ISG Provider Lens™

Cybersecurity – Services and Solutions

Technical Security Services

Analyzing the cybersecurity market and comparing provider portfolio attractiveness and competitive strengths

Customized report courtesy of: unisys

QUADRANT REPORT | JULY 2025 | U.S. PUBLIC SECTOR, GLOBAL

Table of Contents

Report Author: Gowtham Sampath and Bhuvaneshwari Mohan

IT/OT convergence and ransomware persistently threaten critical public infrastructure and operations

The dynamics of cybersecurity in the U.S. public sector are marked by an escalating threat environment, requiring a shift beyond operational continuity to comprehensive mission resilience. Government agencies at the federal, state and local levels face a complex array of sophisticated cyberthreats while pursuing critical digital transformation initiatives, including AI integration.

Evolving threat landscape

Analysis and statistical data from public sector organizations indicate a persistent and evolving threat environment targeting government entities and critical infrastructure. Adversaries, including nation-state actors and sophisticated criminal groups, are increasingly leveraging advanced tactics to compromise public sector systems.

- **Data breaches:** Recent high-profile incidents have highlighted the severe consequences of data breaches on public sector entities, impacting citizen data privacy, critical government operations and national security. For instance, the FBI's Internet Crime Complaint Center (IC3) 2024 Internet Crime Report noted over 859,000 complaints of suspected internet crime with reported losses exceeding $16 billion — a 33 percent increase from 2023 — affecting various segments, including government agencies. Such events necessitate robust data protection strategies and enhanced incident response capabilities to maintain public trust and service delivery.
- **Phishing and ransomware:** Phishing remains a primary initial access vector, with increasingly sophisticated campaigns using advanced techniques to target government personnel. Ransomware attacks continue to pose significant threats, disrupting essential public services and demanding substantial resources for recovery. An industry report analyzing 2024 trends revealed that 117 government entities and agencies reported

U.S. public sector prioritizes **mission resilience** against **evolving cyberthreats**.

ransomware incidents between January and December, highlighting the growing threat to the public sector. The focus has shifted to preventing disruption and ensuring rapid restoration of critical functions.

- **AI-related attacks:** Threat actors are rapidly weaponizing AI to automate and enhance their attack capabilities, including generating highly convincing deepfakes for social engineering, discovering vulnerability automatically and creating more evasive malware. Public sector organizations face heightened risks from AI-enhanced disinformation campaigns and attacks designed to compromise data integrity.
- **IT/OT convergence risks:** The convergence of IT/OT in critical infrastructure sectors such as energy, water, transportation and defense introduces unique vulnerabilities. Compromises in IT environments are frequently leveraged to disrupt or control sensitive OT systems, posing direct risks to national security and public safety. Cybersecurity and Infrastructure Security Agency (CISA) 2023 Year in Review highlighted that its preransomware notification initiative prevented a $350 million ransomware attack on critical transportation infrastructure, underscoring the financial and operational risks in the converged environment.
- **Persistent insider threats:** Insider threats, whether they originate from malicious intent or unintentional actions, remain a significant concern within government agencies due to access to highly sensitive information and critical systems. Comprehensive insider risk management programs are essential to mitigate the potential for data exfiltration, system sabotage or compromise of classified information.

Trending cybersecurity services and solutions

The public sector is increasingly adopting advanced security solutions and services to enhance its defensive posture and bolster mission resilience.

- **Secure cloud adoption:** With accelerated migration to cloud environments, secure cloud adoption, often guided by frameworks such as FedRAMP, is paramount. This approach includes robust cloud security posture management (CSPM) and cloud workload protection platforms (CWPP) to manage misconfigurations and protect sensitive workloads in distributed government settings.
- **Managed detection and response (MDR):** MDR services are gaining traction, providing 24/7 monitoring, AI-powered threat detection, proactive threat hunting and expert-led incident response. These services are vital for government agencies facing internal resource constraints and the need for continuous vigilance.
- **Zero trust architectures:** The never trust, always verify principle is central to modern public sector cybersecurity strategies, aligning with federal mandates. Implementation focuses on robust identity and access management (IAM) and microsegmentation to limit lateral movement and reduce unauthorized access within complex government networks. The Office of Management and Budget (OMB) Memorandum M-22-09 requires U.S. government agencies to achieve specific zero trust security goals by the end of FY24, emphasizing its critical importance.
- **Analytics and automation:** Advanced analytics and automation are streamlining public sector security operations, enabling quick response to threats. This capability includes automated incident triage, vulnerability management and enhanced threat intelligence analysis, improving efficiency and reducing the burden on security teams.
- **AI for cybersecurity and cybersecurity for AI:** The public sector focuses on leveraging AI to enhance threat detection, anomaly identification and predictive analysis for defense, while simultaneously establishing cybersecurity measures to protect AI models and data from adversarial attacks. Frameworks such as the NIST AI Risk Management Framework (AI RMF) guide secure and ethical AI deployment in the public sector.

