IDC MarketScape

IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment

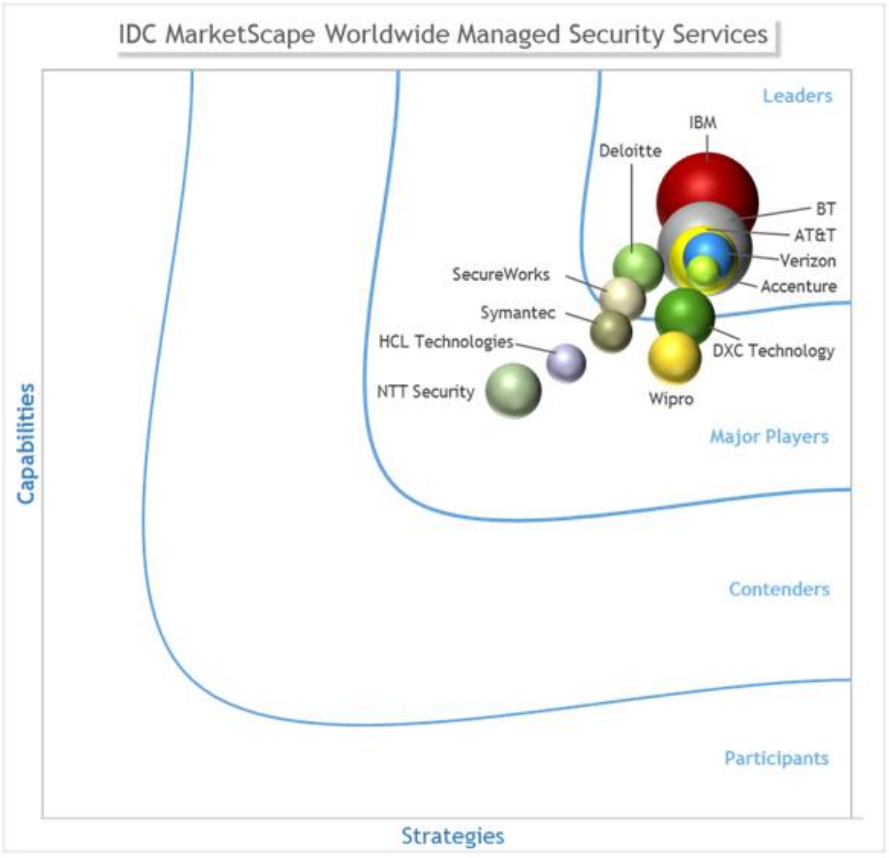
Martha Vazquez

THIS MARKETSCAPE EXCERPT WAS CREATED FOR BT

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Security Services Vendor Assessment



Source: IDC, 2017

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

August 2017, IDC #US41320917e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment (Doc # US41320917). 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 managed security services (MSS) market continues to evolve rapidly. Within just the past few years, even the past 18 months, managed security services providers (MSSPs) have added more capabilities and advanced security services to assist organizations in defending against and responding to today's attacks. Using the IDC MarketScape model, IDC has compared 12 organizations that offer MSS worldwide. Through in-depth MSSP interviews and more than 20 interviews with providers' customers, IDC learned that all the providers included in this study have the necessary capabilities to deliver traditional worldwide MSS. However, most are now able to go beyond the traditional services areas, incorporating advanced services such as distributed denial of service (DDoS), web application security, identity access management (IAM), managed security and information event management (SIEM), and managed security operation center (SOC) (see Appendix for further details) into their propositions. By its very nature, inclusion in this rating study indicates that participants are top-rated global providers and should be considered for managed security services. Furthermore, as a result of this IDC MarketScape evaluation, IDC identified the following eight companies as Leaders: IBM, BT, Verizon, AT&T, Accenture, Deloitte, DXC Technology, and SecureWorks. The group of Major Players consists of Symantec, Wipro, HCL, and NTT Security. Given the rapid pace of development within the MSS market, it is important that all providers continue to develop upon MSS capabilities and go beyond the traditional offerings. This is essential to keep pace with the development of the market, let alone remaining ahead of the chasing pack. Through more granular evaluation, IDC found that each provider possesses some unique strengths and weaknesses when compared with its peer group. At a high level, the major differences centered on their strategies for the next 12 months. Many of the providers now offer a breadth of complementary security transformation services to assist customers with digital transformation. Other factors that were looked at include pricing, marketing, security operation centers staffing, and customer portal capabilities. IDC believes that the following areas will drive the MSS market forward while providing vendors with the opportunity to hone a differentiated proposition:

- Complementary services that provide customizable opportunities for assistance in security transformation and maturity; these can include enabling security within a customer's journey to the cloud
- Cloud monitoring, visibility, and management capabilities that seamlessly enable hybrid implementations
- Flexible consumption models that match customers' preferences for integrating MSSP expertise, processes, and technology
- Pricing models that support the end customer's buying preference
- Mobility and IoT solutions
- Advanced detection methods and analytics techniques, including advanced detection and response capabilities, threat intelligence, and big data

