IDC MarketScape

IDC MarketScape: Canadian Security Services 2017 Vendor Assessment

Kevin Lonergan   David Senf

IN THIS EXCERPT

The content for this excerpt was taken directly from the IDC MarketScape: Canadian Security Services 2017 Vendor Assessment by Kevin Lonergan and David Senf (Doc #CA41971017). 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, Appendix, Learn More, and Related Research. Also included is the IDC MarketScape Figure (Figure 1).

FIGURE 1

IDC MarketScape Canadian Security Services Vendor Assessment
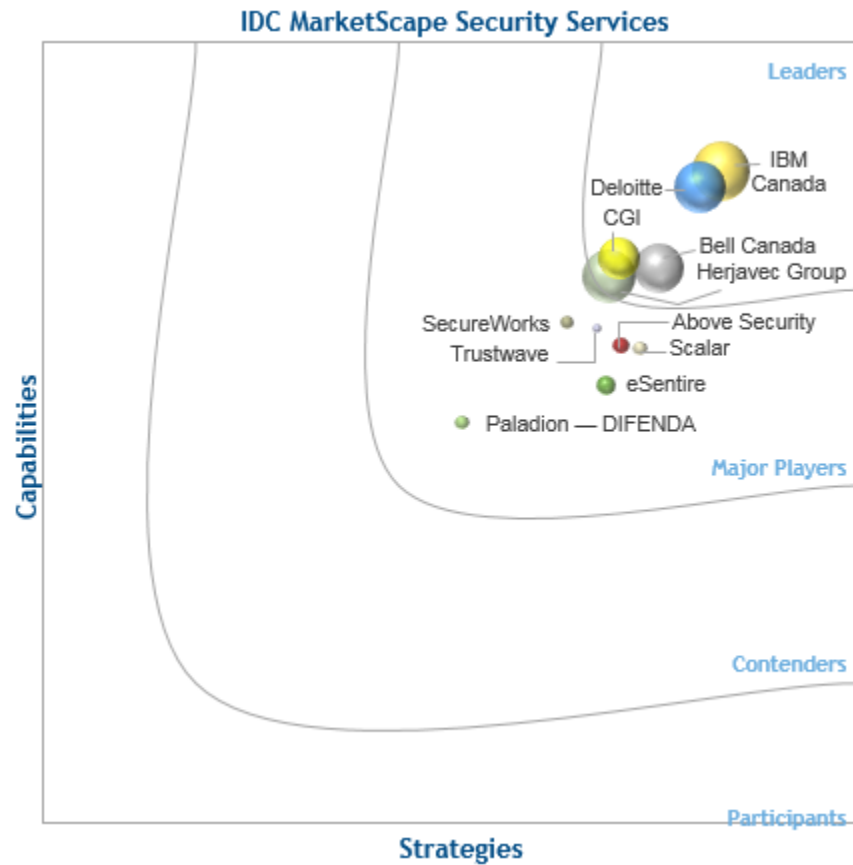
Source: IDC, 2017

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

IDC OPINION

IDC compared 11 security service providers with operations and customers in Canada using our IDC MarketScape model. This process included interviews of the 11 providers and one or more customers from each (if made available). The majority of these vendors were included in *IDC MarketScape: Canadian Managed Security Services 2015 Vendor Assessment* (IDC #CA1SD15, July 2015). This IDC MarketScape has been expanded to include a deeper dive into each participant's professional security services as well as their managed offerings. The Canadian security services market is evolving quickly, and the competitive landscape is quite different from what it was only a few years ago. Included in this study is a range of Canadian 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 five IDC MarketScape Leaders and six IDC MarketScape Major Players in the Canadian security services market. The Leaders provide a complete range of services that can meet the needs of the smallest business and the largest enterprise. However, not all providers' solutions are necessarily the best fit for all organizations as 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. The following are the main differentiators between security service providers operating in Canada:

- Canadian footprint including channel partners, security operation centres (SOCs), offices, sales staff, security engineers, and research teams and their geographic coverage across Canada
- Device management capabilities across the security stack (unified threat management [UTM], intrusion prevention security [IPS], content management, and VPN) 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 traditional SIEM platforms
- Cloud security capabilities including security from the cloud and security in the cloud
- Support for 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
- Tiered levels of service offerings
- Customer portal and reporting capabilities
- Cross-sell capabilities
- Ability to align to customers' security requirements at both a technical and business value level

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

To be included in the 2017 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 2016.** Any hardware or software resale revenue is not included.