- **Continuous threat exposure management (CTEM):** CTEM provides a proactive framework for public sector entities to continuously identify, assess, prioritize, validate and address cyberthreats across the entire attack surface, moving beyond periodic assessments to a dynamic risk reduction approach.

Cybersecurity regulatory and compliance environment

The U.S. public sector operates within a stringent and evolving regulatory framework designed to ensure the security of government information and systems.

- **Federal Information Security Modernization Act (FISMA):** This act continues to mandate information security programs for federal agencies, requiring regular assessments and reporting.
- **NIST Frameworks (CSF and RMF):** The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Risk Management Framework (RMF) serve as foundational standards for federal agencies, guiding risk management and security program development.
- **Cybersecurity Maturity Model Certification (CMMC):** This model establishes cybersecurity hygiene standards for the Defense Industrial Base (DIB), ensuring contractors handling sensitive unclassified information meet specific requirements.
- **Executive Order 14028 (improving U.S. cybersecurity):** This executive order drives significant changes across federal agencies, mandating the adoption of zero trust architectures, enhanced supply chain security and improved incident response capabilities.
- **State-level mandates and privacy laws:** State and local government entities must comply with a growing number of state-specific cybersecurity and data privacy laws, adding layers of complexity to compliance efforts.

Public sector cybersecurity challenges

- U.S. public sector entities grapple with a unique set of challenges that impact their ability to achieve comprehensive mission resilience.
- **Evolving threat landscape:** Constant innovation by adversaries, particularly nation-state actors, demands continuous adaptation and investments in advanced defensive capabilities.
- **Citizen data privacy and trust:** Safeguarding vast amounts of sensitive citizen data and maintaining public trust in government services are paramount and complex challenges.
- **Supply chain vulnerabilities:** Extensive and often complex supply chains involved in government procurement processes introduce inherent risks that require robust vendor risk management and continuous monitoring.
- **IT/OT convergence security gaps:** Securing converged IT/OT environments in critical infrastructure requires specialized expertise and integrated strategies, which are often challenging to implement across diverse agencies.
- **Insider threats and human risks:** Managing risks posed by malicious and unintentional insider actions is particularly sensitive due to the nature of information handled in the public sector.
- **Legacy systems and technical debt:** Operating with legacy IT systems that are difficult to secure and integrate with modern solutions creates significant vulnerabilities and accumulate cost complexities for many public sector organizations.
- **Budgetary and procurement complexities:** Unique government budget cycles and lengthy procurement processes hinder the rapid acquisition and deployment of necessary security technologies and services.

- **Persistent talent shortage and skills gap:** Attracting and retaining skilled cybersecurity professionals remains a significant challenge for government agencies, impacting their capacity for effective security implementation and incident response. The U.S. Government Accountability Office (GAO) noted in a 2024 report that over 850 of its cybersecurity recommendations to federal agencies had not been fully implemented as of February 2023, with 52 designated as priority recommendations, partly due to these capacity challenges.

Role of cybersecurity service providers in addressing public sector challenges

Cybersecurity service providers are indispensable partners in enabling U.S. public sector entities to navigate complexities and bolster mission resilience.

- **Assessing strategic risk and protecting mission investments:** By translating cyber risks into terms relevant to mission objectives, providers demonstrate ROI from protecting critical government digital transformation initiatives and assets. They align security strategies with agency-specific mandates, industry context and national security priorities, thereby managing overall mission risk.
- **Providing effective and consolidated security solutions:** By offering specialized, scalable security capabilities, providers integrate these seamlessly with existing government infrastructure. Their focus is on reducing tool sprawl and consolidating security operations from a technology, process and people perspective, making advanced security more accessible and efficient for agencies of all sizes.
- **Navigating complex regulatory and AI governance landscape:** By demonstrating expertise in federal mandates (FISMA, NIST, CMMC and Executive Orders) and the emerging landscape of AI governance (e.g., NIST AI RMF), providers help agencies meet stringent compliance obligations, manage the unique risks associated with AI and generative AI (GenAI) deployments, and adapt to evolving regulatory requirements.
- **Augmenting internal security teams and talent development:** By offering access to specialized skills such as 24/7 monitoring, threat detection and incident response, providers bridge talent gap in the public sector. They also enhance agency capabilities through training, knowledge transfer and support for mission-critical operations.

