IDC MarketScape

IDC MarketScape: Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment

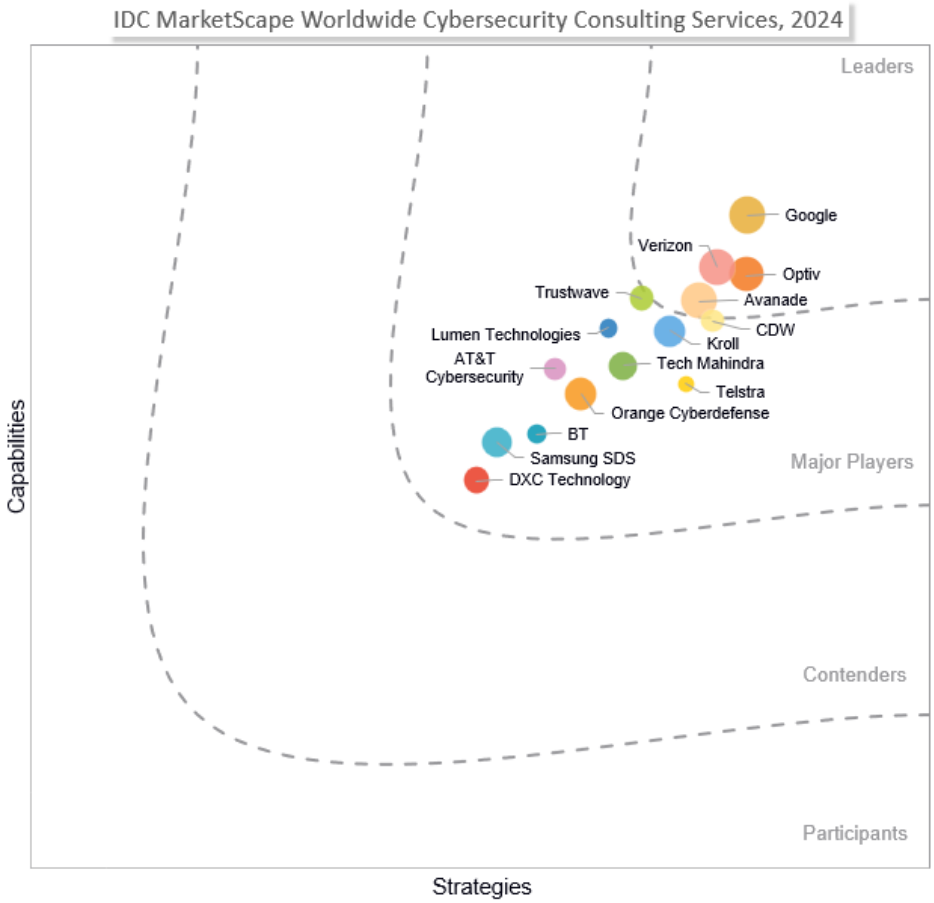
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES GOOGLE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cybersecurity Consulting Services Vendor Assessment



Source: IDC, 2024

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

March 2024, IDC #US50463223e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment (Doc # US50463223). 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

As a growing number of organizations view cybersecurity as a strategic business enabler, along with a surge of regulatory requirements across the world, the quest for quality cybersecurity consultants and trusted cybersecurity advisors hits an all-time high.

In this IDC MarketScape study, IDC assesses the following cybersecurity consulting offerings closely, while most of the featured vendors in this study do have a broader portfolio that goes beyond cybersecurity consulting services:

- Cybersecurity strategy planning and program transformation services
- Security architecture assessment and design services
- Cyber-resilience consulting services

Depending on the requirements, cybersecurity consulting services can be consumed in a discrete, bespoke fashion, but very often services are structured as a component of or integrated into a larger IT or business transformation initiative.

IDC conducted a global survey with 901 organizations to understand the buying trends of cybersecurity consulting services. The survey gathered direct tech buyer feedback for their respective cybersecurity consulting services providers across the world. Most of these firms are featured in *IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment* (IDC #US50463423, January 2024), and the remaining ones are studied in this IDC MarketScape.

IDC finds most of the participating firms have solid technical capabilities and strong cybersecurity skills. Among all the evaluation criteria, "skills and experiences of key personnel engaged in the project" showed positive remarks from the 901 surveyed organizations that utilize the cybersecurity consulting capabilities of the studied firms.