ESSENTIAL BUYER GUIDANCE

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.** The four pillars of cloud, mobile (including IoT), big data, and social are fundamentally changing the role of security service providers and the services their customers will require in the near future. Where providers are in terms of adopting the following should be a key concern for buyers:
  - ▪ **Threat intelligence.** Advanced threat intelligence is being used to complement or replace traditional SIEM solutions. Buyers need to be aware if the security services provider that they are considering has a road map to deliver advanced threat intelligence (which may include big data solutions such as Hadoop and user behavior analytics).
  - ▪ **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).
  - ▪ **Next-generation endpoint security.** Securing endpoints continues to be a challenge for Canadian organizations as their attack surface continues to grow and the threat landscape diversifies. Buyers need to look for a provider that is partnered with or offers a next-generation endpoint security solution based on algorithmic approaches rather than traditional signature-based detection techniques to protect against new types of malware such as ransomware.
- ▪ **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 reason for concern over data residency, but buyers need to be aware of where a provider may store or send their data.
- ▪ **Bundle services.** With a wide variety of telcos, 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 if 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. Although the majority of vendors in this study had a customer portal, their maturity varied. Mature portals have real-time data analysis, customizable visualizations, reporting, and advanced analytics capabilities. As most security service providers are willing to provide a demo of their portal, buyers should take the time to evaluate them.

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. International players, Canadian telcos, and pure-play providers all have unique qualities that are outlined in these profiles providing context to the IDC MarketScape graph depicted previously (refer back to Figure 1). The profiles in the sections that follow focus on key differentiators for device management, monitoring, threat intelligence, and professional security services.

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 is Canada's largest telecom provider and has 20 facilities housing security personnel nationwide. This includes several security operation centres in Eastern Canada as well as additional disaster recovery SOCs. Bell services clients across many verticals, with the majority of security services clients in financial services, business services, and the public sector including the federal government.

Bell is focused on providing complete end-to-end solutions that can be delivered inline from within Bell's network cloud, Bell's hosted datacentres, or on the customer's premise. Each of these delivery models leverages Bell's national professional services and managed services capabilities. Bell is able to bundle telecom network services with managed security services and specialize in inline network and DDoS protection. Bell has solutions that target both the enterprise and midmarket segments. Bell's core MSS offerings include a comprehensive suite of network protection (firewall, IDP, VPN, etc.), DDoS, email and web protection, SIEM, and identity and access management solutions.

Bell sees the future of its managed security services offerings centring on its Network 3.0 network transformation in combination with its national threat intelligence capability. These capabilities are enabling Bell to deliver threat intelligence and security-as-a-service solutions for its business internet customers directly from within Bell's core network instead of the traditional customer premise approach. Bell's Network DDoS service is already available, with threat intelligence and other network security services launching in 2017. To deliver network security solutions off of the Bell network and to broaden the set of network cloud security services available to its business customers, Bell has entered into strategic partnerships with a number of cloud security providers. Bell supports multiple SIEM solutions and is developing a proprietary threat intelligence platform based on big data analytics. In addition, Bell offers a full range of professional security services and is currently developing a new web portal for its customers.

Bell has a national recruitment program in place, working with a range of institutions on curriculum guidance and new grad placement opportunities. In Ottawa, for example, Bell has presence with the University of Ottawa where Bell recruits for a number of programs, including security. Bell works with Willis College on its cybersecurity curriculum and program planning. Bell also sits on the Program Committee for Algonquin College as a security representative.

Strengths

Bell's unique differentiation, like that of other telecom providers, is the ability to leverage threat intelligence derived from its national network. Bell uses that intelligence to help business customers better understand their security risk and protect their networks from attack inline and in real time. Bell is an early adopter of network virtualizations and clean pipe solutions in Canada and will be among the first Canadian telecom providers to offer full UTM/NGFW security directly through the network. When customer premise solutions are desired, Bell can offer its national professional services and managed security infrastructure services as well. Bell's ability to serve large and small customers will be a key asset in the highly competitive security services market. Bell has the ability to consolidate many services for businesses, including security, network, and hosting, which is a benefit for customers looking for a one-stop-shop approach.

