutions
3. **Employ certified experts** (certifications may be vendor-sponsored, association- and organization-led credentials or from government agencies) capable of supporting security technologies
4. **Do not focus exclusively on proprietary products** or solutions
5. Present **case studies** that demonstrate successful design, deployment and management of cybersecurity solutions for companies within the target country

Observations

The increasingly intensive, sophisticated, complex and constantly new cyberattacks are still a challenge for companies in Germany, which is made more difficult by the lack of cybersecurity experts. As a result, companies are increasingly reliant on external service providers. Providers that have mastered the latest technologies and can address different target groups have an advantage here.

SMEs have a particular need to catch up, as they often encounter issues such as a shortage of IT specialists. Increasingly complex security threats and stricter legal regulations are prompting these companies to seek external support. SMEs often appreciate the local presence of service providers for short distances and uncomplicated, fast support.

To be successful in the demanding key account market, providers must be able to present extensive international experience and teams. Providers with a balanced customer structure consisting of key accounts and SMEs benefit from both the large budgets of key accounts and the above-average growth in demand from SMEs.

The German service provider indevis is the new Rising Star. Getronics, LTIMindtree, ORBIT and Xantaro are new to the quadrant. Alice&Bob. Company was no longer included in this quadrant. Riedel Networks from Butzbach, Hesse, has not yet qualified for the quadrant but is well placed for the future due to its modern integration of network and security solutions.

Of the 68 providers that were assessed specifically for the German market in this study, 33 qualified for this quadrant, with twelve Leaders and one Rising Star.

accenture

Accenture's Security Automation Factory supports the transformation of process- and resource-intensive tasks with the help of robotic process automation. Accenture covers an extensive range of topics and services.

Atos

Atos is familiar with the requirements and legal regulations related to security projects and supports its customers in complying with these requirements. Atos pursues a holistic cybersecurity approach that also emphasizes business relevance.

axians

Axians IT Security maintains partnerships with numerous renowned cybersecurity technology providers. Axians' technical IT security services address a broad spectrum of requirements.

BECHTLE

Bechtle has a strong presence in Germany and is represented at numerous locations. It is a high-profile provider of technical security services for the dynamically growing midsize companies market segment.

CANCOM

CANCOM's technical security services cover a comprehensive range of topics and services. With its technical security services, CANCOM has a strong focus on midsize companies.

Capgemini

Capgemini is a security service provider with thought leadership. The provider can use advanced technologies such as security automation and AI in cybersecurity projects for its clients.

Computacenter

Computacenter's technical security services are very broadly based. The company has partnerships with numerous large IT security vendors as well as many smaller and emerging providers.

controlware

Controlware, with its German origins, is particularly well positioned in the key segment of the upper midmarket, which places particular trust in service providers with German roots. Controlware's offering is modularly structured to meet client requirements.

Deutsche Telekom offers its customers seamless technical security services that cover a complete range of topics. The team of cybersecurity experts is very large. With security made in Germany, Deutsche Telekom excels beyond just the SME sector.

DXC TECHNOLOGY

DXC Technology's portfolio includes integrated cybersecurity and connected IT solutions, supported by an extensive global presence and resources.

HCLTech

HCLTech is increasingly successful, having progressed from being a Rising Star to a Leader in the German market for technical cybersecurity services. Its extensive experience, comprehensive portfolio and first-class partnerships contribute to this.

IBM

IBM is an experienced and successful cybersecurity technology provider and has a deep understanding of IT security solutions. IBM is represented in the German market with one of the broadest portfolios for IT security services.

Indevis

Indevis is the new Rising Star for technical cybersecurity services in Germany. Experience, expertise and a strong business expansion strategy contribute to this.

Strategic Security Services

Who Should Read This Section

This report is valuable for providers offering **strategic security services (SSS)** in **Germany** 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 gain a broader outlook on security trends and understand providers' capabilities in devising security strategies.

Technology professionals

Should read this report to understand the emerging trends in the security landscape and assess providers' capabilities in developing tailored security platforms.