- Robust customer support, including incident response (IR) and forensics, to assist with recovery from breaches
- Customer portal and reporting capabilities
- Security orchestration and automation technologies to provide more efficient incident response workflow
- Security operations centers
- Advanced methods of acquiring and retaining security talent

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 12 MSSPs within the 2016 IDC MarketScape worldwide managed security services market assessment. While the market arena for MSS is broad and there are many suppliers that offer these services, IDC narrowed the field of participants for this study based on the following criteria:

- **Service capability across the MSS life cycle.** Each service provider was required to possess full-service MSS delivery capabilities (see the Appendix section for an explanation of MSS).
- **Revenue.** Each service provider was required to have 2015 total MSS global revenue in excess of $180 million and a SOC presence in each of three regions — the Americas, EMEA, and APAC — in addition to having a minimum of five SOCs.
- **Geographic presence.** Each vendor was required to have MSS delivery capability in each of three regions: the Americas, EMEA, and APAC.

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 the vendor's strengths and challenges.

IDC reviewed 12 MSSPs against current capabilities and future strategy criteria as part of its IDC MarketScape on the worldwide MSS market. IDC also conducted customer interviews of more than 20 vendor customers to obtain feedback on how the vendors performed in delivering MSS. Vendors participating in the analysis are Accenture, AT&T, BT, DXC Technology, Deloitte, HCL Technologies, IBM, NTT Security, SecureWorks, Symantec, Wipro, and Verizon.

BT

BT is positioned as a Leader in the IDC MarketScape for worldwide managed security services.

BT Group is a United Kingdom-headquartered multinational communications services company with global operations. Managed security services are contained in the BT security portfolio.

BT has more than 2,500 security practitioners in 180 countries, offering a global reach to a large customer base. Of the company's 15 global SOCs, seven are dedicated SOCs and eight are colocated with other network services, offering around-the-clock coverage with a follow-the-sun model. In addition, BT builds and manages customer-specific SOCs. Support work is handed off between shifts around the globe, and all teams work from a single incident queue, offering continuous monitoring and remediation. A virtual CISO is available to clients as a complementary offering.

BT's differentiation comes from the ability to seamlessly integrate a broad security portfolio of managed services with a customer's BT-provided WAN and LAN compute solutions. This allows BT to be a one-stop shop for its customers. An extensive network gives BT the insight into attacks so that BT can watch, learn, predict, and respond to the latest threats.

BT's investments are focused on assisting customers in their digital journeys as they operate in new environments created by cloud, virtualized services, and IoT. BT offers advanced services that help customers transition with confidence and exploit these new technologies. To respond to the digital ecosystem that customers are facing, BT invested in what it calls "Cloud of Clouds." This initiative combines choice and control of services from key cloud service providers privately pre-connected to BT's network, enabling BT to have a global ecosystem by bringing together multinational corporations.

Strengths

BT's strengths include its focus on big data analytics, threat intelligence, and complementary services. In addition, BT has made strides in addressing enterprise challenges of migrating to the cloud and as a result provides enterprises guidance to migrate to the cloud securely using BT's cloud partnerships and other vendor technologies. BT combines its own innovation with partner technology that may include market leaders or innovating technology from emerging start-ups.

BT makes a practice of developing flexible pricing and payment options and for methods of acquiring and retaining talent. BT uses a variety of tools to identify talent and invests time and resources in developing cybersecurity talent – an example is the BT Security Academy.

Challenges

Although BT is well known in the EMEA region, it has less awareness within other geographic markets. MSS offerings are sold predominantly through a global or regional direct salesforce with limited resale by channel partners.

The current portal does not allow role-based access. In the future, BT plans to include this and provide increased visibility for customers to view events and drill down into data.

APPENDIX

The security landscape is complex and challenging – an understatement, given the number of moving parts that are involved in defending an enterprise from cyberattacks. IDC recommends that companies undertake a holistic, enterprisewide security posture that is proactive and predictive.

It's a daunting effort, however, to sustain the necessary level of threat intelligence and advanced analytics capabilities along with the skills to interpret and act on findings. In-house 24 x 7 security solutions are expensive, and security talent is scarce. As a result, organizations debate "build versus buy," and many are turning to MSSPs. A security services provider can allow organizations to meet several objectives:

- Transfer the cost of ownership, thereby reducing capex and transferring the budget to opex
- Create a predictable expense with a regular cadence in the budget cycle
- Enable a dedicated application of technology, processes, and people to the rapidly changing threat landscape
- Implement best practices that are evolving with a rapidly changing threat landscape

- Benefit from "strength in numbers" from an intelligence perspective

The rise in frequency and complexity of attacks and the need for increasingly sophisticated security solutions have led to a new echelon of MSS that IDC is calling MSS 2.0. An MSSP 2.0 is further "up the stack" than MSSPs that are offering MSS 1.0 services, which include the following:

- Log monitoring
- Basic managed and monitored services (firewalls and intrusion detection services/intrusion prevention services)
- Unified threat management
- Identity and access management
- Vulnerability scanning

MSSPs 1.0 may also offer advanced services such as DDoS, managed SIEM, and managed SOC.

