IDC MarketScape

IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment

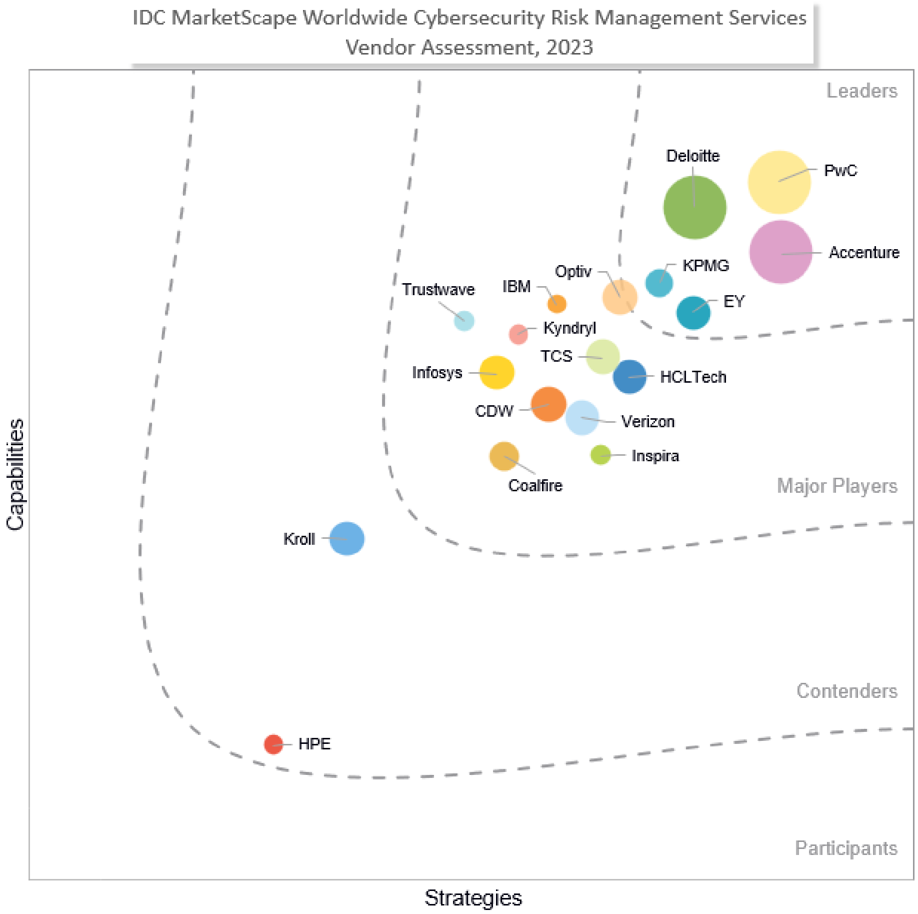
Philip D. Harris, CISSP, CCSK

THIS IDC MARKETSCAPE EXCERPT FEATURES DELOITTE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Cybersecurity Risk Management Services Vendor Assessment



Source: IDC, 2023

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

October 2023, IDC #US49435222e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Cybersecurity Risk Management Services 2023 Vendor Assessment (Doc # US9453222). 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

Cybersecurity risk management (CRM) services continue to evolve not only in value-added service offerings but with making CRM a key component in overall business risk management. This set of services can play a role as a strategic capability enabling organizations to highlight threats and the risks they pose to the organization and drive this strategic capability into ongoing business strategy. This set of services can also provide a tactical escalation of real risks posed to the organization that require immediate risk treatment in a responsible way. Essentially, this service establishes a life cycle of CRM from risk identification to risk closure telling the story along the way to other key stakeholders, informing them these risks have been managed effectively and responsibly.

Within this CRM life cycle, there have been several notable enhancements including standardized assessment and programmatic frameworks, risk quantification, and continuous CRM that are now more a reality and less a dream; elevation to the C-suite and boards of directors and a main topic of concern and discussion; and proprietary and COTS solutions that automate much of the tedious and laborious activities that most always brought news of risks late.

