IDC MarketScape

IDC MarketScape: U.S. Emerging Managed Security Services 2019 Vendor Assessment

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, 2019

August 2019, IDC #US42814718e

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 2019 Vendor Assessment (Doc # US42814718). 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, and especially over the past 18 months, managed security services providers (SPs) have added more capabilities and advanced security services to assist organizations in defending against and responding to today's attacks. Managed security SPs are experiencing a pivotal change in how organizations are viewing security. No longer are organizations looking for that traditional service provider to just provide basic management of security products and management of policies and rule sets. Today, the market has shifted beyond offering basic protection and detection of threats toward offering a response and/or remediation in a rapid fashion that is tailored to an organization's need.

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 managed security SPs. Organizations are turning to service providers and/or managed security SPs for several reasons:

- Gain access to 24 x 7 support and expertise.
- Create a predictable expense with a regular cadence in the budget cycle.
- Improve availability and performance.
- Enable the organizations to have access to emerging technologies, such as threat intelligence, advanced data correlation and analytics, incident response, and forensics, to support legal and compliance requirements.
- Implement best practices that are changing with the threat landscape.
- Stay ahead of the advanced and complex threats in the security landscape.
- Gain depth and breadth of security skills in a marketplace where security talent is scarce.
- Implement a holistic security posture that is proactive and predictive versus reactive.
- Receive correlation and analytics based on multiple sources using big data to maximize visibility into diverse threats on a global basis.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

Using the IDC MarketScape model, IDC studied 10 organizations in the latter half of 2018 that offer MSS in the United States. While not a requirement, many of them do also have global capabilities. The

study does exclude the more established worldwide managed security SPs that have 2017 global revenue that was over 150+ million. Those companies and others that reach that revenue in 2018 will be looked at in the next IDC MarketScape for worldwide MSS to be published in 2020.

To be included in the 2019 IDC MarketScape for U.S. emerging MSS, providers had to meet 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 the participants offer more than five capabilities.
- **Revenue.** Each service provider was required to have 2017 MSS revenue in the range of $20 million to $90 million in the United States.
- **Security operations center.** A minimum of one SOC in the United States is required.

ADVICE FOR TECHNOLOGY BUYERS

Organizations that are undergoing evaluation of managed security services are facing a number of challenges. The entrance of new providers such as cloud, managed SPs, value-added resellers (VARs), security product suppliers, managed detection and response (MDR) providers, and consulting companies into the market has exacerbated the options available to the adopter of services. In addition to new providers in the market, the complex changes in the IT infrastructure and then having to deal with the complexity and volume of threats entering an organization's environment is a lot to understand. The buyer needs to be selective in trusting and picking a managed security SP partner that will assist it in making strategic security decisions. In addition, the managed security SP has to offer the security services needed to protect, detect, respond to, and recover from cybersecurity events in their organizations.

A variety of variables are looked at when selecting a managed security SP, which includes the portfolio of security offerings, staffing, SOC locations, complementary services, onboarding time and methods, pricing options, expertise, portal functionality, customer service delivery methods, and partnerships.

With the ongoing changes occurring today in the security landscape, along with the rapidly evolving pace of technology, organizations must evaluate offerings for today and for the future. This is important to be sure that future offerings align with anticipated business changes 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. A managed security SP's customer satisfaction surveys, pricing benchmarks, use cases, proofs of concept, and/or best practices can aid the decision process.

Figure 2 shows those top functional criteria that are important for an organization when selecting a managed security SP. The number 1 importance is the consistent awareness of threats followed by the ability to provide monitoring services such as for firewalls, IDS/IPS, and other core functions. In addition, users also believed that a highly responsive staff was a critical component as well.