Challenges

Bell provides cloud security services to clients using its own hosting and cloud services but doesn't offer monitoring or identity management solutions for AWS or Azure environments as of yet. Bell needs to continue to build on its work connecting with Canadian academic institutions to ensure it has access to and nurturing of a strong Canadian security labour supply.
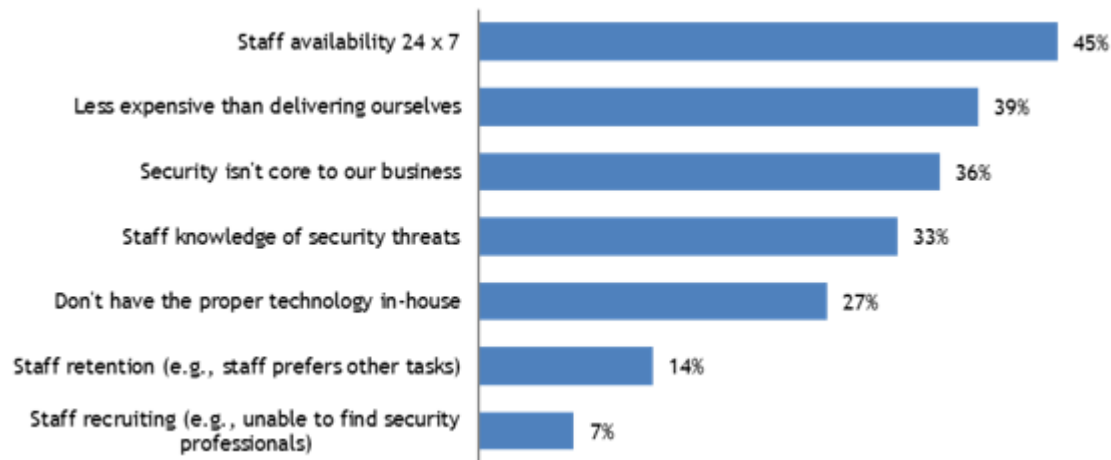
APPENDIX

Situation Overview

The security services market continues to see strong growth in Canada with revenue of $932.5 million in 2016 and is forecast to grow with a five-year CAGR of 8.3% to $1.28 billion in 2020. 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. Figure 2 presents the main reasons why Canadian organizations have migrated to managed security services in 2016.

FIGURE 2

Reasons for Migrating to Managed Security Services

Q.   Why is/would your organization select managed security services?

Staff availability 24 x 7 — 45%
Less expensive than delivering ourselves — 39%
Security isn't core to our business — 36%
Staff knowledge of security threats — 33%
Don't have the proper technology in-house — 27%
Staff retention (e.g., staff prefers other tasks) — 14%
Staff recruiting (e.g., unable to find security professionals) — 7%

n = 214

Source: IDC Canada's *ITAP n3,* 2016

IDC survey data shows that of the various managed security services, Canadian organizations are most comfortable with outsourcing messaging and web security and least comfortable with outsourcing critical infrastructure security such as servers and network.

Growth in security consulting services is expected to be slightly lower than managed services over the forecast period but will be stronger than implementation of training services. Currently the consulting services with the highest adoption in Canada include network penetration testing and incident response, and the least are forensics and device vulnerability management. The strongest-growing consulting service in terms of adoption in 2017 will be network penetration testing.

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 a review board 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
Offering strategy		
Functionality or offering road map	More weight is given for investing in new or more comprehensive security services. Particular weight is given to additional facilities and staff located in Canada.	5.0
Delivery model	More weight is given to participants that are moving toward providing security services from the cloud and security services for the cloud in addition to on-premise.	1.5
Cost management strategy	Superior service calls for ways in which the vendor employs benchmarks to ensure competitive cost and pricing and help clients justify expenditures for security services.	2.0
Portfolio strategy	Providers developing large services and/or product portfolios rate well. A large portfolio provides saving opportunities to customers that bundle multiple services and products.	1.5
Subtotal		10.0
Go-to-market strategy		
Pricing model	Firms have superior planning for future pricing alignment with different verticals and business sizes. This includes specialized offering or services for specific use cases.	2.5
Sales/distribution strategy	Excellence is demonstrated by plans to offer multiple routes of purchase. Particular weight is given for developing a large sales force and specialized onboarding teams.	2.0
Marketing strategy	Successful firms have a well-articulated plan for how they will market their capabilities in the future. More weight is given for plans to utilize more localized marketing and for plans to acquire, upsell, and retain customers.	2.0
Customer service strategy	Successful firms continuously focus on ways to improve retention of customers as it relates to its service and support over the next 12 months. More weight is given for having plans to offer robust portal capabilities and flexible customer service delivery.	3.5
Subtotal		10.0

