IDC MarketScape

IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment

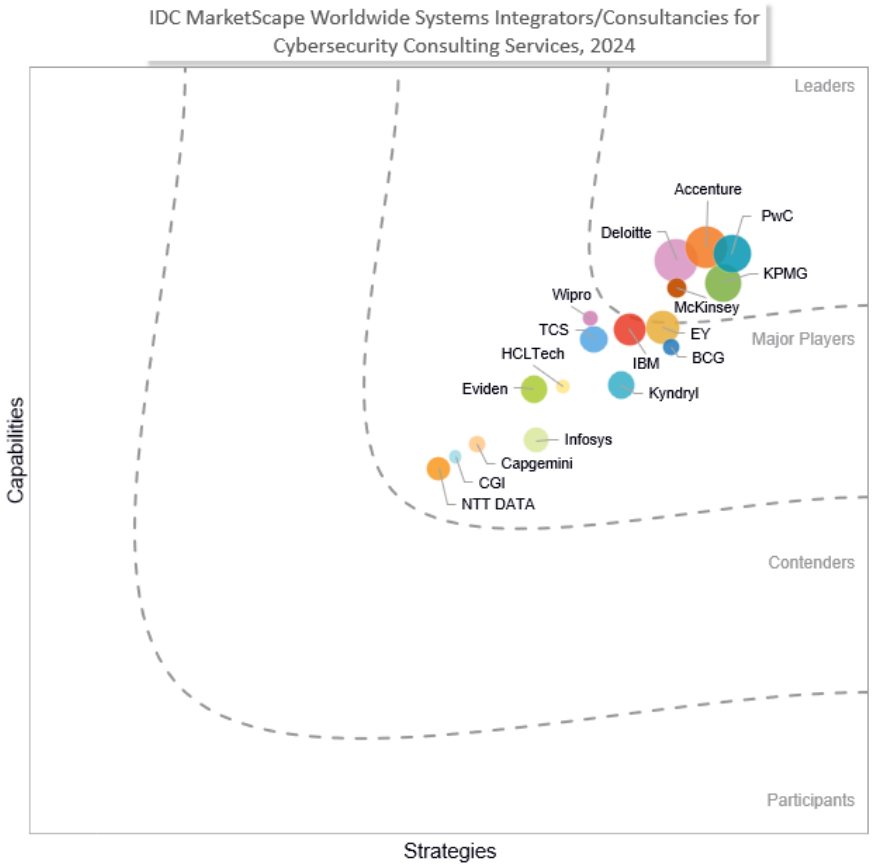
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES PWC

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services Vendor Assessment



Source: IDC, 2024

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

January 2024, IDC #US50463423e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment (Doc # US50463423). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Guidance, Vendor Summary Profile, Appendix and Learn More. Also included is Figure 1.

IDC OPINION

The role of cybersecurity consulting partners has increased significantly given the rising strategic importance of cybersecurity to an organization's digital success and even survival. This IDC MarketScape provides insights into the current capabilities and future strategies of 17 global systems integrators (GSI) as well as leading consultancies. Domains studied in cybersecurity consulting services include cybersecurity strategy advisory, program transformations, and architecture assessments. After evaluating GSI/consultancies, IDC notes key findings in the sections that follow.

Cybersecurity Is No Longer the Exclusive Domain of the CISO or CIO

Cybersecurity has grown in strategic importance over the years. Cybersecurity runs into the business processes, governance, and culture of the organization, making it integral to business rather than just a compliance-driven overhead.

Over the past two decades, organizations have increased their reliance on technology in efforts to improve their customer experience, business operations, supply chain management, and employee productivity. Cybersecurity has become much more relevant as digitally transformed businesses realize that their very existence may depend on their capabilities to withstand a cyberattack and quickly restore to a viable operating status.

As a result, cybersecurity discussion is not only an IT-based discussion but all about business enablement, establishing trust and credibility in the market to compete effectively. The responsibility lies with stakeholders beyond just CISOs.