To enhance the decision-making process in vendor selection, IDC recommends that buyers bear in mind the following considerations:

- **To access capabilities and security maturity.** Many managed security SPs can help an organization access their inventory, assets, data, and security program, but organizations should already have some understanding of what capabilities they have today and what they may need for the future. Organizations should choose a provider vendor that can partner with them as they assess where they are today and what gaps they have in these security programs.
- **Considering business outcome initiatives.** When planning on adopting and/or addressing security challenges, organizations should not just implement the "newest" and "shiniest" technology. A sound security program needs a comprehensive approach, which includes evaluating the people, process, and technology. No one security technology can solve all of an organization's security problems, so understanding and defining what outcome an organization is trying to achieve makes sense before just adopting point security solutions. IDC observes that mature organizations tie the security objective very closely to the business objective. As a result, some security investments are actually coming from the lines of business as part of the business transformation or innovation initiatives.
- **SOC locations and requirements.** Every organization needs and requirements will vary depending on size, scope, compliance needs, budget, and so forth. Since this study is focused around the United States, it's important that organizations review their scope of needs such as the location of the SOC, the methods, procedures, and workflow that is used by the provider being evaluated. Some organizations may choose to have support staff located globally or in the United States. Depending on the provider and location, many follow a 24 x 7 follow-the-sun (FTS), global, or regional workflow.
- **Breadth of managed security services portfolio.** Identify the managed security services that are being offered by each provider. Some have the basic firewall, IDS/IPS, UTM, SIEM, and so forth, so it is important to review the basic monitoring that is needed and the advanced services as well such as identity access management, threat intelligence, and endpoint/network detection and response (EDR/XDR). A number of security solutions are offered also as a bundled service so those organizations looking for more cost-effective services should evaluate the different services offered in a bundle with other IT product and services. Many providers will bundle security offerings designed around compliance regulations, business outcomes, or with other IT offerings.
- **Research and development/road map strategy.** It is no secret that organizations have been undergoing digital transformation (DX) initiatives. It is imperative that the necessary security solutions and services are implemented simultaneously during digital transformation. As these organizations change how they operate, managed security SPs must also be able to support their customer requirements. Future-thinking managed security SPs are paying attention and are evolving as well in their capabilities and investing in research and development such as automation, orchestration, advanced detection techniques, cloud strategy, data analytics, artificial intelligence/machine learning (AI/ML), forensics, and other emerging technologies. Organizations need to evaluate a managed security SP's future road map strategies and determine whether the managed security SP will be able to provide the security support necessitated by digital transformation. For example, cloud monitoring services are becoming more important as organizations adopt cloud or multicloud presences. A knock-on effect of this change is that identity access management will be a critical factor as more applications move to the cloud and users move to hybrid clouds. A further example is provided by the trend of managed security SPs seeking to implement software-defined networking (SDN) and network

function virtualization (NFV) technologies as a means to create internal cost efficiencies and provide more nimble and flexible services.

- **Managed detection and response, threat intelligence, and advanced threat detection capabilities.** Evaluate and demo the services specified as MDR and/or advanced threat detection capabilities and review specific procedures, tools, and methodologies used. The MDR term has been used for several years now. While some providers are specific to only MDR services, managed security SPs have also been evolving and moving beyond just traditional network-based MSS capabilities. IDC views MDR as a portfolio of services, which includes proactive security and threat monitoring, detection, incident analysis, and response service that correlates client environment-specific threat intelligence and telemetry collected from the client's environment and utilizes vendor-supplied technologies that work in a coordinated fashion with all aspects of the solution (endpoint detection and response [EDR], network, threat intelligence, and SIEM) to form a more effective outcome. There are some core technologies and tools used in MDR service such as ML, big data analytics, behavior analytics, threat intelligence, and ongoing threat hunting to identify known and unknown threats (see the Market Definition section).
- **Complementary services.** Managed security SPs 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 managed security SPs offer additional services such as security transformation, IoT, adversary simulation, security awareness training, and cloud security. Buyers should consider a managed security SP that can help develop, strengthen, and continue to evaluate their security programs. 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 resources based on a current state/future state risk analysis.
- **Cloud strategy.** Cloud adoption continues to occur and likely most organizations are already moving workloads to the private, public, and multiclouds. It is pertinent that security follows the workloads especially as organizations move critical workloads to the cloud. In addition, managed security SPs have worked with customers in expanding the delivery in cloud offerings such as identity access management. Cloud delivery models continue to expand and drive managed security SPs to offer hosted and network-based (cloud) security services.

