IDC MarketScape

IDC MarketScape: Canadian Security Services 2018 Vendor Assessment

Kevin Lonergan   David Senf

## IN THIS EXCERPT

The content for this excerpt was taken directly from the IDC MarketScape: Canadian Security Services 2018 Vendor Assessment by Kevin Lonergan and David Senf (Doc # CA43005218). All or parts of the following sections are included in this excerpt: IDC Opinion, IDC MarketScape Vendor Inclusion Criteria, Essential Buyer Guidance, Vendor Summary Profile, and Appendix. Also included is the IDC MarketScape Figure (Figure 1).

FIGURE 1

IDC MarketScape Canadian Security Services Vendor Assessment

IDC MarketScape: Canadian Security Services, 2018
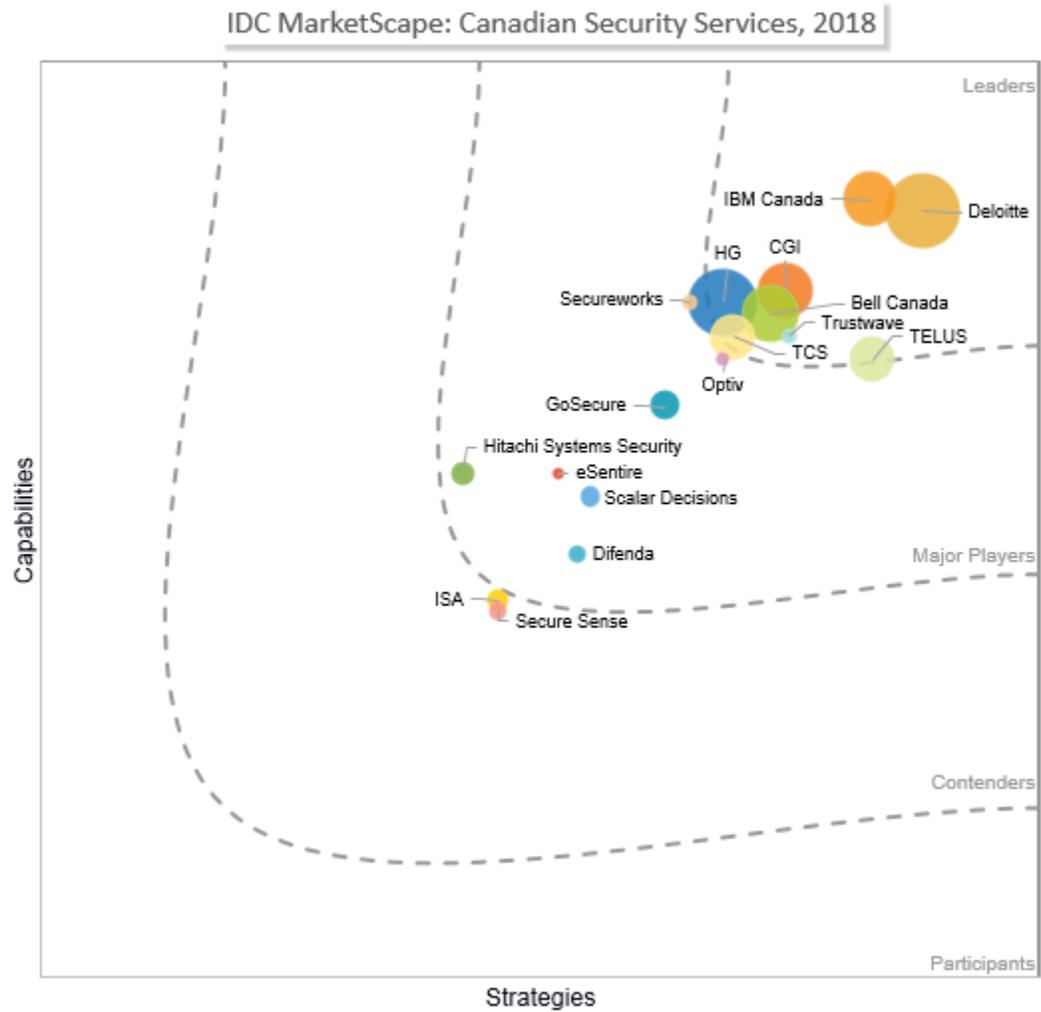
Source: IDC, 2018