The very nature of cybersecurity consulting services relies heavily on the expertise of consultants. Cybersecurity consultants should have in-depth knowledge and experiences of one or multiple security domains, for example network security, security operations, incident response, regulatory compliance, and operational technology (OT) security, to support enterprises' needs. Industry-specific knowledge will be a bonus and highly appreciated by tech buyers.

Many of the firms were showing positive output in regard to delivery and people-related criteria, for instance project governance, meeting data privacy and sovereignty requirements, and engaged cybersecurity professionals being very responsive and professional. In contrast, cybersecurity consulting services providers should improve on the innovation aspects, including the proprietary intellectual property (IP), tools, and frameworks used in the engagement and effectiveness of using emerging technologies like AI and generative AI (GenAI) in the delivery and client engagement.

What is more, a good number of security services vendors package their cybersecurity offerings in a highly flexible way. There is a rising trend to package professional security services into a managed-, subscription-, or retainer-based model, such as expertise on demand (EOD) or cyber as a service (CaaS). These models are particularly attractive to midmarket.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in this IDC MarketScape for cybersecurity consulting services, security services vendors must be able to provide services in the categories of cybersecurity strategy planning, transformation, security architecture assessment and design, and cyber-resilience consulting services. Further:

- A security services vendor must operate with a multinational footprint.
- A security services vendor must have a total revenue of cybersecurity consulting services that exceeds $25 million in 2023.

ADVICE FOR TECHNOLOGY BUYERS

In the highly competitive cybersecurity services market, buyers serve their organizations well by expressing assertive expectations and conducting thorough evaluation. Guiding buyers' evaluation, IDC offers the following advice:

- **Multidisciplinary model:** Evaluate vendor's multidisciplinary model and ensure the ability of the vendor to demonstrate an understanding of issues faced by stakeholders including those from outside the security functions such as risk, compliance, operations, IT, networks, finance, and engineering. On this topic, instead of considering an IT tabletop exercise, it might be more useful to have an entire operational tabletop exercise.
- **Addition of training hours:** For a transformation type of project, mandate a certain number of training hours or some cybersecurity awareness sessions in the scope to enhance the overall awareness to the relevant threats, typical cyberattack techniques. Security breaches often tie back to user actions. Fostering a security-aware culture within the organization is as important as strong security controls. Some of the evaluated cybersecurity services vendors have explicit cybersecurity training or learning and development offerings as part of their portfolio.
- **Innovation:** Innovation demonstrated throughout the engagement is a critical factor to differentiate cybersecurity consulting services vendors. While there is considerable hype around AI, examine the prospect cybersecurity consulting vendors' own way of adopting AI and GenAI, especially how do they ensure security and sovereignty issues of AI. Key questions you must ask include:
  - How do you monitor and audit AI systems?
  - What measures do you take to ensure responsible AI practices, including fairness, transparency, and accountability in your algorithms?
  - How are you protecting against authorized data entry into an AI model?
  - How do you plan to bring continuous improvement?
- **Communication:** Consider a vendor's expertise in communicating at the C-suite and board levels. In a cybersecurity consulting project itself, communication and stakeholder management are critical factors of delivering results successfully and on time. In this study, we have assessed vendors' capabilities to support boardroom communication. A handful of

vendors do have the capability to articulate risk in the boardroom and effectively connect technical risks to the business challenges without so much technical jargon used.

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.

Google

Google is positioned in the Leaders category in this 2024 IDC MarketScape for worldwide cybersecurity consulting services.

In late 2022, Google acquired Mandiant, whose cyberdefense, threat intelligence, and incident response services augment the Google Cloud Security portfolio. Mandiant employs 4,000+ cybersecurity professionals. About 1,300 professionals who are dedicated to consulting services are placed in 27 countries and assist clients in 50+ countries.

Consulting services, which assist clients before, during, and after a breach, are technology agnostic and lead with the company's threat intelligence and attacker techniques. The portfolio consists of four pillars: strategic readiness, incident response, technical assurance (testing controls and operations), and cybersecurity transformation. Transformation services, which feature multiyear road maps and executive/board services, are designed to help clients build or strengthen cyberdefense programs.