Strategy professionals

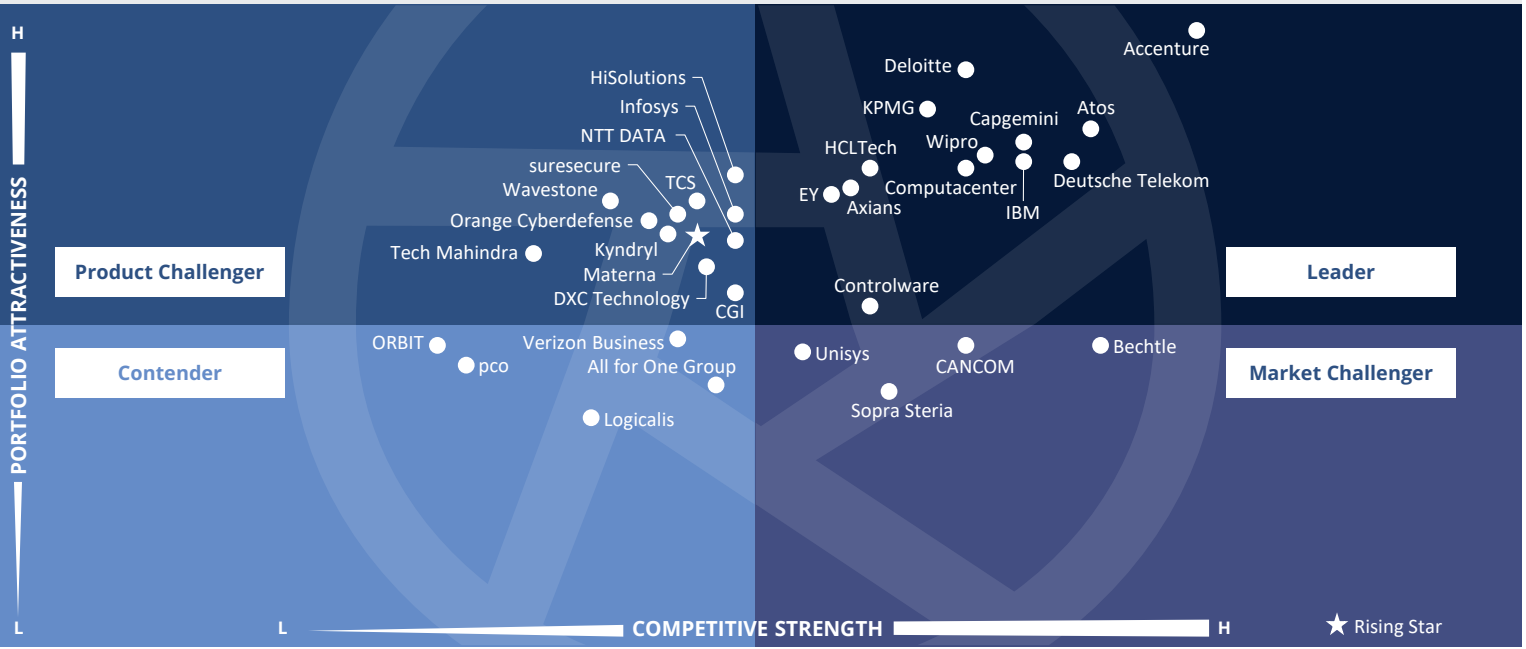
Should read this report to understand providers' relative positioning and capabilities, informing strategic decision-making on partnerships and cost-reduction initiatives.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Strategic Security Services

Germany 2025



This quadrant focuses on the **most relevant** cybersecurity consultants in Germany that provide services **beyond their own products.** Increasing cyber threats and new technologies are driving **demand**.

Frank Heuer

Definition

SSS providers assessed in this quadrant offer IT and OT security consulting. Services include security audits, assessments, and awareness and training. These providers also help assess security maturity and define cybersecurity strategies to meet enterprise-specific requirements.

Providers employ experienced security consultants to plan and manage end-to-end security programs for enterprises. Considering the rising demand from SMBs and talent shortages, SSS providers offer on-demand experts via virtual CISO services. They create business continuity roadmaps, prioritize critical applications for recovery, and conduct tabletop exercises and drills to improve cyber literacy and response among enterprise board members and employees. They also provide guidance on selecting security technologies and suppliers, reviewing organizational structures for cybersecurity, evaluating security processes and practices, and improving them in alignment with the risks faced. This quadrant examines service providers that are not exclusively focused on proprietary products or solutions.

