Gartner

Predicts 2021: Cloud and Edge Infrastructure

Published 8 December 2020

By John McArthur, Arun Chandrasekaran, Thomas Bittman, Tim Zimmerman

Predicts 2021: Cloud and Edge Infrastructure

Published 8 December 2020 - ID G00735107 - 13 min read

By Analysts John McArthur, Arun Chandrasekaran, Thomas Bittman, Tim Zimmerman

Initiatives: Cloud and Edge Infrastructure

Enterprise infrastructures continue to evolve — more cloud, more devices attaching to the network and more requirements at the edge. I&O leaders responsible for cloud and edge infrastructure must be innovative with network security, workload deployments and infrastructure extended to the edge.

Additional Perspectives

- Invest Implications: Predicts 2021: Cloud and Edge Infrastructure
  (10 December 2020)

Overview

Key Findings

- Industry surveys show internet-connected devices on enterprise networks can be hacked in as little as three minutes and breaches may take six months or more to discover.
- The current pandemic and the economic slowdown are serving as catalysts for digital innovation and adoption of cloud services, especially for use cases such as collaboration, disaster recovery, VDI and new digital services.
- Cloud providers are working with data center, micro data center and telecom providers to deploy cloud-tethered footprints closer to the edge, and to offer solutions that can be deployed on enterprise premises.

Recommendations

I&O leaders responsible for cloud and edge infrastructure should:

- Strengthen security by architecting a virtual segmentation strategy across multivendor campus networks that protects segmented and isolated devices.
- Optimize cloud management and performance by creating a cloud center of excellence to formulate best practices across workload selection, governance, operations and organizational skills.
- Future-proof your edge solution by choosing edge computing partnerships and ecosystems that can deliver a total solution over a single-vendor approach.

Strategic Planning Assumptions

Through 2023, enterprises that isolate/segment their campus network devices will experience 25% fewer successful cyberattacks.

By 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020.

By year-end 2023, 20% of installed edge computing platforms will be delivered and managed by hyperscale cloud providers, compared to less than 1% in 2020.

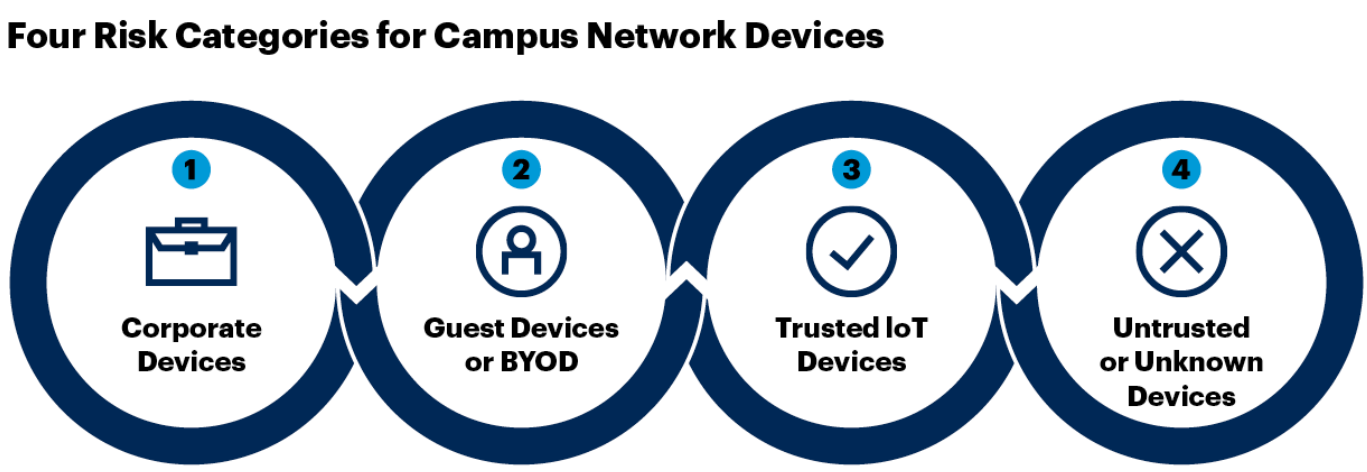
Analysis

What You Need to Know

Enterprise infrastructures are changing, with new opportunities — and new threats. This year's predictions for cloud and edge infrastructures highlight a few key trends that require infrastructure and operations leaders to take action.

