IDC MarketScape

IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment

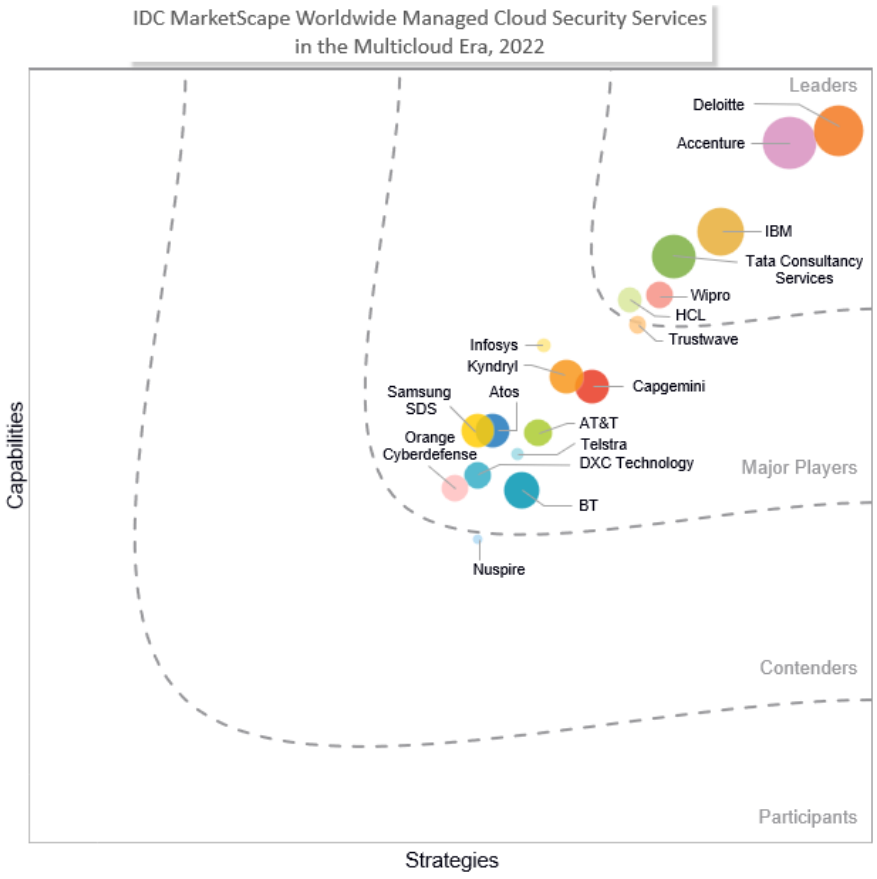
Cathy Huang

THIS IDC MARKETSCAPE EXCERPT FEATURES DELOITTE

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Managed Cloud Security Services in the Multicloud Era Vendor Assessment



Source: IDC, 2022

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

September 2022, IDC #US48761022e

IN THIS EXCERPT

The content for this excerpt was taken directly from IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment (Doc # US48761022). 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, 2 and 3.

IDC OPINION

From day 1, hyperscale cloud providers have advocated the shared responsibility model when it comes to security. The hyperscale cloud providers are responsible for the security of their cloud platforms and the layers below, which include physical, infrastructure, network, and virtualization layers. It is the responsibility of customer organizations to safeguard the operating system, applications, data, and users (refer to IDC's Shared Infrastructure Model depicted in Figure 3) that are in the cloud or accessing the cloud.

With the growing regulatory pressure, savvy enterprise decision makers are becoming aware that "100% cloud" is not their medium- or long-term IT estate plan. Those in regulated industries (as well as regions) recognize that the data must be deployed to the right cloud/venue. This results in a multicloud or hybrid IT scenario, with organizations needing to identify the best practices to secure their workloads, data, and applications.

More organizations are coming to terms with embedding security in their cloud transformation battle plan. Many are looking to the professionals such as managed cloud security services (MCSS) providers to get things done right. The value brought by MCSS providers in the new multicloud/hybrid IT era is clear.

Speed and Scale

- The adoption of various cloud providers is not new, but the speed and scale at which the adoption is taking place is noteworthy.
- By working with MCSS providers, customers get access to prebuilt playbooks and reference architectures covering leading cloud providers such as AWS, Microsoft Azure, and Google Cloud Platform (GCP). Often, providers have a library of proprietary accelerators, templates, and pre-developed codes that accelerate customers' cloud migration journeys.
- To meet customers' unique requirements, many MCSS providers, especially those with strong engineering capabilities, can co-innovate and help customers speed the development of use cases and cloud-native security controls.
- Customers gain scalability and agility by leveraging MCSS providers that can integrate and manage a multifaceted security ecosystem of partners and capabilities, which span on-premises, cloud, hosted cloud, and edge, and then secure the entire environment.

