IDC MarketScape

IDC MarketScape: Canadian Security Services 2022 Vendor Assessment

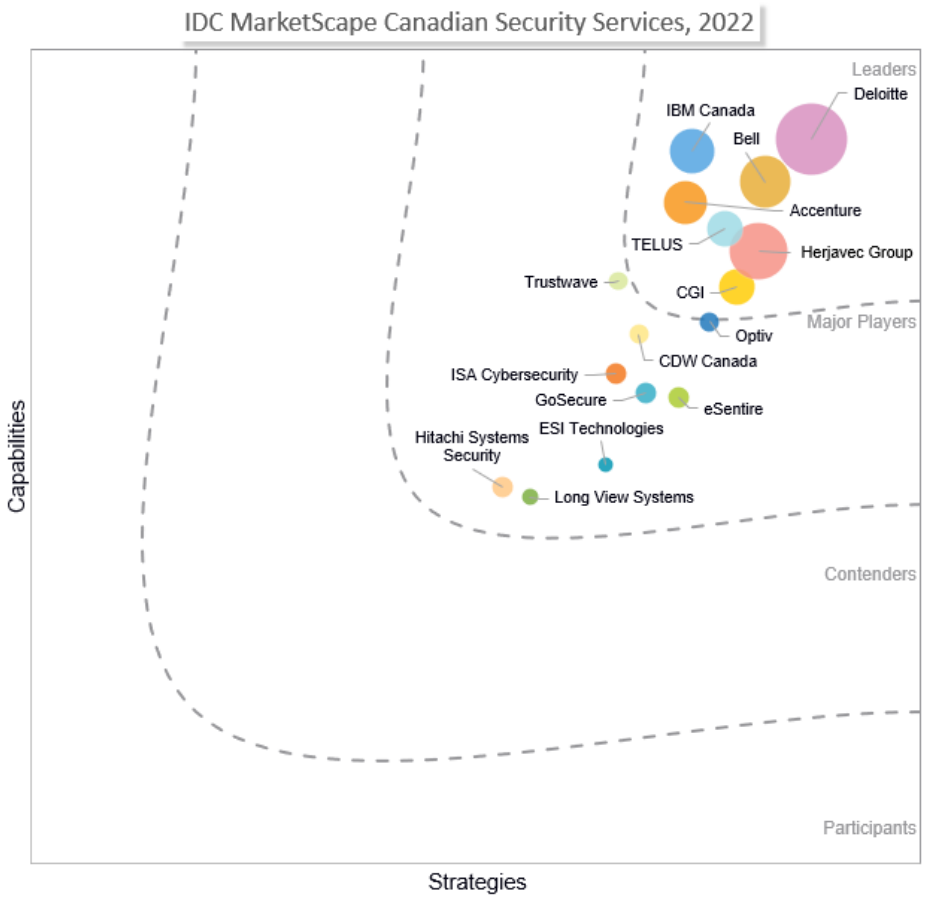
Yogesh Shivhare

THIS IDC MARKETSCAPE EXCERPT FEATURES DELOITTE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Canadian Security Services Vendor Assessment



Source: IDC, 2022

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

March 2022, IDC #CA48060922e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Canadian Security Services 2022 Vendor Assessment (Doc # CA48060922). 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 Canadian security services market continues to evolve rapidly. As technological disruption leads to rapid digitalization of the Canadian economy, organizations are having to reimagine the architecture of the enterprise, and global disruptive events such as the COVID-19 pandemic are accelerating this process. Canadian organizations are no longer looking just for security products and policy management or regulatory compliance management services from external security services providers. Though these are still very important security functions, organizations today are seeking support from their security services providers (SPs) to deliver 24 x 7 security monitoring, improve detections for new and advanced threats, improve response times, and help them with the recovery process. In addition, organizations need support to understand and manage security risk, develop a long-term security program, and elevate their security maturity to secure their digital transformation.

As organizations incorporate intelligence and telemetry data from multiple sources such as multicloud, edge, endpoints, network, and OT/IoT for threat detection, they often face challenges of alert overload and false positives. The prevalent shortage of cybersecurity experts in Canada and globally makes it difficult for organizations to make sense of so much data and has motivated security services providers to invest more in the areas of machine learning/artificial intelligence (ML/AI), security orchestration, automation, and analytics. It has enabled security services providers to offer scalable security services that can be aligned to the unique needs of Canadian organizations of all sizes and industry verticals.

IDC believes that the following areas will drive the Canadian security services market forward while providing vendors with the opportunity to differentiate their offerings:

- One-stop shop – the breadth and scope of professional security services as well as managed security services (MSS) including advanced services such as managed detection and response (MDR) that will continue to grow among providers
- The use of advanced and emerging technologies that will provide greater visibility against sophisticated threats and provide enhanced use of automated processes
- The ability to deliver higher level of orchestration, automation, and openness in the core platform
- Cloud monitoring, visibility, and management capabilities that seamlessly enable multiple cloud implementations
- Flexible deployment models that match the customer's preferences for adopting and consuming services
- Customer portal enhancements such as a mobile app and reporting templates to present to C-suite and board executives
- Hiring and retaining of top-notch security talent

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the 2022 Canadian security services IDC MarketScape, providers had to meet the following criteria:

- **Need to have a presence in Canada.** This criterion could be met by having a Canadian SOC, Canadian offices, or sales staff with a focus on selling security services in Canada.
- **Available services.** Providers need a range of managed and professional security services.
- **Security services revenue of over $10 million for 2020.** Any hardware or software resale revenue is not included.

