Hype Cycle for XaaS, 2023

Published 20 July 2023 - ID G00791200 - 97 min read

By Analyst(s): Jason Donham, Philip Dawson

Initiatives: I&O Platforms

> Everything as a service is a services delivery model that drives agility, operational efficiency, ease of management and cost optimization through strategic migration of services and projects into XaaS. I&O leaders should use this Hype Cycle to prioritize resources and investment for their needs.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Strategic Planning Assumptions

By 2027, migration to XaaS-based application offerings will result in a 35% decline in enterprise-owned data center capacity, when compared to 2022 levels.

By 2027, 35% of data center infrastructure will be managed through a cloud-based control plane, up from less than 10% in 2022.

By 2026, I&O will spend more than half its budget working with technology the organization does not directly own.

Analysis

What You Need to Know

The drive toward cloud architecture and away from the traditional data center is accelerating. I&O leaders that need innovative new ways to consume cloud services in an operating expenditure (opex) model can look to everything as a service (XaaS) as a potential solution. XaaS can be used to replace on-premises or cloud infrastructure and services, especially where these can be bundled together. Once business objectives are fully understood, I&O leaders can align costs of consumption models with objectives by comparing data center refresh to equivalent services.

A mix of on-premises and cloud services is often the optimum design for businesses today. I&O leaders can embrace consumption and subscription services where they are most efficiently utilized and still leverage the investments already made in data center hardware and software until the next refresh cycle arrives and the evaluation process begins anew. Future data center architecture is defined by services targeted toward specific functions bound by tightly defined service-level agreements (SLAs), with little to no overlap between services.

XaaS is also used to temporarily fill the skills gaps in organizations where advanced technology is adopted but IT administrators do not yet have the skills to operate the systems efficiently.

The Hype Cycle

This research describes 27 of the most-hyped innovations in the XaaS market. For each technology, we define and analyze the value to enterprises, the level of adoption, and the anticipated rate of future growth. I&O leaders should use this research to determine whether and/or when to invest in these innovations.

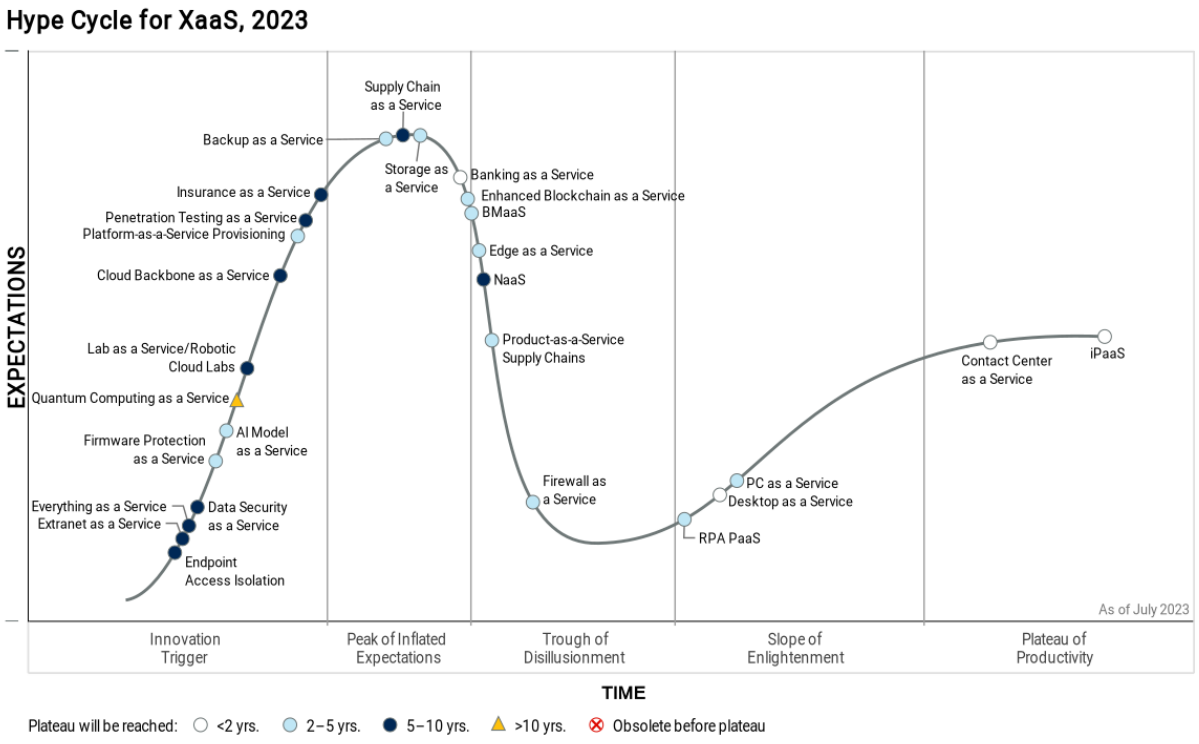
Peak Hype: Storage as a service (STaaS) is at the peak of hype. Vendors are bringing new products and capabilities to market while businesses are demanding elastic storage systems to meet modern application demands.

Fast Movers: Backup as a service (BaaS) is moving quickly toward the plateau due to rapidly developing capabilities among multiple vendors in the enterprise backup and recovery market. Customer interest is on the rise for these solutions to protect SaaS applications and cloud-native workloads, including infrastructure as a service (IaaS) and platform as a service (PaaS).

Slow Movers: Quantum computing as a service (QCaaS) is moving slowly, partly due to lack of standardization across software and development stacks, relatively lower value returns from quantum investments in the near term, and lack of customer maturity to take advantage of a continuously evolving ecosystem. Hype is increasing as these systems move slowly toward deployment in realistic use cases.

In the Trough: Firewall as a service (FWaaS) is approaching the bottom of the trough as enterprises rationalize the narrow requirement for edge firewall hardware refreshes with FWaaS options. This is primarily for thin branch use cases against broader security service edge (SSE) requirements or more comprehensive secure access service edge (SASE) transformations.

Figure 1: Hype Cycle for XaaS, 2023



The Priority Matrix

The Priority Matrix maps the benefit rating for each technology against the amount of time required to reach the beginning of mainstream adoption. This alternative perspective can help users determine how to prioritize their services investments.

Transformational technologies delivered as services have the potential to affect how rapidly changing, specialized compute infrastructure is made available to customers at significantly lower risk than an upfront capital expenditure (capex) purchase. PaaS provisioning gives clients the ability to deploy full stack applications without purchasing any underlying hardware infrastructure or software. I&O leaders should begin long-term planning for the impact these technologies will have.

High benefit services such as XaaS, STaaS, BMaaS and banking as a service offer new ways to store, process and protect data. Security services such as firmware protection as a service (FPaaS) and data security as a service (DSaaS) focus on delivering enhanced security features that would traditionally require advanced skill sets plus hardware and software.

Desktop as a service and PCaaS will continue to show significant benefits to end users and IT organizations by delivering a secure and scalable end-user computing solution in a consumption model.

Table 1: Priority Matrix for XaaS, 2023

(Enlarged table in Appendix)

Benefit ↓	Years to Mainstream Adoption: Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational		Platform-as-a-Service Provisioning		
High	Banking as a Service Desktop as a Service iPaaS	AI Model as a Service BMaaS Edge as a Service Enhanced Blockchain as a Service Firmware Protection as a Service PC as a Service Product-as-a-Service Supply Chains Storage as a Service	Data Security as a Service Everything as a Service Supply Chain as a Service	
Moderate	Contact Center as a Service	Backup as a Service Firewall as a Service RPA PaaS	Endpoint Access Isolation Insurance as a Service Lab as a Service/Robotic Cloud Labs Penetration Testing as a Service	Quantum Computing as a Service
Low			Cloud Backbone as a Service Extranet as a Service NaaS	

Source: Gartner (July 2023)

On the Rise

Endpoint Access Isolation

Analysis By: Chris Silva, Stuart Downes

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Endpoint access isolation (formerly VDI/DaaS endpoint security) facilitates secure access to applications, VDI/DaaS environments, and data using local apps that isolate the session data from the device. Deployed as an agent, browser-based app or extension, the technology extends access to external PCs where a traditional VPN or virtualization client software can't be used. Local controls include session-hijacking protection, keylogging and screen-capture prevention, and local user verification.

Why This Is Important

Endpoint access isolation is client-side software that can offer use-case-specific isolation of the client device when interacting with workplace apps and data. The technology can be delivered as a dedicated secure access agent, browser-based-app or extension isolating the systems being accessed from local vulnerabilities. Endpoint access isolation tools differ from traditional access clients by adding active prevention and detection features to posturing and profiling.

Business Impact

Traditional remote access tools like classic VPN can profile a device but can't actively neutralize local threats. As organizations rethink allowing access to SaaS apps via any browser, from any device, this technology can offer a more secure way to reach these apps. This technology allows organizations to simplify both the standard IT "stack" and its deployment to end users for remote access. This is particularly important as hybrid working remains a day-to-day reality for most organizations.

Drivers

- Trading physical hardware for virtual desktop infrastructure (VDI) and desktop as a service (DaaS) sessions for contractors and partners won't address the underlying security issues of the local machine — a viable vector for credential and IP theft.

- There has been strong investment in enterprise browser solutions — one manifestation of endpoint access isolation.
- There is a trend of adding a layer of security through enforcing consistent browser configuration and control for any user accessing productivity apps and company data from an unmanaged PC.
- Methods to better secure these sessions relied on proxy- or private-network-based tools. These impact performance and users may not be authorized or equipped to install or configure them.
- There is a need for detailed session monitoring, including the ability to monitor users in front of a device camera or to use camera data to validate that users require these tools.

Obstacles

- Despite their low user appeal and complexity, extending the life of traditional, VPN-based access is a low-cost option in comparison to adding endpoint access isolation technology.
- A mix of endpoint access isolation methods may be required to meet all use cases, such as a browser-based app for employees and a secure access client for contractors.
- Some browser-centric tools may face competition from security service edge (SSE) vendors touting similar capabilities, or from browser vendors that are building or incorporating similar functionality.
- Labor and privacy regulations render the most obtrusive functions of some tools untenable — for example, camera surveillance in the home.
- Organizations may be put off by the cost of adding VDI- and DaaS-specific security tools, in addition to the cost of the underlying infrastructure. This is exacerbated by an environment in which the trend is toward consolidating security tools.

User Recommendations

- Specify control gaps that app-level security or VDI/DaaS tools cannot solve natively (for example, copy/paste restrictions). This will help identify the class of solution needed.

- Faithfully replicate existing security posture used on physical endpoints in the VDI or DaaS environment before considering an additional VDI or DaaS endpoint security tool.
- In addition to these baseline controls, identify where to apply use-case-specific controls such as biometric identity verification, and when you need to validate the physical identity of specific users.
- When considering point-solutions, compare their efficacy and their cost to traditional alternatives like VPN.
- Coordinate with legal and human capital teams to examine regulatory privacy obligations when using biometric authentication or camera-based user monitoring.

Sample Vendors

Citrix Systems; Island; Rapid7 (Minerva Labs); SessionGuardian; SentryBay; Talon; ThinScale

Gartner Recommended Reading

Emerging Tech: Security — The Future of Enterprise Browsers

Cool Vendors in Hybrid Work Security

Everything as a Service

Analysis By: Jason Donham, Philip Dawson

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Definition:

Everything as a service (XaaS) as a Hype Cycle innovation encapsulates the whole umbrella services delivery program that drives agility, operational efficiency, ease of management and cost optimization through strategic migration of services and projects into XaaS.

Why This Is Important

Organizations can free themselves from the commitment of a long-term investment in infrastructure by adopting the XaaS model. IT leaders have never had more data center infrastructure deployment choices than they do today. Traditional on-premises infrastructure has given way to the hybrid platform and cloud operating model, which in turn has increased complexity and resulted in myriad architecture choices. XaaS drives and packages the portfolio of services.

Business Impact

Business objectives are the driver behind any move toward the XaaS model. Agility, operational efficiency, ease of management and cost optimization are four objectives that are directly addressed by strategic migration of services to XaaS. In-house talent and service providers will assist in the design of a horizontal services model to meet the needs of the organization.

Drivers

- The gradual shifting of the control plane from on-premises to cloud-based, along with increasing migration to SaaS, is driving a reduction in traditional data center infrastructure footprints.
- XaaS is the bundling together of cloud computing services to create an economical, easy-to-consume product for hybrid cloud environments. It is the result of the disaggregation of traditional IT projects into components, domains and services that are then bundled together for consumption.
- Organizations are seeking to establish new predictable cost and consumption models. This is in contrast to vendors who are rapidly moving toward XaaS in an effort to provide as many services as possible to customers.
- Another vendor-offered XaaS solution to the supply chain issues has been the use of consumption-based pricing models. In these models, capacity is installed and managed by the vendor and then paid for when actually consumed — unlike traditional procurement models.