Future of cybersecurity services in the public sector

As digital transformation and AI initiatives continue to accelerate across government entities, cybersecurity services are evolving to meet heightened demands for mission resilience, robust governance and strategic alignment.

- **Strategic security services:** These services will emphasize deep integration with agency mission planning, quantifiable risk management, and the secure enablement of AI and other digital transformation initiatives. A core imperative will be addressing AI-related governance, risk and compliance (GRC), embedding security from the outset of any AI deployment.
- **Technical security services:** Continued emphasis will be placed on advanced analytics and automation to enhance operational efficiency and threat response. This approach includes integrating diverse security tools, employing proactive threat hunting methodologies and adopting CTEM tailored for government environments. Specialization in securing emerging technologies such as IoT and OT will also be critical.
- **Next-generation SOC/MDR offerings:** These offerings will evolve to leverage sophisticated, AI-powered threat intelligence and advanced analytics for proactive threat hunting. Next-generation security operations centers (SOCs) will understand the agency mission context for prioritizing threats and incorporate significant automation for rapid incident response, with AI augmenting human analyst capabilities rather than replacing them.

Government executives must recognize that strategic investment in cybersecurity is paramount to protecting mission-critical systems, safeguarding citizen data and ensuring the integrity of AI and other digital investments. AI-related GRC is rapidly becoming a cybersecurity imperative that demands proactive attention and dedicated resources.

Forging a resilient public sector future

The U.S. public sector faces an unprecedented challenge in securing its digital assets and maintaining mission resilience. The escalating sophistication of threats, a dynamic regulatory environment and a persistent talent shortage necessitate proactive, adaptive security strategies. The strategic adoption of secure cloud solutions, MDR, zero trust architectures, analytics, automation and CTEM signifies a critical shift toward robust cyber and business resilience.

In 2025, digital transformation and AI initiatives are expected to further shape the cybersecurity landscape. Strategic and technical services, alongside next-gen SOC/MDR, must evolve to provide intelligent, proactive and context-aware defenses. Public sector entities must prioritize a holistic security posture that integrates people, processes and technologies. Agency leadership must champion AI risk governance and invest strategically in security to safeguard digital assets. Continuous learning, adaptation and a proactive and resilient mindset are paramount to navigating the evolving cyberthreat environment and ensuring the continuity of essential government functions.

> The escalating sophistication of threats, including AI-enhanced attacks and IT/OT convergence risks, necessitates a strategic shift from mere operational continuity to comprehensive mission resilience. Government agencies must embed security into every digital transformation initiative to safeguard critical public services and sensitive data.

Report Author:
Bhuvaneshwari Mohan (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 (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 security tools and third-party applications.

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

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 (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.

