

IDC MarketScape: Worldwide Cloud Security Services in the AI Era 2024–2025 Vendor Assessment

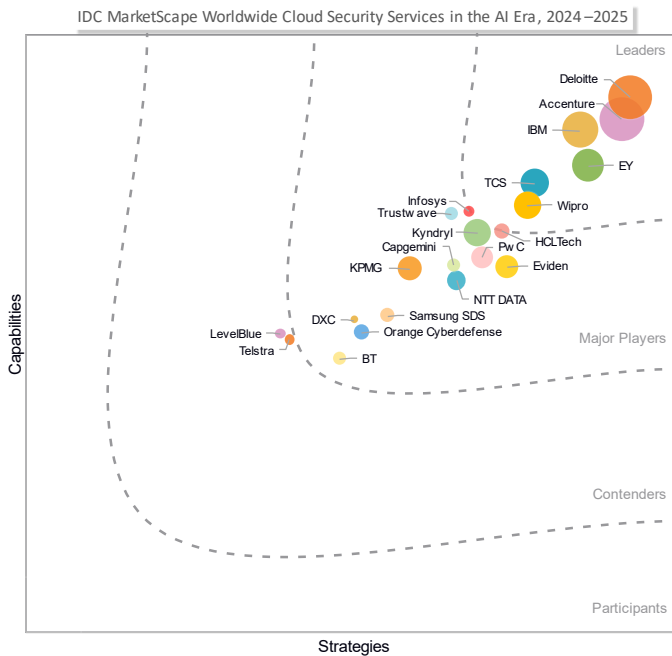
Cathy Huang

THIS IDC EXCERPT FEATURES TRUSTWAVE AS A MAJOR PLAYER

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cloud Security Services in the AI Era Vendor Assessment



Source: IDC, 2024

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cloud Security Services in the AI Era 2024–2025 Vendor Assessment (Doc # US52048124).

IDC OPINION

This IDC MarketScape study evaluates 21 global cloud security service providers in the artificial intelligence (AI) era. The study assesses their capabilities in cloud security strategies, managed cloud security services, embedding security in cloud transformations, leveraging AI for enhanced security measures, and maintaining cloud security compliance.

The convergence of cloud and artificial intelligence, coupled with the rapid adoption of cloud-based services, is ushering in a new era that revolutionizes business operations through greater flexibility, scalability, resilience, and innovative capabilities. This is evident from IDC's 2024 *Worldwide Cloud Security Services Survey* results: More than 21% of the 1,020 respondents surveyed across industries cited "better resilience" as their primary motivation for cloud adoption, followed closely by "access to innovative capabilities."

- **Early adoption challenges:** Organizations initially faced significant resistance to cloud adoption due to security concerns. Many hesitated because of their substantial investments in on-premises security systems. Regulatory compliance requirements further complicated the transition to cloud services.
- **Current landscape:** As organizations progress in their cloud journey, they encounter increasingly sophisticated security demands. Traditional manual security management tools have become insufficient for managing the dynamic nature of cloud environments.

The rush to adopt cloud has led to several critical security challenges. Organizations often struggle with insecure software development practices and limited visibility across cloud environments. Misconfigurations, especially those related to user identity, can lead to accidental data disclosures and security breaches.

The Evolution of Cloud Security

Cloud security has evolved significantly over time. Initially, the focus was on establishing basic cloud enablement and setting up fundamental guardrails to ensure security and compliance. The primary concern was setting up essential security measures while maintaining regulatory requirements.

As organizations have matured in their cloud adoption, the emphasis has shifted toward integrating and scaling their operations. This includes automating incident response processes in the cloud and cloud posture management, which has become a priority for clients that now recognize the need for more advanced automation.

The cloud is no longer just a cost-saving play but is critical to enabling companies to tackle their most pressing business issues. Companies that double down on agility, cloud-native approaches, and innovation are likely to come out ahead. The advent of generative artificial intelligence (GenAI) has brought newer investments and adoption cycles for hyperscalers, shifting the focus toward industry cloud, hyper-personalization, and sovereignty.

The integration of AI and GenAI in cloud security is proving to be a game changer — not only streamlining compliance and enhancing security operations but also significantly enhancing productivity and improving response times.