Obstacles

- XaaS only temporarily fills the skills gap in organizations where advanced technology is adopted and IT administrators do not have the skills to operate the systems efficiently.
- Long-term commitments to enterprise-owned data center capacity may limit flexibility. Moreover, migrating business-critical workloads to SaaS- and XaaS-based offerings will result in large, incremental reductions in the requirement for application modernization and transformation.
- Hardware vendors who are not unified in their approaches and offerings are attempting to layer cloudlike platform solutions onto their infrastructure. Application and platform vendors are offering distributed platforms that focus on the integration of infrastructure as a service (IaaS), platform as a service (PaaS) and/or SaaS.
- Migrating applications into a services model is complex. Some workloads are cloud-ready or currently running in a public cloud, so applications need to be redefined in order to operate in a new services infrastructure framework.

User Recommendations

- Migrate legacy applications not suited for cloud migration to on-premises consumption-based infrastructure. This brings cloudlike XaaS operating model benefits to legacy workloads that are otherwise incompatible with public cloud computing.
- Implement a mix of XaaS and on-premises consumption solutions. These solutions are billed together in an opex model as consumption-based services.
- Move beyond the traditional limitations of purchase, ownership and depreciation by expanding the range of possible XaaS consumption options for DC infrastructure replacement.
- Prepare for increasing variability and spend as a result of XaaS and consumption-based costs for virtual infrastructure.
- Adopt The Gartner Framework for Public Cloud Financial Management best practices and integrate with existing expense management tooling.

Sample Vendors

Amazon Web Services (AWS); Cisco; Dell; Google; Hewlett Packard Enterprise (HPE); IBM; Lenovo; Microsoft; Oracle

Gartner Recommended Reading

Predicts 2023: XaaS Is Transforming Data Center Infrastructure

How Do I Plan for Migrating My Data Center Infrastructure Into an XaaS Model?

Beyond FinOps: The Gartner Framework for Public Cloud Financial Management

Extranet as a Service

Analysis By: Andrew Lerner

Benefit Rating: Low

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

ExtranetaaS is a networking software offering that delivers extranet as a service. An extranet is a logical network zone that connects multiple independent parties together, typically under different administrative domains, often with diverse requirements. These are sometimes also referred to as B2B networks.

Why This Is Important

ExtranetaaS can help accelerate the sharing of information between partners using cloud services. Although extranets have been around since the 1980s (and the term extranet has been in use since 1995), ExtranetaaS simplifies the ability to set up and secure operation of an extranet in the modern era, as enterprises increasingly use public cloud and SaaS services.

Business Impact

Extranets are a way for enterprises, partners, customers and other outside parties to access data and systems resident on a network. It allows these parties to connect and exchange needed information such as application components or financial transactions, and is helpful in connecting independent parties with common interests. An example is within the financial services industry where local connectivity between regulatory agencies, stock exchanges, market data companies and trade clearing is often required.

Drivers

- Traditionally, extranets were established in data centers, nearby applications and data, using dedicated circuits or IPsec VPN. As organizations are migrating applications to the public cloud and SaaS, it is causing them to rethink their existing extranet approaches.
- The native public cloud providers don't offer robust advanced networking configurations to support complex extranet connectivity scenarios, driving enterprises to entertain ExtranetaaS solutions.
- There is a desire to simplify and replace physical infrastructure, including routers, firewalls and VPN appliances, with software with solutions that are more API- and software-oriented.
- There is also a desire to remove expensive dedicated lines such as MPLS or dedicated broadband.
- Smaller and startup network vendors are aggressively targeting enterprises to help them solve the technical and security challenges as organizations migrate their applications to cloud services.

Obstacles

- ExtranetaaS is a new and unknown technology to most enterprises.
- Extranets often support mission-critical environments that lead to a desire for moderate incremental change. This is in contrast to a shift to ExtranetaaS, which entails a software-only aaS delivery from lesser-known vendors.
- The public cloud providers' native capabilities are good enough for some extranet use cases.
- Organizations can use colocation in cloud data centers to address the challenge of getting the services closer to public cloud, SaaS and partner services without using ExtranetaaS.
- Most enterprise network teams take a "set it and forget it" perspective toward extranet deployments, preferring not to rearchitect the entire deployment. This drives moderate incremental modernization of existing extranets versus conversion to ExtranetaaS.
- The ROI of ExtranetaaS is unproven.
- The supply of vendor solutions is immature as many of the vendors focused on this technology are smaller companies that are unproven.

User Recommendations

- Investigate ExtranetaaS if using the native cloud provider constructs doesn't support your B2B networking requirements.
- Look to ExtranetaaS if you're migrating an existing on-premises, hardware-based extranet or B2B network to a public cloud environment.
- Shortlist ExtranetaaS offerings as an option for connecting to a large number of customers' data in a secure fashion.

Sample Vendors

Alkira; Graphiant; Trustgrid

Gartner Recommended Reading

Market Guide for Multicloud Networking Software

Data Security as a Service

Analysis By: Joerg Fritsch, Brian Lowans

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Data security as a service (DSaaS) provides data security and protection capabilities as APIs. Organizations hand over their data to the service provider, which protects, transforms and shares it back to them or with third parties, while achieving the required compliance and secrecy goals.

Why This Is Important

With the exception of payment processing, data security controls are generally managed and applied by the end-user organizations directly. Data security as a service (DSaaS) provides cloud-based, automated data security and protection capabilities such as encryption and masking. Data security and protection provided by cloud-based services is a paradigm change applying the appropriate controls for multiple use cases, ecosystem partners or jurisdictions in a scalable and flexible model with impressive performance.

Business Impact

DSaaS makes complex or expensive data security controls accessible to mainstream organizations. It enables clients to shorten the deployment times of data security controls, bringing them into a position to match the speed of cloud and DevOps initiatives. It achieves this by making the required data security controls and data transformations readily available through, for example, cloud-based APIs. Customers can, in theory, start right away, without the need for in-depth expertise.

Drivers

- Data security controls and data security architectures are frequently complex, and the customer is loaded with both hardware and software — putting thorough, scalable and agile data security out of reach of most organizations. At the same time, most organizations must rearchitect data security controls to balance privacy regulations and a constantly evolving threat landscape with an increased need to share data internally and externally. For example, this may be required for artificial intelligence and machine learning use cases, or monetization of data with ever-changing ecosystem partners. This tension will lead to accelerated adoption of DSaaS.
- Startup DSaaS vendors have new, proprietary intellectual property that could potentially mitigate lack of trust in the DSaaS provider. Alternatively, selected DSaaS are using privacy-enhancing computation to achieve this.
- Mature clients believe that if data can flow securely among individuals, organizations and governments, wiser decisions can be made and better outcomes can be delivered, both for business and society as a whole. However, an increased amount of data-related regulations and associated legal, security and privacy risks are blocking this data sharing. DSaaS will be instrumental in solving this challenge.

Obstacles

- Organizations involved with data security are often tentative toward cloud and SaaS adoption. Data security controls (for example, encryption and tokenization) applied on-premises before load are seen as compensation for a lack of trust in the cloud service provider. However, it is exactly these controls that DSaaS delivers as cloud-based services.
- Companies may refrain from DSaaS adoption if the required data security controls cannot fully be matched with DSaaS offerings. DSaaS solutions that exclude certain data types represent a common limitation.
- Privacy regulation uncertainty for controls that are used to secure personal data may significantly delay adoption of DSaaS in some geographies.
- DSaaS offerings are not interoperable. Each assumes to be the authority for its data. At a minimum, vendors will need interoperable capabilities to support external data sharing between customers that do not use the same DSaaS.
- Current DSaaS offerings focus on data encryption, data tokenization, data masking and sharing use cases. They do not include behavioral-based controls and authorization.

User Recommendations

- Validate if the integration approaches offered by DSaaS (e.g., API-based approaches and proprietary connectors or agents) are viable for your environments and will lead to the desired user experience.
- Question and plan for DSaaS constraints like API request limits, delivered event limits, network latency and storage quotas.
- Ensure the DSaaS provider's approach is compliant with your applicable privacy regulations. Question the security practices and posture of the DSaaS (for example, use shared assessments and certifications such as ISO 27001 to aid in evaluation).

Sample Vendors

Basis Theory; Google; InCountry; Inpher; Skyflow; Spring Labs; VectorZero; Very Good Security

Gartner Recommended Reading

The State of Privacy and Personal Data Protection, 2020-2022

AI Model as a Service

Analysis By: Rajesh Kandaswamy

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

"AI Model as a Service" is an AI-based model offered as a consumable service by cloud providers. The underlying AI models are from the cloud providers themselves, other tech companies or open-source initiatives. As foundation models and other AI models proliferate, cloud providers seek to offer such models to their clients. This includes both direct access to pretrained models and the ability to fine-tune such models for custom use.

Why This Is Important

Models are key building blocks in artificial intelligence. They vary in purpose and technique. A subset of AI models such as the foundation models (e.g., large language models such as GPT-3.5, which powers ChatGPT, and PaLM 2, which powers Bard) are pretrained on a large corpus of data using extensive computing resources. These models have a variety of uses, but are prohibitively expensive for most enterprises to train and manage. Cloud providers have the infrastructure and capital to invest in and offer such AI model as a service offerings.

Business Impact

A variety of AI model "as a service" offerings will emerge from cloud providers, providing an easy entry point for most enterprises to leverage AI through pre-trained models, fine-tuning such models or integrating them with other applications. The scope for where AI model as a service can be used is vast and includes:

- Technical tasks such as entity extraction, image classification and code generation
- Business tasks such as marketing content generation, financial application and scientific research

Drivers

Few underlying drivers caused the emergence of AI model as a service and will propel its growth further:

- The growing capabilities of foundational models are expanding their potential across a variety of horizontal and vertical applications for companies of all sizes and kinds. This leads to a proliferation of models from many sources, including the cloud providers themselves. This proliferation makes it hard for customers to invest — an opportunity that cloud providers are only eager to capture.
- The use of GenAI in technology products and business is poised to grow, but the costs of utilizing the models are likely to become a serious concern for most businesses. Cloud economies of scale promise users optimized efficiencies and will increase their use.
- Beyond foundational models, AI tooling and nonfoundational models continue to grow. Cloud providers are investing in these complementary services to capture as much AI revenue as possible through these investments.
- There has been significant investment in startups that are leveraging AI capabilities in their own technical and business offerings, directly or through partnerships. These startups typically do not possess the capital or resources to manage their own infrastructure and rely on cloud providers for models and other AI services.
- Enterprises have been shifting large chunks of their IT to cloud providers over the past few years and are operationally ready to use cloud-based services in many aspects of their IT. Such enterprises have a cloud-first approach for most technology investments and will apply the same for their AI investments.
- Automated agents driven by generative AI can propel growth as enterprises start to leverage other models as part of their processes and workflows.

Obstacles

Although AI model as a service plays a key role in the growth of AI in enterprises, a good part of its growth is predicated on the growth of generative AI itself. These obstacles can hinder growth:

- Many solutions, especially foundation models, still suffer from inaccuracies, hallucinations, bias and lack of explainability.

- Model security, data privacy, IP issues due to the data models are trained on, and other areas are murky.
- Lack of standards and incompatibilities between various models can inhibit growth.
- The use of AI-based models is still fairly new. AI-based models do not always easily fit in within today's products, processes and services. Maximizing the use of AI demands rethinking of processes or even the advent of new business and operating models. This shift is beginning, but may take years due to a few reasons. These reasons include maturity of technologies, the need for new processes and business models, and a delay as older assets are fully depreciated.

User Recommendations

- Evaluate different offerings for a given need rather than defaulting to your current cloud provider's recommendations.
- Ensure that you think strategically (i.e., prepare for potentially transformative changes), but act tactically (i.e., experiment, but make no long-term commitments constraining future change in a fast-moving space).
- Develop a bimodal strategy in what services your IT teams can use. One strategy should allow for faster experimentation with a variety of models, but with restricted use of data in sandboxes. The other should be geared toward wider enterprise use with more controls and robustness.
- Perform a detailed analysis of the security, privacy, accuracy, explainability and IP protections and involve internal compliance, security and legal teams.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google; Hugging Face; IBM; Microsoft; OpenAI; Oracle

Gartner Recommended Reading

Quick Answer: What is GPT-4?

Magic Quadrant for Cloud AI Developer Services

Quantum Computing as a Service

Analysis By: Chirag Dekate, Mark Horvath, Matthew Brisse

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Quantum computing as a service (QCaaS) provides enterprises with access to quantum computing systems and associated services that enable them to explore enterprise-relevant use cases and devise quantum algorithms for highly specialized sets of problems. QCaaS provides vendors with access to their own technologies, and some cloud service providers offer QCaaS that supports access to various quantum computing implementations, vendors and solution approaches.

Why This Is Important

The torrid pace of innovation in quantum computing systems means that on-premises quantum systems are impractical for most users today, given their limited utility and rapid aging. QCaaS enables enterprises to derisk quantum strategies and leverage cloud services to access, test, validate and utilize diverse quantum technologies. QCaaS environments enable enterprises to focus on exploring a variety of use cases and devising quantum algorithms, as opposed to negative ROI, on-premises acquisitions.