Cybersecurity buyers continue to examine and view CRM from a strategic, business, and industry viewpoint – the right direction and context – to understand how they can be proactive and demonstrate a trusted brand. Cybersecurity buyer priorities include relieving the cumbersome and tedious nature of identifying, prioritizing, and remediating risks; conducting both control and maturity assessments; creating reports that speak to executives in financial terms; tracking risks from identification to closure; having a complete CRM program; and quantifying risks. Many struggle to understand their current state and are unclear how to proceed and make poor buying choices without understanding their complete risk posture, prioritizing these risks over time, and what the total cost of ownership is. Some CRM service providers are stepping up to aid such organizations in solving these challenges.

IDC believes CRM programs can be powerful and effective because of technology automation and orchestration integration, strong processes, and trained risk management professionals. This will elevate the awareness and management of cybersecurity risks shepherded through identification, treatment, and closure of risks, with executive management involvement. Optimally, CRM services enable organizations to maintain a consistent level of awareness and protection, along with the flexibility to reprioritize, reassess, and reconfigure their risk as well as detection and response tolerances and activities. Increasingly, security buyers view CRM as a necessity to help mature their cybersecurity programs.

CRM services is not just about having a service provider come into your organization and perform a one-time risk assessment and then helping you remediate the findings. The goal should be for any organization to engage a CRM services provider that can establish a complete program from beginning to end with cybersecurity teams, IT, and the business and executive management all being aligned as to how this new program will contribute to adding value to the business and ultimately aiding the organization in demonstrating that its brand, services, products, and so forth are trusted.

The most complete CRM services portfolios include the following capabilities:

- Ensures a clear picture of current cybersecurity risk posture and a strategy for risk reduction
- Establishes an appropriate security framework as a baseline set of requirements that is rightsized for the maturity of the organization
- Enables executive management to understand how, where, and why to invest in managing cybersecurity risks
- Implements and executes a strategy and overarching cybersecurity program that allows for rigorous, structured decision making and financial analysis of cybersecurity risks
- Includes technology components that provide orchestration and automation of processes within the program
- Achieves and sustains compliance (regulatory or otherwise) using an appropriate security framework as a base set of requirements for the outcome of a well designed and executed CRM function
- Builds a risk-aware culture through education and awareness to reduce the impact of human behavior
- Operates a sustainable program that is resilient in the face of ever-evolving cyberthreats and digital business strategies
- Develops an in-depth strategic road map and total cost of ownership (TCO) analysis

Ultimately the risk management program is designed to ensure all cybersecurity risks are properly handled, documented, and closed. If successful, this program could be a model for managing all risks within the company eventually. You want the program to be "beyond reproach."

The Market Definition section in the Appendix provides a description of what IDC believes is the minimum set of capabilities a CRM services provider should offer.

IDC encourages buyers to evaluate CRM service providers based on the outcomes they want to achieve related to day-to-day identification, treatment, and closure of risks.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

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

- **Geographic presence.** Each vendor is required to operate CRM services in more than one region throughout the world.
- **Sales presence.** Each vendor has a sales force across one or more regions throughout the world.
- **Customer base.** Each vendor has at least 100+ customers.
- **Revenue.** Vendor revenue exceeds $20 million per annum.
- **CRM services capability.** Each vendor possesses a CRM service that has trained professional cybersecurity staff with expertise in cybersecurity risk management.

ADVICE FOR TECHNOLOGY BUYERS

Technology buyers should consider several factors when looking at CRM services. A couple of key questions to ask at first are:

- Do I want to build and run this service myself?
- Do I want a service provider to build the service and then I run it?
- Do I want a service provider to build and run the CRM service?

Once you have concluded how you want to proceed, then utilize one or more of the advised factors:

- Understand the service provider's distinctive service capabilities, how long it has been performing such work, are there customers to speak with for testimonials, and so forth.
- Determine whether the service provider is interested in understanding the problem to solve and its willingness to work with you to refine the problem statement versus just giving you a rundown of its services in the hope that you will just buy.
- Understand what the differences in services are from other service providers in the field. What do they really bring to the table?
- Ask yourself if the service provider has demonstrable knowledge and skill in competence.
- Get clarity on the limits of the service provider's knowledge and skill in this area.
- Understand the various use cases from the service provider as to the types of projects it has engaged successfully and also, if the service provider is willing, have it describe instances where a project did not result in complete satisfaction.