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

IDC OPINION

IDC compared 17 security service providers with operations and customers in Canada using our IDC MarketScape model. This process included interviews of the 17 providers and one or more customers from each provider (if made available). The majority of the providers were included in *IDC MarketScape: Canadian Security Services 2017 Vendor Assessment* (IDC #CA41971017, February 2017). For this year's study, five additional providers were included, and the range of participants include pure-play security providers, IT consulting firms, systems integrators, and large multinational security vendors/providers. As a result of this study, IDC Canada has found eight IDC MarketScape Leaders, seven IDC MarketScape Major Players, and two IDC MarketScape Contenders in the Canadian security services market. The vendors positioned as Leaders provide a complete range of services that can meet the needs of the widest range of organizations with the largest scope of capabilities. However, not all providers' solutions are necessarily the best fit for all organizations because pricing, support levels, and other variables are valued differently depending on need. For example, budget is the top roadblock to improving security for Canadian organizations and finding a security provider that can offer appropriately priced solution can be as or even more important than breadth of service for some. Providers in the Contender and Major Player categories can be the optimal fit for some organizations. The following are the main differentiators between security service providers operating in Canada:

- Canadian footprint including channel partners, security operation centres (SOCs), number of offices, sales staff, security engineers, developers, analysts, and research teams and their geographic coverage across Canada
- Device management capabilities across the security stack (unified threat management [UTM], intrusion prevention security [IPS], VPN, and content management) for a wide variety of appliance and software vendors
- Breadth of professional services including security strategy and planning, compliance and auditing, security policy assessment and development, penetration and vulnerability tests, network architecture assessment, breach or incident response, and forensics
- Support of and the ability to enhance SIEM platforms
- Cloud security capabilities including security from the cloud and security of the cloud
- Support for endpoint detection and response or next-generation endpoint security solutions
- Capability to aid in or conduct IT security research through either a post-secondary institution partnership, internal lab, or partnership with a security organization
- Use of machine learning and advanced analytics to enhance security service quality and delivery
- Tiered levels of service offerings
- Customer portal and reporting capabilities
- Bundling/one-stop shop capabilities outside of security services
- Ability to align to customers' security requirements at both technical and business value levels

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the 2018 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 $2 million for 2017.** Any hardware or software resale revenue is not included.

ADVICE FOR TECHNOLOGY BUYERS

Assessing the many current capabilities and strategic alignment of a security service provider to your IT and business needs can be a lengthy process. Selecting a trusted advisor requires due diligence around a number of factors. IDC has rated a number of essential criteria that firms should consider when comparing one provider with the others. Key areas to consider during your selection process are:

- **Plan ahead.** 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.
- **Match requirements to provider capabilities.** The participants in this study have been assessed on their abilities to offer all services to all business sizes and verticals and may not represent the needs of every organization. Pure-play providers, telecommunication providers, vendors, and consulting firms all have unique capabilities and it's important to assess the benefits and challenges of consuming services from each.
- **Use threat 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 advanced threat intelligence (such as user behavior analytics).
- **Check for cloud security services.** Cloud identity and access management (IAM) and cloud monitoring capabilities are going to be increasingly important for organizations as cloud adoption continues. This is especially true of hybrid cloud deployments, where single sign-on (SSO) and user provisioning become challenging. Ingress/egress filtering of traffic in whichever deployment your data is moving from and to is critical as well. Traditional firewall, IDP, DLP, and other filters from the legacy world still apply in cloud (particularly in IaaS and PaaS).
- **Determine data residency requirements.** Although Canadian data residency legislation (and United States-compelled disclosure rules such as the Patriot Act) only affects a small number of organizations and a small amount of data, many are still wary of data crossing the border. Outside of customer perception issues, there are likely little reasons for concern over data residency, but some buyers will want to be aware of where a provider may store or send their data.
- **Bundle services.** With a wide variety of telecommunication providers, systems integrators, and product vendors offering security services in the market, there are opportunities for savings or at least ease of relationship management through the bundling of multiple services. Buyers

should approach multiple providers to see whether they can find a suitable security solution that they may be able to bundle with other products and services.

