



IDC MarketScape

IDC MarketScape: U.S. Emerging Managed Security Services 2016 Vendor Assessment

Christina Richmond

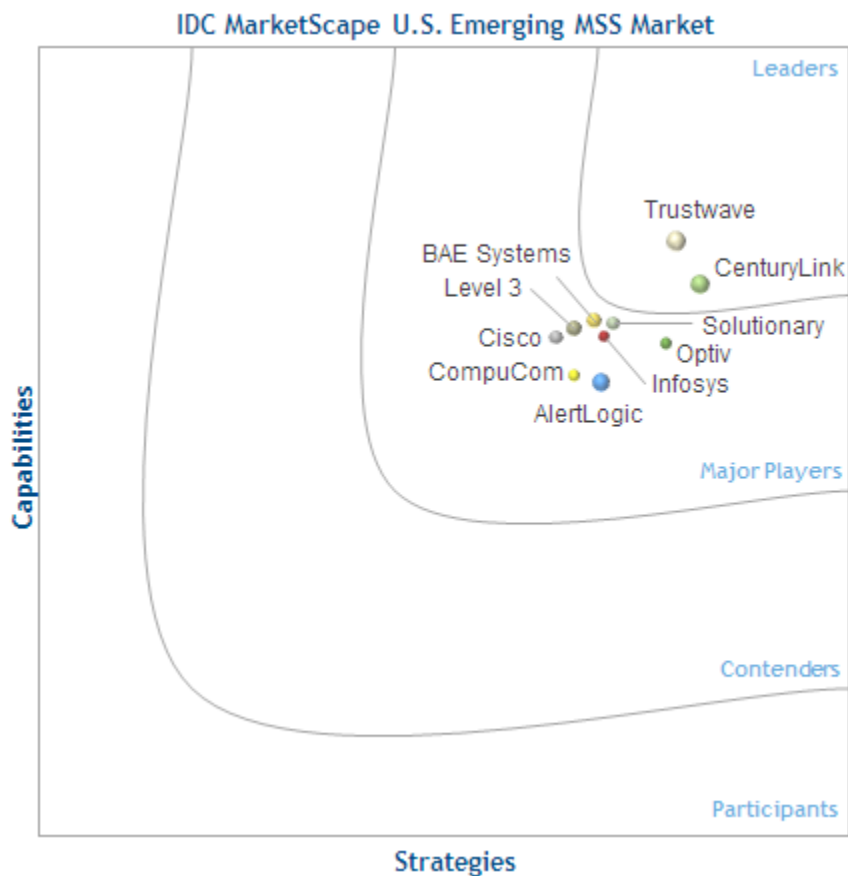
Martha Vazquez

THIS IDC MARKETScape EXCERPT FEATURES: CENTURYLINK

IDC MARKETScape FIGURE

FIGURE 1

IDC MarketScape U.S. Emerging Managed Security Services Vendor Assessment



Source: IDC, 2016

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

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: U.S. Emerging Managed Security Services 2016 Vendor Assessment (Doc # US41320816). 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

Using the IDC MarketScape model, IDC studied 10 organizations in the first quarter of 2016 that offer managed security services (MSS) in the United States, although several of the study participants deliver services worldwide. This study excludes the more established worldwide managed security services providers (MSSPs), which may also be considered the top providers in the United States. These companies were studied in 2014 and will be evaluated again in 2017 and are not included in this study. Through in-depth managed security services provider interviews and more than 25 interviews with providers' customers, IDC learned that the providers offer traditional (basic) MSS and advanced MSS capabilities in varying degrees. Through granular evaluation in early 2016, IDC found that each provider possesses some unique strengths and weaknesses when compared with its peer group. Major differences centered on both current capabilities and strategies for the next 12-18 months. As a result of IDC's evaluation, IDC found two Leaders – Trustwave and CenturyLink. The second group of Major Players consists of Alert Logic, BAE Systems, Cisco, CompuCom, Infosys, Level 3, Optiv, and Solutionary. As MSS continues to mature, it is incumbent upon these 10 emerging U.S. MSSPs to participate in the next generation of MSS, which IDC calls MSS 2.0. Buyers certainly face complex choices in selecting a vendor with which to partner. However, despite these complexities in vendor selection, buyers purchasing MSS have plenty of options. IDC believes the following areas will drive the MSS market forward and differentiate the providers:

- Complementary consulting services that provide customizable opportunities for customers to plan and enable their security journeys
- Flexible consumption models that match customer preferences for integrating MSSP expertise, processes, and technology
- Cloud management capabilities that seamlessly enable hybrid implementations
- Pricing models that align with customer preferences
- BYOD/mobile solutions
- Advanced detection 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
- Security operations centers (SOCs) and advanced methods of acquiring and retaining much sought-after security talent

IDC MARKETSCOPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 10 MSSPs within the 2015 IDC MarketScope U.S. emerging 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:

- **MSS capabilities.** Each service provider was required to offer at least five traditional MSS delivery capabilities that are viewed by IDC as basic. A majority of participants offer more than five capabilities. See the Situation Overview section for an explanation of traditional MSS.
- **Revenue.** Each service provider was required to have 2014 MSS revenue in the range of \$25 million to \$75 million in the United States.
- **Security operations center.** A minimum of one SOC in the United States.

ESSENTIAL BUYER GUIDANCE

Buyers face complex choices in selecting an MSSP due to the number of providers and a multitude of variables: breadth and depth of offerings; staffing, capabilities, and locations; complementary services; onboarding methods; service-level agreements (SLAs); payment options; customer portal capabilities; customer service delivery methods; partnerships; and more. Given the pace of technology change, buyers should evaluate current and future MSSP offerings, along with the MSSPs' product/service/investment road maps, to be sure that future offerings align with anticipated business and cost projections. It can be expensive and disruptive to change providers, so it is worthwhile for buyers to take the time to find the right fit, no matter how many security services are being outsourced. An MSSP's customer satisfaction surveys, pricing benchmarks, use cases, proofs of concept, and/or best practices can aid the decision process.

IDC suggests that buyer organizations pay particular attention to the following decision factors:

- **Investigate MSS research and development (R&D) focus areas.** Forward-looking MSSPs are paying attention to cloud evolution, threat intelligence, incident response, forensics, big data and analytics, and advanced detection techniques. It is important to evaluate the MSSP's future road map strategies to determine whether the MSSP will be able to offer future technology changes needed for your business. For example, some MSSPs are making investments in security related to Internet of Things, BYOD/mobility, big data analytics capabilities, user behavior analytics (UBA), secure web gateways, and cloud hosting providers like Amazon and Microsoft.
- **Clarify cloud adoption strategy and timeline.** Workloads are shifting to different cloud platforms, so it is important to select an MSSP that can deliver offerings that best fit your business needs and can be flexible to meet future changes occurring within your infrastructure. Typically, MSSPs have some equipment on-premises for log collection, but software-as-a-service (SaaS) and hybrid delivery are gaining momentum. A typical MSSP can manage/monitor on-premises equipment for the customer and/or correlate log aggregation or security events through SaaS/cloud services. MSSPs are using multiple delivery processes to manage, monitor, and correlate security. Given ongoing concerns about cloud security, however, buyers should evaluate offerings carefully. MSSPs are expanding cloud capabilities and expertise, perhaps opportunistically, through acquisition, organic development, and partnerships. Current and upcoming cloud-based managed security services include threat

intelligence, analytics, threat detection, web security, identity, distributed denial of service (DDoS), mobile, and email security.

- **Embrace the necessity of threat intelligence and the use of big data.** Cyberattacks are only going to increase in frequency and severity. Organizations can no longer afford a "do the minimum" security strategy, which is simply not sufficient to thwart advanced persistent threats, distributed denial of service, identity theft, and other sophisticated attack strategies. The commonsense best practice is to acquire and use reliable, "predictive" intelligence that results from a robust combination of technology and expertise. Buyers may want to evaluate MSSP capabilities such as large databases (for long-term analysis), data aggregation and correlation, behavioral- and heuristic-based detection (versus signature-based detection), machine learning, emulation/sandboxing, virtual containerization, and forensic analysis/interpretation.
- **Evaluate customer portals.** Portals are the primary conduits of information between MSSPs and their customers, and they determine the scope and ease of visibility and control. Portals can be a competitive differentiator, and as such, they should be able to satisfy broad user requirements. Basic portals typically include some visibility of data, ticketing functions, limited reports, and contact links. Advanced portals are built with Web 2.0 tools and offer a rich customer experience that may include sophisticated analytics and visuals, real-time updating, and configurability/customization choices, especially for reports. Increasingly, portals include role-based access, querying of security and information event management (SIEM) data with broad correlation capabilities, and real-time chat or instant messaging. MSSPs should be able to demonstrate how their MSS are integrated into the portal and how the portal can be customized for different types of users (e.g., executives and security personnel). Portals can also be used for providing workflow analysis for the client to see what incidents are being addressed by the MSSP and the ticket status.
- **Consider complementary services.** MSSPs included in this study offer some or all of the following services that are complementary to MSS: assessment of architecture and design, breach management, incident response, forensics, and compliance services. Some MSSPs offer additional complementary services around advanced malware analysis or in other areas that will help strengthen a customer's security program. Enterprises must have a strategy to respond to incidents and collect forensic evidence for legal and/or compliance reasons. A preemptive strategy is even better – one that does not treat all security threats as equal and apportions budget based on a current-state/future-state risk analysis.
- **Evaluate SOC capabilities and security expertise.** Depending on organizational requirements, SOC staff certifications, which are relevant to specific industries, security regulations, and operating systems, may be crucial in a proactive, predictive security strategy.