  Cloud access security broker (CASB) solutions are being used to provide monitoring in cloud scenarios. Some managed security SPs are providing workload protection to support public cloud environments. It is important to evaluate a managed security SP that will assist and provide recommendations for the organization moving and utilizing cloud strategies.
- **Security expertise and 24 x 7 support.** Organizations need to consider the security expertise of the provider being evaluated. The number of support staff and type of support should be evaluated especially if looking for support from only the United States or looking for one to work on on-premises or to augment the IT/security team. Managed security SPs should be investing in their own people by providing ongoing trainings, incentive opportunities, and additional career paths for those wanting to expand their careers in security. Since the security market is experiencing skill shortages, it's important that a managed security SP creates innovative ways to acquire new talent by partnering with universities and developing core curriculum and programs. Managed security SPs with strong training programs will be more likely to retain their security talent.
- **Customer engagement and satisfaction.** Buyers should consider how the engagement will occur between them and a managed security SP once the services are established. It is

important that the managed security SP acts as a trusted advisor and as an extension to the customer's IT team. Not many organizations will want to talk to a different support/analyst person all the time. They prefer to have that one person who understands their IT environment and one who can discuss, make recommendations, and provide ongoing guidance to them.

- **Customer portal capabilities.** Portals are the primary conduits of information between managed security SPs 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. Many providers are revamping their managed security SP portals to make them user-friendly and easy to navigate with visualization tools and customizable reporting capabilities. In addition, portals typically include real-time data analysis and advanced analytic capabilities to improve investigation workflow for the purposes of enhancing detection and response times. Managed security SPs are expanding search and communication, self-service capabilities, and in-depth reporting and enhancing visibility for customers. Managed security SPs 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) and if a mobile app is offered for ongoing access to tickets and alerts.
- **Reviewing security orchestration and automation technologies.** Providers are investing in automation and orchestration of technologies. The new techniques have a variety of benefits that can help customers order new services on demand and provide a more efficient workflow for analyzing threats. Buyers should be aware of what the managed security SP road map looks like in implementing these new efficient technologies.

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.

CenturyLink

CenturyLink is positioned as a Leader in the IDC MarketScape for U.S. emerging managed security services.

CenturyLink has gone through a number of changes and acquisitions in the past five years. The last acquisition of Level 3 positioned the company as a major U.S. communications provider to global enterprises. CenturyLink has and continues to invest in a number of capabilities within the security services portfolio. As a result of the number of acquisitions, the company has broadened its global footprint with eight SOCs, four of which are located in the United States (Broomfield and Littleton, Colorado; Phoenix, Arizona; and St. Paul, Minnesota), two in APAC, and one each in LATAM and EMEA. CenturyLink provides a blended 24 x 7 x 365 and "follow the sun" model where proper shift turnover is required to ensure knowledge transfer of the current state of operation as well as any pending activities, tasks, events, and so forth. In addition, CenturyLink operates dedicated North American and U.K. SOCs to support national government contracts.

CenturyLink has a breadth of managed security services as well as complementary services available for midsize, enterprises, and government entities. CenturyLink has focused around offering services that enable enterprises to work with various type of infrastructure, meaning those in the hybrid cloud and premises environment. There are four pillars within the security services business, which include

network security services, professional/consulting, premises, and analytics and threat management services. CenturyLink's advanced security monitoring service allows for advanced detection with 24 x 7 eyes on glass monitoring. These pillars are supported by a number of services including adaptive network security services, DDoS mitigation, adaptive threat intelligence, and traditional services such as managed firewall, managed web application firewall (WAF), and managed IDS/IPS. In addition, CenturyLink has a solid threat intelligence research and operations team, Black Lotus Labs, that provides visibility into the threat landscape to proactively detect and mitigate threats and alert and provide guidance and recommendations to its customers.

From a strategy perspective, CenturyLink is stitching its services together to design security platforms that are adaptive to customer environments. CenturyLink is working on reducing infrastructure costs by delivering transformation enterprise security solutions and deliver embedded solutions as well into existing offers. In turn, CenturyLink is focused on enabling simpler and more cost-effective solutions for organizations.