Business Impact

Enterprises pioneering quantum initiatives are focusing on five key applications: optimization, simulation, search, linear systems and security-related use cases. QCaaS enables enterprises to explore different types of quantum systems and accelerate quantum skills development in a relatively low-risk environment. QCaaS continues to evolve in maturity. However, these environments are not ready for production use cases, primarily due to the limited scale of underlying quantum systems.

Drivers

- Many scientific problems are unsolvable using traditional computing technology. QCaaS offers access to quantum computing technologies for organizations pursuing solutions to computationally hard problems, without the risks and costs associated with dedicated systems that are likely to age faster, given the pace of innovation in the industry.
- Rather than acquiring expensive quantum systems on-premises, enterprises can minimize cost, complexity and time to value by using QCaaS-based quantum computing services.
- Some leading cloud service providers offer access to diverse quantum systems, simulators, resource estimators and high-performance computing (HPC) for hybrid workflows, simplify identity and data management and offer streamlined pricing across diverse quantum providers. In some cases, this approach can simplify exploration of quantum technologies and significantly lower risk.
- Continued scaling of underlying quantum computing systems and implicit advancement of the field (including scalable error correction schemes) is seminal to the evolution and eventual success of QCaaS.
- The ability to address the growing set of use cases beyond the traditional five — optimization, simulation, search, BQP and security — will be essential to create virtuous business cycles.

Obstacles

- A lack of ROI, limited applicability and the inability to demonstrate value creation are key business obstacles limiting enterprise investments in quantum.
- A lack of sufficient scale in underlying quantum computing systems powering QCaaS limits the scale of applications that can be explored or run. Current classical approaches deliver better, more impactful results than any quantum alternative.
- Quantum computing systems continue to be nascent in maturity, with more than half a dozen different ways of representing qubits and organizing systems to deliver error correction and scaling. Quantum technologies that now look promising may not be the ones that deliver value in the future.
- There remains a lack of skills to leverage QCaaS effectively, including the development of applications to fully exploit quantum computing capabilities.

User Recommendations

- Leverage QCaaS to devise quantum initiatives: Avoid acquiring on-premises quantum systems. The rapid pace of innovation in quantum technologies means that most on-premises systems will be obsolete faster, as newer systems and scalable technologies come online. QCaaS minimizes the risk associated with these dynamics.
- Select single-provider QCaaS for specialization and value creation: Direct QCaaS capabilities enabled by quantum vendors can provide highly specialized access to quantum systems, while derisking your strategies. Engage in this approach if your main goal is value creation and scaling.
- Select multiquantum system QCaaS for exploration and broader enterprise cloud strategy integration: Some CSPs offer access to multiple quantum providers, enabling enterprises to evaluate diverse technologies and simplified integration to existing cloud practices.

Sample Vendors

Google; IBM; Origin Quantum; Oxford Quantum Computing; PASQAL; Quandela; Quantinuum; Rigetti Computing; Xanadu

Gartner Recommended Reading

Cool Vendors in Quantum Computing

Infographic: How Use Cases Are Developed and Executed on a Quantum Computer

Preparing for the Quantum World With Crypto-Agility

Lab as a Service/Robotic Cloud Labs

Analysis By: Michael Shanler

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Lab as a service (LaaS) or “robotic cloud labs” are automated, scientific wet labs that are hosted in the cloud and can be accessed remotely. The labs can be managed by contract research organizations as well as internal teams. The cloud lab enables remote access, facilitated design, protocol transfers, live instrument monitoring and dynamic scheduling.

Why This Is Important

Laboratories represent a cost-related barrier to performing high-velocity scientific experimentation. Startup costs for assets begin from $5 million to $10 million. LaaS represents an opportunity for clients to externalize some of the work into a contract research organization (CRO) to perform complex laboratory-based activities with clusters of instruments, analyzers and robotics. Some providers can extend the same cloud-lab platform back to sponsors to internally duplicate the model.

Business Impact

LaaS enables life science organizations to rapidly deploy automation and testing capabilities without having to pay for and maintain expensive laboratory automation infrastructure. By centralizing the activities in the cloud, organizations can better share assets and harmonize approaches for science, experimentation and quality testing. Thus, LaaS reduces the barrier to entry for laboratory activities.

Drivers

- ROI for R&D investment continues to decline, which causes executive leadership to look for ways to improve productivity and evolve the science using any means possible. This includes shifting from internal R&D models toward external relationships with partners, as well as more open innovation models where information is collaborated with groups of partners, consortia members and academic researchers. These newer innovation models require new infrastructure for real-time collaboration across multiple time zones and locations. In most cases, researchers are pursuing similar models for both wet bench work as well as in-silico methodologies.

- Cloud technology is on the rise for standing up lab infrastructure and instrumentation software. Most new product launches in the lab-automation space have cloud and SaaS models.

- New biotech and upstart labs need quick entry into the lab automation space. As-a-service delivery models lower barriers to entry for these organizations and can reduce costs and accelerate scientific and lab-testing initiatives.

- Work-from-home policies and a push to enable remote access to systems in laboratories have pushed organizations to investigate quicker and easier ways to deploy solutions for lab automation and assays.
- Live event streaming technology and Internet of Lab Things (IoLT) are driving instrument connectivity.
- AI, ML and data science technologies to enable "insight engines" for lab processes are on the rise.
- Physical automation of robotics (such as lab instruments, analyzers, liquid handlers and peripherals) as well as automation of data (such as data processing, pipelining and workflow automation) are becoming less expensive and easier to deploy.
- Since LaaS product launches are fairly recent, and the reasons listed above are drivers, this technology is located in the Innovation Trigger phase.

Obstacles

- **Cultural:** Some organizations have a distrust for CRO-based staff when it comes to evolving science. Also, the domain expertise of partners may not be viewed as "equivalent" to sponsor companies within a certain scientific space or therapeutic domain.
- **Unclear financial implications:** Many organizations have existing internal assets that are still being depreciated, as well as staff who are dedicated to running laboratory and scientific operations. The movement toward cloud labs often means writing off or accelerating depreciation of those assets.
- **Risk of IP theft:** Intellectual property can potentially be exposed to third parties. Risk-averse organizations often view cloud or externalized resources as a potential for loss or theft.
- **Validation:** Good lab practice (GLP) studies require a higher level of validation than non-GLP studies. Many organizations are not set up with validation principles to support SaaS-based work.

User Recommendations

Start by evaluating how a LaaS strategy can either accelerate the science and/or improve the quality of the scientific method. To do this:

- Address projects that are good candidates for cloud-based labs. Consider externalizing this work to get experience with these types of vendors.
- Model the central lab infrastructure that can be deployed via cloud-lab approaches. Identify the laboratory assets and projects in your own organization to discover where it can make sense to centralize the control and deploy an internal cloud lab using either LaaS software or the vendors in your existing portfolio. Many vendors now have SaaS offerings for instrument control, drivers, instrument data lakes and dynamic scheduling, and can integrate into lab informatics solutions such as an electronic laboratory notebook (ELN), scientific data management system (SDMS) or laboratory information management system (LIMS).
- Evaluate the four major obstacles listed above and develop a plan to conquer these risks by talking to stakeholders in the scientific, laboratory, regulatory and governance, risk and compliance (GRC) groups.

Sample Vendors

Automata; Emerald Cloud Lab; Strateos

Gartner Recommended Reading

Your Lab of the Future Strategy Must Enable Life Sciences Digitalization

Quick Answer: How Do You Know That You’re Building a Truly Digital Life Science Lab of the Future?

7 Key Questions Life Science CIOs Should Ask When Selecting Laboratory Informatics Software

Quick Answer: What Are the Advantages of Leveraging Cloud Technologies in Life Science Omics R&D?

Life Science Manufacturer CIO Top Actions for 2023

Cloud Backbone as a Service

Analysis By: Lisa Pierce, Andrew Lerner

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Cloud backbone as a service (CBaaS) uses a public cloud provider's backbone for WAN transport, allowing network traffic to traverse that backbone to connect enterprise users, devices and locations. CBaaS offerings are delivered as a cloud service to customers and are occasionally marketed as WANaaS. Customers are responsible for ingress to the provider, typically via VPN or private WAN service. CBaaS can be delivered by a cloud provider or by a software vendor utilizing a cloud provider.

Why This Is Important

Heavy cloud users continue to seek out alternative WAN services to connect public cloud services. CBaaS is another example. But typically, the traffic transiting the particular cloud provider's backbone is limited to customer traffic that the particular IaaS provider and node(s) serve.

Business Impact

These offerings provide an alternative to existing WAN services to support cloud node to cloud node use cases. However, CBaaS typically doesn't support the full set of WAN requirements for most enterprises.

Drivers

- Aggressive marketing and sales from public cloud providers, including Amazon Web Services (AWS), are urging enterprise clients to discard their legacy WANs.
- The shift of enterprise workloads to public cloud providers makes the cloud provider's backbone a more logical choice for transport.
- As an architecture, CBaaS is compelling for organizations heavily focused on one public cloud provider, and that lack data center investments.
- CBaaS provides additional route diversity for clients seeking to enhance their WAN business continuity architectures.
- There also has been aggressive marketing from value-added resellers that acquire multiple CBaaS offerings and repackage them to sell to enterprises seeking CBaaS from multiple cloud service providers (CSPs).

Obstacles

- Prices from some CBaaS providers are multiple times more expensive than traditional WAN services.
- Because CBaaS is typically tied to a particular CSP, it is less attractive to clients whose traffic is significantly distributed across multiple CSPs.
- Offers are not end to end because access is excluded, as is WAN transport to the CBaaS node, forcing clients to procure separately.
- Compared with facilities-based carriers, the number of CBaaS nodes is very small.
- SLAs focus mainly on availability, and apply only between the CBaaS provider's nodes.
- Limited CBaaS telemetry data makes it less attractive to traditional network personnel, and to clients that operate their own SD-WAN networks.
- CBaaS offerings are fairly narrow. They do not seek to rival common carrier services, which serve all customers. Thus, customers must procure WAN transport for other use cases.
- These types of offerings continue to fracture the WAN, so clients must secure alternate WAN transport and employ consistent performance monitoring across all WAN providers.

User Recommendations

- Evaluate CBaaS offerings as a complement to your existing WAN, but don't expect CBaaS to replace your WAN.
- When applicable, use CBaaS selectively as part of your larger business continuity plan.
- Look at CBaas offerings if you're heavily invested with a particular IaaS provider for the mid to long term (three to five years or longer).
- Given their siloed nature, recognize that CBaaS maturation and price declines will be introduced at a very slow pace. I&O clients should assess the attractiveness of CBaaS offerings accordingly.

Sample Vendors

Alkira; Amazon Web Services; Microsoft

Gartner Recommended Reading

Optimize WAN Architectures for Workloads That Span the Hybrid Cloud and the Multicloud

How to Architect Your Network to Optimize Internet Performance and Reliability

Penetration Testing as a Service

Analysis By: Mitchell Schneider, Jeremy D'Hoinne, Carlos De Sola Caraballo, William Dupre

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Penetration testing as a service (PTaaS) provides technology-led, point-in-time and continuous application and infrastructure testing aligned with penetration testing (pentesting) standards, which have traditionally relied heavily on human pentesters using commercial/proprietary tools. The service is delivered via a SaaS platform, leveraging a hybrid approach of automation and human pentesters (crowdsourced or vendors' in-house team) to increase the efficiency and effectiveness of the results.

Why This Is Important

Pentesting is foundational in a security program and mandated by various compliance standards (e.g., PCI). PTaaS delivers a platform that enables faster scheduling and execution of pentests, and real-time communications with testers and visibility of test results. It provides API access to enable integration with existing DevOps and ticketing solutions for workflow automation. It also provides the ability to document and track pentesting results to demonstrate progress over time to leadership/auditors.

Business Impact

PTaaS complements vulnerability scanning and application security testing, and provides cost-optimization and quality improvement of pentesting output and validation of vulnerability status. PTaaS enables organizations to elevate their security posture through continual assessment. It integrates validation earlier in the software development life cycle compared with traditional pentesting phases by giving access to real-time findings delivered through the platform, therefore enabling faster reduction of exposure.

Drivers

- Organizations are turning to PTaaS to deal with the increase of attack surfaces due to accelerating use of public cloud and expansion of public-facing digital assets. PTaaS allows developers to talk to and receive guidance from pentesters instead of arguing with scanners, such as dynamic application security testing/static application security testing (DAST/SAST) scanners.
- Organizations with limited in-house security expertise must meet their compliance and risk management objectives, in addition to improving their security posture, and therefore look to pentesting services to meet these initiatives.
- In order to meet fast production deadlines, security-aware organizations must integrate a more agile way of conducting pentesting into their continuous integration/continuous delivery (CI/CD) pipelines for their DevSecOps practices.
- Gartner clients have expressed an appetite to test on a more frequent basis; however, manual pentesting is cost-prohibitive in modern infrastructure (e.g., IaaS, SaaS and third-party subscriptions).