Eligibility Criteria

1. Demonstrate abilities in SSS areas such as **evaluation, assessments, vendor selection, solution consulting and risk advisory**
2. Display competence in the application of good practices and market security frameworks such as ISO 27000, NIST and CIS
3. **Offer at least one of the above** strategic security services in the respective countries assessed for this study
4. Provide **security consulting services using frameworks such as NIST and ISO**
5. **Do not focus exclusively** on **proprietary products** or solutions

Observations

Cybersecurity threats are becoming ever more menacing, affecting new target groups. The war in Ukraine and its associated repercussions are just one example of how threats are intensifying; commercially motivated cyber attacks are no less a cause for concern. New, technically sophisticated threats are also emerging.

It is no longer just well-known large companies and public authorities that are affected by cyber threats; increasingly, small and midsize companies are experiencing the same issues. At the same time, the shortage of IT specialists continues to make this situation more difficult; SMEs, in particular, are suffering as a result. Consequently, companies increasingly need external support, which often starts with consulting.

Among other things, service providers that can offer their customers security consulting along with implementation and operation, so that the strategy can be implemented seamlessly, have an advantage. This is also true for providers that, in addition to security consulting, can also offer associated IT solutions — and possibly also associated redesigned business processes — from a single source. Consultants are increasingly turning to consulting to defend against quantum-based cyber attacks — especially as the *harvest now - decrypt later* approach means that the threat is more pressing than previously assumed.

Materna is the new rising star. ORBIT and pco are new to the quadrant, Secureworks is no longer represented. DGC AG from Flensburg has not yet qualified for the quadrant. However, this service provider is well placed for the future due to its focus on cybersecurity consulting and its origins in Germany.

Of the 68 providers that were assessed specifically for the German market in this study, 34 qualified for this quadrant, with thirteen Leaders and one Rising Star.

accenture

Accenture's consultants are distinguished by their considerable expertise and experience, which is one of the reasons it has access to board-level discussions. The service portfolio is extensive and is being systematically developed.

Atos

Atos takes a holistic approach to cybersecurity consulting. The provider is able to create trust among its (potential) customers through numerous certifications as part of its security consulting services.

axians

Axians IT Security can score points in the German market for cybersecurity consulting with pragmatic, targeted solutions, especially for midsize companies. The provider has a strong partner network.

Capgemini

Capgemini offers an extensive range of cybersecurity consulting services, which are currently being further expanded. The company distinguishes itself through its experienced team of consultants, who possess a comprehensive understanding of both theoretical concepts and practical applications.

Computacenter

Computacenter can establish itself as a strategic partner with a holistic approach to security and an understanding of its customers' infrastructure and business requirements. The consulting portfolio and the addressed security topics are extremely extensive.

controlware

Controlware, with its expertise and customer focus, has become a leader in strategic security services in Germany.

Deloitte.

Deloitte has a strong global presence and a deep understanding of the specific business needs of its clients in Germany in the context of security consulting.

Deutsche Telekom offers its customers end-to-end services from a single source. It also has expertise in demanding environments and has many years of certified cybersecurity expertise.

EY

EY's comprehensive industry knowledge, holistic consulting approach and extensive experience will contribute to its return as one of the leading providers of strategic security services in Germany.

HCLTech

HCLTech has become one of the leading providers of strategic security services in Germany, supported by a comprehensive and up-to-date range of consulting services.

IBM

IBM's cybersecurity consulting portfolio is comprehensive, integrated and innovative. The security consulting is based on deep technical insights derived from its extensive experience as a provider of security products.

KPMG

KPMG is able to skillfully combine business and technical understanding while offering advice on cybersecurity issues. Its consultants have a high level of strategic expertise in security consulting.

wipro

Wipro offers a comprehensive portfolio of cybersecurity consulting services and has extensive technical expertise that flows into cybersecurity consulting.

MATERNA

Materna is the new Rising Star in the strategic security services market in Germany. The service provider has achieved this by increasing its focus on consulting services.