Internet of Things (IoT) devices are proliferating (doubling every five years), they are connecting to the enterprise infrastructures, and there are security risks that need to be mitigated. There are at least four risk categories that should be used to determine how to segment or isolate these devices (see Figure 1).

Figure 1. Four Risk Categories for Campus Network Devices



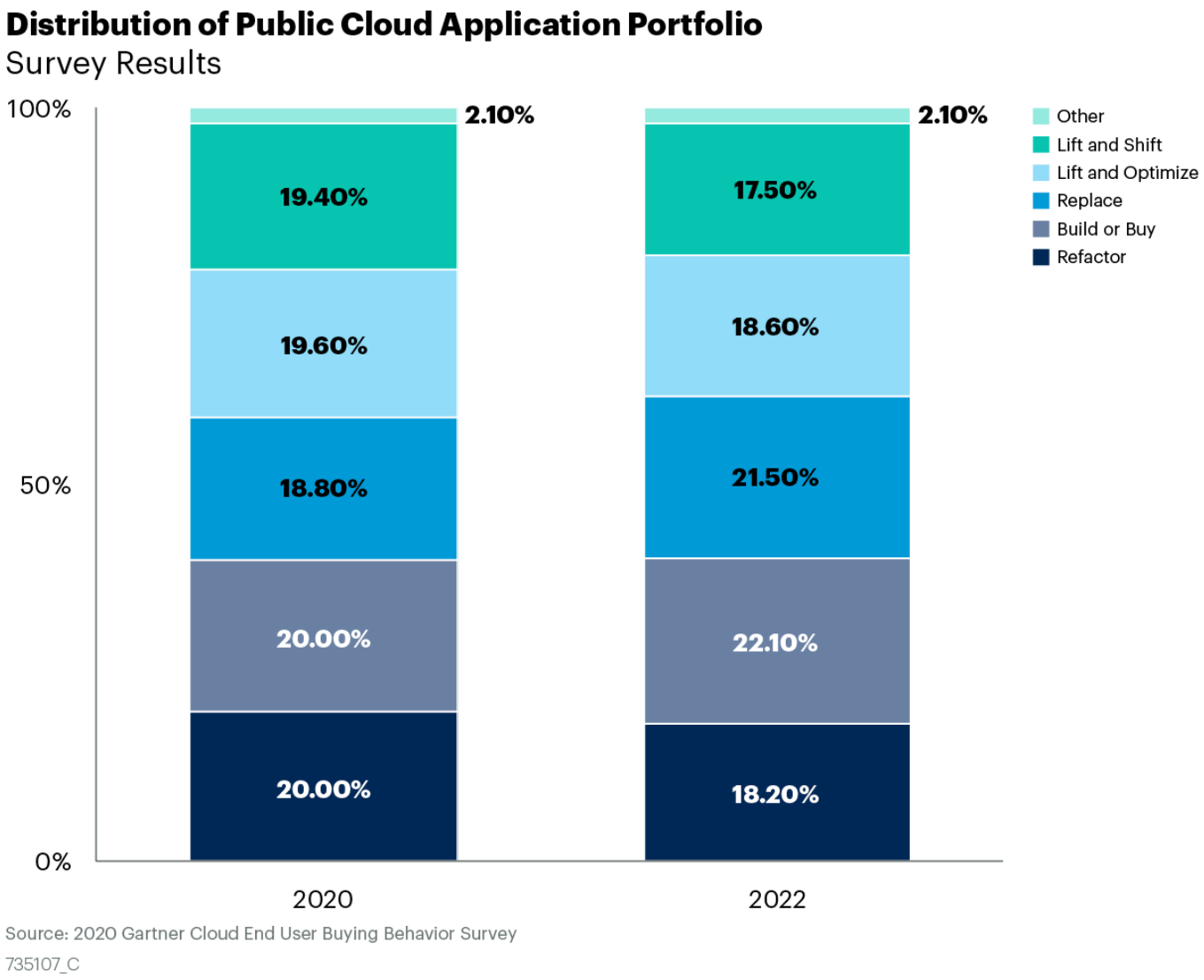
Source: Gartner
735107_C

Failure to address the growth in connected devices will cause enterprises to experience significant growth in the number of cyberattacks.