TABLE 1

Key Strategy Measures for Success: Canadian Security Services

Strategies Criteria	Subcriteria Definitions	Subcriteria Weights
Business strategy		
Growth strategy	Firms poised for growth in the near term provide relevant specialized offerings, which address specific needs, particularly for industries, geographic markets, or the size of the client.	3.0
Innovation/R&D	Excellence is demonstrated by developing proprietary threat intelligence platforms, portals, cloud security offerings, and software and hardware products.	4.0
Employee strategy	Firms have clearly articulated plans for attracting and cultivating talent. More weight is given for partnerships with Canadian educational institutions to increase security talent in the marketplace and engaging in research.	3.0
Subtotal		10.0

Source: IDC, 2017

TABLE 2

Key Capability Measures for Success: Canadian Security Services

Capabilities Criteria	Subcriteria Definitions	Subcriteria Weights
Offering capabilities		
Functionality/offering delivered	Ideal offerings include a complete range of managed and professional security services. More weight is given for Canadian SOCs and facilities, threat intelligence capabilities, supported SIEM solutions, big data analytics, and team sizes.	5.0
Delivery model appropriateness and execution	This is how well a security services provider's current delivery model meets end-user preference for adoption and consumption. More weight is given to participants that provide security services from the cloud and security services for the cloud.	1.5
Cost competitiveness	Pricing must be competitive with market pricing and modular and scalable to meet customer requirements.	2.0
Portfolio benefits delivered	Providers offering large services and/or product portfolios rate well. A large portfolio benefits customers as they can bundle multiple services, licenses, and products together for cost savings.	1.5
Subtotal		10.0
Go-to-market capabilities		
Pricing model options and alignment	The split of Canadian organizations is heavily weighted toward SMB, and it's important for providers to offer services to all size segments and verticals. Particular weight is given for providers that have had success with offerings for multiple verticals and business sizes.	2.0
Sales/distribution structure and capabilities	Excellence is demonstrated by providers offering multiple routes of purchase. Particular weight is given for a large Canadian-based salesforce and specialized onboarding teams.	2.0
Marketing	A provider's ability to market its services is assessed. More weight is given for websites/collateral that provide a detailed and concise overview of services and amount/quality of brochures and white papers/studies.	2.0
Customer service	Customer service excellence is marked by how well a provider can offer customer service and support. More weight is given to robust portal capabilities and flexible customer service delivery.	4.0
Subtotal		10.0

TABLE 2

Key Capability Measures for Success: Canadian Security Services

Capabilities Criteria	Subcriteria Definitions	Subcriteria Weights
Business capabilities		
Growth strategy execution	Market momentum and growth is shown through acquisitions as well as organic growth. Particular weight is given to evidence of multifaceted business growth through organic development, acquisition, and/or partnering.	3.0
Innovation/R&D pace and productivity	Excellence is demonstrated by developing a significant amount of in-house intellectual property. This can include threat intelligence platforms, portals, cloud security offerings, and software and hardware products.	3.0
Employee management	The provider demonstrates a method of attracting and cultivating talent. More weight is given for partnerships with Canadian educational institutions to increase security talent in the marketplace. More weight is also given to organizations that actively engage in research with academic institutions.	4.0
Subtotal		10.0

Source: IDC Canada, 2017

LEARN MORE

Related Research

- *Canadian IT Security Hardware, Software, Services, and Cloud Forecast, 2016-2020* (IDC #CA40660116, September 2016)
- *IDC's Worldwide Security Products Taxonomy, 2016* (IDC #US41149416, April 2016)
- *Brand Perceptions of Security Consulting Service Providers in Canada, 2016* (IDC #CA40660316, April 2016)
- *Canadian Security Products Market Shares, 2014: UTM/NGFW Vendors Make Big Gains* (IDC #CA3SD15, December 2015)
- *IDC MarketScape: Canadian Managed Security Services 2015 Vendor Assessment* (IDC #CA1SD15, July 2015)
- *Brand Perceptions of Security Appliance Vendors in Canada, 2015* (IDC #CA4SD15, April 2015)

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