Next-Gen SOC/MDR Services

Who Should Read This Section

This report is valuable for providers offering **next-gen SOC/MDR services** in **Germany** 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

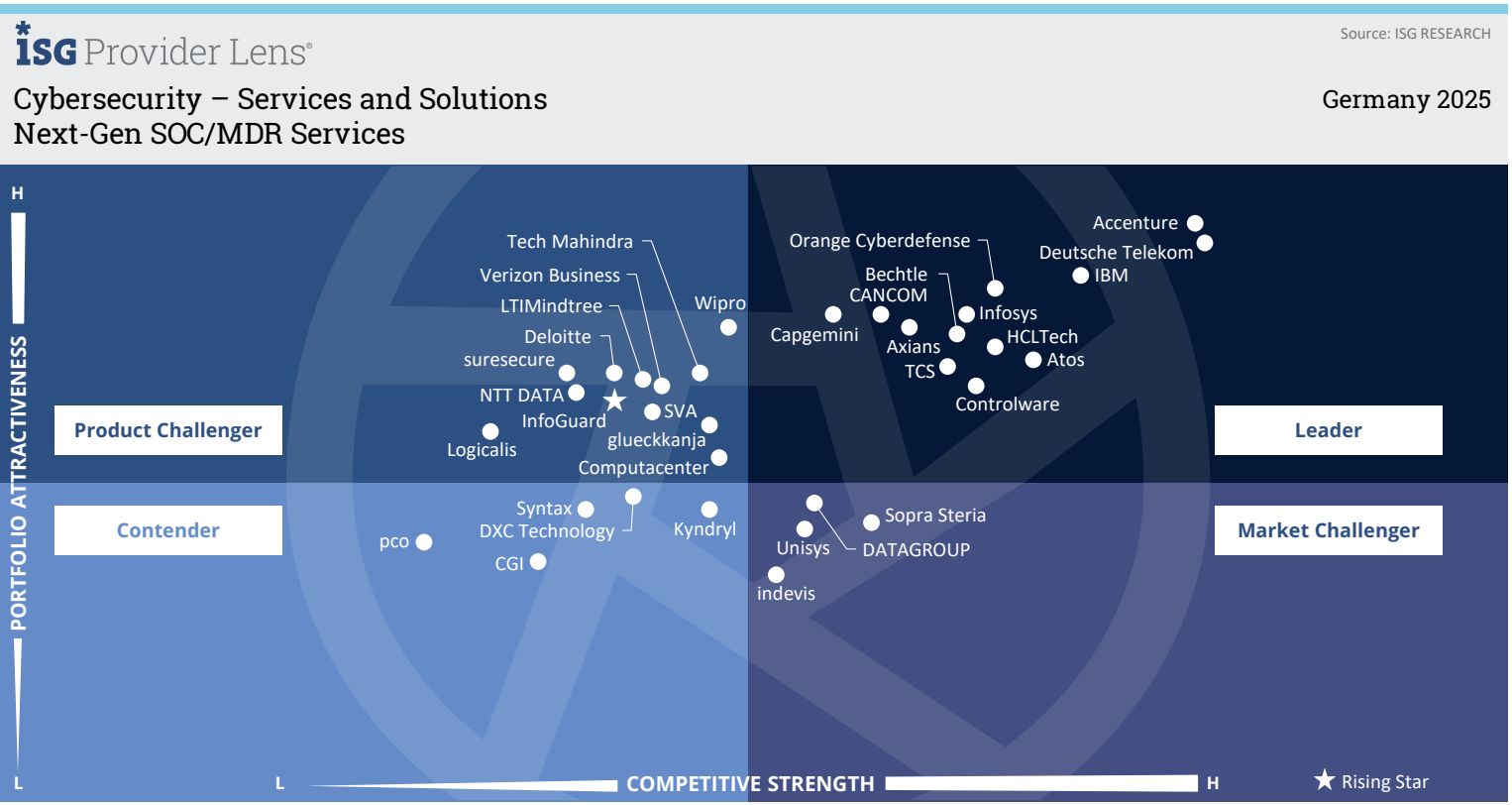
Should read this report to understand the emerging trends and immediate threats. The report can aid in strategic decision-making while enhancing productivity and reducing security complexity.