VENDOR SUMMARY PROFILES

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.

Deloitte

Deloitte is positioned in the Leaders category in the 2023 IDC MarketScape for worldwide cybersecurity risk management services.

Quick facts about Deloitte include:

- **Years in business:** 30+ years providing cybersecurity support
- **Employees:** 25,000+ practitioners
- **Number of clients:** 3,000+ cyber clients
- **Ecosystem:** Across hyperscalers, cyber, technology, data, industry, government, and academia

Deloitte, one of the largest professional services firms in the world, operates in more than 150 countries. The firm advises, implements, and operates a full range of cyber services and solutions with capabilities across strategy and transformation, cloud, detect and respond, identity, infrastructure security, data and privacy, application security, and emerging technologies.

Deloitte maintains three global delivery centers, augmented by a network of in-region satellite delivery centers, for 24 x 7 x 365 delivery of cyber services and SaaS-based modular platform solutions such as MXDR by Deloitte and Digital Identity by Deloitte. Its 30+ cyber client experience centers enable local contextualization of services, development of new solutions, connected device testing, threat intelligence collection, and delivery of client labs and simulations. Its team of 250+ dedicated threat intelligence experts has a specialized focus on malware research, geopolitical insights, regional threat landscapes, and threat actor groups and collaborates with proactive threat hunting, SOC monitoring, incident response, and cyber strategy teams to develop customized, industry-specific intelligence, in addition to qualifying and contextualizing third-party intelligence feeds. DISP, Deloitte's proprietary threat intelligence platform, is integrated with other solutions (e.g., MXDR by Deloitte) and includes analytics capabilities and tools such as Deloitte's Codex Gigas breach and malware database and a threat library that enables threat modeling and mapping of threat actor groups to the MITRE ATT&CK framework.

Deloitte's approach to cybersecurity can be summed up as helping secure success for organizations by positioning cyber as a strategic business enabler, balancing the needs of protection and enablement for the enterprise. Secure success is its value proposition — the outcome from cybersecurity solutions that are powered by business acumen to help organizations not just operate securely but grow successfully. Protection intends to achieve peace of mind and resilience through risk management and mitigation, and protecting employee and customer data, revenue streams, and reputation. Enablement aids organizations with achieving confidence and growth through future-proofing, creating new products and services, adding value to existing products and services, entering new markets, and serving new customers.

For cyber-risk management programs, Deloitte either engages clients as part of a larger set of business transformation initiatives or as a standalone initiative for CRM. In either situation, Deloitte brings a full suite of CRM services that can be customized to the client's specific needs and include ties into its broader cyber portfolio (e.g., data and privacy, application security, cloud, identity) for offering-specific needs beyond core CRM (which includes assessments, readiness, strategy, governance, training, metrics/reporting/cyber-risk quantification [CRQ], etc.). Further, when there are projects specific to an offering (e.g., detect and respond), Deloitte couples its CRM capabilities as part of the solution that the company advise, implement, and operate for the client.

Key differentiators for Deloitte include being business led and outcome driven, drawing upon multidisciplinary DNA across all of Deloitte, possessing a talent pool that is both diverse and specialized, and bringing innovation that adds value to the delivered outcomes.

Strengths

Deloitte has strong brand recognition as one of the Big Four accounting firms, which has established the company as a trusted and respected brand in the industry. This recognition attracts clients, talent, and partners, giving the firm a competitive edge. Deloitte offers a wide range of services across various industries. Within those diverse services is its Risk Advisory service geared toward helping clients manage risks related to cybersecurity, financial, operational, regulatory, and reputational matters. Deloitte serves clients across multiple industries, including consumer products, energy and resources, financial services, government and public services, life sciences and healthcare, manufacturing, real estate, technology, media, and telecommunications.

Challenges

Some clients may not be able to engage Deloitte due to the firm's audit independence restrictions.

Consider Deloitte When

Consider Deloitte if you are a large enterprise that needs a service provider that can provide cross-organizational support especially when designing and implementing the appropriate cybersecurity program that fits the organization and that can deal with the various types of businesses that large enterprises typically have. Deloitte also aids clients in combining business cybersecurity needs with appropriate solutions integrated into the overall environment.