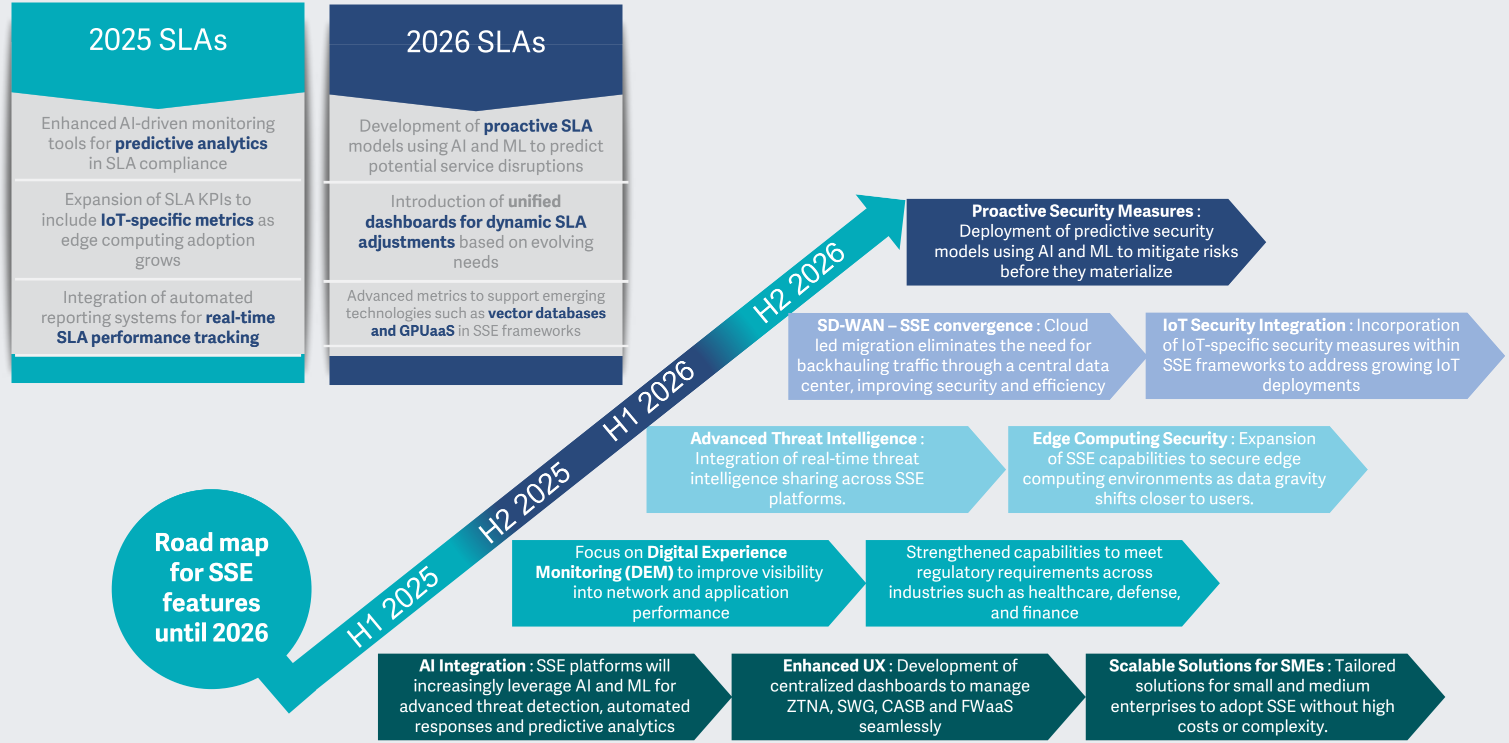
SSE provides the cloud-delivered security stack to implement zero trust principles at scale across distributed environments. It replaces traditional perimeter security with a flexible, identity-centric approach to secure remote work, cloud adoption and mobile access scenarios without sacrificing protection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



2025 SLAs

Enhanced AI-driven monitoring tools for **predictive analytics** in SLA compliance

Expansion of SLA KPIs to include **IoT-specific metrics** as edge computing adoption grows

Integration of automated reporting systems for **real-time SLA performance tracking**

2026 SLAs

Development of **proactive SLA** models using AI and ML to predict potential service disruptions

Introduction of **unified dashboards for dynamic SLA adjustments** based on evolving needs

Advanced metrics to support emerging technologies such as **vector databases and GPUaaS** in SSE frameworks

Road map for SSE features until 2026

AI Integration : SSE platforms will increasingly leverage AI and ML for advanced threat detection, automated responses and predictive analytics

Enhanced UX : Development of centralized dashboards to manage ZTNA, SWG, CASB and FWaaS seamlessly

Scalable Solutions for SMEs : Tailored solutions for small and medium enterprises to adopt SSE without high costs or complexity.

Focus on **Digital Experience Monitoring (DEM)** to improve visibility into network and application performance

Strengthened capabilities to meet regulatory requirements across industries such as healthcare, defense, and finance

Advanced Threat Intelligence : Integration of real-time threat intelligence sharing across SSE platforms.

Edge Computing Security : Expansion of SSE capabilities to secure edge computing environments as data gravity shifts closer to users.