Another important trend is the growth of cloud computing as an extension of enterprise infrastructure. Infrastructure and platform services based in public cloud have attracted a mix of existing applications

(lifted and shifted, lifted and optimized, or refactored) and new applications (full application replacements, newly built, or bought). In the 2020 Gartner Cloud End-User Buying Behavior Survey, 366 respondents were asked, “What is your organization’s plan for public cloud application portfolio distribution today/in the next two years?” (see Figure 2).

Figure 2. Survey Results: Distribution of Public Cloud Application Portfolio

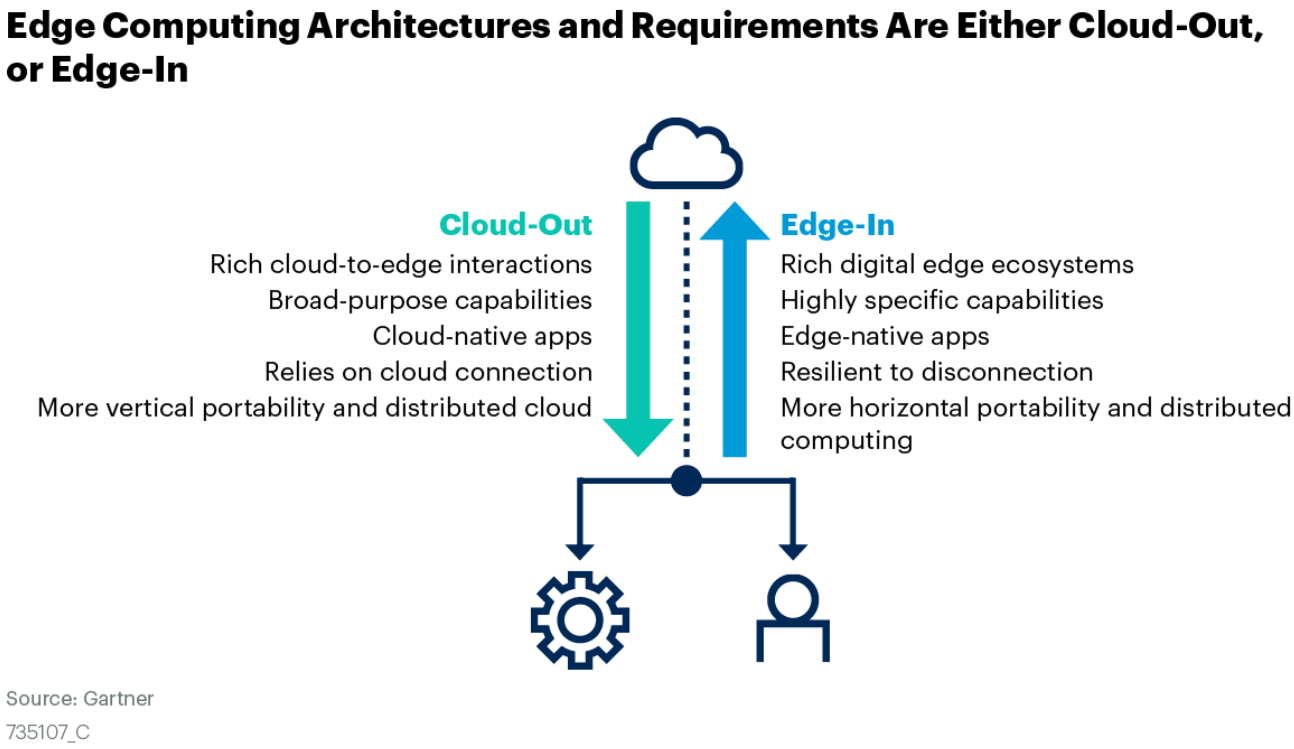


The results show a shift in portfolios toward more applications being fully replaced, built anew, or bought. While enterprise applications continue to migrate to public cloud, enterprises are becoming more cloud-native with their deployments — and public cloud has become the default for a larger percentage of new workloads.