Transformation and Transparency

- Cloud is often perceived or used as a change agent or foundation for companies to take an enterprisewide transformation journey. Similar thinking applies to security.
- Cloud requires new ways to handle challenges in terms of visibility and security policy governance. At the same time, cloud enables various facets of security to be faster and more transparent.
- Creative deal structures will be required to enable transformation (shift to variable costs in both legacy and cloud environments). Moreover, devices are no longer defining the perimeter, but the user. "Per user" pricing suggests ultimately "secure the user."
- A growing number of MCSS providers develop tools powered by analytics to provide insights into how to maximize savings and track the key value benefits in the engagement. For example, MCSS providers help users predict energy consumption by calculating changes in a customer's carbon footprint upon migration to cloud.

Compliance and Sovereignty

- As regulatory pressures grow, particularly related to data privacy and data sovereignty laws, MCSS providers play a critical role in helping customers follow the resilience and sovereignty principles, thereby ensuring that infrastructure is always available to provide critical services.
- Many MCSS providers have a solid compliance management practice, along with related labs/centers of excellence (COEs) that continuously monitor the regulations, analyze business impact, and advise customers on implementation strategies to help them remain compliant.
- Many organizations leverage MCSS providers' broad capabilities and industry know-how, which enable MCSS offerings tailored to industry-specific pain points and help customers with their respective industry and business requirements.
- Almost all the providers in the study have cloud-related consulting, advisory, and assessment capabilities. They usually begin the managed cloud security engagement with assessment or advisory workshops and then identify security gaps against standards or regulations, followed by low- or high-level security architecture design.

Higher Security Efficacy Through Automation

- Traditional security policies designed to protect on-premises applications are largely ineffective in the cloud where the scale is bigger, and things happen faster than in traditional IT environments.
- Moreover, there are more things in more places that need to be monitored and protected, which make automation essential for multicloud security management.
- Many MCSS providers have developed code-defined assets or policies to enable an automated security function.

IDC MARKETSCAPE VENDOR INCLUSION CRITERIA

IDC collected and analyzed data on 18 service providers (SPs) for this IDC MarketScape for worldwide managed cloud security services in the multicloud era assessment. In determining the group of vendors for analysis in this IDC MarketScape, IDC utilized the following set of inclusion criteria:

- **Service capability**. Each service provider is required to possess many of the capabilities mentioned in the following list (for more details, see the Market Definition section):
  - Multicloud network management
  - Cross-cloud operation management
  - Data security and privacy management
  - Identity and access management (IAM)
  - Secure software development
  - Threat intelligence
  - Compliance and risk management
  - Detection and response for multicloud/hybrid cloud environments
- **Geographic presence**. Each vendor is required to have local delivery capability in a minimum of two regions: Americas, EMEA, or APAC.
- **Partnership**. Each vendor is required to have partnerships with a minimum of two public cloud providers.
- **Certified cloud security resources**. Each vendor is required to have a minimum of 70 certified cloud security resources (e.g., Microsoft Certified Azure Security Engineers, AWS Certified Security, or GCP Certified Professional Cloud Security Engineer).

ADVICE FOR TECHNOLOGY BUYERS

IDC's *Global Managed Cloud Security Services Survey* reveals the typical scope of MCSS engagements identified by buyers (see Figure 2). The top 3 areas of engagement are related to protection of data stored in clouds, regulatory compliance, and the development of consistent security policies across multicloud IT environments.

FIGURE 2

Scope of Managed Cloud Security Engagements

Q. Please select the statements that best describe the scope of the managed cloud security engagements with your vendor.

n = 500

Source: IDC's *Global Managed Cloud Security Services Survey,* June 2022

As buyers of managed cloud security services evaluate potential providers, they should keep in mind the core capabilities identified by IDC. IDC encourages buyers to explore the core managed cloud security services capabilities described in the Market Definition section and offers the following advice:

- Ask MCSS providers to explain how they ensure clear ownership and accountability among their businesses, the cloud service providers, and customer organizations in each engagement. Focus less on the product definition of the service that they provide and more on desired outcomes.
- Learn about vendors' histories in managed security services (MSS), their managed cloud security services portfolio, their road maps for future innovation, and the principles and/or strategies that guide development and go-to-market plans. Emerging security services, such as data residency as a service, the convergence of Internet of Things/operational technology (IoT/OT), and cyber-recovery services may be of particular interest to some buyers.