SD-WAN – SSE convergence : Cloud led migration eliminates the need for backhauling traffic through a central data center, improving security and efficiency

IoT Security Integration : Incorporation of IoT-specific security measures within SSE frameworks to address growing IoT deployments

Proactive Security Measures : Deployment of predictive security models using AI and ML to mitigate risks before they materialize

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 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
ActioNet	Not In	Not In	Not In	Contender	Contender	Contender
Aryaka	Not In	Not In	Contender	Not In	Not In	Not In
Atos	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Beta Systems	Contender	Not In	Not In	Not In	Not In	Not In
BeyondTrust	Rising Star ★	Not In	Not In	Not In	Not In	Not In
Bitdefender	Not In	Product Challenger	Not In	Not In	Not In	Not In
BlackBerry (Arctic Wolf)	Not In	Contender	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Market Challenger	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Leader
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In

Provider Positioning

Page 2 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
CGI	Not In	Not In	Not In	Market Challenger	Market Challenger	Market Challenger
Check Point Software	Not In	Product Challenger	Leader	Not In	Not In	Not In
Cisco	Not In	Market Challenger	Leader	Not In	Not In	Not In
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In
Cross Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In
CyberArk	Leader	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Leader
DXC Technology	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Entrust	Product Challenger	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 3 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In
ESET	Not In	Contender	Not In	Not In	Not In	Not In
Evidian IAM (Eviden)	Product Challenger	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Leader	Leader	Leader
Fischer Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In
Fortinet	Market Challenger	Leader	Leader	Not In	Not In	Not In
Fortra	Market Challenger	Not In	Not In	Not In	Not In	Not In
Fujitsu	Not In	Not In	Not In	Contender	Contender	Contender
FusionAuth	Contender	Not In	Not In	Not In	Not In	Not In
Gopher Security	Not In	Not In	Contender	Not In	Not In	Not In

Provider Positioning

Page 4 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
HCLTech	Not In	Not In	Not In	Leader	Leader	Leader
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In
IBM	Leader	Leader	Not In	Leader	Leader	Leader
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In
Imprivata	Product Challenger	Not In	Not In	Not In	Not In	Not In
Infosys	Not In	Not In	Not In	Leader	Leader	Leader
JumpCloud	Contender	Not In	Not In	Not In	Not In	Not In
Kaspersky	Not In	Product Challenger	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Product Challenger	Leader	Leader
Kroll	Not In	Not In	Not In	Not In	Contender	Not In
Kudelski Security	Not In	Not In	Not In	Contender	Contender	Not In

Provider Positioning

Page 5 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
Kyndryl	Not In	Not In	Not In	Contender	Product Challenger	Not In
Leidos	Not In	Not In	Not In	Rising Star ★	Leader	Rising Star ★
LMNTRIX	Not In	Product Challenger	Not In	Not In	Not In	Not In
Lookout	Not In	Not In	Product Challenger	Not In	Not In	Not In
Lumen Technologies	Not In	Not In	Not In	Product Challenger	Product Challenger	Contender
ManageEngine	Leader	Not In	Contender	Not In	Not In	Not In
Menlo Security	Not In	Not In	Contender	Not In	Not In	Not In
Microsoft	Leader	Leader	Market Challenger	Not In	Not In	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In
NTT DATA	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Okta	Leader	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 6 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
One Identity (OneLogin)	Leader	Not In	Not In	Not In	Not In	Not In
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In
OpenText	Product Challenger	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Leader	Leader	Not In	Not In	Not In
Ping Identity	Leader	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In
Rapid7	Not In	Product Challenger	Not In	Not In	Not In	Not In
RSA	Market Challenger	Not In	Not In	Not In	Not In	Not In
SailPoint	Leader	Not In	Not In	Not In	Not In	Not In
Saviynt	Leader	Not In	Not In	Not In	Not In	Not In
SecureAuth	Contender	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 7 of 8