A third trend in enterprise infrastructures is the emergence of edge computing. As the requirements become better understood, and computing and operations patterns are more fully developed, we will see more solutions delivered as “edge packages” that can be deployed across a broad set of use cases. Early deployments have been highly customized assemblages of technologies, usually very unique to a specific use case — but always complemented by centralized cloud services. As demand has grown,

vendors have been starting to build offerings that can be multipurpose, and they are coming from two distinct directions (see Figure 3).

Figure 3. Edge Computing Architectures and Requirements Are Either Cloud-Out or Edge-In



Early deployments are highly edge-in (i.e., from the edge into the cloud) — from industrial IoT and edge computing replacing or augmenting OT, to net new edge use cases. Hyperscale cloud providers have been developing solutions to distribute their cloud capabilities and services closer to the edge (and working in conjunction with telecom providers). There is value in both in the highly diverse world of edge computing, and strategies should reflect that.

Strategic Planning Assumptions

Strategic Planning Assumption: Through 2023, enterprises that isolate/segment their campus network devices will experience 25% fewer successful cyberattacks.

Analysis by: Tim Zimmerman

Key Findings:

- Gartner inquiry confirms that IT organizations find IoT devices on their network that they did not install, secure or manage.
- Industry surveys show internet-connected devices on enterprise networks can be hacked in as little as three minutes and breaches may take six months or more to discover.

- The lack of standards for isolating or segmenting devices on multivendor campus networks makes deploying a strategic framework for all devices very difficult.

Market Implication:

Gartner's IoT forecast is showing that, by 2029, more than 15 billion IoT devices will attach to the enterprise infrastructure. The convergence of building-automation and lines-of-business devices onto the network means that organizations will need to coordinate when and how these devices will be connected. When video surveillance cameras and HVAC, as well as line-of-business devices like medical devices or point of sale, are vulnerable to some kind of security breach, the door to the network is increasingly open to cyberattacks. A total of 76% of U.S. businesses have experienced a cyberattack in the past year, the cost of damage can be over $1 million.

IT organizations must work to bring the entire organization together to agree on a common governance for device connectivity or risk losing control of being able to secure the network. Defining a policy where all parties agree to how devices will be tested and added to the network is a huge but necessary first step. Separating devices into logical segments or groups is the next component of the strategy. Virtual segmentation must replace virtual LANs (VLANs) when devices must access the internet to reach cloud-based applications. This functionality is now offered by every major enterprise networking vendor, but must be implemented as part of a cohesive enterprise strategy.

Recommendations:

- Create a device certification process for all devices, written by a cross-functional team, that must be passed before any device is connected to the enterprise network.
- Segment or isolate devices by creating and implementing a minimum of four device risk categories.
- Strengthen security by architecting a virtual segmentation strategy across multivendor campus networks that protects segmented and isolated devices.

Related Research:

Segmentation or Isolation: Implementing Best Practices for Connecting 'All' Devices

Critical Capabilities for Wired and Wireless LAN Access Infrastructure

IoT Solutions Can't Be Trusted and Must Be Separated From the Enterprise Network to Reduce Risk

Designing and Implementing a Ransomware Defense Architecture

Don't Be the Next Victim: Defense Through the Ransomware Life Cycle

Strategic Planning Assumption: By 2023, 40% of all enterprise workloads will be deployed in cloud infrastructure and platform services, up from 20% in 2020.

Analysis by: Arun Chandrasekaran

Key Findings:

- The rapid pace of innovation in cloud infrastructure and platform services is making them the de facto platforms for not only new digital services but also for transforming traditional workloads.
- Distributed cloud services, which decouple cloud services from a centralized physical location, can potentially address client concerns around operational control, performance and geographical location of the services, providing a new growth engine for hyperscale providers in the next five years.
- The current pandemic and the economic slowdown are serving as catalysts for digital innovation and adoption of cloud services, especially for use cases such as collaboration, disaster recovery, virtual desktop infrastructure (VDI) and new digital services.

Market Implication:

Public cloud is becoming the epicenter of innovation in infrastructure and platform services. In the past decade, organizations have shed their initial reluctance to take advantage of these innovative services. In the 2020 Gartner Cloud End-User Buying Behavior Survey, 96% of respondents indicated that their organization plans to maintain or increase its IT spending on cloud computing in the next 12 months. [1] IT leaders need to formulate a cohesive cloud strategy that is expansive and forward-looking to fully reap the business value of cloud. Such a cloud strategy should encompass foundational elements (see The Cloud Strategy Cookbook, 2019), new industry developments such as distributed cloud services, newer application architectures and anywhere cloud operations.