MSSPs 2.0 deliver basic and advanced MSS plus professional/complementary services (for more details, see the Market Definition section). They are also investing in mobile/IoT, cloud, threat intelligence/big data analytics, incident response/forensics, and advanced detection techniques. Cloud, mobile/IoT, and big data are three of four pillars that IDC has identified as top trends. The fourth pillar, social media, doesn't factor into this IDC MarketScape; however, advanced MSSP capabilities can help detect, analyze, and protect against security threats in the social media arena.

Security, in general, is complicated by the shortage of security talent. Innovative MSSPs focus on short- and long-term employee acquisition, training, and retention using both traditional and progressive practices. Some of their tactics are apprentice programs, scholarships, in-house universities, university partnerships, and flexible career paths.

Further, regulatory requirements continue to evolve, and MSSPs can provide the expertise and evidence needed for oversight and compliance based on industry-standard certifications.

Businesses increasingly are turning to MSSPs to monitor and manage some or all of their security needs. Based on IDC market sizing, the MSS market is expected to continue to see growth in double digits in coming years.

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

Managed Security Services

For the purposes of this research, IDC defines managed security services as "the around-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs), not through personnel onsite."

Exceptions and Inclusions

Managed security services can include complementary consulting and advisory activities that are typically defined under professional security services. The study did seek to understand whether the MSSPs offer complementary services as IDC believes these services are critical to the evolution and maturity of MSS. The MSSPs in this study do provide complementary services; although, there is no standard approach for how they are offered. Commonly, an initial assessment is bundled with the onboarding fees, and some may bundle other services. Most, however, offer complementary services as optional add-ons and may charge separately for them.

Complementary services surveyed in the study include breach management, incident response, forensics, compliance services, and assessment of architecture and design. Not all MSSPs provide all of these services. Some MSSPs provide all of the listed complementary services and others such as managed security testing, application security testing, advisory services, integration services, and data privacy assessment.

Terminology

- **Managed security and information event management (managed SIEM).** This managed on-premises event collector transmits the raw log data to an MSSP's SOC for analysis, reporting, and archiving. This is an advanced, niche capability that is offered currently by half of the participants in this study.
- **Managed SOC.** A security operations center includes the people, processes, and technologies involved in detecting, containing, and remediating security threats. Some MSSPs take over the operation of SOCs that their customers have built and no longer want to manage. This is an advanced, niche offering that is offered currently by a majority of the participants in this study.
- **Security operations center types:**
  - **In-region.** A standalone SOC in a country or region
  - **Follow the sun.** A type of global workflow in which tasks are passed around daily at the end of work shifts among sites that may be in different time zones
  - **Global.** Workflow that occurs in one global location in a 24 x 7 multishift arrangement

LEARN MORE

Related Research

- *IDC MarketScape: Western Europe Managed Security Services 2017 Vendor Assessment* (forthcoming)
- *Worldwide DDoS Prevention Products and Services Forecast, 2017-2021* (IDC #US42570517, May 2017)
- *IDC MarketScape: U.S. Emerging Managed Security Services 2016 Vendor Assessment* (IDC #US41320816, August 2016)

Synopsis

This IDC study presents a vendor assessment of providers offering managed security services (MSS) through the IDC MarketScape model. The assessment reviews both quantitative and qualitative characteristics that define current market demands and expected buyer needs for MSS. The evaluation is based on a comprehensive and rigorous framework that assesses how each vendor stacks up to one another, and the framework highlights the key factors that are expected to be the most significant for achieving success in the MSS market over the short term and the long term.

"The security landscape is changing rapidly, and organizations continue to struggle to maintain their own in-house security solutions and staff. As a result, organizations are turning to managed security service providers (MSSPs) to deliver a wide span of security capabilities and consulting services, which include predicative threat intelligence and advanced detection and analysis expertise that are necessary to overcome the security challenges happening today as well as prepare organizations against future attacks. The MSSP market is highly competitive, and many MSSPs have a breadth of security services in their MSS portfolio. The differentiation among these MSSPs will be tied around their flexibility in delivering security services and advanced MSS capabilities and how these MSSPs can continue to assist organizations with their security needs today and in the future." – Martha Vazquez, senior research analyst, Infrastructure Services

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

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com