Obstacles

- Selecting a suitable PTaaS vendor in the market will be difficult, as their capabilities vary. Vendors use one or a combination of automation and human testers, which are in-house or community-led — typically vetted freelancers — to perform penetration testing for the client organization.
- Most of the PTaaS vendors in the market focus on the internet-facing digital assets, like web and mobile applications, which may only partially fulfill client requirements.
- There is confusion between PTaaS and bug bounty programs, as many bug bounty vendors also now offer PTaaS.
- Heavily regulated industries may still be required to contract a third party to perform a traditional, consulting type of pentest due to compliance requirements; therefore, PTaaS may not be an acceptable alternative.

User Recommendations

- Determine which option/mix of penetration testing programs is best for your organization: compliance-driven service engagement; PTaaS; in-house red team leveraging an automated pentesting tool; or bug bounty.
- Identify and evaluate the pentesting scope and requirements that PTaaS vendors will be able to fulfill before engaging with vendors. PTaaS is well-aligned to both application testing and external infrastructure testing. Not all of the vendors will be able to replace internal infrastructure pentests, wireless, social engineering and physical assessments.
- Favor hybrid scanning models that combine human analysis and automation to increase both effectiveness and efficiency.
- Select a PTaaS vendor that aligns with relevant compliance requirements, and not just focused on internet-facing infrastructure and applications.
- Seek PTaaS vendors that provide customized and tailored guidance throughout the life cycle of their service to alleviate the security skills gap.

Sample Vendors

Bishop Fox; BreachLock; Bugcrowd; Cobalt Labs; Evolve Security; HackerOne; NetSPI; OccamSec; Raxis; Synack

Gartner Recommended Reading

How to Select a Penetration Testing Provider

Understand the Types, Scope and Objectives of Penetration Testing

Platform-as-a-Service Provisioning

Analysis By: Jason Donham

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Platform-as-a-service (PaaS) provisioning is a cloud-based workload delivery mechanism provided to clients as a consumption model. PaaS provisioning solutions include all necessary infrastructure and platform development tools to efficiently deliver the complete application life cycle. This reference to PaaS is for workload delivery only and not to be confused with software developer consumption.

Why This Is Important

Platform as a service allows organizations to develop a full application stack without procuring and building all the underlying hardware and software infrastructure necessary to accomplish this task. The result is a quick, efficient and scalable method for application development and deployment. Organizations only pay for the resources they use and do not need to build an entire team dedicated to managing the underlying infrastructure or software tools.

Business Impact

The inherent flexibility of PaaS provisioning solutions is critical for businesses to be able to respond quickly to changing market demands. PaaS supports cloud-first initiatives by giving businesses a robust toolset to rapidly develop and deploy cloud-based upgrades and replacements for on-premises legacy applications. PaaS provisioning is not as advanced as application engineering because mechanisms that support applications do not scale.

Drivers

- PaaS supports modernization efforts by providing a single set of tools and services to develop new applications.
- Standardization is a key element of agile, efficient operations and management. PaaS gives developers a common platform toolset to build, deliver and manage applications.
- PaaS provides prebuilt code components that can be used repeatedly across many applications as they are being constructed. The repeatability aspect of PaaS greatly speeds up the development process and results in faster time to market for applications.
- Security, stability and supportability are improved by using prebuilt code. Whenever code sections are updated or patched, applications using this code benefit immediately.

Obstacles

- Data sovereignty and control may be a concern with PaaS deployments since data is stored and managed by a third party.
- In many cases, PaaS vendors must supply data protection and disaster recovery, which is outside the control of the client.
- Integration of PaaS with existing development environments can cause compatibility issues between different programming languages and toolsets.
- There is a potential risk of vendor and platform lock-in when moving to a PaaS solution. The possibility of IaaS lock-in with the vendor's underlying infrastructure and/or cloud provider compounds this issue.
- Clients are responsible for their own application security. PaaS vendors are only responsible for securing the underlying infrastructure.
- Transition from one PaaS platform to another will be difficult due to incompatibilities in services.

User Recommendations

- Build standardized applications on a PaaS platform utilizing prebuilt code blocks to achieve maximum efficiency and reduce operating cost.
- Utilize PaaS to access state-of-the-art tools and infrastructure at a fraction of the cost of building your own development environment.
- Use PaaS capabilities to rapidly develop applications and deploy them across multiple platforms to take advantage of more market opportunities.

Sample Vendors

Amazon Web Services (AWS); Google; Microsoft; Oracle; Red Hat; Salesforce; SAP; VMware

Gartner Recommended Reading

I&O Platforms Primer for 2023

Predicts 2023: XaaS Is Transforming Data Center Infrastructure

Use Open-Source Software in Data Center Infrastructure

Insurance as a Service

Analysis By: Sham Gill

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Gartner defines “insurance as a service” as a platform offering insurance products (typically exposed via APIs) along with technologies for digital customer engagement and service that are delivered on the cloud via a subscription-based pricing model.

Why This Is Important

Insurance-as-a-service offerings are being marketed as platforms for insurance CIOs and other partners, to leverage prebuilt insurance products and distribution capabilities on a subscription basis. They aim to enable insurers to launch new products and services to market them far more rapidly than they could do themselves. These platforms have the potential to enable CIOs to meet CEO’s ambitions for growth, transformation and entry into new markets.

Business Impact

Insurance-as-a-service has the following business impacts:

- Insurance CIOs will need to seek innovative solutions to deliver to market radically new customer experiences and products faster. Insurance-as-a-service offerings may help CIOs meet the demand for rapid product launch and innovation for selected products serving new demands.
- Insurers may seek to launch insurance-as-a-service offerings to expand distribution and service opportunities through new partners to attract net new revenue for growth and counter the threat from insurtechs.

Drivers

- Access to insurance-as-a-service models could enable insurance CIOs to explore the creation of new products, services and business models to accelerate digital transformation, drive net new revenue and enter new markets.
- Insurance CIOs facing pressure to deliver business outcomes more quickly, or in new geographies, will look to solutions that enable them to overcome challenges with legacy technology and internal skills.
- They require lower capital expenditure than self-build options as the platform service is made available to many, with costs shared across users, offering a lower-risk innovation opportunity to trial a product offering and decide whether to pursue it.
- Inherent scalability and in-built regulatory compliance for products reduces the obstacles to rollout innovation in products and servicing.
- Insurance becomes plug-and-play capabilities that insurers can stitch together to suit their business needs.
- Insurance-as-a-service offer a diverse set of capabilities designed to offer speed to market. They can include: (1) The ability to create or co-create brand new products directly on the platform, (2) the ability to white-label preexisting insurance products. These are typically constrained to simple or niche P&C insurance products, or products designed to service new target markets, such as gig economy workers, (3) digital customer engagement tools and accelerators, such as mobile apps, portals and chatbots, (4) customer analytics, contextualization and personalization tools, (5) AI-based risk selection algorithms, (6) compliance and regulatory support, (7) marketplaces for accessing third-party vendor content, (8) insurance capacity and reinsurance management, (9) externally exposed APIs for enabling partners to access and distribute the products through different channels, and (10) cloud deployment for resilience, elasticity and usage-based pricing.

Obstacles

- There is no single, consistent market definition. Offerings are currently a confusing mix of business models, technologies, services and products where marketing is often ahead of reality.
- Platforms are evolving rapidly, with little uniformity in business capabilities, technology capabilities and insurance LOB product coverage. Most products offered on insurance-as-a-service platforms are simple P&C insurance products, such as travel insurance and gadget insurance.
- Given that many commercial insurance-as-a-service platforms offer their own insurance direct to consumers while also offering access to products and tech capabilities as-a-service B2B, there is often unease on whether these platforms are competitors, frenemies or true partners.
- Insurance-as-service quite often morphs into establishing that insurers are actually seeking to explore embedded insurance opportunities, questioning the viability of insurance CIOs investing in these platforms.

User Recommendations

- Ascertain what the business is trying to accomplish, to avoid misplaced investments and missed business outcomes. Each of the insurance-as-a-service models will lead to a shift in control of insurance products, technology, distribution, customer experience and technology.
- Host visioning workshops with business partners, such as scenario planning, to ascertain the enterprise's appetite for a more service-driven model that engages third-party partners for digital transformation and cost optimization.
- Validate who will have access to products, services and intellectual property developed on the platform. This ensures that investments in insurance-as-a-service models do not inadvertently fuel competitors.
- Pay special attention to regulatory-required data privacy that impacts consumer trust, security and data integrity, thus ensuring that technology investments support strong data privacy and security.

Sample Vendors

Boost Insurance; bolt; ELEMENT Insurance; Qover; Slice

Gartner Recommended Reading

Quick Answer: Insurance as a Service — What Is It, and Why Should CIOs Care?

To Prepare for Open Insurance Opportunities, CIOs Should Strategically Invest in APIs

Case Study: An Insurance API-Driven Digital Ecosystem Transformation

At the Peak

Firmware Protection as a Service

Analysis By: Jason Donham

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Embryonic

Definition:

Firmware protection as a service (FPaaS) is a managed service that provides firmware security and policy-based remediation. It uses a centralized hash repository to determine the trust/untrust status of the firmware for each node in the data center.

Why This Is Important

As the threat landscape for infrastructure continues to change rapidly, infrastructure and operations (I&O) leaders must adapt their strategies to prevent ransomware and malware attacks. FPaaS adds an extra, necessary security layer to prevent or mitigate damage to critical underlying hardware systems.

Business Impact

When malicious actors seek to compromise firmware on cloud provider or data center systems, FPaaS provides business value by helping enterprises to prevent:

- Infection of systems with ransomware or other malware.
- Service outages as a means of business disruption.
- Exfiltration of sensitive data for personal gain or to damage the business.
- Evasion of standard detection tools that have no visibility into firmware threats and stay active even after a full system reimage.

Drivers

- Compromised supply chains or other physical asset tampering is virtually undetectable without the comprehensive firmware scanning provided by FPaaS.

- Increasing sophistication of attacks on core data center system hardware requires more robust monitoring and intervention techniques to prevent costly downtime.
- Firmware attacks are undetectable using standard tools, as these run at the operating system (OS) or hypervisor level. Also, firmware operates at a higher privilege level.
- Firmware attacks can cause physical failures, thus leading to extended downtime.

Obstacles

- Requires central repository and management server to track each node in the data center.
- Agent-based solutions require OS-resident agents to perform their functions.
- The general belief that the threat of firmware compromise is overstated or nonexistent.

User Recommendations

- IT organizations do not fully understand firmware attacks. A business impact analysis (BIA) must be performed to quantify hidden risks.
- I&O leaders must build a business case for FPaaS. They can do this by comparing the cost of the solution versus the risk of ransomware impact and/or potential costs derived from a BIA.
- A formal process for firmware upgrades must be developed similarly to OS patching. Remote update tools using scripting and automation can assist with developing a regular cadence for firmware upgrades.

Sample Vendors

AMI; Eclypsium; Phoenix Technologies

Backup as a Service

Analysis By: Jason Donham

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Backup as a service (BaaS) solutions deliver backup and recovery operations to protect data located within on-premises and cloud environments, including SaaS applications. BaaS provides clients with the flexibility of consumption-based pricing, minimizes management overhead and improves backup storage security.

Why This Is Important

I&O leaders struggle to adapt and manage backup systems for new and existing workloads in their data centers and cloud. They also find it difficult to hire and retain staff that can support a variety of backup systems. BaaS provides flexible backup systems that are free from overprovisioning and scalable to immediate needs for both on-premises and cloud applications. BaaS leverages the expertise of the vendor's staff to fill in any staffing or knowledge gaps the client may have.

Business Impact

BaaS solutions provide I&O leaders with a pay-as-you-go solution that grows with the organization's needs, eliminates large capital expenditures, and simplifies day-to-day operations and maintenance. BaaS offers solutions to provide protection for a growing number of cloud environments, including IaaS, PaaS and SaaS applications. BaaS also allows IT organizations to expand backup with minimal staffing impacts.

Drivers

- Data proliferation to the edge requires I&O leaders to rethink their overall backup strategy. BaaS can provide a scalable solution across the widely dispersed footprint of edge and remote office/branch office (ROBO) deployments.
- Many small to midsize organizations do not have the skill sets in-house that are required to build and operate a complex backup system.
- Enterprise organizations can utilize BaaS to augment existing backup capabilities to protect hybrid and multicloud data.
- Organizations lack the necessary levels of automation to deploy and easily manage modern backup and recovery systems for on-premises, IaaS, PaaS and SaaS application backups.
- SaaS data is rarely backed up by the SaaS application vendor on the client's behalf. This leaves clients exposed to security flaws in the vendor ecosystem that are beyond client control to identify or remediate.
- The threat of ransomware requires modernization of backup architecture which can be prohibitively expensive. BaaS eliminates the need to periodically replace or upgrade backup systems.
- Organizations want to move from a capital expenditure (capex) model to an operating expenditure (opex) model that is based purely on resource consumption.

Obstacles

- Some clients are not equipped to quickly pivot from a capex model to an opex model which is a requirement for BaaS solutions.
- Significant investment in existing backup solutions precludes adoption of BaaS until a refresh cycle occurs or until the client believes sufficient value has been extracted from the existing solution. Also, BaaS solutions can be difficult to compare to one another based on the wide variety of billing methods in use for these services.
- BaaS adoption is hampered by client belief that ransomware and data loss only affect enterprise companies and that cloud vendors are already backing up client data.
- Many BaaS solutions rely entirely on public cloud for backup storage which can slow recovery for on-premises systems due to bandwidth constraints. Privacy or local regulations can prevent the adoption of BaaS since storage for backup data is now hosted on BaaS vendor-owned infrastructure.