Clear Metrics and Measurements of Cybersecurity Investment Are Needed

Organizations today face tremendous financial stress due to inflation and economic uncertainty. While the security spend will remain largely resilient, security investments are under scrutiny. CEOs and business executives now expect clear metrics and measurement of results to assess and validate investments made in their organizations' security programs.

The metrics include tangible artifacts and benefits such as cost reduction through security modernization, automation, vendor/tool rationalization, enhanced visibility, expanded security control coverage, and expedited breach detection through continuous monitoring and integrated, insights-driven solutions.

Moreover, if cyber is taken into account earlier in the continuous integration/continuous delivery (CI/CD) development cycle, there are better outcomes. It is said risks, gaps, or vulnerabilities caught late in the development cycle cost five to six times more than if caught early in the development cycle. Hence the trend of an equitable distribution of funding from line of business, IT, and cyber is rising.

Industry-Specific Cybersecurity Consulting Is Driven by Business Outcomes

A lot of cybersecurity consulting demand is going into strategic road maps looking at not only technology but also the critical use cases within the businesses that are unique to the industry vertical.

Cybersecurity consulting service engagements are less SLA specific and more business outcome/business impact specific.

The spectrum of future cyberinnovations, tools, technologies, and services are centered on specific client use cases, including cybereducation and upskilling, continuous assessment, risk detection and monitoring, threat intelligence, incident readiness and response, and risk quantification and reporting.

Full Life-Cycle Model Address from Advise-Implement-Operate-Optimize

The boundary between consulting, implementation, and management service is becoming less clear. Most cybersecurity consulting vendors have managed/operate services, a symbiotic relationship with their consulting services.

The depth of understanding of client operations across industries and cyberdomains from operation /managed services provides the critical insights and offers more programmatic strategies and plans when the provider is also in the position to deliver advisory/consulting services. As vendors broaden their capabilities and portfolio range, they drive continuous value and important innovation for its clients.

Client Satisfaction Is Generally High Toward Their Cybersecurity Consulting Providers

Clients globally rated their cybersecurity consulting providers, in aggregate, best at helping them with the following:

- Skills and experiences of key personnel engaged in the project
- Meeting data privacy and sovereignty requirements
- Overall communication and stakeholder management
- The breadth of cybersecurity consulting capabilities

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied vendors that provide cybersecurity consulting services throughout the world. The vendors included in the study must meet certain criteria to qualify for this vendor assessment:

- A provider operates with a multinational footprint.
- Cybersecurity consulting services portfolio meets more than 50% of IDC's definition and scope of the study, including:
  - Security road map development
  - Security strategy advisory
  - Security operator center (SOC) design and build
  - Security sourcing strategy
  - Data security and sovereignty advisory

    - Identity access management (IAM) design and transformation
    - Integrated threat intelligence design and consult
    - Cybersecurity transformation
    - Cyber-recovery consulting
    - Cyber-supply chain resilience planning
    - Architecture assessments across networks/endpoints/edge/cloud/IoT/OT
- A provider has a total revenue from cybersecurity consulting services that exceeds $120 million in 2023.
- A provider has at least 100+ cybersecurity consulting customers.

ADVICE FOR TECHNOLOGY BUYERS

There is an increased board oversight over cybersecurity. The announcement of the finalized SEC ruling asks for more accountability, governance, transparency, and formal reporting around how companies are managing their cyber-risks. Participation of the C-suite and the board in cybersecurity resilience tabletop exercise is becoming necessary. Cyber-resilience is a prominent theme. It is important evaluating security services vendors' definitions and approaches with respect to cyber-resilience:

- Are there standard definitions for cyber-resilience?
- Are vendors delivering different approaches and solutions?
- How would companies measure resilience?