All services are agnostic to Google Cloud, AWS, and Microsoft Azure and are suitable for multicloud, on premises, and OT. Specialist ICS/OT teams contribute to the IoT cybersecurity architecture service. The consultants' technical toolkit includes products built by Google engineers, by in-house Mandiant experts, and by third parties.

Consulting offerings incorporate security frameworks and regulations, homegrown and third-party tools and technologies, proprietary IP, and partners including Trellix, CrowdStrike, SentinelOne, and Carbon Black. Technology includes the purpose-built ESPIR investigation platform for incident response workflow; FACT, a tool developed by Mandiant to deliver investigations using EDR tools to support activities such as look-back forensics; and extensive internal use of AI.

Mandiant offers a three-pronged approach for helping clients use AI: securing the use of AI in the business, enhancing security with AI, and malicious use of AI. Assessments can identify AI pipeline issues, and consultants address AI risk factors.

Mandiant delivers all core cybersecurity consulting services. Partners and contractors deliver a small percentage of services. Mandiant project delivery comprises a designated account representative who is the key client contact, an engagement manager who manages the delivery of services, a project manager who tracks the plan and schedule, a defined escalation path, and a post-engagement customer survey. A Mandiant global function runs quality assurance and quality control on every service offering.

The Mandiant Consulting group partners with the Office of the CISO to share knowledge and best practices. The group protects Google Cloud assets and the Google Cloud Platform. The Mandiant Communications Center gathers and disseminates threat information through multiple channels and

directly with consultants who deliver threat intelligence consulting services and product teams that update offerings and assist clients.

Mandiant supports client success through a program consisting of customer success managers, customized success plans, escalation management, operational reviews, and executive business reviews. It offers flexible consumption models, such as expertise on demand, which includes an incident response retainer plus components to be used on proactive readiness and technical assurance services.

Strengths

- Mandiant has a history of breach investigations. The company's library of threat actor activity is compiled from machine, adversary, and operational intelligence. There is a dedicated team for malware analysis. Trends, intelligence, and guidance are shared with the security community.
- Mandiant Academy offers certifications and courses, which are developed in-house and delivered by practitioners with frontline experience alongside professional instructors. One Academy focus area is training governments to protect themselves through coursework and cyber-ranges.
- A "team of teams" approach enables consultants to deliver work rapidly across time zones. The team is able to support in more than 30 languages. Work with clients to leverage their technology (past, present, and future) to solve challenges versus recommending specific vendors or products.
- A client commented that Mandiant is "top tier when it comes to incident response" and would "recommend Mandiant to anyone." The effective use of emerging technologies like machine learning and GenAI is also showing positive feedback by global end-user survey respondents.

Challenges

- While Mandiant has a strong brand recognition in the incident response market, the provider should enhance the visibility for its broader services portfolio catering to customers with different levels of maturity.
- IDC's *Worldwide Cybersecurity Consulting Services Survey* participants identify several areas that can improve, and these include demonstrating innovation in the engagement, cost management, and value-added services.

Consider Google When

Companies of 2,000+ employees with varying cybersecurity maturity levels that desire to solve challenges related to response, strategy, testing, and training should consider Mandiant. Client priorities may include threat intelligence–led services, protection of critical infrastructure, cyber-risk management, and cyberpreparation for executive/board level.

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 plan, design, assess, or transform across their cybersecurity practice. In the scope of this particular IDC MarketScape study, the cybersecurity consulting services include strategy planning and program transformation, architecture assessment and design services, and cyber-resilience consulting. 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

- *IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment* (IDC #US50463423, January 2024)
- *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)

Synopsis

This IDC study represents a vendor assessment of cybersecurity consulting services for enterprises through the IDC MarketScape model. It assesses 15 cybersecurity services vendors offering cybersecurity strategy advisory, architecture assessment and design, cyber-resilience consulting, and cybersecurity transformation services. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for cybersecurity consulting services. The document provides detailed vendor profiles, highlighting their strengths, challenges, and key offerings.

"The role of a trusted cybersecurity partner has increased given the rising importance of cybersecurity to an organization's overall resiliency and success," says Cathy Huang, research director, IDC's Worldwide Security Services. "This trend is manifested in the growing demand for security and risk assessment, security strategy, and program advisory that drives all kinds of vendors, be it telecom providers, managed security pure players, cybersecurity specialists, IT outsourcing providers, or value-added resellers, to put strategic focus to grow their own cybersecurity consulting capabilities."

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