User Recommendations

- Perform a proof of concept (POC) to determine if a vendor's BaaS solution is a fit for your environment.
- Implement BaaS solutions where cost savings can be realized over a build-and-maintain approach or where significant technical gaps or security risks exist.
- Use BaaS implementations to back up data in cloud and SaaS applications that are otherwise difficult or impossible to back up with existing solutions.
- Establish exit terms in the contract negotiation process which address data access and export of protected data and end of contract.

Sample Vendors

Clumio; Cohesity; Commvault (Metallic); Druva; HYCU; Keepit; Rubrik; Veritas

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Market Guide for Backup as a Service

Supply Chain as a Service

Analysis By: Michael Dominy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Supply chain as a service (SCaaS) is the ongoing management of one or more supply chain functions for other enterprises. SCaaS is a revenue-generating, digitally enabled service that taps into the business process or operational capabilities of an enterprise.

Why This Is Important

SCaaS is an opportunity to directly grow revenue by using existing or new capabilities to perform a supply chain activity for another company. There are two primary types of SCaaS: Operations as a service, which involves contracting out physical operations. Business process as a service which involves performing a nonphysical operational activity for another enterprise.

Business Impact

- Increased revenue for manufacturers, retailers, distributors or healthcare providers with factories, private fleets, warehouses, stores or other leverageable physical assets with operational capacity or business process capabilities to deliver physical or digital SCaaS to organizations.
- Reduced cost by better utilization of supply chain assets from physical assets such as warehouses and trucks to business process and technology assets such as supply chain planning.
- Expanded relationships with existing customers by offering additional services.

Drivers

- **Capabilities and capacity.** Operational capability, capacity or availability of supply chain business and technology expertise present opportunities for organizations with advanced supply chain capabilities to directly deliver revenue to their organizations by monetizing their supply chain through services provided to other enterprises.
- **Cloud platforms and applications.** Cost-effective availability of cloud computing infrastructure services, multitenant SaaS applications, open-source software and analytics tools have enabled service providers and some enterprises to create, launch and sustain supply chain business process services.
- **Connected and intelligent things.** Lower technology costs and increased connectivity with products changes what the supply chain function must do. In the past, the supply chain managed products. Today, intelligent connected things are starting to manage the supply chain, essentially turning the supply chain organization into a service provider for the physical object. For example, a piece of equipment or appliance that is tracking inventory or activity on its own can order replacement inventory or create a service order.

Obstacles

- **Identifying and selling physical operational SCaaS.** Most buyer and provider matchmaking in physical operations has been between companies and providers versus company to company.
- **Onboarding SCaaS customers.** Whether it is physical operations as a service or business process services, integrating systems and defining roles, responsibilities and required activities are complex and time-consuming.
- **Differing commercial arrangements.** Instead of an order-to-cash process, with invoicing and collections triggered by a shipment, a contract with service agreements governs payments.
- **Transforming talent**. SCaaS requires new ways of working. Supply chain professionals must switch from an internal orientation to an external client mindset. Not all individuals are comfortable and skilled to do so. Because all SCaaS involve digital skills, individuals in the supply chain organization will need to develop or expand digital competencies.

User Recommendations

Enterprises such as retailers or manufacturers contemplating offering SCaaS should:

- Determine physical asset SCaaS opportunities by analyzing capex and capacity forecasts.
- Evaluate which processes can technically support multitenancy and scalability requirements by reviewing IT architecture.
- Assess competitiveness by benchmarking an offering against existing providers including 3PLs, contract manufacturers and BPO providers.
- Create customer journey maps by documenting physical and digital flows from customers back through the supply chain.

Enterprises considering contracting for SCaaS should:

- Target lower-performing supply chain activities by using maturity assessment and benchmarking.
- Audit and monitor areas of higher risk, such as global trade management, by asking how systems such as denied-party lists are updated.
- Assess SCaaS for specialized purposes, such as network design or inventory optimization, by assessing skills of those in the supply chain organization.

Sample Vendors

Amazon; Arrow Electronics; Avnet; Cardinal Health; Lenovo; Mayo Clinic; Primary Connect; Quiet Platforms; Target

Gartner Recommended Reading

Take Four Steps to Develop Your Supply-Chain-as-a-Service Strategy

Operationalize and Scale SCaaS Through Multienterprise Organization, Governance and Talent Capabilities

Supply Chain as a Service Converges Physical and Digital Supply Chain to Deliver Revenue

Market Guide for Supply Chain Strategy, Planning and Operations Consulting

Storage as a Service

Analysis By: Jason Donham, Philip Dawson

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Storage as a service (STaaS) is a managed service that provides a way for organizations to manage and consume storage without the overhead costs of upfront capital for storage assets and staff time. STaaS provides managers with flexibility, resilience and efficiency. STaaS solutions include both on-premises storage and cloud storage.

Why This Is Important

Infrastructure and operations (I&O) leaders struggle to leverage on-premises cloud operating model benefits while their environment becomes more complex and less agile to business demands. STaaS provides many benefits such as improved asset management through aligning costs to utilization, higher levels of operational efficiency through outsourcing hardware administration and support, and cost savings through a consumption-based as-a-service model with increased levels of automation.

Business Impact

Budget and spend (capex) inefficiencies are driving higher total cost of ownership (TCO) compared to consumption-based (opex) spending that is much more in line with storage needs.

STaaS solutions enable organizations to:

- Shift from capex to opex to eliminate IT budget inefficiencies.
- Improve workload asset management and reduce capitalization costs.
- Eliminate life cycle management issues and technology refresh cycles.
- Reduce cyber liabilities and threat exposure through data services offerings.

Drivers

- Infrastructure managers need options when reconfiguring and resizing storage environments to meet the rapidly changing demands of applications.
- Threats of ransomware and other cyberattacks require higher levels of data security.
- Traditional storage is inflexible when deployed in a hybrid operating model.
- STaaS can increase labor costs on the back of intensive budgeting cycles.
- Inefficient life cycle management and constant infrastructure turnover conspire to create an inflexible environment that hampers innovation and ability to respond to business demands.
- The lack of subject matter experts (SMEs) or staff attrition issues (offset by moving responsibility and accountability to vendors) around critical elements of the infrastructure lead to a less resilient platform and exposure to untenable events.

Obstacles

- Finance or procurement members believe they are better stewards of capex assets or don't fully understand the indirect cost savings or benefits afforded by STaaS.
- Vendor sales and marketing narratives and selling strategies are reluctant to promote or advocate the benefits of as-a-service models over capex-related product features.
- Vendor business models are immature in terms of backend operations — metering, billing — and integration with supply chain and logistics.
- Vendor channels are not fully equipped to enable or support the transition to an as-a-service consumption model.

User Recommendations

- Implement consumption-based STaaS to reduce or eliminate capex budgets and IT refresh cycles.
- Add SLAs to drive critical requirements such as ransomware protection to improve security posture.
- Utilize artificial intelligence for IT operations (AIOps) combined with STaaS to create an intelligent infrastructure platform that proactively and dynamically responds to IT operating model outcomes and business priorities.

Sample Vendors

Amazon Web Services (AWS); Backblaze; Dell Technologies; Hewlett Packard Enterprise (HPE); IBM; Microsoft Azure; NetApp; Pure Storage; Wasabi Technologies; Zadara

Gartner Recommended Reading

Leverage Storage as a Service Platform SLAs and Capabilities to Transform IT Outcomes

Banking as a Service

Analysis By: Don Free

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Banking as a service (BaaS) can be a discrete or broad set of financial service functions exposed, consumed or offered in collaboration with or by chartered banks or regulated entities. BaaS powers business models deployed by conventional and unconventional banking market participants.

Why This Is Important

BaaS is gaining traction from banks that both consume and deliver services, while nonbanks are primarily just consuming BaaS. Their common aspiration is establishing or enhancing direct and intermediated revenue streams. These collaborative models support customer experiences such as a broader set of products and innovative customer experiences. Nonbank participants benefit from a quick onramp to the banking market by leveraging a regulated entity's license instead of pursuing their own charter.

Business Impact

Banks can:

- Pursue nontraditional revenue expansion through manufacturer, intermediary or distributor roles that leverage API products to serve a wide variety of BaaS participants.

- Benefit competitively with BaaS deployed in partnership with software and service provider partnerships to tap into communal markets that serve both regulated and unregulated entities.
- Consume BaaS to facilitate innovative customer services and broaden existing product portfolios.

Drivers

- Architecture advances inclusive of APIs, microservices and event-driven architecture facilitates faster time to market, reduced operational volatility and the capacity to retire functionality when it's no longer needed. The latter, the capacity to retire functionality, also reduces the total cost of ownership (TCO) and complexity.
- API aggregators are inserting themselves into the BaaS value chain by streamlining integration and opening markets to both fintechs and banks alike. Their capacity to act as an intermediary reduces banks' scope of API development and boosts banks' business time to market.
- Software applications are evolving to support composable technologies that promote economies of access to granular business functions; critical for enabling and sustaining BaaS.
- Embedded finance is a prominent demand side driver among nonbanks.
- Banks and fintechs are increasingly motivated to collaborate and extend addressable markets as a means of offering deeply personalized products and services to their customers.

Obstacles

- The lack of pervasive global financial services standards will inhibit frictionless and scalable commerce.
- The intermediary market of API aggregators will gain traction, but the number of providers will also grow beyond overall market demand. Since consolidation is inevitable, banks must continuously monitor the capabilities and relative viability of their API aggregators.
- As BaaS introduces multiple partners into markets that historically were supported by individual banks, it seems likely that regulatory pressures will increase to drive transparency and highlight systemic risks.
- The cardinal rule for any CIO planning to leverage IT and operational resources for any external venture must first verify that their bank and direct customers are served at the same level or better.

User Recommendations

- Acknowledge what your bank is trying to accomplish — technology investments, strategic objectives and skill sets will differ among BaaS operating models. Cultural and organizational changes will also need to be managed.
- Align technology investments that manage API products through external marketplaces, drive fintech collaboration through ecosystems and build support for development portals.
- Analyze possible diversification of revenue streams by determining whether your capabilities and operations would support BaaS and fintech processing.
- Make sure resources critical to the operation of the bank are well-defined to support a new service offering by creating a support model specific to the venture and distinct from business-as-usual responsibilities.

BMaaS

Analysis By: Bob Gill, Philip Dawson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Bare metal as a service (BMaaS) supplies physical infrastructure (e.g., compute, networking and storage) via a cloudlike consumption model. BMaaS differs from infrastructure as a service (IaaS) in that the provider offers physical infrastructure dedicated to a specific user at the individual host level, and users provide all of the software installed into it. A provisioning layer coordinates requests for specific infrastructure combinations to discrete equipment in the provider's data center.

Why This Is Important

BMaaS runs workloads without hypervisor or OS compatibility restrictions on workload performance. This improves performance (no sharing/overhead), security (no sharing) and uptime (nothing else brings the system down). BMaaS is often chosen over virtual public cloud infrastructures to conform to legacy software licensing needs, based on permanent deployment onto fixed physical hosts. BMaaS isn't new, but it is gaining momentum augmenting, rather than replacing, on-premises equipment.

Business Impact

- BMaaS offers the advantages of dedicated infrastructure (e.g., predictability, security and performance) with elasticity closer to IaaS than actual physical deployments.
- For example, it provides a cloudlike experience in a data center location better suited to customer needs for low network latency and data residency.
- BMaaS supplies a flexible integration platform at the nexus of public cloud access locations, such as colocation hubs or content delivery network (CDN) points of presence (POPs).

Drivers

- Include the capability to act like a public cloud, rather than a dedicated hosting environment — programmable automation, elastic scalability down to the individual host level, and pay-as-you-go (PAYG) economics and consumption models.
- There is interest in cloud-native technologies as a path toward cloud independence that reduces lock-in.
- Bare metal may solve the issue of physical workload location, addressing the concerns that highly centralized offerings may pose, due to latency concerns, enterprise control, or data sovereignty and regulations.
- Bare metal offers the speed and agility of the public cloud, with far greater control over workload and data placement.
- The noncontinuous use of bare metal can be less costly than physical infrastructure; it does not tie up capital expenditure (capex) and is faster to deploy operationally as operating expenditure (opex).

Obstacles

- Adding another infrastructure environment increases complexity.
- Customer or service providers must supply and configure much of the software, bearing the risk and cost of a greater portion of the full stack.
- Unique network offerings may be required or multiple offerings may need to be integrated.
- Ease and flexibility of consumption may vary, especially up from infrastructure into application delivery.
- Economics may vary by application delivery, workload type, networking and included storage services.

User Recommendations

- Build BMaaS into cloud assessment models by identifying the attributes that can be addressed only through the software licensing compatibility, hypervisor independence and the location specificity of bare metal.
- Leverage bare metal's unique location benefits by identifying applications that require low latency or sovereignty through proximity to cloud onramps.
- Select BMaaS for "cloud-native hosting" of legacy applications, with licensing terms optimized for dedicated physical hosts.