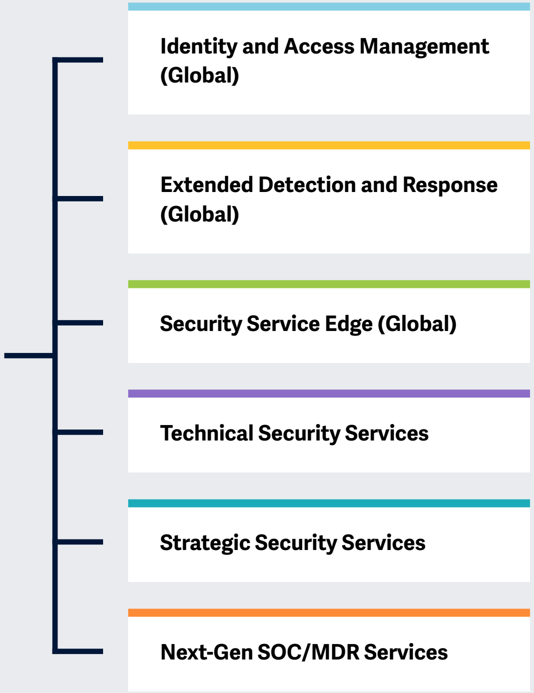
	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
SenseOn	Not In	Contender	Not In	Not In	Not In	Not In
SentinelOne	Not In	Leader	Not In	Not In	Not In	Not In
Seqrite	Not In	Contender	Not In	Not In	Not In	Not In
Sequretek	Contender	Contender	Not In	Not In	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In
SonicWall (Banyan Security)	Not In	Not In	Contender	Not In	Not In	Not In
Sophos	Not In	Rising Star ★	Not In	Not In	Not In	Not In
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Tech Mahindra	Not In	Not In	Not In	Contender	Product Challenger	Product Challenger
TEHTRIS	Not In	Product Challenger	Not In	Not In	Not In	Not In
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In

Provider Positioning

Page 8 of 8

	Identity and Access Management (Global)	Extended Detection and Response (Global)	Security Service Edge (Global)	Technical Security Services	Strategic Security Services	Next-Gen SOC/MDR Services
Trellix	Not In	Leader	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In
Trustwave	Not In	Not In	Not In	Product Challenger	Product Challenger	Product Challenger
Unisys	Not In	Not In	Not In	Leader	Leader	Market Challenger
Verizon Business	Not In	Not In	Not In	Market Challenger	Contender	Product Challenger
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Rising Star ★	Product Challenger
Zensar Technologies	Not In	Not In	Not In	Contender	Not In	Not In
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In

Key focus areas for Cybersecurity – Services and Solutions 2025.



Identity and Access Management (Global)

Extended Detection and Response (Global)

Security Service Edge (Global)

Technical Security Services

Strategic Security Services

Next-Gen SOC/MDR Services

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 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

In this ISG Provider Lens™ quadrant study, ISG includes the following six quadrants: Identity and Access Management (Global), Extended Detection and Response (Global), Security Service Edge (Global), Technical Security Services, Strategic Security Services and Next-Gen SOC/MDR Services.

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

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

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

Provider Classifications

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

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

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

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

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.

Technical Security Services

Who Should Read This Section

This report is valuable for service providers offering **technical security services (TSS)** in the **U.S. public sector** 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. The report evaluates transformations, focusing on designing and providers specializing in enterprise security managing multilayered architectures using SASE, IAM and OT security to counter threats and ensure compliance globally.

Technology professionals

Should read this report to gain insights into provider compliance, market trends and integration for innovation, scalability and threat reduction using advanced technologies.

Security and data professionals

Should read this report to gain insights into provider compliance, market trends and integration of vendor-neutral solutions in large-scale architecture transformations.