Technology professionals

Should read this report to understand emerging trends and gain insights into tailored security platforms and strategic objectives to stay apace with the changing security landscape.

Business professionals

Must read this report to gain valuable insights into simplifying security operations and learn about practical solutions that can reduce complexity and enhance efficiency.



This quadrant focuses on the **most relevant** providers of **next-gen SOC/MDR services** in Germany, excluding service providers that only offer their services for their own products. The shortage of skilled workers and the threat situation **are driving** the market.

Frank Heuer

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.

In the following, "Managed Services" is used synonymously for "Next-Gen SOC/MDR Services".

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

Observations

The demand for Managed Detection & Response (MDR) services and services from security operations centers (SOCs) is being driven by increasingly sophisticated, frequent, complex and versatile cyberattacks. The need for constantly updated specialist knowledge and the simultaneous shortage of qualified specialists are increasingly bringing these managed services into the focus of companies in Germany.

Globally distributed SOCs play a special role for large companies due to their often international presence. However, large companies also value SOC locations in the EU and Germany due to the increased importance of data protection.

Midsize companies are increasingly interested in SOC and MDR services to tackle the growing challenges posed by a severe shortage of skilled workers. SOCs in Germany and German-speaking contacts are significant advantages for this target group.

In general, providers are also expected to be highly innovative. This includes the expansion of SOCs toward cyber defense centers, where threats are countered using AI and automation. In addition to reactive measures, proactive services are becoming increasingly important. For industrial customers, the incorporation of OT security to safeguard networked production facilities is becoming increasingly relevant.

InfoGuard is the new Rising Star. pco is newly represented in the quadrant, Materna Radar is no longer, as the focus has changed. Advens, CyberProof, I-TRACING and Riedel Networks have not yet qualified for the quadrant, but they show promising approaches for a future presence in provider evaluation.

Of the 68 providers that were assessed specifically for the German market in this study, 34 qualified for this quadrant, with thirteen Leaders and one Rising Star.

accenture

Accenture offers its clients a very comprehensive range of services and can cover all topics from a single source. Accenture meets the requirements of its often globally active major clients very well due to its own international presence.

Atos

Germany is one of **Atos'** SOC locations, which is also of interest to many large companies. Both the topics covered and the services provided by Next-Gen SOC/MDR Services address a broad spectrum.

axians

Axians IT Security offers a wide range of services and managed security topics as part of its next-gen SOC/MDR services. An increased level of security and flexible solutions are offered for particularly vulnerable data and systems.

BECHTLE

Bechtle's Next-Gen SOC/MDR services cover a wide range of services and managed technologies. They are also modular and customizable. Bechtle also operates a dedicated SOC in Germany with German-speaking support.

CANCOM

CANCOM's Next-Gen SOC/MDR services portfolio covers a broad spectrum of managed technologies and offers numerous services. Among other things, CANCOM operates a dedicated security operations center in Germany.

Capgemini

As part of its Next-Gen SOC/MDR Services, **Capgemini** offers a wide range of services that address a broad spectrum of managed security topics. Capgemini has a large team of experts in Germany, especially when measured by the number of customers.

controlware

Controlware has a large team of experts in Germany in terms of the number of customers, in particular, and it offers modular, customizable next-gen SOC/MDR services.

Deutsche Telekom operates Next-Gen SOC/MDR services in Germany, among other countries, and also maintains an extremely large team for its services in this country. The provider is continuously developing its already comprehensive offering.

HCLTech

HCLTech operates several dedicated security operations centers in Germany alone. HCLTech is also strongly positioned in terms of personnel for its next-gen SOC/MDR services in Germany. The portfolio covers many services and technologies.

IBM offers one of the broadest portfolios of IT security services in the market. The provider's next-gen SOC/MDR services are based on high-performance, in-house technology. Its worldwide network of SOCs enables global operations.

The services provided by **Infosys** as part of the Next-Gen SOC/MDR services leave nothing to be desired. Infosys is also strongly positioned in terms of personnel for these services in Germany.