Sample Vendors

Amazon Web Services; Cyxtera; Digital Realty Trust; Equinix; Oracle; Rackspace Technology

Gartner Recommended Reading

Break Down 3 Barriers to Cloud Migration

Enhanced Blockchain as a Service

Analysis By: Adrian Leow, Avivah Litan

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Enhanced blockchain as a service (eBaaS) is a cloud-based service that provides an application layer for developers to build, deploy and host their blockchain-based applications, functions and smart contracts. eBaaS abstracts the underlying blockchain infrastructure, enabling developers to focus on the application layer without having to worry about the underlying blockchain technology. It enables developers to deploy their applications across multiple clouds and blockchains.

Why This Is Important

eBaaS simplifies blockchain adoption for enterprises and accelerates deployments by providing a secure and scalable environment for app development and deployment. It offers standardized APIs and tools for easier development and integrates with existing enterprise systems. With robust monitoring and management capabilities, eBaaS ensures optimal operation, supports multiple blockchain platforms and provides greater flexibility and choice for developers and enterprises.

Business Impact

eBaaS unlocks new opportunities for businesses to leverage blockchain technology by reducing entry barriers, accelerating time to market and fostering business-related innovation. With the ability to integrate with existing enterprise systems, eBaaS can improve efficiency, security and transparency across industries, helping businesses stay competitive in a rapidly evolving digital landscape. eBaaS removes a good portion of the technical obstacles for businesses looking to take advantage of the benefits of blockchain technology.

Drivers

- eBaaS enables enterprises to focus on their applications without worrying about which blockchain and cloud to use, which smart contract development platform to use and how to connect legacy data to new Web3 applications.
- The benefits of unique blockchain features, such as smart contracts and immutable distributed ledgers, are much more accessible to enterprises when they use eBaaS, as they are shielded from most of the complexities of blockchain infrastructure and protocols.
- Low-code development environments enable developers to deploy applications quickly and avoid costly professional services.
- Some eBaaS vendors have off-the-shelf application templates that accelerate deployment for specific use cases.
- Blockchain application maintenance and performance monitoring are simplified through eBaaS services.
- Some eBaaS vendors support the relatively straightforward migration of applications from permissioned blockchains to public blockchains that support security through decentralization.

Obstacles

- Most eBaaS vendors support limited options for back-end blockchains, so users may be tied to the vendor's blockchains of choice. The historical lack of industry standardization across different blockchain platforms can make it challenging for businesses to select the best fit for their use cases, whether they use eBaaS or not.
- eBaaS vendors may lag in the adoption of public chain innovations unless their architectures are modular and open to allow easy integration of new capabilities.
- For a successful blockchain deployment, enterprises must participate equally with other organizations using their applications. eBaaS services may find it difficult to satisfy the requirements of multiple organizations.
- Enterprises participating in eBaaS (or any non-eBaaS application) must agree on data exchange formats, governance and permissions before deploying their applications.
- Enterprises are often confused on how they can use and benefit from blockchain technology in the first place. eBaaS can help guide them toward worthwhile business scenarios, but does not guarantee alignment.

User Recommendations

- Evaluate and use eBaaS services to accelerate the deployment of your applications, once you have agreed on business and process terms and addressed funding and governance issues with your ecosystem partners.
- Select an eBaaS provider that targets your use case or industry and has experience with it.
- Select an eBaaS provider that supports permissioned blockchain today, and which either can or is planning to support public blockchains in the future. This will ensure that your organization benefits from blockchain decentralization and fast-moving innovations in the public blockchain arena.

Sample Vendors

Alchemy; Fujitsu; IBM; Kaleido; NTT DATA; Oracle; SettleMint; Sky Republic; Vendia

Sliding into the Trough

Edge as a Service

Analysis By: Bob Gill

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Edge as a service (EaaS) describes a model in which some or all edge software and/or hardware is offered via provider-owned and operated assets, requiring little to no ownership of infrastructure on the part of the customer.

Why This Is Important

A lack of standards and the diversity of edge devices and workloads make edge implementation challenging, while the potential for selecting a technical “dead end” is high. EaaS is a delivery model for edge computing in which a vendor (e.g., a systems integrator, independent software vendor or cloud provider) offers some or all of the infrastructure required to deliver edge-based applications, shielding the customer from technical complexity and market volatility.

Business Impact

Many enterprises choose to procure edge services managed by a third party, as:

- Most enterprises do not possess the skills or experience to build and manage complex, distributed systems that incorporate diverse end systems and software stacks.
- EaaS delivers and maintains prebuilt solutions with a primary focus on meeting SLAs that are based on business outcomes.
- EaaS simplifies adoption of complex edge initiatives, while lessening complexity, risk of obsolescence and technical debt incurred.

Drivers

- Organizations looking to deploy edge computing are finding that the crowded and rapidly shifting technology space is making platform selection difficult.
- Enterprises looking to limit risk find EaaS lowers the barrier to entry. Rather than making technology choices, they can contract for a business outcome (for example, retail store operations with explicit SLAs) and be insulated from the infrastructure that the provider uses to deliver the solution.
- EaaS solves for a lack of skills and experience in building and operating edge computing solutions.
- EaaS helps avoid incurring technical debt and reduces exposure to technology obsolescence.
- EaaS Lowers the barrier to implementation of edge computing and enables growth.

Obstacles

- Edge use cases are so individual that providers may not be in a position to solve all enterprise requirements economically.
- Ongoing operations at scale may be more costly than if the enterprise operated the infrastructure at a high degree of efficiency and automation.
- Placing all responsibility in the hands of the provider naturally drives vendor lock-in, and some EaaS offerings may not support future edge requirements.
- Sourcing a solution externally may limit integration with other internal applications and systems.

User Recommendations

- Evaluate edge as a service offerings by creating a build-versus-buy model for edge deployment and operations.
- Reduce initial cost outlays and pressure on accurate configuration sizing by positioning the edge capabilities as a more elastic service, rather than an explicit hardware configuration and purchase.
- Weigh enterprise needs for customization and differentiation against realistic assessments of in-house technical expertise, the organization's stance on "opex versus capex," and the breadth of the solution (a targeted, specific application set versus a more general, distributed infrastructure platform).

- Examine EaaS as a means to speed time to market for many use cases by lowering the initial cost outlays, technical hurdles, operational expertise required and "platform risk" present in such a nascent market.

Gartner Recommended Reading

Market Guide for Edge Computing

NaaS

Analysis By: Ted Corbett, Gaspar Valdivia, Jonathan Forest, Lisa Pierce

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Network as a service (NaaS) is a standardized and highly automated delivery model for networking functionality. It offers support for dynamic scaling up and down of network resources. The NaaS vendor primarily owns and operates NaaS offerings. Pricing is on a pay-for-use basis, or as a subscription based on usage metrics. Typically, self-service interfaces — including an API and a user portal — are exposed directly to customers.

Why This Is Important

Many network service providers (NSPs) and non-NSPs are creating NaaS offerings for enterprises seeking consumption-based spending for networking — similar to what cloud offers for compute. Enterprise network equipment market spending is projected to reach $94 billion in 2023. This reflects a 6.1% five-year CAGR through 2027. New entrants see growing enterprise spending, while many incumbents seek to hold on, invest in their NaaS strategy and grow amid emergent competition.

Business Impact

Currently, some enterprises pursue a flexible, consumption-based networking model — regardless of user or application location. NaaS seeks to provide enterprises with agility, service delivery quality, automation and end-to-end customer experience — with up/down scalability and adaptive billing based on usage amid all-opex spending. Emerging NaaS providers' goal is to disrupt current customer sourcing norms. Over time, this disruption may expand enterprise buyer options and pricing models.

Drivers

- Many enterprises envision a future where complete life cycle network operations are delivered via a consumption-based, predictable spending model. This future would include their end-to-end networking estate spanning LAN, wireless-LAN, data center and WAN edge, for both on-premises or cloud-based network functions — including private 5G and other emerging network services.
- Buyers increasingly seek full life cycle management of their network estate, not simply all-opex network product procurement where operational leases (rentals) have long served the purpose of amortizing payment for networking products.
- The key drivers for an all-opex model for the enterprise have evolved. Enterprise buyers seek a greater focus on end users and their applications for improved service delivery quality, automation and predictable customer experience from the market. Also, WAN services from NSPs have evolved from enterprise locations to virtually any cloud-based provider or hosted endpoint. These continue to drive enterprise objectives for increased agility, more flexible consumption models and a seamless experience across their network consumption life cycle.
- In response to evolving enterprise needs, non-NSPs are seeking to drive revenue by pursuing their own emergent offers for NaaS.

Obstacles

- Most NaaS offerings in the market are limited to pricing/licensing changes. This confuses and frustrates customers, limiting true adoption.
- Compared to traditional pricing models, positive ROI models for a NaaS proposition do not yet exist.
- Enterprises entering into NaaS agreements hand over control of their network design and face full replacement of NaaS product components upon early or end-of-term-based exit events.
- Current NaaS offerings (primarily from NSPs) are not comprehensive, focusing on the provider's points of presence, where many NaaS components such as gateways and cloud connectivity bandwidth on demand reside.
- All-opex procurement is complicated by refresh timing of different network product technologies.
- Most NaaS offerings include network hardware, but do not meet the definition of NaaS and are not different from the vendor's labeling of current offerings as new; these packages are not owned and operated by the network vendor in this case, and are not NaaS offerings.

User Recommendations

IT leaders:

- Exert caution with NaaS due to widespread confusion created by the provider community.
- Procure network products more traditionally with financial leasing methods to smooth spending.
- Retain network design control by separately procuring kit as an operations lease and add managed operations.
- Calculate before and after ROI by capturing all in-scope costs and uniformly comparing proposals to identify the differences.
- Choose NaaS to achieve operational, lease-based network product spending when this is the primary goal, and you have a predictable consumption pattern.

Technology service providers:

- Build NaaS capabilities by investing in consumption-based, commercial models across LAN, WAN and cloud connect services.
- Build trust in NaaS by providing itemized pricing, standardized service definitions, and scale-up and down commercial flexibility.
- Prove to prospective buyers the value of NaaS offers by disaggregating proposals and providing detailed comparisons against alternative options.

Sample Vendors

Nile

Gartner Recommended Reading

What Is NaaS, and Should I Adopt It?

Magic Quadrant for Managed Network Services

Magic Quadrant for Network Services, Global

Navigating Emerging Network-as-a-Service Promises and Challenges

Early NaaS Pricing Lessons to Drive Adoption

Product-as-a-Service Supply Chains

Analysis By: Michael Dominy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Product-as-a-service supply chains are integrated and coordinated forward, reverse and service supply chains that enable subscription, consumption or outcome-based business models. They are digitally enabled through a range of technologies from unified commerce applications for basic subscription offerings to IoT-connected products with embedded software and predictive analytics to support usage or outcome business models.

Why This Is Important

Product-as-a-service supply chains provide increased value to the business by enabling a differentiated customer value proposition, opportunities for premium pricing, recurring revenue and deeper customer relationships. Customers expect companies to offer their products or solutions that address their needs in commercial arrangements that extend beyond buying and owning a product. Supply chains must be designed and optimized to deliver such offerings to ensure new business models are profitable.

Business Impact

Supply chains that enable products as a service offerings can help improve revenue and sustainability by:

- Serving customers or market segments that are unable or unwilling to buy in a commercial arrangement where ownership of the product transfers to the customer.
- Managing products through more of the product life cycle and applying circular economy principles.

Drivers

- Increasing percentage of revenue driven by as-a-service business models. According to the 2022 Gartner Digital Business Impact on the Supply Chain Survey, companies that have implemented a digital business model, report that 66% of revenue is being driven by existing products and services enabled by digital or by digital offerings including as-a-service, up from 59% in 2019.
- Digital business models, such as subscription- or usage-based-as-a-service business models force a blurring or blending of what was historically the forward or delivery supply chain with the service and support supply chain. The supply chain organization must monitor the location, performance and needs of the product or asset after it has been delivered or installed. Service must be orchestrated from a physical supply perspective for items such as parts, but also from a digital perspective for needs like software patches and upgrades.
- Increased availability of enabling technologies including product connection technologies (i.e., IoT) and cloud technologies (infrastructure services, platform services and software-as-a-service) reduce the barriers to entry.
- Sustainability strategies, goals and objectives in response to customer demands and pressure from investors.
- Commoditization of physical products in industries such as electronics and industrial equipment requires companies to expand and differentiate their offerings. Product-as-a-service offers competitive action against low-cost competitors, new entrants or other innovators.

Obstacles

- Lack of maturity: New relationship dynamics, collaboration approaches and partnerships inside and outside the company require high maturity levels.
- Scaling challenges: Most supply chains already support multiple business models, but digitally enabled value propositions increase complexity. Due to late involvement in business innovation, supply chains miss opportunities to align processes, resulting in an inability to scale efficiently.
- Lack of cost transparency: Data, software and digital service over the lifetime of the service are part of the value proposition rather than just operational support. This complicates an understanding of the cost to serve, making profitability in solution-oriented business models difficult.
- Decision-making challenges: Across the life cycle of a solution, coordinating decisions within and across companies is the top challenge cited by those fulfilling solutions.