IDC reviewed 16 security service providers with operations and customers in Canada using our IDC MarketScape model. This process included interviews of 13 providers and one or more customers from these providers, while 3 providers did not actively participate in this study and their evaluation is based on IDC's knowledge of their security services offerings. Most of the providers featured in this study were included in *IDC MarketScape: Canadian Security Services 2019 Vendor Assessment* (IDC #CA44419519, August 2019). As a result of this study, IDC Canada has found seven IDC MarketScape Leaders and nine IDC MarketScape Major Players in the Canadian security services market.

ADVICE FOR TECHNOLOGY BUYERS

Assessing the current capabilities and strategic alignment of a security service provider against your IT and business needs can be a lengthy process. It's important to fully understand the security requirement of your organization before selecting a provider. IDC recommends referencing common cybersecurity frameworks such as those provided by NIST, ISO 27001/27002, and CIS to ensure you have properly classified all assets on your network. Visibility into your network will aid in selecting the proper services from the right provider.

IDC has rated several essential criteria that firms should consider when comparing one provider with the others. Key areas to consider during your selection process are:

- **The breadth of the MSS portfolio.** There is a broad spectrum of providers offering standardized services to heavily customized managed security services. Therefore, it is important for an organization to map various types of offerings to its IT requirements. The buyer in this market could be looking for traditional security controls such as firewalls, intrusion detection system (IDS)/IPS, security information and event management (SIEM), vulnerability scanning, and secure messaging. All providers in this document provide these capabilities, but these offerings have also expanded to include advanced services such as identity and access management (IAM), threat intelligence, web application scanning, managed detection and response, managed SOC, and vulnerability management/risk monitoring. MSS providers have also started to offer complementary services such as incident response (IR), forensics, and other digital consulting capabilities.

- **Digital consulting capabilities.** A sound security program needs a comprehensive approach, which includes evaluating the people, processes, and technologies involved. Vendors listed in this document can assist technology buyers to understand the current security maturity, gaps, and future requirements. Breadth of professional services includes security strategy and planning, training, compliance and auditing, security policy assessment and development, penetration and vulnerability tests, network architecture assessment, breach or incident response, and forensics.
- **Use of security intelligence and machine learning.** Threat intelligence and machine learning models are being used to complement or replace traditional SIEM solutions. Buyers need to be aware whether the security services provider that they are considering has a road map to deliver these advanced capabilities.
- **Platform that provides visibility across endpoints, network, and cloud.** A security partner should be able to demonstrate innovation capabilities in its core platform as well as its use of emerging technologies. A true value to the organization is the ability to choose a vendor that can provide complete visibility of a detection and response management life cycle.
- **Integrations of orchestration and automation processes.** Service providers are focusing more on orchestration and automation tools and integrating these technologies into their core delivery platforms. Along with advanced ML and AI, technologies such as orchestration and automation are assisting service providers to enhance SOC efficiency and help analysts prioritize, analyze, and respond to threats faster.
- **Threat intelligence, threat hunting, and other advanced capabilities.** Service providers are going beyond the normal abilities and deepening into areas such as threat intelligence. Threat intelligence has become an important component of advanced services such as MDR and is being integrated into MSS and MDR offerings. Some service providers are also providing regular usage of human-led or automated threat hunting from the integrated threat intelligence feeds and creating processes and playbooks from its discoveries.
- **Cloud security strategy.** One of the areas that continues to be developed and enhanced is cloud security. The ability of a provider to deliver flexible cloud models across multiclouds and work in environments for cloud services providers such as Amazon Web Services (AWS), Microsoft, and Google is important based on the organization's needs. It is important to evaluate a service provider that will assist and provide recommendations for the organization moving to and utilizing these diverse IT environments.
- **Evaluate customer portals.** Customer portals provide a convenient, web-based view of all security-related activities. Portals have evolved to become more than a simple reporting tool and popular offerings include interactive visuals, user-defined dashboards, audit report generation, and health reporting capabilities.
- **Security expertise and support.** The tenure of the cybersecurity team and available skill sets is increasingly becoming a differentiator, and talent retention and training are critical to be a reliable security provider. Buyers must select a provider that will act as a trusted partner and as an extension to the IT team. Knowing that the provider understands the organization's IT environment and challenges will simplify the ability to continue to make recommendations and tweaks and provide ongoing guidance along their security journey.

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

According to IDC analysis and buyer feedback, Deloitte is positioned in the Leaders category in this 2022 IDC MarketScape for Canadian security services vendor assessment.