Strengths

With four SOC locations in the United States, CenturyLink has a strong foothold and brand name in the United States, with four SOCs serving the needs of United States-based global companies. In addition, the company continues to make acquisitions that have filled gaps within their security portfolio. The company currently has a number of managed security services that organizations can choose from. Its portal continues to be improved and has capabilities for advanced users to write custom query language to drive search and custom reporting. In addition, the iOS mobile app for CenturyLink's Security Log Monitoring SIEM service enables end users to resolve security incidents more quickly and efficiently. Customer stated, "CenturyLink is better than some other competitors because the company listens to its customers and propose innovative solutions."

Challenges

CenturyLink has made lots of enhancements but has been slower to adopt the advanced automated response tools for managed detection and response. The company strategy is to develop and widen its scope in this area.

Consider CenturyLink When

Midsize and large enterprises and governments looking for a network provider to also handle its day-to-day managed security can benefit from CenturyLink's breadth of security services and network visibility that the company provides.

APPENDIX

Situation Overview

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 managed security SP 2.0 is further "up the stack" than managed security SPs that are offering MSS 1.0 services, which include the following basic services:

- Log monitoring

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

Managed security SPs 1.0 may also offer advanced services such as DDoS, managed SIEM, and managed security operations center (SOC). Managed security SPs 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 managed security SP capabilities can help detect, analyze, and protect against security threats in the social media arena.

Through in-depth briefings with providers, surveys, and interviews from customers, IDC learned that providers continue to offer traditional security services but are also offering advanced services that are enabling organizations to move from a reactive to a proactive stance in their security posture.

Many of the organizations listed in this IDC MarketScape offer a breadth of basic services such as management and monitoring of firewall, intrusion detection/prevention systems (IDPS), unified threat management (UTM), secure gateways, endpoint protection, and log management. Many are also offering advanced services such as endpoint/network detection and response, SIEM, DDoS prevention, threat intelligence, identity access management (IAM), remote/on-premises incident response, and proactive threat hunting and integrating other advanced detection and analytic methods, which include big data analytics and machine learning/artificial intelligence (AI) (see the Market Definitions section).

Given the rapid pace of development within the MSS market, it is important that providers continue to keep pace with the development of the market, let alone remaining ahead of the chasing pack. Through research conducted, IDC found that each provider has its own differentiators and key strengths and weaknesses, which may be important to an organization when evaluating a managed security SP. While many factors were reviewed during the evaluation process, IDC believes the following areas will drive the MSS market forward while providing operations in the United States:

- The size of the U.S. footprint including channel partners, delivery centers and models, number of analysts, and support within the United States
- The breadth of service offerings delivered today and in the next 12–18 months (These include advanced services such as managed detection and response capabilities, encryption, IAM, managed SOC, penetration testing, web application firewall, threat intelligence, and other advanced analytic techniques.)
- The breadth of complementary services, which include incident response, breach management, compliance, digital transformation services, security strategy and planning, security policy assessment and development, and forensics
- Customer satisfaction and support services
- Customer portal and reporting capabilities
- Ability to address market changes and expand R&D capabilities and emerging technologies into its security service platform and portfolio

- Security expertise
- Advanced methods of acquiring and retaining security talent

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

Managed Security Services

For the purposes of this research, IDC defines managed security services (MSS) as "round-the-clock remote management or monitoring of IT security functions delivered via remote security operations centers (SOCs)." We include all MSS, whether these involve the management of security solutions deployed on a customer's premises or solutions hosted in a datacenter external to a customer's premises.

There is a steady stream of new services offered by MSS providers that extend beyond traditional managed security solutions. The primary reason for many of these services is essentially to manage the security operation as a whole, including integration across various security technology domains, such as managed SOCs and different phases, such as managed response services.