User Recommendations

- View a transformation to a product-as-a-service model similar to large-scale change management initiatives. Chief supply chain officers (CSCOs) must act as catalysts in the transformation by demonstrating how the supply network drives efficiency, value and competitive advantage.
- Promote supply chain expertise in value stream mapping, network optimization, sales and operations planning, and advanced analytics.
- Leverage upstream and downstream ecosystem linkages to provide required technologies, innovations or services to connect resources, orchestrate activities, synchronize information, monetize assets and align processes around offerings.
- Utilize dedicated roles and technology to speed the adoption of offerings.
- Use a partially modular operating model to allow composability of who completes processes and how and where they do it.
- Segment the supply chain operating model to support multiple business models, including as-a-service models.

Gartner Recommended Reading

4 Competencies Required for Supply Chain to Support Digitalized Products

Infographic: The Evolving Impacts of Digital Business on Supply Chain

Now Is the Time to Deliver IoT-Enabled Product Servitization to Manufacturers

Top 3 Digital Business Execution Challenges in the Manufacturing Supply Chain CIOs Must Resolve

Firewall as a Service

Analysis By: Adam Hils, Rajpreet Kaur

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Firewall as a service (FWaaS) is a multifunction security gateway delivered as a cloud-based service, often to protect small branch offices and mobile users. FWaaS can provide a simpler, more flexible architecture using centralized policy management, multiple enterprise firewall features and traffic tunneling to move network security inspections partially or fully to a cloud service.

Why This Is Important

Hybrid working is here to stay, and growing adoption of software-defined WAN (SD-WAN) and hybrid WAN architectures is increasing interest in using FWaaS to help secure small branches and securely enable hybrid work. We expect this trend to continue. FWaaS offerings are of varying levels of maturity.

Business Impact

- FWaaS offers significantly different architecture for small branches or single-site organizations. It offers visibility with centralized policy, flexibility and the reduced capital costs associated with a fully or partially hosted security workload.
- FWaaS enables inspection of web and nonweb protocols, providing more outbound protocol coverage.
- FWaaS changes budgetary considerations as organizations move from capital to operational spending.
- Organizations with hybrid workforces will find FWaaS helps them work securely in a widely distributed network.

Drivers

- Organizations rearchitecting their networks by implementing SD-WAN technology sometimes want FWaaS to secure outbound network traffic. FWaaS can also support inbound traffic use cases.
- FWaaS is a component of most SD-WANs and security service edge (SSE) offerings, which makes it part of the secure access service edge (SASE) framework sometimes offered as part of a larger SASE architecture.
- Hybrid mesh firewall architecture may include FWaaS.
- FWaaS can decrypt outbound traffic for inspection on a large scale. Alternative hardware or virtual branch firewalls often lack the performance to do this.
- The continuing move toward hybrid working necessitates bringing security services closer to workers in order to minimize latency.

Obstacles

- Network firewall hardware appliances comprise the largest security equipment market. The appliance approach has been predominant, and many organizations use appliances effectively and efficiently. Many organizations lack compelling reasons to change to a new form factor.
- Security teams find some FWaaS solutions difficult to implement and manage. New FWaaS deployments often require professional services engagements.
- Over 80% of outbound traffic in organizations uses HTTP and HTTPS. Cloud-based SSE services can protect and inspect this traffic at scale to offload existing hardware firewalls. This makes it much easier and less costly to extend investments in existing firewall hardware than to rearchitect the edge to forward all traffic to a FWaaS.
- FWaaS licensing is based on per-user per-year subscription pricing. This can be more expensive for large organizations with high user counts than hardware-based solutions that may have lower subscription costs, and that can be deployed and used beyond their capital depreciation life span.

User Recommendations

- Verify that the additional hop to FWaaS infrastructure does not create unacceptable latency for some of your sites, and look at models that limit initial investment until acceptable latency is proven. Simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance.
- Determine whether your organization is ready to move its entire security workload to the cloud, or whether you need thicker local devices to address privacy concerns and perform some on-premises segmentation or virtual LAN trunking.
- Assess how FWaaS might impact your branch architecture. Current FWaaS offerings offer mostly outbound security or protect mobile workers or companies that are primarily cloud-hosted. Consider maintaining on-premises firewalls for data center use cases.
- Evaluate the strength of the cloud service in three key respects: data center locations, points of presence and SLAs.
- Determine whether the complexity of an FWaaS project will necessitate a professional services engagement for initial setup and configuration.

Sample Vendors

Barracuda; Cato Networks; Check Point Software Technologies; Cisco; Fortinet; Juniper Networks; Palo Alto Networks; Versa Networks

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Select the Right Strategy for Securing Web Access

Climbing the Slope

RPA PaaS

Analysis By: Arthur Villa, Saikat Ray, Fabrizio Biscotti, Cathy Tornbohm

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Robotic process automation (RPA) platform as a service (PaaS) is a set of public-cloud-hosted services to create and execute RPA scripts against customer applications. It consists of RPA development environments, orchestrators and a performance dashboard. The orchestrator interacts with lightweight agents installed in the client environment that execute bots. Unlike RPA SaaS options that offer a ready-to-use service, RPA PaaS is intended for developers to create a new business function/service.

Why This Is Important

Currently, the majority of RPA implementations have been delivered on-premises, but RPA PaaS adoption will increase significantly over the next few years. This trend will enable greater citizen development, scalability and AI integration.

Business Impact

Like many software markets that begin with an on-premises focus and shift to the cloud, RPA PaaS will reduce barriers to RPA adoption, improve scalability and enable tighter integration with cloud-native services. RPA PaaS allows organizations to realize the value of on-premises RPA with improved process automation and the reduction of manual, repetitive tasks. RPA PaaS further distributes development access, improves governance and enables customers to access new features and capabilities.

Drivers

- One of the main factors driving the adoption of RPA PaaS is demand from business buyers. Through RPA PaaS, business buyers can quickly realize value from RPA without the need to ask busy IT departments to provision servers for RPA orchestration and analytics features. Demand for RPA is often driven by business buyers and RPA PaaS eliminates a major barrier to business buyer adoption.

- For several large software providers that entered the RPA market in recent years, cloud orchestration is the only option offered, driving RPA PaaS adoption. The majority of legacy RPA providers now also offer cloud-delivered access to their development environments and orchestration tools. These legacy providers have created pricing and sales strategies encouraging customers to migrate to cloud delivery, further driving RPA PaaS adoption.

- Organizations interested in the benefits of hyperautomation often require integrating RPA with process automation tech, like intelligent document processing (IDP), business process automation (BPA), integration platform as a service (iPaaS) and low-code application platforms (LCAPs).

- RPA PaaS improves integration with complementary process automation technology by centralizing the development platform in the cloud instead of requiring the installation of add-ons and version control challenges of managing multiple development environments distributed across an organization's developer workstations.

- Another factor driving adoption is decreasing buyer concerns about the security risks created by RPA PaaS. Early RPA buyers had concerns about new security risk vectors since RPA tools often had privileged access to an organization's core applications. As a result of those concerns, the RPA vendors mitigate those risks by developing strong security features including data encryption, credential vault integration, robust role-based access control (RBAC) capabilities, and bot accountability through log integrity and identity-centric approaches.

Obstacles

- Regulated industries may be unable to adopt RPA PaaS due to regulatory and compliance challenges. For example, banking and insurance industries are the greatest adopters of RPA, but many customers may be unable to use RPA PaaS due to data privacy regulations like GDPR.

- Buyers frequently express concerns about RPA tool access to personal information and the transfer of confidential data outside of an organization's firewalls. Years of RPA adoption with limited security events have mitigated buyers' security concerns; however, a highly publicized breach enabled by RPA would affect buyers' willingness to place orchestration and development in the cloud.

- Customers that encounter connectivity issues (e.g., due to latency or incorrect network configurations) between on-premises bots and cloud orchestration have shared this negative experience with other potential buyers, dissuading them from adopting RPA PaaS capabilities.

User Recommendations

- Examine cloud in the form of RPA PaaS to overcome the hurdle of how to implement, maintain and update on-premises orchestrators to manage the bots. Because RPA demand will continue to grow as organizations seek to rapidly digitize and automate legacy processes. RPA PaaS can reduce the total cost of ownership (TCO) of RPA by reducing the maintenance burden of upgrades, patches and so on.
- Pilot a simple use case with a clearly defined ROI achievable within four to eight weeks. Focus on key business outcomes, such as productivity gain, higher accuracy and client satisfaction. When evaluating an RPA PaaS offering, be prepared to define and operationalize your cloud governance model jointly with business and IT to identify applicable processes, acknowledge technical debt and evaluate the performance of the application portfolio.

Sample Vendors

Automation Anywhere; Microsoft; NICE; Pegasystems; SS&C Technologies (Blue Prism); UiPath; WorkFusion

Gartner Recommended Reading

Beyond RPA: Build Your Hyperautomation Technology Portfolio

Magic Quadrant for Robotic Process Automation

Quick Answer: How to Choose the Right Use Cases for Robotic Process Automation

Secure Robotic Process Automation Initiatives With These 4 Essentials

Desktop as a Service

Analysis By: Stuart Downes, Mark Margevicius, Tony Harvey, Craig Fisler, Sunil Kumar, Eri Hariu

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Desktop as a service (DaaS) is the provision of virtual desktops by a public cloud or service provider. DaaS is bought by IT leaders seeking to provide desktop or application experiences from virtual machines accessed using a remote display protocol. DaaS vendors incorporate a fully managed control plane service into their offerings, which facilitates user connections and provides a management interface. DaaS can be delivered preconfigured as a service or can be delivered as a DaaS platform.

Why This Is Important

With DaaS, no data resides on the endpoint, offering a solution that can increase security, resilience and application responsiveness for remote workers. DaaS offers scalable services without adding infrastructure, allowing clients to appropriately size and consume their environments hour by hour, day by day, and month by month; however, not all DaaS solutions offer such granular billing options.

Business Impact

With DaaS, IT leaders can increase security for desktops and applications. Other benefits of DaaS, compared to traditional VDI, include:

- Flexible procurement options that allow scalable deployments.
- Simplified rollout of services to new geographic regions.
- Applicability to a broader range of industries and use cases.
- Lesser skills required for IT operations teams to deploy and operate virtual desktops and applications.
- More rapid expansion or contraction of workloads.

Drivers

DaaS will continue to mature and witness increased adoption through 2026. The technology has moved through the Trough of Disillusionment onto the Slope of Enlightenment due to the following factors:

- DaaS enables business continuity and remote work, with no data residing on the endpoint.
- The technology securely extends services to external contractors and third parties.
- Endpoint computing models allow device-independence and bring your own PC (BYOPC) endpoints.
- On-demand desktops enable a financial model that allows scaling of cloud resources and an operating expenditure (opex) model.
- DaaS can be purchased for short periods, enabling use cases such as seasonal workers or short-term contracts.
- DaaS enables rapid access to systems during mergers, acquisitions and divestitures.
- Rich graphics use cases like engineering, games development, video editing and geographic information systems (GIS) benefit from GPU-enabled workstation-class virtual desktops and applications.
- DaaS can be delivered to users in hours. The supply of a physical device, on the other hand, can take weeks, incur shipping costs and retrieval is not always guaranteed.
- The technology eliminates the need for complex and static VDI implementations.

Obstacles

- Usually, the business case turns positive only when security and user cost impacts are included.
- Organizations struggle when there is a change in financial models from capex to opex.
- GPU use cases can be extremely expensive and often need advanced protocols, which increases complexity.
- Multimedia streaming, web meetings and video call performance in DaaS are not equivalent to that of a physical endpoint.
- Performance issues may occur in DaaS because application architectures introduce network-related issues (i.e., latency and hairpinning).
- Some DaaS solutions require self-assembly, which, although simpler than VDI, can still be too complex for some clients.
- The full range of desktop management requirements may not be completely fulfilled by DaaS providers.
- Microsoft product terms that prevent the installation of Microsoft 365 applications on “Listed Providers” (see 3 Compliance Questions to Ask When Licensing Microsoft Windows and Office for VDI and DaaS).

User Recommendations

- Get familiar with the three DaaS market segments — self-assembled DaaS, vendor-assembled DaaS and vendor-managed DaaS — and select a vendor from the appropriate segment (see Market Guide for Desktop as a Service).
- Ensure your operational teams have the necessary skills if you select self-assembled DaaS solutions.
- Select a vendor-defined DaaS or vendor-managed DaaS solution if you do not have the operational skills.
- Choose a DaaS vendor whose services best align with your requirements; even within each segment, there are differences between the services vendors offer.
- Optimize multimedia streaming, web meetings and video calls.
- Select a DaaS vendor that offers the billing granularity you require.