Another topical theme arises when organizations engage a cybersecurity consulting service vendor to decide whether to transform its cybersecurity program as a whole or if it is better to tackle specific functions within the cybersecurity program (i.e., identity access management, security operations, or third-party risk management). Demonstrations of relevant experiences and expertise on types of frameworks (e.g., zero trust), partnerships, and assets/accelerators/intellectual property (IP) are becoming important deciding factors.

While many providers will highlight their growing investment in artificial intelligence (AI) and automation, it is useful for end users to understand the mechanism of collecting the right telemetry and data sets for training the models and the number of AI tools.

Organizations should use this study to support their vendor selection evaluation process and consider reference criteria used in this study to shape their own individual selection evaluation process. For example:

- Determine whether the provider has the necessary breadth and depth of expertise to support their cybersecurity transformation journey. In particular, examine the provider's industry-specific expertise and region-specific knowledge (e.g., local compliance).
- Learn about the vendor's portfolio strategy and road maps for future innovation. Emerging security services such as AI security and privacy, IoT security, and quantum risk assessment may be of particular interest to some buyers.
- Understand the provider's client success programs (e.g., the possibility to provide executive sponsorship for the project, frequency of scheduled meetings, customer education sessions/workshop, and the board-level communication support).

- Scrutinize the delivery model, along with stakeholder management and change management capabilities presented by the provider. Be aware of the sourcing models and the level of automation used behind the delivery. Transparency is essential.
- Dig into the vendor's pricing and commercial models. Some vendors have innovative pricing approaches, and some may have very rigid contractual processes. Try to arrange conversations with other customers to discuss outcomes, engagement models, and satisfaction.

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.

PwC

PwC is positioned in the Leaders category in this IDC MarketScape for worldwide systems integrators/consultancies for cybersecurity consulting services.

PwC is a multinational professional services network of firms headquartered in the United Kingdom with 328,000 people and offices in 152 countries. The firm delivers assurance, tax, and advisory services through local firms but operates with global leadership. The cybersecurity business, which is one part of PwC Global Risk Services, includes 7,000 dedicated cybersecurity consultants. Cybersecurity and all facets of risk management are brought together under a global platform. Acceleration Centers in Mexico, India, and Argentina support local delivery teams.

PwC is diversifying from traditional people-based services to technology-enabled services, services with products, managed services, and platforms such as SaaS and PaaS. Territories take the lead on developing products, and global funds are available to scale, roll out, and maintain a productized solution globally. Board Central, for example, provides risk and cybersecurity knowledge to board members. As another example, Connected Identity provides rapid application onboarding and enablement of identity and access management services.

Cybersecurity consulting services encompass design, assessment, strategy, implementation, investigatory, regulatory, and monitoring. A single source of global threat intelligence feeds advisors, managed services, and products. The following core services are aligned with technical cyber and regulatory capabilities:

- Cybersecurity strategy, risk, and consulting
- Cyberdefense and engineering
- Investigations and forensics
- Financial crimes management
- Data risk and privacy
- Risk consulting in financial services and health industries
- Enterprise cyber, risk, and controls
- Enterprise technology solutions

PwC's alliance partners span multiple levels of partnership. Anchor alliances include AWS, Microsoft, Google, Oracle, SAP, and Salesforce.

Consultants use digital assets and technologies to assess cyber-risk; track and report cybersecurity; detect, control, and solve cyber-risks; upskill the cyberorganization; and provide cyber-risk management. Among the tools are Cyber Tech Rationalizer, an accelerator that supports portfolio rationalization, and Secure Cloud Shield, which speeds cloud transformation security assessments and analysis.

Connected Source is a knowledge sharing platform containing industry-specific and cloud security frameworks, software components, and other technical assets that can be shared by delivery teams to support consistency and quality. PwC's digital assets are proprietary IP developed during client engagements and standardized in PwC Digital Labs.

A risk and compliance industry cloud addresses the risk of errors common in manual processes that rely on email and spreadsheets. Applications and use cases include security controls definition, risk control policy mapping, policy enforcement, and automated testing. Clients can manage compliance functions using a single platform.