- Determine whether MCSS providers have the necessary expertise and experience to support customers through all stages of the cloud journey, with security foremost and embedded throughout. In particular, examine the providers' industry-specific expertise and region-specific knowledge (e.g., for local compliance).
- Identify areas of the cloud journey map for which an MCSS provider can accelerate the use of cloud-native security controls and/or the migration to hyperscale cloud platforms securely. The use of artificial intelligence/machine learning (AI/ML), automation, and orchestration are essential to delivering a high level of accuracy and consistency. Vendors vary in the degree of automation they have attained in services and tools. In particular, understand the following:
  - The vendor's prebuilt connectors, solutions, reference architectures, and other assets such as templates, coded functions, and policy libraries
  - Acceleration tools or solutions — for example, migration factories and cloud security guardrails specific to public cloud service providers
  - The portal that enables organizations to view and manage their multicloud/hybrid cloud security posture (Explore ease of use, self-service capabilities, support options, and ability to integrate third-party services.)
  - Talent that is knowledgeable about cloud, engineering, and security (Certifications by the hyperscalers and security partners are a useful indicator.)
- Scrutinize the core platform used in managed cloud security engagements and look for market-leading technical capabilities. Be aware of the technologies behind managed cloud security services and whether they are proprietary, partner based, or a combination. Transparency is essential in all things related to managed cloud security.
- Learn about the vendors' delivery models and the extent to which services are tailored to organizational security maturity level. Determine whether a delivery model meets buyer preferences for adoption and consumption, as well as for data residency and sovereignty requirements.
- Explore onboarding, change management, and support model (security operations centers [SOCs], cyberexperts, service-level agreements [SLAs], and so on). Some vendors organize support teams in pods or squads focused on one or more customers and/or specific cloud SP-native security controls.
- Explore pricing models. Some vendors have developed innovative approaches that go beyond established models — such as utility pricing, per-user pricing, data consumption pricing, fixed/tiered pricing, and pricing based on the number of indicators of compromise (IOCs).
- Dig into vendors' cyber-resiliency strategies — people, processes, and technology — to help contain risk as the threat landscape worsens.
- Understand the customer success model, including how and where customers are engaged and by whom — along all stages of the cloud journey.
- Ask vendors to arrange conversations with other customers in the same industry to give buyers the opportunity to discuss engagements, outcomes, and satisfaction.

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.

The vendor summary profiles in this document contain customer feedback about these core capabilities that was obtained through IDC's *Global Managed Cloud Security Services Survey*.

Deloitte

Deloitte is positioned in the Leaders category in the 2022 IDC MarketScape for worldwide managed cloud security services in the multicloud era.

Deloitte, one of the largest professional services firms in the world, operates in more than 150 countries. The firm has more than 2,500 cloud professionals with hyperscaler and cloud security certifications who are aligned with its cyberpractice. Deloitte supports several cloud service providers such as AWS, Microsoft Azure, Google Cloud, IBM Cloud, Alibaba Cloud, and Oracle.

Deloitte maintains four Global Cyber Operate Delivery Centers, 30 Cyber Operate Offices with additional local SOC capabilities, 200+ dedicated threat intelligence experts, 24 x 365 incident alerting and response, AI-enabled threat detection, and a threat library that enables threat modeling and mapping of threat actor groups to the MITRE ATT&CK framework. A proprietary threat intelligence platform ingests threat feeds from partners to supplement internal intelligence and produces reports, custom research, and external risk monitoring information.

A follow-the-sun SOC approach is available when customers do not require 24 x 7 local support and can rely on offshore SOCs. Service delivery consistency is supported by monitoring the configuration of cloud platform security standards, cloud-based SOAR tools, and cloud-based workflow management that maps vulnerabilities to assets and routes remediation and patching tickets.

Deloitte's layered approach to security includes MXDR by Deloitte, vulnerability management, data protection and privacy, endpoint protection, perimeter security, SIEM with auto-remediation, IAM controls for managing privileged access, service accounts, user life cycle, advanced authentication, and access governance through its Digital Identity solution and standard SOC2 certified processes. Solutions, tools, and playbooks that aid customers' migration include a cloud readiness assessment, a zero trust model, Deloitte Fortress for continual multicloud compliance, attack path modeling, predictive analytics, and cloud security policy orchestration.

Deloitte builds security and compliance into its Cloud Managed Services (CMS) portfolio and its OpenCloud cloud management platform, although security also is available as a standalone service bundle. Cyberautomation within the portfolio includes cloud configuration, patching, identity processes, threat detection and response, and security analytics. The platform combines cloud-native, open source, and third-party tools and Deloitte IP to enable visibility and management across customer workloads in single, multiple, and hybrid cloud deployments.