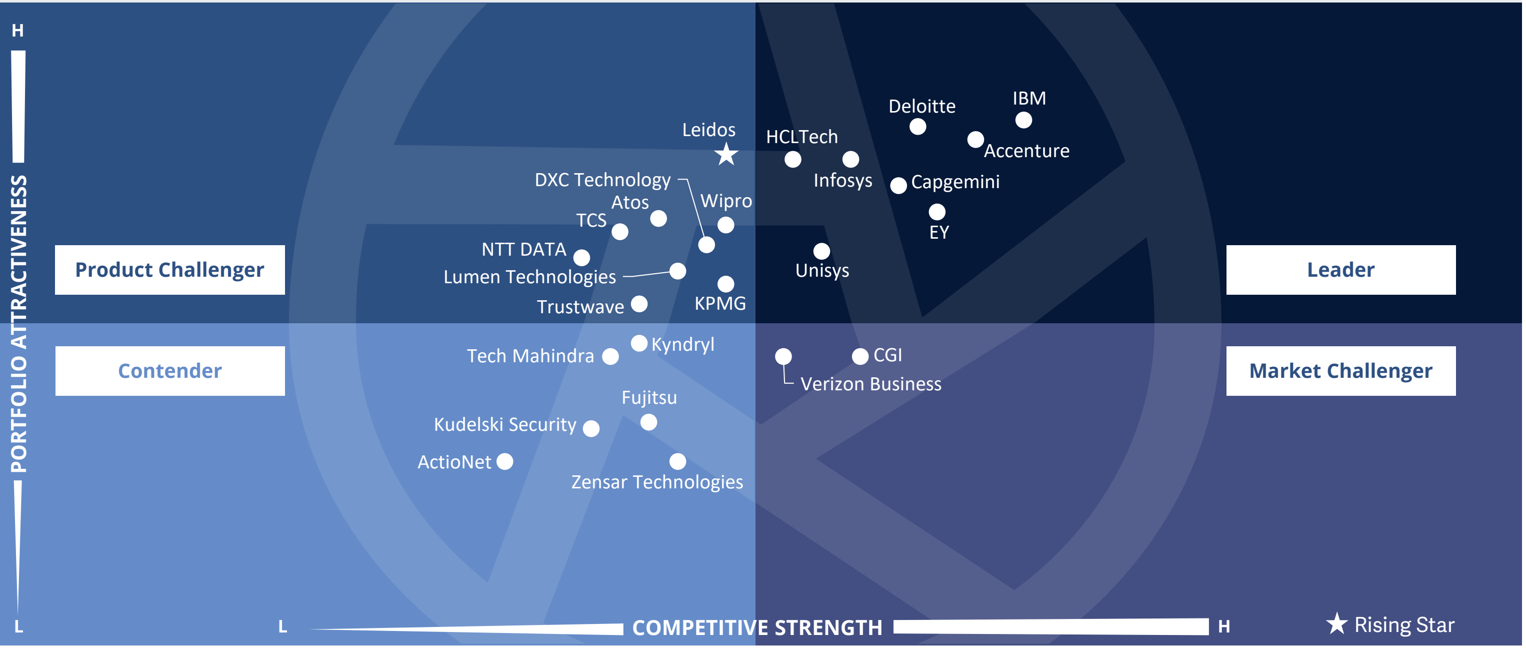
Business professionals

Should read this report to balance data security, CX and privacy as digital transformation takes center stage in businesses.

Source: ISG RESEARCH

Cybersecurity – Services and Solutions
Technical Security Services

U.S. Public Sector 2025



The quadrant assesses providers delivering **modular and scalable** technical services by combining **industry-specific** frameworks, **advanced threat detection, cloud, IT/OT** and **identity** expertise to **modernize** enterprise security and drive **risk reduction**.

Gowtham Sampath

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 U.S. public sector agencies are intensifying their investments in TSS as they confront a rising wave of sophisticated cyberthreats, regulatory mandates and infrastructure modernization initiatives. A defining trend is the federal-wide push toward zero trust architectures, catalyzed by Executive Order 14028 and further shaped by CISA's maturity models. Public agencies are increasingly implementing identity-centric security controls, microsegmentation and continuous authentication to safeguard networks, data and applications in alignment with secure-by-design principles.

Another prominent development is the convergence of IT/OT security across critical infrastructure sectors, such as transportation, public utilities and emergency services. As cyber physical systems become central to operational continuity, public sector entities are adopting hybrid security architectures that integrate legacy on-premises systems with cloud-native platforms, balancing modernization with mission assurance.

Federal agencies are also increasingly utilizing modular playbooks and standardized implementation road maps to accelerate compliance with frameworks such as FedRAMP, NIST 800-53 and CMMC. These playbooks are being codeveloped with midsize and specialized providers that offer agility and mission-specific expertise, especially in areas including identity management, postquantum cryptography (PQC)-readiness and threat hunting. Strategic acquisitions and public-private partnerships are also shaping the cybersecurity landscape, with system integrators and niche cybersecurity firms expanding their capabilities through alliances with hyperscalers, AI vendors, and red and blue team providers.

From the 86 companies assessed for this study, 25 qualified for this quadrant, with eight being Leaders and a one Rising Star.

accenture

Accenture's deep integration of AI and cloud security enables public sector agencies to proactively identify and mitigate threats in real time. Its ability to align security services with compliance and operational objectives makes it a trusted partner for mission-critical environments.

Capgemini

Capgemini, through its acquisition of VariQ, has strengthened its position in the U.S. federal market by expanding capabilities in software development, cybersecurity and cloud services. This acquisition bolsters its ability to deliver TSS through increased talent and best-in-class contract vehicles.

Deloitte.

Deloitte's partnership with Rubrik integrate cyber resilience services that combine data, identity and cyber recovery solutions. These services include secure vault implementation and data protection capabilities for business continuity and disaster recovery in the public sector.