The future of cloud security lies in automation, AI-driven enhancements, and zero trust and secure-by-default principles, all of which promise to improve security operations and better manage cybersecurity risks and support business continuity in today's dynamic threat landscape.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC has narrowed down the field of players based on the criteria that follow and subsequently collected data on these vendors, including vendor request for information (RFI), briefings, customer reference interviews, data from IDC's 2024 *Worldwide Cloud Security Services Survey*, and public information:

- **Service capability:** Each vendor was assessed based on the following cloud security services offerings (i.e., both professional security services and managed security services) closely, while most of the featured vendors in this study do have a broader cybersecurity portfolio that goes beyond cloud security services:
 - Cloud security assessment and design
 - Cloud security risk review
 - Cloud security compliance advisory
 - Cloud security posture management (CSPM)
 - Cloud-native app platform (CNAPP)
 - Cloud workload protection
 - Infrastructure-as-code (IaC) scanning
 - Cloud infrastructure entitlements management (CIEM)

- Cloud security automation
- **Geographic presence:** Each vendor was required to have the local delivery capability in at least two of the three regions: the Americas, EMEA, and Asia/Pacific (APAC).
- **Certified cloud security resources:** Each vendor was required to have a minimum of 100 certified cloud security resources (e.g., Microsoft Certified Azure Security Engineers, Amazon Web Services (AWS) Certified Security, GCP Certified Professional Cloud Security Engineer).

ADVICE FOR TECHNOLOGY BUYERS

The journey to cloud adoption presents significant security challenges. Successful organizations tackle cloud security challenges by selecting providers with proven cloud security frameworks/strategy, proficient in unlocking the value of technologies like CNAPP, CSPM, DevSecOps, and fostering strong partnerships with cloud hyperscalers and cloud security solution providers.

IDC recognizes that not all organizations enter the process of securing their cloud infrastructure from the same starting point. Some organizations start from a relatively low-maturity standpoint. Others are looking for more nuanced improvements that fit their particular situations. Some security leaders are looking for a “do-over,” while others are looking for a provider to give them a managed offering. These examples are highlighted for buyers to note that there are some variances within the cloud security services providers on the consulting and transformation capabilities and their capabilities of taking on some or all of the managed cloud security needs that your particular organization is seeking.

To effectively navigate hybrid cloud environments, organizations need solutions that offer comprehensive visibility and robust data protection. Moreover, the path to robust cloud security lies in multilayered identity authentication, real-time security posture management, and continuous compliance validation.

Cloud security services providers are essential partners, offering specialized expertise, operational excellence, and proven best practices. This study discusses various types of cloud security vendors and provides key selection criteria for organizations to consider:

- **Breadth of the cloud security services portfolio:** Including the core and adjacent capabilities that can be utilized to secure cloud transformations and enable cloud security modernizations

- **Technical agility:** The ability to be scalable, agile, and capable of addressing the unique security challenges posed by multicloud and hybrid cloud environments
- **Operational excellence:** Including customer service quality, global monitoring capabilities, and the ability to meet industry-specific compliance
- **Partnerships:** The depth of partnerships with cloud hyperscalers and cloud security solution vendors for accessing the latest innovations is a critical differentiating factor
- **Innovation:** Experiences of leveraging advanced tools, automation, and AI/GenAI to enhance their cloud security engagements

VENDOR SUMMARY PROFILE

This section briefly explains IDC's key observations resulting in a vendor's position in the IDC MarketScape. While every vendor is evaluated against each of the criteria outlined in the Appendix, the description here provides a summary of each vendor's strengths and challenges.

Trustwave

Trustwave is positioned in the Major Players category in this IDC MarketScape for worldwide cloud security services in the AI era 2024–2025 vendor assessment.