Cyberdefense

Orange Cyberdefense is represented worldwide with SOCs, enabling the global operation of cybersecurity solutions. Germany is also one of the countries in which Orange Cyberdefense operates security operations centers.

TCS's Next-Gen SOC/MDR services enable the operation of all cybersecurity technologies, including OT security. TCS has a large team in Germany, both in terms of absolute numbers and the number of customers.

InfoGuard has emerged as a Rising Star among providers of next-gen SOC/MDR services. Its increased commitment in Germany is contributing to this success.

Next-Gen SOC/MDR Services – Midmarket

Who Should Read This Section

This report is valuable for providers offering **next-gen SOC/MDR services** in **Germany** 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.

Business professionals

Must read this report to gain valuable insights into simplifying security operations and learn about practical solutions that can reduce complexity and enhance efficiency.

Cybersecurity professionals

Should read this report to understand the emerging trends and immediate threats. The report aids in strategic decision-making while enhancing productivity and reducing security complexity.

Technology professionals

Should read this report to gain insights into emerging trends, tailored security platforms and strategic objectives to stay apace with the changing security landscape.

ISG Provider Lens®

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Next-Gen SOC/MDR Services – Midmarket

Germany 2025

This quadrant focuses on the **most relevant** providers of **next-gen SOC/MDR services** for German SMEs, excluding providers that only support their own products. The shortage of skilled workers, in particular, is leading to **increasing demand**.

Frank Heuer

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.

In the following, "Managed Services" is used synonymously for "Next-Gen SOC/MDR Services".

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

Observations

Midsize companies in Germany are more affected by the shortage of cybersecurity specialists than large companies. At the same time, they are confronted with increasingly new and complex security challenges and are more often targeted by cyber criminals who believe this target group to be easy victims. As a result, midsize companies are also increasingly reliant on external services such as security operations centers and MDR services.

For the SME segment, SOCs in Germany are an advantage for reasons of trust and data protection. German-speaking contacts also play an important role for this customer group. Many SMEs expect their service providers to provide uncomplicated, fast implementation and, therefore, rapid onboarding for SOC services.

SMEs also expect SOC service providers to be highly innovative in order to stay ahead in the race against cyber criminals. This includes the use of AI and automation to master even more complex threats. In addition to reactive measures, proactive prevention services are also becoming increasingly important. For industrial customers, the inclusion of OT security to secure networked production facilities is becoming increasingly interesting.

The previous Rising Star, suresecure, has positioned itself as Leader this year. SVA is the new Rising Star. Getronics is a new addition to the quadrant. NVISO, Skaylink and Vodafone have not yet qualified for the quadrant, but they show promising approaches for a future presence in the provider ranking.

Of the 68 providers that were assessed specifically for the German market in this study, 22 qualified for this quadrant, with eight Leaders and one Rising Star.

axians

Axians IT Security impresses its SME customers with comprehensive next-gen SOC/MDR services tailored to their needs.

BECHTLE

Bechtle's deep understanding of the requirements of SMEs and its comprehensive and adaptable services contribute to its success in the market for next-gen SOC/MDR services in Germany.

CANCOM

CANCOM is making a name for itself as a leading provider with an extended range of SOC/MDR services for German SMEs.

controlware

Controlware specifically addresses the needs of German SMEs. The modular next-gen SOC/MDR services and SOC operations in Germany contribute to this.

DATAGROUP

With high-quality services provided by its own experts and a strong partner, **DATAGROUP** has achieved a leading position in the market for next-gen SOC/MDR services for the German Mittelstand.

Deutsche Telekom is consolidating its clear leadership position in the midmarket next-gen SOC/MDR market by investing in its attractive offerings and the provision of services from Germany.

InfoGuard
SWISS CYBER SECURITY

InfoGuard has succeeded in becoming one of the top providers of next-gen SOC/MDR services for German SMEs. The decisive acquisition of Com-Sys also plays a significant role in this achievement.

sure[secure]

suresecure, last year's Rising Star, has established itself as a leading provider of SOC services for German SMEs by focusing on the dynamically growing target group and an innovative technology platform.