Deloitte offers a comprehensive breadth of managed security and professional services to advise, implement, and operate security solutions for its clients in Canada. Deloitte integrates cybersecurity with all its business services such as risk advisory, financial advisory, consulting, audit, and tax and legal services. Security services are offered in eight core areas, namely application security, cloud, data and privacy, detect and respond, emerging technologies (IoT, ICS, 5G, connected products, etc.), identity, infrastructure security, and security strategy. Deloitte's managed detect and respond is an integrated service that combines monitoring technology, advanced analytics, security expertise, and intelligence-based operations. The service is further differentiated with advanced capabilities such as threat hunting, attack surface management, and incident management services incorporated within the broader "detect and respond" service. Deloitte has made significant enhancements to its threat intelligence practice by bringing together malware research (CodexGigas is its proprietary malware analysis platform), geopolitical insights, regional threat insights, and knowledge of threat actor groups. Its threat intelligence solutions, available through the customer-facing portal DISP, includes a global threat library, which is a repository of curated intelligence insights on threat groups with their TTPs mapped to MITRE's ATT&CK framework. Deloitte's other investments in AI/ML and security orchestration and automation include IP such as Deloitte Fortress (continuously monitors multicloud environments for misconfigurations and auto remediates), CyberAI Hunter (integrates UEBA and SIEM to anticipate cyberbreaches before they occur), and CyFI APM (an AI-led tool that integrates asset network, vulnerability management, and threat intelligence data to offer ongoing assessment and unified visualization of cyber-risks and possible attack paths).

Deloitte operates 3 out of 30 global cybercenters in Canada along with 1 out of 5 cyber-regional delivery centers in Toronto. Its delivery network is extensive and can support clients across the country as well as those that have international operations. Deloitte has investments planned for new services and enhancements across its portfolio, with special focus on IoT and OT security, cloud, digital identity, and threat intelligence. There are several enhancements planned for its client-facing portals to grow third-party integrations and improve visualizations, reporting, and overall user experience.

Strengths

Deloitte's security team is the biggest in Canada, and with its experience in business risk consulting, wide span of security services, and large ecosystem of security technology and cloud vendors, it can provide customized, industry-specific security services to Canadian customers.

Challenges

Deloitte may not be suitable for organizations looking for low-cost, small-scale standard services. However, Deloitte has a renewed focus on midsize organizations and has made investments through Deloitte Private to offer end-to-end business services, including cybersecurity, to Canadian clients.

Some customers indicate that it could be a challenge to find the right services within Deloitte's wide service portfolio. Deloitte is addressing this challenge with deeper collaboration with its clients to drive offerings alignment.

Consider Deloitte When

Large to midsize organizations looking for security services that can be tailored to their specific industry or unique needs should consider Deloitte.

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

Security services involve a holistic view of all activities necessary to plan, design, build, enhance, and manage security product environments and operations programs. These can span business processes, application, and IT infrastructure. Security services can be either purchased standalone or embedded with other services. In a standalone (aka "discrete") security services purchase, the client has contracted with the services provider to purchase a purely security-centered engagement while, in an embedded or bundled security services purchase, the client has engaged with the client for a larger IT services project in which security is a just one component. An example of a standalone security services purchase would be a client that contracted with a services provider to deploy and integrate a new identity and access control technology within an existing IT environment. An example of an embedded security services contract would be a client that has engaged with a services provider to deploy a new cloud-based CRM system and must extend the current security infrastructure to cover the new systems. For a detailed explanation of security services, see *IDC's Worldwide Services Taxonomy, 2021* (IDC #US47191221, May 2021).

LEARN MORE

Related Research

- *Canadian Cybersecurity Market Outlook, 4Q21: 2020-2025 Security Forecast* (IDC #CA47049621, November 2021)
- *Canadian Cybersecurity Market Snapshot, 4Q21* (IDC #CA47049421, November 2021)
- *IDC's Worldwide Security Services Taxonomy, 2021* (IDC #US47681721, May 2021)
- *Brand Perceptions of Managed Security Service Providers in Canada, 2021* (IDC #CA46282421, March 2021)

Synopsis

This IDC study presents a vendor assessment of security services in Canada through the IDC MarketScape model. Using the IDC MarketScape model, 16 security service providers with operations and customers in Canada were evaluated. This process included interviewing 13 providers and one or more customers from each provider, while for others that did not actively participate in this study, the evaluation was based on IDC's knowledge of their security services offerings and capabilities. Providers were measured in terms of current capabilities and future strategies for delivering services to customers in the Canadian market.

Yogesh Shivhare, research manager, Cybersecurity, at IDC Canada, says, "The Canadian security services market is very diverse and includes pure-play managed security SPs, telecommunication providers, security technology vendors, MDR providers, and boutique security consulting firms that compete aggressively in this market. Each of these vendors has unique capabilities that can meet the specific and unique needs of all Canadian organizations. Security talent and expertise, technology leadership, and availability of advanced security services such as MDR are among the prominent differentiating factors in the Canadian security services market."

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.

IDC Canada

33 Yonge St., Suite 902
Toronto, Ontario Canada, M5E 1G4
Twitter: @IDC
blogs.idc.com
www.idc.com