EY

EY actively supports federal agencies in their cloud migration journey, emphasizing security, reliability and compliance with government directives such as Cloud Smart. Its Dignari team has experience in applied AI for border security and biometric system implementation.

HCLTech focuses on AI-driven security and endpoint protection, making it suitable for U.S. public sector agencies facing advanced persistent threats. Its commitment to regulatory compliance and innovative approaches to cloud security reinforces its value in highly dynamic government landscapes.

IBM integrates AI with advanced threat intelligence tools to offer unparalleled proactive defense for U.S. federal agencies. Its hybrid cloud security approach ensures flexibility and scalability, critical for securing diverse and evolving public sector infrastructures.

Infosys has been actively promoting zero trust architectures and collaborating with partners such as Zscaler to deliver scalable, cloud-native security solutions. These initiatives are designed to meet the stringent security requirements of U.S. public sector clients.

Unisys emphasizes advanced cybersecurity solutions such as security service edge (SSE), highlighting its role in addressing challenges, including lax data privacy and governance in decentralized IT environments, while complying with U.S. federal regulations.

Leidos' (Rising star) IT and OT security capabilities provide a distinct edge in safeguarding critical federal infrastructure. Its resilience-focused services approach and strong integration with OT make it highly suitable for national security environments.

Unisys

Leader

> "Unisys combines technical innovation and regulatory alignment in public sector cybersecurity, offering quantum readiness, zero trust frameworks and tailored managed detection and response (MDR) services focused on securing public infrastructure."
>
> *Gowtham Sampath*

Overview

Unisys is headquartered in Pennsylvania, U.S. It has more than 16,500 employees across 48 offices in 22 countries. In FY23, the company generated $2.0 billion in revenue, with Enterprise Computing Solutions as its largest segment. The public sector is a primary focus of Unisys globally, especially the U.S., where it has a long-standing history and expertise in hardware, software and services across security and other technology domains. Unisys delivers tailored technical security services for the U.S. public sector, emphasizing cybersecurity, cloud modernization and digital transformation, and aligned with federal mandates such as EO 14028 and CISA's maturity model.

Strengths

Zero trust implementation and identity-centric security: Unisys embeds zero trust principles into its public sector offerings through identity-based access controls, microsegmentation and real-time monitoring. These solutions align with the U.S. government's Executive Order 14028 and CISA's Zero Trust Maturity Model. Agencies benefit from tailored implementations that minimize lateral movement and fortify network perimeters. Unisys' ability to integrate these principles across on-premises and cloud systems enhances mission assurance and operational integrity.

PQC and crypto agility: Unisys is among the few providers in the public sector space offering a dedicated PQC service, making it a strategic partner for agencies with high-value assets vulnerable to harvest-now, decrypt-later attacks. Its hybrid encryption approach ensures interoperability between legacy systems and new cryptographic standards.

Secure cloud modernization and FedRAMP expertise: Unisys helps public sector clients modernize their IT environments while complying with federal standards such as FedRAMP and FISMA. The company's expertise in securing mainframes and hybrid infrastructures makes it a fit for agencies transitioning legacy systems into cloud-native environments.

Caution

Unisys' specialized services, particularly legacy system modernization and quantum readiness, come with premium pricing that may challenge state and local agencies with limited cybersecurity budgets. Agencies should also consider the operational complexity of integrating these advanced offerings within older IT ecosystems.

Appendix

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

Study Sponsor:
Heiko Henkes

Lead Authors:
Bhuvaneshwari Mohan (U.S. PS, Global - IAM), Gowtham Sampath (U.S. PS, Global - XDR), Yash Jethani (Global - SSE)

Editors:
Indrani Saha and Padma Mohapatra

Research Analyst:
Sandya Kattimani

Data Analysts:
Rajesh Chillappagari and Laxmi Kadve

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 & Editor Biographies

Author (U.S. PS, Global - XDR)

Gowtham Sampath

Assistant Director and Principal Analyst, ISG Provider Lens™

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

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

Author (U.S. PS, 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 - 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.

Research Analyst

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.

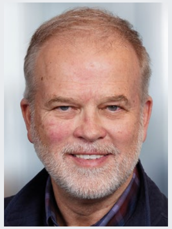
Study Sponsor

Heiko Henkes

Director & Principal Analyst, Global IPL Content Lead

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

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



IPL Product Owner

Jan Erik Aase

Partner and Global Head – ISG Provider Lens™

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

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