- **Evaluate customer portals.** Customer portals provide a convenient, web-based view of all things security related on the network – and "things" connected to the network. Portals have evolved to become more than a simple reporting tool, and leading offerings include interactive visuals, user-defined dashboards, audit report generation, and health reporting capabilities.

VENDOR SUMMARY PROFILES

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

Bell Canada

According to IDC analysis and buyer perception, Bell Canada is an IDC MarketScape Leader in the security services market in Canada.

Bell Canada operates three commercial SOCs and multiple facilities housing over 300 security staff. Bell Canada offers security services through Bell Business Markets (BBM) to midmarket and large enterprise organizations across multiple verticals. Bell has an extensive customer base across Canada, particularly in the Atlantic region, Québec, Ontario, and Manitoba.

As Canada's largest telecommunications provider handling the largest amount of Canada's internet traffic, Bell has a competitive advantage of collecting threat intelligence from its own network. Using software-defined networking (SDN) and network function virtualization (NFV), Canadian communication service providers have been working toward offering NaaS security capabilities via their networks to customers. Currently, Bell offers DDoS as a service, blocking incoming attacks before they reach customer environments where otherwise they can overwhelm customer premise security appliances. Bell is working toward virtualizing more of the IT security stack, with pilot programs in place to offer full NGFW capabilities. Bell expects to release these services to customers in 2018.

Bell offers a complete portfolio of traditional on-premise managed and monitoring services. The company also offers cloud-hosted SIEM, email, and messaging security solutions. Moreover, Bell has an extensive professional security services practice offering a full portfolio of services from a team of over 100 consultants. Professional services include security risk, strategy and compliance, infrastructure and network protection, identity, credential and access management, and advanced threat detection.

Leveraging third-party threat intelligence feeds and its own network visibility, Bell Business Internet and Network DDoS customers receive its cyberthreat intelligence (CTI) service as part of their subscription. The CTI combines top-tier analysts with a correlation engine based on machine learning, to provide richer insights into threats.

To grow security talent in Canada, and its own recruitment pipeline, Bell recently announced a partnership with the Canadian Institute for Cybersecurity at the University of New Brunswick and is actively seeking out similar partnerships with other academic organizations.

Strengths

As a telecommunications provider, Bell can become a one-stop shop for connectivity, communication, hosting, and IT security. For customers, this can simplify vendor relationships, billing, and management and may lead to improved bundled pricing. The CTI has the ability to enhance traditional SIEM solutions via machine learning models built on Canada-specific data at carrier scale.

Challenges

Bell offers IaaS and PaaS security solutions for its own datacentres, but it does not offer management or monitoring for third-party platforms such as AWS or Azure yet.

APPENDIX

The security services market continues to see strong growth in Canada. Of the security services markets, managed services continues to be the strongest performing as Canadian organizations struggle to find qualified security personnel and budget to implement a proper in-house security solution and 24 x 7 protection.

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

Security services involve a holistic view of all activities necessary to plan, design, build, and manage information security across the enterprise IT infrastructure. These services can either be purchased discretely or bundled with other services. In a discrete security services purchase, the client has contracted the services provider to purchase a mainly security-focused engagement, while in a bundled security services purchase, the client has engaged the services provider for a larger IT services project in which security is a small component. IT security services are provided by systems integrators, software/hardware vendors, technology resellers, and specialist and management consulting firms. They focus on the implementation, management, operation, and auditing of IT systems to ensure the security of physical assets and/or sensitive information. For a detailed explanation of security services, see *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016).

Strategies and Capabilities Criteria

This section includes an introduction of market-specific weighting definitions and weighting values (see Tables 1 and 2).