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 a certain set of criteria, the description here provides a summary of the vendor's strengths and challenges.

CenturyLink

According to IDC analysis and buyer perception, CenturyLink is an IDC MarketScape Leader in the U.S. Emerging Managed Security Services market.

CenturyLink is currently the third-largest telecom company in the United States. Since 2008, CenturyLink has transformed its business by acquiring some strategic companies, each of which has given CenturyLink new capabilities. This transformation included the acquisition of Qwest Corp. and Savvis Communications in 2011, which helped broaden CenturyLink's services portfolio by adding in managed security services as well as domestic and international enterprise networking, hosting, colocation, and cloud infrastructure and services.

Along with the acquisition of Savvis and many others such as AppFog, Tier 3, Cognilytics, and netAura, CenturyLink has demonstrated its commitment to strengthening its security services as well as supporting its customers' transition from a traditional networking infrastructure to a hybrid IT world. In 2016, CenturyLink expanded its managed security service portfolio with the announcement of five key enhancements and a new customer portal.

In 2016, CenturyLink relaunched its customer-facing portal, which is built on the elastic search stack ELK. This architecture allows customers to access their data by using this elastic ELK stack and then do detailed searches, analytics, and visualization of their data. The portal also provides clients with complete transparency into what the CenturyLink analysts are doing for them in real time. They can see what incidents or alerts are open and active, can interact with the SOC analysts in real time, and can change the status of open incidents in real time.

CenturyLink has three SOCs in the United States, with two others located in the United Kingdom and India. The MSS business focuses on midmarket and enterprise customers but also has a breadth of government customers. CenturyLink has been providing security services for over a decade and has a number of offerings that are customizable to its customers. CenturyLink sells security in two ways: as an add-on to core company offerings such as network and hosting (mainly basic services) and/or as a standalone network-agnostic service for larger organizations that desire a true MSS partner.

Federal government entities and/or compliance-driven midmarket and enterprise organizations will find CenturyLink MSS a good option.

Strengths

CenturyLink has a strong foothold in delivering services to the federal and government entities and can provide custom-based security services for enterprises. CenturyLink also delivers advanced services such as DDoS, web application scanning, web application firewall, managed SOC, penetration testing, and file integrity monitoring and is providing advanced detection and analytics techniques. Also, the company added five new services in its SIEM platform, which were log monitoring, threat analysis, incident response, vulnerability management, and managed protection services.

CenturyLink also offers different price models and payment options for customers. The company has a strong channel program, with seven channels to support the implementation of service sales. Also, the go-to-market plan consists of vertically focused sales teams. CenturyLink has a senior leadership team with security expertise that act as advisors to multiple federal agencies and contributors to the NIST cybersecurity framework and a team of 30+ security consultants and 250 researchers and testers in its SOCs that are GIAC Certified Intrusion Analysts covering multiple security domains.

CenturyLink received solid marks for its talent acquisition and retention programs. Century Link employees are offered numerous academic programs to attend in the United States. For example, Innovations in Communications, Information and Cyberspace (IC3) at Louisiana Tech University is a unique and innovative certificate program in information technology that is offered to students and employees of CenturyLink.

Customer feedback applauded CenturyLink for its responsiveness to customers' RFP and its service management group.

Challenges

Portal capabilities were lacking in 2015, but moving into 2016, the portal is now enhanced, and many customers are trying out its new capabilities. Before the new integrated portal, there were two separate portals, in which the Savvis portal did not have any capabilities such as real-time updating, enhanced analytics, reporting, or visualization tools. Unfortunately, there will be more challenges to work through as these portals are integrated. To compete competitively, CenturyLink should also look at enhancing its MSS capabilities with threat intelligence services and BYOD/mobility.

APPENDIX

Situation Overview

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, 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). And they are investing in mobile/BYOD, cloud, threat intelligence/big data analytics, incident response/forensics, and advanced detection techniques. Cloud, mobile/BYOD, 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.