Distributed cloud enables organizations to deploy cloud services close to the users or where the data is being generated to ensure data privacy or to boost performance, while abstracting the maintenance and governance of the services back to the public cloud providers. The advent of distributed cloud services will be a key inflection point, driving further growth in workload migration for use cases where data privacy, operational control and performance were major constraints in the past.

Cloud innovation around microservices runtime infrastructure (containers, APIs, serverless functions etc.), continuous integration/continuous delivery (CI/CD) and other automation tools is making cloud the preferred platform for a vast majority of new application development.

The current pandemic has resulted in a recalibration of cloud strategies, where use cases such as collaboration, mobility and virtual desktops are rapidly moving to the cloud to enable a distributed workforce to work together in a more secure, scalable and reliable manner. In addition, disaster recovery

and scale-out applications that can benefit from the elasticity and rapid provisioning capabilities of cloud are also seen as high priority for cloud migration.

Recommendations:

- Enable effective collaboration across your business ecosystem and deliver resilient services by leveraging cloud services amid this pandemic.
- Revise your cloud strategy and migration timeline by accommodating new industry developments in the areas of cloud-native platforms and distributed cloud services.
- Create a cloud center of excellence to formulate best practices across workload selection, governance, operations and organizational skills and know-how.

Related Research:

Top 10 Trends in PaaS and Platform Innovation, 2020

The Future of Cloud in 2025: From Technology to Innovation

A CIO's Guide to Serverless Computing

Innovation Insight for the Cloud Center of Excellence

Strategic Planning Assumption: By year-end 2023, 20% of installed edge computing platforms will be delivered and managed by hyperscale cloud providers, compared to less than 1% in 2020.

Analysis by: Thomas J. Bittman

Key Findings:

- Edge computing will be delivered by software and hardware located closer to the physical edge — where data is generated and consumed, and where interactions are taking place — usually outside of data centers.
- Cloud providers are working with data center, micro data center and telecom providers to deploy cloud-tethered offerings closer to the edge, and to offer solutions that can be deployed on enterprise premises.
- Edge computing requirements are defined by use cases, and specialized hardware and software may be needed.

Market Implication:

Edge computing tackles a growing demand to address lower latency, process the growing amount of data on the edge, and support resilience to network disconnection. Cloud providers already work with content delivery networks (CDNs) and colocation providers to address this to some extent. However, emerging edge requirements are pushing the need for compute in or near fixed locations such as stores, offices, plants, and distribution facilities in both urban and rural locations and in mobile use cases such as planes or trucks.

Edge computing platforms are software and hardware that enable a zero-touch, secure, distributed computing architecture for applications and data processing at or near the edge.

Distributed cloud is an emerging trend for cloud providers to expand their services to new modes of deployment, including software and possibly hardware deployed wherever a customer needs to deploy it, but still managed and provisioned using the cloud providers' tools and interfaces. Cloud providers have also established new partnerships with telecom providers to offer edge computing capabilities together with 5G services.

Given the challenges of managing edge locations, enterprises are highly motivated to use edge-as-a-service solutions when feasible. However, edge requirements can be highly diverse and are difficult to address with general-purpose solutions. Examples include predictive maintenance in industrial equipment (leveraging embedded compute capability), assembly line use cases that require response within hundreds of microseconds, or extremely lightweight and low-power mobile edge computing. In many situations, organizations will need to seek customized solutions from edge solution suppliers with deep industry knowledge.

Edge computing complements cloud computing. Through centralized, cloud-hosted management and a growing portfolio of common cloud and edge capabilities, hyperscale cloud providers are in an excellent position to address a broader range of requirements for computing closer to the edge. However, there will be use cases that have a large enough market for highly specific edge solutions. Hyperscale cloud providers will focus on partnerships, rich integration capabilities, cloud-based management and cloud-based functional services for a wide range of diverse edge computing solutions. In the end, edge computing will be delivered by ecosystems of partners that vary across use cases. In some cases, the cloud provider manages and delivers the edge computing software and, possibly, hardware platforms. In many others, diverse edge computing platforms will be managed and delivered by others but integrate tightly with cloud providers in a complementary way.