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 to provide an accurate and consistent assessment of each vendor's characteristics, behavior, and capability.

Market Definition

Cyber-risk management services is a multibillion-dollar value-added service offering that supports organizations with making CRM a key component in overall business risk management. Organizations of any size and industry can be a target of attack with attackers generally being motivated for financial gain. The threat of potential disruption to the business or to a business reputation by a cyberattack is called cybersecurity risk. Cybersecurity risk also includes any risk of monetary loss, disruption, or damage to the reputation of an organization from some sort of failure of its information technology (IT) systems. Cybersecurity risks can materialize in the following ways:

- Deliberate and unauthorized breaches of security to gain access to information systems for the purposes of espionage, extortion, or embarrassment
- Unintentional or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed
- Operational IT risks due to poor systems integrity or other factors

The set of processes for identifying potential cyber-risk is at the core of a cyber-risk management program, which can be utilized by a cybersecurity services provider either to execute for an organization or to develop and implement a program for an organization. Many cybersecurity consulting service providers offer cyber-risk management programs in the form of services. A cyber-risk management program includes a set of activities conducted with the intention of identifying those control and maturity risks faced by an organization. The services performed by providers with experts in the field of cybersecurity aim to assist organizations with:

- Providing a clear picture of current cyber-risk posture and a strategy for risk reduction
- Understanding how, where, and why to invest in managing cyber-risks
- Development, implementation, and execution of a strategy and overarching CRM program that allows for rigorous, structured decision making and financial analysis of cyber-risks
- Achieving and sustaining compliance (regulatory or otherwise) using an appropriate security framework as a base set of requirements for the outcome of a well designed and executed cyber-risk management function
- Building a risk-aware culture through education and awareness to reduce the impact of human behavior
- Operating a sustainable program that is resilient in the face of ever-evolving cyberthreats and digital business strategies
- Development of an in-depth strategic road map and total cost of ownership analysis
- Execution models where the organization fully operates the program, or a hybrid where both the service provider and the organization execute aspects of the program, or the service provider solely executes the program on behalf of the organization
- Establishing the organization as a “trusted” organization with which to do business
- CRM services being performed throughout the world in regions such as North America, EMEA, LATAM, and APAC

LEARN MORE

Related Research

- *Worldwide and U.S. Comprehensive Security Services Forecast, 2023-2027* (IDC #US50047523, June 2023)
- *Worldwide and U.S. Governance, Risk, and Compliance Professional Services Forecast, 2023-2027* (IDC #US50824523, June 2023)
- *IDC's Worldwide Security Services Taxonomy, 2023* (IDC #US50332523, March 2023)
- *IDC TechScape: Worldwide Cybersecurity Risk Management Services, 2022* (IDC #US49710322, December 2022)
- *IDC PlanScape: Cybersecurity Risk Management Services* (IDC #US49076222, May 2022)
- *IDC's Worldwide Cybersecurity Risk Management Services Taxonomy, 2021* (IDC #US48407121, December 2021)

Synopsis

This IDC study explores the services underpinnings required to enable a successful and fully implemented CRM program that can be managed either by the end customer or by the service provider that built it and recommends questions that buyers and vendors in this space can ask to get actionable direction in approaching the right decisions and outcomes. The discipline and design of CRM services can provide a framework for orienting organizations from optimizing standard check box outcomes to optimizing a value-added program to effectively manage cybersecurity risks and a very prescriptive way as a life-cycle approach that drives commitment and support from senior executives and board members throughout the different stakeholders in between.

"A well-defined CRM program is critical in today's ever-changing and growing threat landscape," says Phil Harris, research director, IDC's CRM Services. "Attackers are in their business for the long game where they can extract as much valuable data or intelligence over a long period of time undetected to reap as much money as possible. A key way to combat this is having an ongoing methodical approach for inspecting the depth and breadth of cybersecurity controls and maturity to cull out those new or not so apparent vulnerabilities and exposures that attackers exploit. This is an ongoing race, and organizations with strong CRM programs will be better prepared to withstand ongoing attacks."

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. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

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