Essential Service Provider Guidance

Organizations turn to MSSPs for the top 3 reasons:

- The challenges and costs associated with maintaining in-house solutions and expertise
- The opportunity to move from a capex to an opex expense model
- The need of assistance to combat adversaries that are increasingly "one step ahead"

The vendor selection process typically involves multiple decision makers, including C-level executives and even board members, who are well aware of the consequences of a breach. Enterprise priorities include risk reduction and compliance with applicable existing and emerging regulations and laws. Cost is always a factor, of course, but it is weighed in the context of what an MSSP can provide: overall breadth and depth of protection for an enterprise, threat detection/containment, brand and reputation preservation, perceived peace of mind, and even competitive differentiation.

Buyers can choose from pure-play MSSPs, systems integrators, consultancies, value-added resellers, and telcos – all of which can make a case for outsourcing some or all security functions.

For MSSPs that aspire to lead the U.S. MSS marketplace, IDC recommends:

- Determine how to define, package, and deliver cutting-edge services to targeted customer segments. Forward-thinking MSSPs have a vision, can articulate their approach, and demonstrate discipline and consistency from R&D through customer support.
- Understand that MSSPs without MSS 2.0 capabilities are likely to be at a competitive disadvantage. The future of MSS is cloud, mobile/BYOD, threat intelligence/big data, advanced detection techniques, and incident response/forensics. Marshaling the investment dollars, IP, technology, people, partnerships, and delivery/support mechanisms is advisable and necessary.
- Develop different versions of go-to-market messaging that highlight strengths and differentiation. Savvy MSSPs are prepared to speak to all levels of an enterprise (from workers to board

members) with appropriate language, examples, demonstrations, and benefits. Other useful tools may include ROI scenarios and industry benchmarks. Furthermore, ongoing education is a value-added service that goes a long way toward establishing credibility and loyalty.

- Map out each customer's security journey that includes current and future states. Develop a living document that is the basis for ongoing conversations about strategy, technology, staffing, certifications, SLAs, and so on. Demonstrate thought leadership and mastery of the big picture and the details.
- Stay on top of target customers' security requirements, and implement the appropriate SOC model(s). SOC's and portals must provide a seamless user experience, which includes the desired visibility and control. Make it a priority to inform customers of new or improved services, and assist them with adoption. Send the right message about customer service and value.
- Be creative when it comes to identifying, acquiring, and retaining security talent. The people behind the technology matter a lot to customer satisfaction and growth.

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 SOC's 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

- *BrightPoint Security: Increasing the Relevance of Threat Intelligence with Trusted Circles* (IDC #US41151515, April 2016)
- *Worldwide Threat Intelligence Security Services Forecast, 2016-2020: Strength in Numbers* (IDC #US41053415, March 2016)
- *IDC's Worldwide Security Services Taxonomy, 2016* (IDC #US41053315, March 2016)
- *Vendor Profile: HackerOne – Bringing Hackers and Companies Together* (IDC #US40751416, February 2016)
- *Market Analysis Perspective: Worldwide Security Services, 2015 – Breach Is a Foregone Conclusion* (IDC #259239, September 2015)
- *Worldwide Cloud Hosted Enterprise Security Services (Security as a Service) Forecast, 2015-2019* (IDC #257959, July 2015)

- *Market Analysis Perspective: Worldwide Security Services, 2014* (IDC #253061, December 2014)
- *IDC FutureScape: Worldwide IT Security Products and Security Services 2015 Predictions – Moving Toward Security Integration* (IDC #253026, December 2014)
- *IDC MarketScape: Worldwide Managed Security Services 2014 Vendor Assessment* (IDC #248646, June 2014)

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.

"In-house security solutions are expensive and challenging to maintain in the face of a rapidly evolving threat landscape and formidable adversaries. As a result, enterprises increasingly are considering managed security services providers (MSSPs). MSSPs that offer MSS 2.0 services provide a plethora of security and consulting services along with the predictive threat intelligence and advanced detection and analysis expertise that are necessary to thwart attacks and protect assets. In the highly competitive security services marketplace, enterprise leaders need to be discerning buyers that understand their requirements and evaluate MSSP capabilities accordingly, regardless of how many security services are being outsourced." – Christina Richmond, program director, Security 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

Copyright and Trademark Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or web rights. IDC and IDC MarketScape are trademarks of International Data Group, Inc.

Copyright 2016 IDC. Reproduction is forbidden unless authorized. All rights reserved.