PwC uses AI and ML in several ways. The PwC Fusion Center, powered by AWS, combines data from multiple sources to create centralized, near-real-time security views. GenAI is being used in cyber and regulatory use case pilots. The Microsoft relationship focuses on creating scalable offerings using GPT-4/ChatGPT and Azure OpenAI Service.

Strengths

- PwC's industry and regulatory expertise are highly appreciated by its customers. Protocols align with industry sector requirements and frameworks to prepare clients for regulatory examination.
- The Global Centre for Crisis & Resilience consists of a dedicated team of 1,000 senior professionals that enable the PwC network to support clients with crisis readiness, response, and recovery.
- Clients praise PwC highly in areas of stakeholder communications, overall cybersecurity strategy, skills, and expertise. Identity and access management, management of staff turnover, and pricing flexibility receive the highest marks.
- A client states that PwC is an identity expert, excellent in strategy, and stands out for collaborative thinking.
- IDC's *Worldwide Cybersecurity Consulting Services Survey* respondents gave PwC a top mark for delivery of measurable outcomes. Areas that are highly rated include key assets, tools, and frameworks used in the engagement; tenure/experience level of the engaged cybersecurity professionals; meeting data privacy and sovereignty requirements; and value-added services.

Challenges

- According to client feedback, PwC can further improve its internal communication and collaboration. In addition, PwC's internal review process is seen as risk averse, which causes a challenge related to documenting objectives and describing the scope of work.

- IDC's *Worldwide Cybersecurity Consulting Services Survey* respondents identified the areas that PwC can improve, including delivery of work that achieves technology objectives and effective use of emerging technologies.

Consider PwC When

Large and/or multinational organizations that prefer a cyber and risk portfolio aligned to their maturity and transformation journeys should consider PwC. Priorities may include data trust and management, identity and access management, cyber-resilience, cyber integration into the business and cyber-risk management.

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 cybersecurity consulting services as a range of professional services activities that help organizations to plan, design, assess, or transform across its cybersecurity practice. In the scope of this particular IDC MarketScape study, the cybersecurity consulting services include strategy planning and program transformation, cyber-resilience advisory, and architecture assessment and design services. Examples of these services include:

- Security road map development

- Security strategy advisory
- Security operator center (SOC) design and build
- Security sourcing strategy
- Data security and sovereignty advisory
- Identity access management design and transformation
- Integrated threat intelligence design and consult
- Cybersecurity transformation
- Cyber-recovery consulting
- Cyber-supply chain resilience planning
- Architecture assessment services across networks, endpoints, edge, cloud, IoT, OT, and so forth

LEARN MORE

Related Research

- *What Are the Top Factors Deciding the Selection of Cybersecurity Consulting Services Providers?* (IDC #US51361823, November 2023)
- *Market Analysis Perspective: Worldwide Security Services, 2023 and Beyond* (IDC #US51228723, September 2023)
- *Worldwide and U.S. Comprehensive Security Services Forecast, 2023-2027* (IDC #US50047523, June 2023)
- *IDC's Worldwide Security Services Taxonomy, 2023* (IDC #US50332523, March 2023)
- *IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment* (IDC #US48761022, September 2022)

Synopsis

This IDC study assesses 17 global systems integrators or consultancies offering cybersecurity consulting services through the IDC MarketScape model. The role of cybersecurity consulting partners has increased significantly given the rising strategic importance of cybersecurity to an organization's digital success and even survival. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for cybersecurity consulting services.

"While the cybersecurity consulting services providers are engaged for broader themes like cyber-resilience and cybersecurity transformation, the demonstration of technology understanding, especially innovation or point of views around emerging technologies like AI and quantum computing, is playing an important role for buyers to decide for their cybersecurity consulting services provider," says Cathy Huang, research director, IDC's Worldwide Security Services. "This trend is reflected in the growing use of assets or proprietary IP when cybersecurity consulting vendors engage its clients."

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