Strengths

Deloitte provides flexible models to onboard customers, along with detailed customer transition plans and numerous tools to support migration and use of native cloud security controls. A global network of talent specializes in cloud, engineering, and security. The Deloitte ecosystem includes co-development activities with cloud service providers and security vendors, as well as collaborations with government, academia, customers, and other organizations to enable innovation and orchestration.

Customers rate Deloitte highly for its breath and depth of managed cloud security capabilities, including data security and privacy management, cross-cloud operation management, threat intelligence, cloud security advisory services, and zero trust advisory services. Quality of staff is rated

highly for Deloitte, from both technical expertise and business acumen perspectives. One customer says Deloitte really understands security. Another customer mentions the staff at Deloitte is very approachable and the firm is strong in terms of stakeholder management.

Technical capabilities of the core platform used in the engagement, along with emerging technologies, also are highlighted positively by Deloitte customers. In addition, customers think highly of Deloitte's OpenCloud platform, which delivers holistic visibility and management for cloud managed services. The platform offers critical transparency and operational insights such as predictive maintenance, real-time performance, automated provisioning, and AI/ML-enabled anomaly detection to support 24 x 7 monitoring and threat hunting in cloud environments.

Challenges

Customer feedback indicates opportunities for improvement in collaboration among cross-functional teams and managing staff turnover. In addition, Deloitte should continue investments in automation used in customer engagements.

Deloitte has completed a series of cloud and cyberacquisitions as part of its portfolio expansion strategy. While these acquisitions may create integration and go-to-market challenges, Deloitte believes its custom integrator approach and robust integration methodology should minimize disruption while focused on value creation.

Consider Deloitte When

Large organizations that seek industry and business domain knowledge, a high level of senior management oversight of customer engagements, and a hybrid pricing model should consider Deloitte.

Companies that prefer to work with a partner that supports the entire cloud migration and transformation journey should evaluate Deloitte. Its pod delivery model (with multidisciplinary skills) is applied in various ways to meet customer requirements.

APPENDIX

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 shares 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.

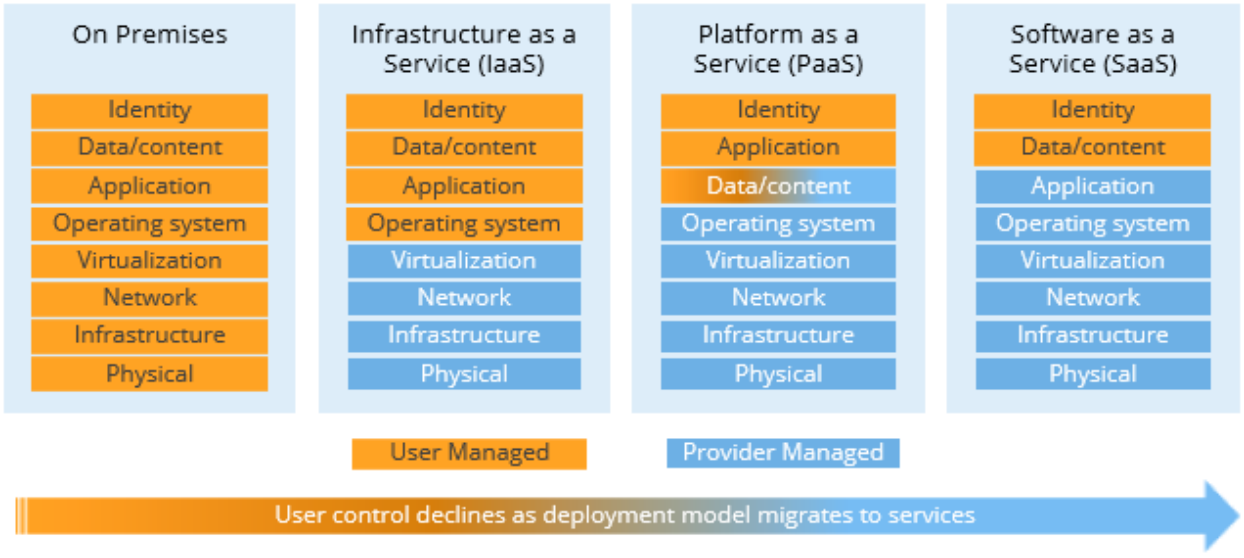
Market Definition

Multicloud/hybrid cloud is the reality for many if not most organizations today. IDC has observed that more organizations are moving toward two or three clouds for their environments. Off-premises, public, and private clouds make up the mix, depending on the sensitivity of the workload.