Sample Vendors

Alibaba; Amazon; Anunta; ATSG; Citrix Systems; Microsoft; Nutanix; oneclick; VMware; Workspot

Gartner Recommended Reading

Market Guide for Desktop as a Service

How to Choose a Desktop Delivery Model for the Digital Workplace

Video: PCs, Virtual Desktops or DaaS: What's the Best Fit for Midsize Enterprises

3 Compliance Questions to Ask When Licensing Microsoft Windows and Office for VDI and DaaS

PC as a Service

Analysis By: Stephen Kleynhans, Autumn Stanish, Erin Pierre

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

PC as a service (PCaaS) refers to a PC procurement model in which customers pay for a configured PC that is fully supported throughout its life cycle. It builds on a combination of leasing, management support and added services, but offers more flexibility than traditional leasing or opex models. Changes in the dynamics of PCaaS offerings have necessitated a change in naming. In future Gartner reports, the name will be managed device life cycle services (MDLS) for better alignment.

Why This Is Important

Enterprises are pressured to transform IT delivery services to support and add value to new business initiatives and improve the employee experience. This is driving them to examine alternatives to traditional PC acquisition and management practices. PCaaS is available from several providers (including manufacturers, value added resellers and outsourcers) and can relieve IT teams of tedious device management processes, provide a predictable financial model, and scale to support a remote workforce.

Business Impact

PCaaS can help IT teams with:

- Enabling customers to outfit users with a PC at a predictable monthly fee.
- Reducing the number of touchpoints and contracts needed for service delivery, potentially improving accountability.
- Aligning with modern tools, such as Windows Autopilot, to automatically enroll new devices to distributed employees, potentially providing improved user experience.

Drivers

- Economic challenges have driven organizations to seek solutions that will help them cut costs through process efficiencies. Outsourcing internally inefficient device support operations can offset the added costs of PCaaS in some organizations. However, this is not generally true for most.
- New forms of PCaaS offerings are emerging to appeal to organizations that prioritize sustainability, such as the option to refurbish and remarket/redeploy to keep devices in use longer.
- Widespread remote work and now the shift to hybrid work, has made device management more challenging for many organizations, making PCaaS an increasingly attractive alternative to traditional PC procurement options.
- Offerings have matured and expanded with varied terms and conditions and service options. While there are still a number of custom deals, overall there is less confusion for customers about what PCaaS offers.
- Vendors continue to grapple with building attractive, profitable and affordable solutions by expanding their services while ensuring their internal capabilities are mature enough to deliver these offerings effectively. Initially, it will appeal to many of the same organizations that are looking at PC leasing today, or those looking to offload basic logistical activities associated with PC hardware deployment and maintenance.

Obstacles

- Understanding what services and financial models are available can be confusing, as “PC as a service” is a blanket term for many variations of PC leasing and/or services. In some cases, the services are offered on an “as-a-service” model independent of the actual device purchase.
- Providers occasionally overpromise on their services to make deals more attractive. This leaves customers with unmet delivery expectations as providers attempt to balance growing their service offerings with maturing their own internal capabilities.
- Elevated costs for basic services can be hidden within bundled overall pricing if it is not clearly broken out in proposals.
- Vendor lock-in causes customers to lose their autonomy over the endpoint management tools and processes.

User Recommendations

- Investigate PCaaS offerings as an alternative to standard leasing by weighing the benefits of reduced IT burden and a potential opex model with the additional cost of services.
- Ensure that the bundled services and/or tools are not duplicative of existing contracts or internal capabilities by selecting the offerings most valuable to unique IT team needs.
- Challenge suppliers to prove their ability to provide the services offered by establishing appropriate SLAs and a monitoring process.
- Prioritize vendors that have a broader range of modern software-enabled services, rather than those that still rely on manual processes.
- Prepare for potential volatility in the price of the services as vendors evaluate the true cost of providing these capabilities, by ensuring pricing or price caps are established for the entirety of the agreement.

Sample Vendors

CDW; CompuCom; Computacenter; Dell Technologies; HP Inc.; Insight; Lenovo; SHI

Gartner Recommended Reading

Customization and Automation Redefine the PCaaS Landscape

Critical Capabilities for Outsourced Digital Workplace Services

When to Purchase, Lease or Use PC as a Service

Entering the Plateau

Contact Center as a Service

Analysis By: Steve Blood

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Contact center as a service (CCaaS) is a cloud-based application service platform that enables customer service organizations to manage multichannel customer interactions holistically with prepackaged applications that support the customer and employee experience. CCaaS solutions are used by organizations that need to manage front-office operations such as customer service, telemarketing, employee service and support centers.

Why This Is Important

CCaaS is a growth market, fueling investment in innovation and customer service applications, and surpassing the offers of legacy premises-based or server-based technology. Now that CCaaS is a foundation of multichannel customer service, application leaders can explore the advantages of the suite offer. Leaders can add workforce engagement management and analytics in place of stand-alone applications, offering a more integrated set of services for a lower total cost of ownership.

Business Impact

The business impact of CCaaS is broad and deep:

- CCaaS offers an agile business model for investing in technology for engaging with customers through self- and assisted-service channels.
- A range of packaged applications and marketplace add-ons enables organizations to extend the services offered to customers and employees for improved experiences and lower operational costs.
- Cloud enables organizations to focus on transforming the customer experience, rather than managing the day-to-day technology.

Drivers

- Greater software agility with a lower cost of ownership has always been a key driver for investing in CCaaS. Agility has accelerated in recent years as IT organizations decommission premises-based communications infrastructure and, in its place, invest in specialized cloud services to meet specific organizational use cases for customer and employee experience.
- For most organizations, contact center investment is a cloud-first approach. Customer service leaders are working with IT leaders to consolidate multiple instances of premises-based contact centers and first-generation CCaaS into a common organizationwide platform. This is leading to a greater scale of contract (more than 5,000 user licenses is becoming typical) and broader geographical reach across multiple continents.
- CCaaS platforms are well-placed to manage both voice and digital channels, and are becoming the preferred option when a single skills engine is required to support CSRs trained in multiple modalities.
- Flexible working has become a core work style for customer service organizations and CCaaS platforms provide a superior experience to employees working remotely as well as in the office.

Obstacles

- Organizations with very large numbers of users (10,000+) are still challenged with justifying the costs of migrating users, the shift in operating mode from capital expenditure (capex) to operating expenditure (opex) and demonstrability for CCaaS parity with complex customization needs of premises-based platforms.
- As organizations grow CCaaS to thousands of users, there needs to be a stronger focus on resilience and uptime. While 99.99% uptime rate as a standard service-level agreement (SLA) is acceptable for most organizations, a more mature approach to service credits for nonperformance and service meeting structure is necessary.
- Most CCaaS providers have been focused on replacing legacy PBX-based contact center infrastructure with a core focus on the telephone channel. As organizations adopt a digital-first, self-service strategy, telephony-centric licensing may not look as attractive as offers from digital customer service technology and customer engagement center software providers.

User Recommendations

- Reduce the impacts of transitioning off legacy systems by focusing on providers with referenceable transition frameworks and methodologies for migrating from relevant on-premises systems to their CCaaS offerings.
- Focus on CCaaS solutions that leverage native functionality or are accessed through provider marketplaces that span all four capability areas of the reference model for the customer technology platform — contact routing and interactions, process orchestration, knowledge and insight, and resource management.
- Place increased evaluation weighting on flexible pricing models that can accommodate plans for shifting customer engagement away from live assistance and toward digital self-service, especially as development in generative AI improves the speed to value of self-service.
- Incentivize service uptime by defining tight SLAs and service terms, and agreeing on responsibilities between the CCaaS provider and the business unit for the duration of the contract.

Sample Vendors

8x8; Amazon Web Services; Cisco; Content Guru; Five9; Genesys; NICE; Talkdesk; Vonage

Gartner Recommended Reading

Magic Quadrant for Contact Center as a Service

Quick Answer: What Does a Technology Reference Model for a Customer Technology Platform Look Like?

2023 Strategic Roadmap for Customer Service and Support Technology

How to Choose Your Best-Fit Vendor for Contact Center as a Service

Toolkit: RFP Template for Contact Center and Workforce Engagement Management Applications

iPaaS

Analysis By: Keith Guttridge

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Gartner defines integration platform as a service (iPaaS) as a vendor-managed cloud service that enables end users to implement integrations between a variety of applications, services and data sources. iPaaS platforms support at least one of the three main uses of integration technology — data consistency, multistep processes and composite services. iPaaS provides adapters to simplify configuration connectivity. It provides a low-code workflow environment and supports hybrid deployment models.

Why This Is Important

The shift to the cloud along with digital and automation initiatives is boosting the iPaaS market, making it the biggest segment of the integration platform technology market (valued at $6.5B in 2022). Its functional breadth makes it the natural alternative to classic integration software such as enterprise service bus (ESB), and extract, transform and load (ETL) software for large organizations.

Business Impact

By addressing integration needs in a rapid and cost-effective way, iPaaS enables organizations to improve efficiency, increase business agility and introduce innovation faster. iPaaS adoption helps organizations achieve these goals cost-effectively, efficiently and with less specialized personas than are needed for classic integration software. Also, iPaaS makes these benefits accessible to midsize and small organizations that cannot afford the costs of a classic platform.

Drivers

- iPaaS is frequently adopted by organizations that seek to modernize their integration capabilities. This way, they can support digital transformation and cloud adoption (especially SaaS), and enable new roles and personas to be part of the integration delivery.
- There has been relative success for iPaaS targeting particular industries, SaaS ecosystems, business processes or geographies. This is due to its appeal to time-, skill- and resource-constrained organizations.
- The main goal of iPaaS providers now is to maximize opportunities to upsell and cross-sell to their vast installed base. Therefore, they are evolving their offerings into enterprise-class suites that address a wide range of hybrid, multicloud scenarios. Hence, large and global organizations now position iPaaS as a strategic option to complement — but increasingly also to replace — classic integration platform software. This drives deeper commitment among enterprises.
- A growing number of SaaS providers “embed” in their applications their own iPaaS, or one from a third party, which they typically extend with a rich portfolio of packaged integration processes (PIPs). This makes embedded iPaaS offerings attractive to organizations that need to quickly integrate a SaaS application.
- Providers will keep investing to improve developers’ productivity, reduce time to value and shorten the learning curve. The goal is to further expand their potential audience to include business users. Hence, providers’ R&D efforts might focus on using AI, machine learning and natural language processing. These capabilities can assist development and operation, enrich PIP portfolios, and enable continuous integration or delivery (CI/CD) and DevOps to entice professional developers.

Obstacles

- The market's extreme fragmentation (more than 175 providers) and diversity of capabilities makes it hard for user organizations to select the best-fit iPaaS for their needs. This could generate a proliferation of diverse, stand-alone and embedded iPaaS offerings. It could also risk fragmenting service providers' investments in skills building.
- The top five iPaaS providers command about 56% of the market, and only 10 providers have more than a 2% share. The vast majority of providers are smaller vendors with limited brand awareness. This may discourage risk-averse organizations from making strategic investments in smaller vendors or less familiar brands.
- Key obstacles are the API rhetoric of seamless "plug-and-play" integration, and confusion among less technically savvy users about the differences between iPaaS and API management platforms. There is also a growing trend for code-based integration encouraged by the cost of integration platforms and serverless PaaS functions.

User Recommendations

Adopt iPaaS when looking for:

- An integration platform for midsize organizations moving to the cloud and for "greenfield" integration initiatives.
- A strategic complement to traditional integration platforms — increasingly in the context of integration strategies based around hybrid integration capability framework— in order to empower a collaborative, democratized approach to integration.
- An enabler of self-service integration for business technologists, such as SaaS administrators or citizen integrators.
- A platform to support well-defined, tactical integration projects with low budgets, severe time constraints, and informally defined and incrementally formulated requirements.
- A potential replacement for classic integration platforms that are obsolete or cannot support changing requirements.

Sample Vendors

Boomi; Jitterbit; Microsoft; Oracle; Salesforce (MuleSoft); SAP; SnapLogic; TIBCO Software; Tray.io; Workato

Gartner Recommended Reading

Magic Quadrant for Integration Platform as a Service

Critical Capabilities for Integration Platform as a Service

Choose the Best Integration Tool for Your Needs Based on the Three Basic Patterns of Integration

How to Select the Right Mix of Integration Technologies

Appendixes

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	Status	Products/Vendors
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Predicts 2023: XaaS Is Transforming Data Center Infrastructure

How Do I Plan for Migrating My Data Center Infrastructure Into an XaaS Model?

Table 1: Priority Matrix for XaaS, 2023

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Platform-as-a-Service Provisioning		
High	Banking as a Service Desktop as a Service iPaaS	AI Model as a Service BMaaS Edge as a Service Enhanced Blockchain as a Service Firmware Protection as a Service PC as a Service Product-as-a-Service Supply Chains Storage as a Service	Data Security as a Service Everything as a Service Supply Chain as a Service	
Moderate	Contact Center as a Service	Backup as a Service Firewall as a Service RPA PaaS	Endpoint Access Isolation Insurance as a Service Lab as a Service/Robotic Cloud Labs Penetration Testing as a Service	Quantum Computing as a Service

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Low			Cloud Backbone as a Service Extranet as a Service NaaS	

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constrains replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)