TABLE 1

Key Strategy Measures for Success: Canadian Security Services

Strategies Criteria	Subcriteria Definitions	Subcriteria Weights
Functionality or offering strategy		
Planned managed security service offering (introduce next year)	Adding services across managed security services such as SIEM, device management, and endpoint monitoring to fill any existing gaps	15.0
Planned professional security service offering (introduce next year)	Adding services across professional services such as forensics, incidence, response, and compliance to fill in gaps	15.0
Delivery		
Cloud-based delivery	Adding additional services to fill gaps or add new capabilities to offer services from the cloud or for the cloud (Additional weight is given to organizations making considerable investments in these areas.)	10.0
Financial/funding		
Profit and growth	Provider's expected revenue growth across MSS and professional services in 2018 (More weight is given to organizations with strong revenue growth for the year.)	10.0
R&D pace/productivity		
Overall R&D strategy	Provider's investments in creating intellectual property over the next year (If a provider does not perform in-house research, then partnerships with leading vendors will be considered instead.)	10.0
Growth		
Geographic growth	Depending on the current footprint of the provider, there is plans to fill gaps with respect to offices, facilities, and/or SOCs located across Canada	10.0
Customer growth	Provider is making services more scalable by increasing bench size, offering tiered offerings, and/or improving customer portal for better depth/usability.	10.0
Business strategy		
Employee management	Provider plans to work closer with academic institutions for recruitment and/or sponsor conferences and/or participate in community education	10.0
Go-to-market strategy		
Marketing and sales	Provider plans to increase sales and/or marketing bench size and/or onboard channel partners	10.0
Total		100.00

Source: IDC, 2018

TABLE 2

Key Capability Measures for Success: Canadian Security Services

Capabilities Criteria	Subcriteria Definitions	Subcriteria Weights
Functionality or offering capabilities		
Essential capabilities	Ability of the provider to service the Canadian market (More weight is given for Canadian SOCs, offices, and facilities that span across Canada.)	10.0
Degree of cloud	Ability to offer security services from the cloud as well as offer services for the cloud (More weight is given to organizations that offer a full range of cloud-based services and can manage popular public cloud environments.)	10.0
Segmentation alignment	Services scale from providers that can offer services to all organization sizes score higher (More weight is given to providers with tiered service models and large customer base.)	10.0
Predictive analytics	Ability to offer analytics to aid in malware detection and response (More weight is given for custom SIEM add-ons, machine learning models, and threat intelligence feeds.)	10.0
Customer portal	Portals that have evolved to become more than a simple reporting tool (More weight is given for portals with interactive visuals, user-defined dashboards, and audit report generation capabilities.)	10.0
Range of services		
Managed services offerings	Ability to offer managed security services (More weight is given for a complete range of device management and monitoring services across the network and endpoint including identity management.)	10.0
Adjacent services (implementation services, consulting services, etc.)	Ability to offer professional services (More weight is given for a complete range of device management and monitoring services across the network and endpoint including identity management.)	10.0
Portfolio benefits		
Related offering portfolio	Ability to offer one-stop shop capabilities for products, services, and/or connectivity (More weight is given for providers that can consolidate services and solutions for customers.)	5.0

TABLE 2

Key Capability Measures for Success: Canadian Security Services

Capabilities Criteria	Subcriteria Definitions	Subcriteria Weights
Go-to-market strategy		
Marketing	Utilize extensive marketing campaigns (More weight is given to providers that are active in digital advertising, have excellent websites, and run regional and national campaigns/community building.)	5.0
Sales and distribution	Ability to sell across Canada (More weight is given to providers with a large, national sales force or utilize the channel.)	5.0
Business capabilities		
Community education	Involvement with the Canadian security community (More weight is given for providers that are active in security groups and conferences, and publish free content.)	5.0
Employee management	The ability to recruit new talent and minimize employee turnover (More weight to organizations that have recruitment and/or co-op placements with academic institutions and offer employee benefits to retain employees.)	5.0
Customer service delivery		
Customer service	Offer 24 x 7 SOC support in Canada, 24-hour call centre	5.0
Total		100.0

Source: IDC, 2018

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 420
Toronto, Ontario Canada, M5E 1G4
Twitter: @IDC
idc-community.com
www.idc.com