Trustwave offers a comprehensive set of offensive and defensive cloud security services, including the following core offerings:

- **Managed detection and response:** Trustwave's MDR service is tailored for cloud security, offering 24 x 7 threat detection, investigation, and response capabilities. This service is bolstered by proactive threat hunting and the deployment of cutting-edge endpoint detection and response technology, ensuring rapid identification and neutralization of threats.
- **Managed XDR:** Trustwave's managed XDR service integrates with Microsoft's cloud security ecosystem, providing comprehensive coverage across endpoints, identities, cloud applications, and email. This service includes 24 x 7 monitoring, threat hunting, investigation, and native response capabilities against threats. This service includes integration with clients' implementation of copilot for security and security advisory team to help comanage content, configurations, and overall support for Microsoft Defender XDR subsystems and Microsoft Sentinel.
- **Comanaged SOC and managed cloud SIEM services:** Trustwave's expertise extends to helping organizations manage their cloud SIEM deployments effectively. It offers round-the-clock monitoring, threat hunting, and in-depth investigation, augmented with tailored use cases and technical advisory to enhance security policies and architectures.

- **Cloud security accelerator services:** Recognizing the need for a strategic approach to cloud security, Trustwave offers accelerator services to assess cloud security readiness and provide actionable road maps for achieving desired security postures. These services are designed to maximize the value of cloud security investments and ensure a secure transition to cloud environments.
- **Hybrid/cloud vulnerability management:** This service focuses on providing clients with a comprehensive understanding of the assets within their environment and their susceptibility to cyberattacks.
- **Hybrid/cloud penetration testing:** This service offers penetration testing for GenAI, LLMs, cloud/hybrid networks, cloud applications, and so forth. This service includes red and purple teaming and attack simulations. The service is also delivered with penetration testing as a service (PTaaS), which allows clients to have a more controlled and programmatic approach to penetration testing. It enables clients to conduct penetration tests on a dynamic basis including catering to unique needs such as assessments for Microsoft Azure and operational technology or during significant organizational changes like mergers and acquisitions (M&A).

Trustwave's Fusion platform is a cloud-native security operations platform that both Trustwave analysts and clients use for delivery of outsourced security services. The investment and road map of the Fusion platform represents the vendor's innovation focus and strategy. For example, the vendor focuses on building an AI-first data architecture and scalable data ingestion model for its Fusion platform. The use of AI will achieve more accurate threat identification, reduction of false positives, and efficient workload distribution among security analysts.

The Fusion platform's interfaces, both web and mobile, will get a refreshed look and feel by incorporating suitable AI technologies. The Fusion platform reporting engine will be upgraded too.

As a value-added service, Trustwave's Digital Forensics and Incident Response (DFIR) service provides emergency response and forensic investigation to mitigate impact, collect evidence, and support litigation efforts.

Strengths

- **Integration and expertise with Microsoft environments:** Trustwave has shown good expertise with Microsoft environments, including Azure and Microsoft 365, and has successfully integrated its services with these platforms. Trustwave has many Microsoft security certifications and recognitions (e.g., Microsoft Verified MXDR Partner and Microsoft Copilot for Security Partner).
- **Technical assurance and continuous testing:** Trustwave excels in providing technical assurance through penetration testing and application security monitoring. It has developed a model for continuous testing, allowing clients to

purchase days of technical assurance for 24 x 7 testing, moving from bespoke to continuous testing.

- **Commitment to innovation:** Trustwave is innovating by using AI and proprietary LLMs to test faster and on a larger scale. Although the results from its AI/LLMs are still in the proof-of-concept stage and not yet fully realized, its commitment to innovation is clear. It has also demonstrated the ability to minimize false positives and provide valuable insights through its Fusion platform.
- **Customer satisfaction and flexibility:** Trustwave delivers high customer satisfaction, with clients appreciating its operational and communication styles and flexibility. Its consultants are highly regarded, contributing to a positive reputation among clients. Trustwave has been proactive and responsive in addressing client issues.

Challenges

According to customer feedback, Trustwave should further enhance its industry understanding. The contextualization of its SpiderLabs is a good starting point. While Trustwave is making strides in using AI, there is a perception that it should embrace AI and analytics more fully and quickly to stay ahead. The native integration and interoperability for its Fusion platform can be further enhanced too.

Consider Trustwave When

Enterprises with varying levels of security maturity that require customized hybrid approach and depth of offensive and defensive security capabilities should consider Trustwave. Companies that have invested in Microsoft technologies and are looking for security solutions and expertise to maximize value of Microsoft investment should also consider Trustwave.