SVA

SVA is the new Rising Star among providers of next-gen SOC/MDR services for SMEs in Germany due to its attractive offerings and delivery from Germany.

Leader

"Last year's Rising Star suresecure will become the leader among providers of SOC services for German SMEs in 2025."

Frank Heuer

suresecure

Overview

Founded in 2017, suresecure GmbH is a pureplay cybersecurity service provider based in Düsseldorf, Germany. After just five years, suresecure hired its 100th employee. The focus market is Germany. suresecure offers a wide-ranging portfolio for the cybersecurity market in Germany, from consulting and technical services to managed security services. The provider also offers the SOC services specifically for midsize companies.

Strengths

Focus on growth segment: suresecure's customer focus for SOC services is clearly on the SME segment. This means that suresecure benefits from the particularly strong growth in demand in this target group. suresecure, being a midsize company, operates on an equal footing with its customers and offers them uncomplicated, direct access to service employees.

Fast start: suresecure is one of the few Google partners for the Chronicle platform in Germany. With the help of this cloud-native SOC solution, suresecure can offer its customers rapid onboarding.

Success story in the SOC market: suresecure's development story is particularly remarkable. The company is only eight years old, but has already amassed a high number of employees with extraordinarily high growth rates. The management of suresecure is also ambitious. suresecure aims to become a quality leader in the market for cybersecurity services. To achieve this, suresecure invests heavily in specialists and expertise. As a result, suresecure has become a leading provider of SOC services for SMEs in Germany.

Caution

suresecure is thriving in its SOC business and is growing rapidly. On one hand, this is positive, but on the other hand, a relatively small company must pay attention to this and ensure that it can keep pace with this growth as an organization.

Appendix

Methodology & Team

The market research study "ISG Provider Lens 2025 - Cybersecurity – Services and Solutions" analyzes the relevant software providers and service providers in the German, Global markets on the basis of a multi-stage market research and analysis process and positions these providers based on the ISG research methodology.

Study Sponsor:
Heiko Henkes

Lead Authors:
Frank Heuer (Germany), Bhuvaneshwari Mohan (Global – IAM), Gowtham Sampath (Global – XDR), and Yash Jethani (Global – SSE)

Editor:
Ananya Mukherjee

Research Analysts:
Monika K and Sandya Kattimani

Data Analysts:
Rajesh Chillappagari and Laxmi Sahebrao

Consultant Advisors:
Tim Merscheid and Marco Ezzy

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.

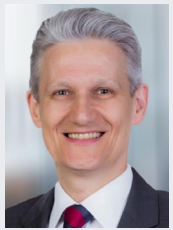
The research and analysis presented in this study will include data from the ISG Provider Lens® program, ongoing ISG Research programs, interviews with ISG advisors, briefings with service providers and analysis of publicly available market information from multiple sources. The data collected for this 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

Author

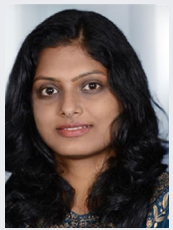


Frank Heuer
Principal Analyst

Frank Heuer is a Principal Analyst at ISG Germany. His focus is on cybersecurity, digital workspace, communication, social business & collaboration and cloud computing.

His main areas of responsibility include advising ICT providers on strategic and operational marketing and sales. Mr. Heuer is a speaker at conferences and webcasts on his main topics and a member of the IDG expert network. Mr. Heuer has been active as an analyst and consultant in the IT market since 1999.

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.

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 Lens® quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices.

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

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.

Enterprise Context and Global Overview

Monica K

Assistant Manager, 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.

Research Analyst – Global region

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.

Study Sponsor

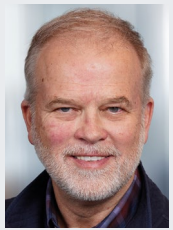
Heiko Henkes

Managing Director & Principal Analyst, Global IPL Content Lead

Heiko Henkes serves as Managing Director and Principal Analyst at ISG, overseeing the Global ISG Provider Lens® (IPL) Program for all 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 CX 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.

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.

ISG Provider Lens®

JULY, 2025

REPORT: CYBERSECURITY – SERVICES AND SOLUTIONS