Managed cloud security services offer customers the ability to offload various technology and security infrastructure that would be managed by in-house staff. The managed cloud security services are services delivered solely via the cloud and managed through the cloud, with no on-premises infrastructure required. Managed cloud security services can come in the form of three types such as managed public cloud security services, managed private cloud security services, and managed multicloud security services (see Figure 3).

FIGURE 3

IDC's Shared Infrastructure Model



Source: IDC, 2022

In addition to providing security monitoring, reporting, and technical support, external service providers can provide management of intrusion detection, firewall management, oversight of the company's virtual private network, encryption management, identity access management, data security and vulnerability testing, compliance management, and so forth.

IDC defines the following core capabilities of managed cloud security services:

- **Multicloud network management,** which enables IT teams to manage network security across cloud environments, including monitoring of network resource alerts and resolution tracking
- **Cross-cloud operation management,** which monitors cloud resource configurations and routine reporting of the current state of risk levels
- **Data security and privacy management,** which allows secure data sharing across cloud providers and regions (It may include data classification, data recovery, key management, and encryption management.)
- **Identity access management,** which may be delivered as a standalone service or through solutions such as SASE
- **Secure software development,** which may include cloud code review, DevSecOps, and software supply chain management
- **Threat intelligence,** which comprises multiple internal and external sources, a threat intelligence team, a threat library, AI/ML analytics and, ideally, integration with industry-leading frameworks such as MITRE ATT&CK
- **Compliance and risk management,** which encompasses processes, templates, and regulation-specific reports
- **Detection and response for multicloud/hybrid cloud environments,** with services typically including MDR and MXDR powered by AI/ML
- **Complementary services:**
  - Cloud security advisory services that assist enterprises with cloud security assessments, plans, and implementation
  - Zero trust advisory services that assist enterprises with defining and implementing strategies to protect data and other assets with controls such as least-privileged access, Layer 7 threat prevention, and prevention of bad actor lateral movement

Security as a Service and Managed Cloud Security Services

The security-as-a-service market includes any security service that is managed remotely in the cloud for on-premises or off-premises environments. Thus security as a service may be used to secure internally hosted and managed applications and functionality as well as externally hosted and managed (cloud) applications and functionality. However, security as a service does not include managed security or any other security solution that requires the presence of on-premises hardware or software.

LEARN MORE

Related Research

- *IDC Global Managed Cloud Security Services — Buyers' Perspectives* (forthcoming)
- *Worldwide and U.S. Comprehensive Security Services Forecast, 2022-2026: Steady Growth Continues Amid Global Headwinds* (IDC #US48549022, July 2022)

- *MDR/MSS Trends - Perspectives from Tech Buyers* (IDC #US48548021, May 2022)
- *IDC's Worldwide Security Services Taxonomy, 2022* (IDC #US48548722, April 2022)

Synopsis

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

IDC defines the following core capabilities of managed cloud security services:

- **Multicloud network management,** which enables IT teams to manage network security across cloud environments, including monitoring of network resource alerts and resolution tracking
- **Cross-cloud operation management,** which monitors cloud resource configurations and routine reporting of the current state of risk levels
- **Data security and privacy management,** which allows secure data sharing across cloud providers and regions (It may include data classification, data recovery, key management, and encryption management.)
- **Identity access management,** which may be delivered as a standalone service or through solutions such as SASE
- **Secure software development,** which may include cloud code review, DevSecOps, and software supply chain management
- **Threat intelligence,** which comprises multiple internal and external sources, a threat intelligence team, a threat library, AI/ML analytics and, ideally, integration with industry-leading frameworks such as MITRE ATT&CK
- **Compliance and risk management,** which encompasses processes, templates, and regulation-specific reports
- **Detection and response for multicloud/hybrid cloud environments,** with services typically including MDR and MXDR powered by AI/ML

"The managed cloud security services market is highly dynamic and fast evolving. Cloud is often perceived or used as a change agent for companies to take an enterprisewide transformation journey. Similar thinking applies to security. Cloud requires new ways to handle challenges in terms of visibility and security policy governance. At the same time, cloud enables various facets of security to be faster and more transparent," says Cathy Huang, research director, Worldwide Security Services at IDC. "It is interesting to see that many managed cloud security services providers have developed code-defined assets or policies to enable an automated security function and drive high level of accuracy and efficacy through the use of AI/ML, automation, and orchestration."

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

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com