APPENDIX

Reading an IDC MarketScape Graph

For the purposes of this analysis, IDC divided potential key measures for success into two primary categories: capabilities and strategies.

Positioning on the y-axis reflects the vendor's current capabilities and menu of services and how well aligned the vendor is to customer needs. The capabilities category focuses on the capabilities of the company and product today, here and now. Under this category, IDC analysts will look at how well a vendor is building/delivering capabilities that enable it to execute its chosen strategy in the market.

Positioning on the x-axis, or strategies axis, indicates how well the vendor's future strategy aligns with what customers will require in three to five years. The strategies category focuses on high-level decisions and underlying assumptions about offerings, customer segments, and business and go-to-market plans for the next three to five years.

The size of the individual vendor markers in the IDC MarketScape represents the market share of each individual vendor within the specific market segment being assessed.

IDC MarketScape Methodology

IDC MarketScape criteria selection, weightings, and vendor scores represent well-researched IDC judgment about the market and specific vendors. IDC analysts tailor the range of standard characteristics by which vendors are measured through structured discussions, surveys, and interviews with market leaders, participants, and end users. Market weightings are based on user interviews, buyer surveys, and the input of IDC experts in each market. IDC analysts base individual vendor scores, and ultimately vendor positions on the IDC MarketScape, on detailed surveys and interviews with the vendors, publicly available information, and end-user experiences in an effort to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

IDC defines cloud security services as a range of security services offerings that help customers securely plan, migrate, operate, and optimize cloud security functions with automation and engineering capabilities. It includes activities like advising customers on the cloud security guardrails, compliance, cloud security operations, design, and selection of cloud security tools. In the scope of this particular IDC MarketScape, the study will assess the following capabilities from the perspective of both professional security services and managed security services:

- Cloud security posture management
- Cloud-native app platform (CNAPP)
- Cloud workload protection
- Infrastructure-as-a-code scanning
- Cloud infrastructure entitlements management (CIEM)
- Cloud security automation
- Cloud security assessment and design
- Cloud security risk review

- Cloud security compliance advisory

LEARN MORE

Related Research

- *What Are the Top-Ranked Professional Cloud Security Services and Managed Cloud Security Services?* (IDC #US52654424, October 2024)
- *Market Analysis Perspective: Worldwide Security Services, 2024* (IDC #US50635824, October 2024)
- *What Are the Primary Reasons Organizations Using Cloud Security Services State for Using the Cloud?* (IDC #US52592824, September 2024)
- *Worldwide Cloud-Native Application Protection Platform Market Shares, 2023: A Bull Market* (IDC #US52472324, August 2024)
- *IBM Consulting Advantage — The GenAI-Powered Platform to Turbocharge IBM Consulting Services* (IDC #lcUS52447224, July 2024)
- *IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment* (IDC #US48761022, September 2022)

Synopsis

This IDC study evaluates 21 global cloud security services providers in the AI era. It assesses their capabilities in integrating AI, cloud security strategies, and managed cloud security services. The study also assesses their capabilities of embedding security in cloud transformations, leveraging AI for enhanced security measures, and maintaining compliance and security. Key strengths and challenges of each vendor are discussed, providing insights for technology buyers to make informed decisions.

“As organizations navigate the complexities of digital transformation in the AI era, leveraging AI-driven cloud security services can streamline operations, enhance compliance, and unlock new growth opportunities. The future of cloud security lies in automation, AI enhancements, and a zero trust model, promising to reduce cybersecurity risks and ensure business continuity in an increasingly digital world,” says Cathy Huang, research director, IDC Cybersecurity Consulting and Professional Security Services.

ABOUT IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology, IT benchmarking and sourcing, and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives. Founded in 1964, IDC is a wholly owned subsidiary of International Data Group (IDG, Inc.).

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, and web conference and conference event proceedings. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/about/worldwideoffices. Please contact IDC report sales at +1.508.988.7988 or www.idc.com/?modal=contact_repsales for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights.

Copyright 2024 IDC. Reproduction is forbidden unless authorized. All rights reserved.