Managed Detection and Response

Now more than ever, service providers are racing to offer in-depth advanced detection and response capabilities to compete in the ever-evolving cybersecurity market. As competition stiffens, IDC is

seeing the market bring in a breadth of different competitors such as the consultants, integrators, pure-play security vendors, telecoms, and cloud/hosting companies. These different providers are all partnering and developing their own proprietary technology to stay ahead of the curve. Since the market has evolved, the role of a traditional managed security SP has matured and expanded in which IDC acknowledges the expansion of managed detection and response (MDR) providers and services, which we could consider the next generation of MSS or MSS 3.0. IDC defines MDR as a combination of number of technologies that provides continuous and proactive security and threat monitoring, detection, incident analysis, and response services that correlates and collects client environment-specific threat intelligence and telemetry. MDR utilizes vendor-supplied technologies in a coordinated fashion with all aspects of the solution including endpoint detection response, network (EDR/XDR), threat intelligence, and SIEM to form a more effective outcome. MDR services monitor activity and apply advanced analytics on endpoints, user activity, application layer, and at the network perimeter as well as traffic moving laterally within an enterprise network. Another key component in MDR services are incident response orchestration services and automated containment. MDR monitoring spans on-premises, private cloud, and public cloud environments. The core technologies and tools used in MDR services include advanced detection and analytics techniques such as:

- Machine learning
- Behavior analytics
- Big data analytics
- NetFlow analysis
- Threat intelligence
- Ongoing threat hunting to identify known and unknown threats
- Automated scripts and playbooks

The combination of technology, human expertise, and specific methodologies allows MDR providers to move from a reactive to proactive approach to threat detection, which allows for faster time to remediate an incident. MDR services generate highly impactful output with high fidelity security situations that will provide customers with recommendations and guidance and the intelligence to help clients achieve their desired business outcome.

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 managed security SPs offer complementary services as IDC believes these services are critical to the evolution and maturity of MSS. The managed security SPs 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 managed security SPs provide all of these services. Some managed security SPs 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.

Customer Perceptions of Managed Security SPs

The evaluation of this IDC MarketScape is based on input from the vendors, buyers, and survey work. The evaluation looks at both the key characteristics and the capabilities of the vendors evaluated. Included in the survey are insights to what is driving the managed security SP market and key areas that buyers in the United States are expecting from their providers during evaluation. It is important to highlight that the survey included 402 respondents in the United States that were utilizing managed security services. (see survey results throughout document)

Figure 5 displays the core security detection methods and techniques that organizations believe are important today and what will be important to implement in the next three years. Threat intelligence has become more widely adopted and accepted in the past few years in which organizations believe they need to have it implemented already. In the next three years, organizations feel that machine learning and artificial intelligence will become more critical in detecting and analyzing advanced security threats.

LEARN MORE

Related Research

- *Pricing Considerations Rank at the Bottom of the List When Choosing Third-Party Security Service Providers* (IDC #US45364819, July 2019)
- *IDC Market Glance DDoS Prevention Products and Services, 2Q19* (IDC #US45176319, June 2019)
- *Worldwide and U.S. Comprehensive Security Services Forecast, 2019-2023* (IDC #US44976419, May 2019)
- *Machine Learning and Artificial Intelligence Drive Future Advanced Threat Detection Techniques* (IDC #US45055219, May 2019)
- *IDC MarketScape: Worldwide Managed Security Services 2017 Vendor Assessment* (IDC #US41320917, August 2017)

Synopsis

This IDC study presents a vendor assessment of U.S. emerging 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 evolving security landscape, growing compliance requirements, and the changing IT environment have caused many challenges for organizations. Organizations are struggling to acquire the security expertise to assist in managing and monitoring the constant flow of security threats and to fully implement and integrate the growing number of tools that their security teams have acquired. As a result, organizations are turning to managed security SPs to deliver the security expertise, span of security capabilities and consulting services to assist in preparing, detecting, and responding against future attacks. The managed security SP market is highly competitive, and many managed security SPs have a breadth of security services in their MSS portfolio. The differentiation among these managed security SPs will be tied around their flexibility in delivering security services and advanced

detection and response capabilities and how these managed security SPs can provide holistic solutions that are tied to their clients' unique needs, both 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