Edge computing solutions will shake out over the next five years. Over time, ideal niche solutions with limited market and profit opportunity for the suppliers will be replaced by more general-purpose solutions that have greater market opportunity and more sustainable business models. Edge computing is broad enough to support many submarkets, but it will evolve from today's thousands of often custom patterns to dozens of viable patterns, and cloud providers will take a larger and larger role.

Recommendations:

- Prioritize a distributed cloud-based solution as the default, and only choose otherwise when use cases demand.
- Determine edge computing architecture and topology based on use-case requirements — but balanced with extensibility and leverage.
- Future-proof your edge solution by choosing edge computing partnerships and ecosystems that can deliver a total solution over a single-vendor approach.

Related Research:

4 Steps to Successful Edge Computing Deployments

How to Overcome Four Major Challenges in Edge Computing

Why and How I&O Should Lead Edge Computing

Top 10 Strategic Technology Trends for 2020: Distributed Cloud

How to Bring the Public Cloud On-Premises With AWS Outposts, Azure Stack and Google Anthos

Market Trends: How TSPs Are Preparing 5G Solutions With Cloud Edge Providers

A Look Back

In response to your requests, we are taking a look back at some key predictions from previous years. We have intentionally selected predictions from opposite ends of the scale — one where we were wholly or largely on target, as well as one we missed.

This topic area is too new to have on-target or missed predictions.

Evidence

[1] **2020 Gartner Cloud End-User Buying Behavior** study was conducted to understand how technology leaders approach buying, renewing, and using cloud technology.

The research was conducted online from July 2020 through August 2020 among 850 respondents from midsize and larger ($100 million plus in revenue) organizations in the U.S., Canada, the U.K., Germany, Australia and India. Industries surveyed include energy, financial services, government, healthcare, insurance, manufacturing, retail and utilities. All organizations were required to currently have cloud deployed.

Respondents are involved, either as a decision maker or decision advisor, in new purchases, contract renewals, or contract reviews for one of the following cloud types in the past three years: public cloud

infrastructure (IaaS), public cloud platform (PaaS), public cloud software (SaaS), private cloud infrastructure, hybrid cloud infrastructure or multicloud infrastructure. Respondents were also required to work in IT-focused roles, with a small subset of procurement respondents.

The study was developed collaboratively by Gartner Analysts and the Primary Research Team.

Disclaimer: Results of this study do not represent global findings or the market as a whole but reflect sentiment of the respondents and companies surveyed.

Recommended by the Authors

Innovation Insight for Digital Twin Tools for Enterprise Campus Networks

Differences Between AWS Outposts, Google Anthos, Microsoft Azure Stack and Azure Arc for Hybrid Cloud

Choose the Right Approach to Modernize Your Legacy Systems

Learn more. Dig deep. Stay ahead.

Changing business and technical requirements, including the shift toward digital business and automation, require I&O leaders to evolve and advance their skills to stay relevant. I&O leaders must implement innovative strategies that embrace technology innovations to stay ahead and impact business outcomes.

Gartner insights, advice and tools help infrastructure and operations leaders find solutions to their most pressing challenges and help them learn about the latest developments that matter most to their role.

Learn more: gartner.com/en/information-technology/role/infrastructure-operations-leaders

Become a Client

Get access to this level of insight all year long — plus contextualized support for your strategic priorities — by becoming a client.

gartner.com/en/become-a-client

U.S.: 1 800 213 4848

International: +44 (0) 3331 306 809

About Gartner

Gartner is the world's leading research and advisory company and a member of the S&P 500. We equip business leaders with indispensable insights, advice and tools to achieve their mission-critical priorities today and build the successful organizations of tomorrow.

Our unmatched combination of expert-led, practitioner-sourced and data-driven research steers clients toward the right decisions on the issues that matter most. We are a trusted advisor and an objective resource for more than 14,000 enterprises in more than 100 countries — across all major functions, in every industry and enterprise size.

To learn more about how we help decision makers fuel the future of business, visit gartner.com.

Gartner®