Hype Cycle for Managed IT Services, 2022

Published 12 July 2022 - ID G00769959 - 111 min read

By Analyst(s): Brett Sparks, Danellie Young, Alan Stanley

Initiatives: IT Sourcing Strategy Development and Execution

Driven by complexity and constant change, IT services remain highly focused on automation, acceleration and cloud adoption. Sourcing, procurement and vendor management leaders should use this Hype Cycle to assess the maturity of emerging managed IT services when planning their sourcing strategy.

Strategic Planning Assumptions

By 2025, legacy IT services will shrink to 21% of spend, from 54% in 2019.

By 2026, 30% of organizations will have products and services ready for the metaverse, up from a negligible amount in 2022.

By 2028, more than 60% of larger enterprises will use external Internet of Things (IoT) services for at least half of their IoT solution build and run efforts, up from 20% in 2022.

Analysis

What You Need to Know

New in 2022, this Hype Cycle focuses solely on managed IT services across the entire technology stack. The past approach of efficiently supporting technology products, albeit new technologies, is being replaced by a paradigm of delivering outcomes and enabling business transformation. Accelerating digital transformation to achieve adaptable, resilient business platforms — as well as improved outcomes from such platforms — remains paramount for enterprises.

This new Hype Cycle will be relevant across the organization as business stakeholders expand the search for technology solutions to achieve their business outcomes. Those technology solutions will increasingly be sourced rather than built using internal resources. Although a need for traditional services will still exist, traditional will not be enough. This Hype Cycle does not feature those maturing services. Rather, it highlights the transformative and innovative IT services that are emerging and will be adopted in the near future.

The Hype Cycle

This new Hype Cycle describes the pace and maturity at which managed IT services are evolving to support the continued need for:

- Digital acceleration
- Business agility
- Resilient platforms using intelligent, emerging technologies
- Services from anywhere

It is an eclectic mix, but the services fall into three groups: [1]

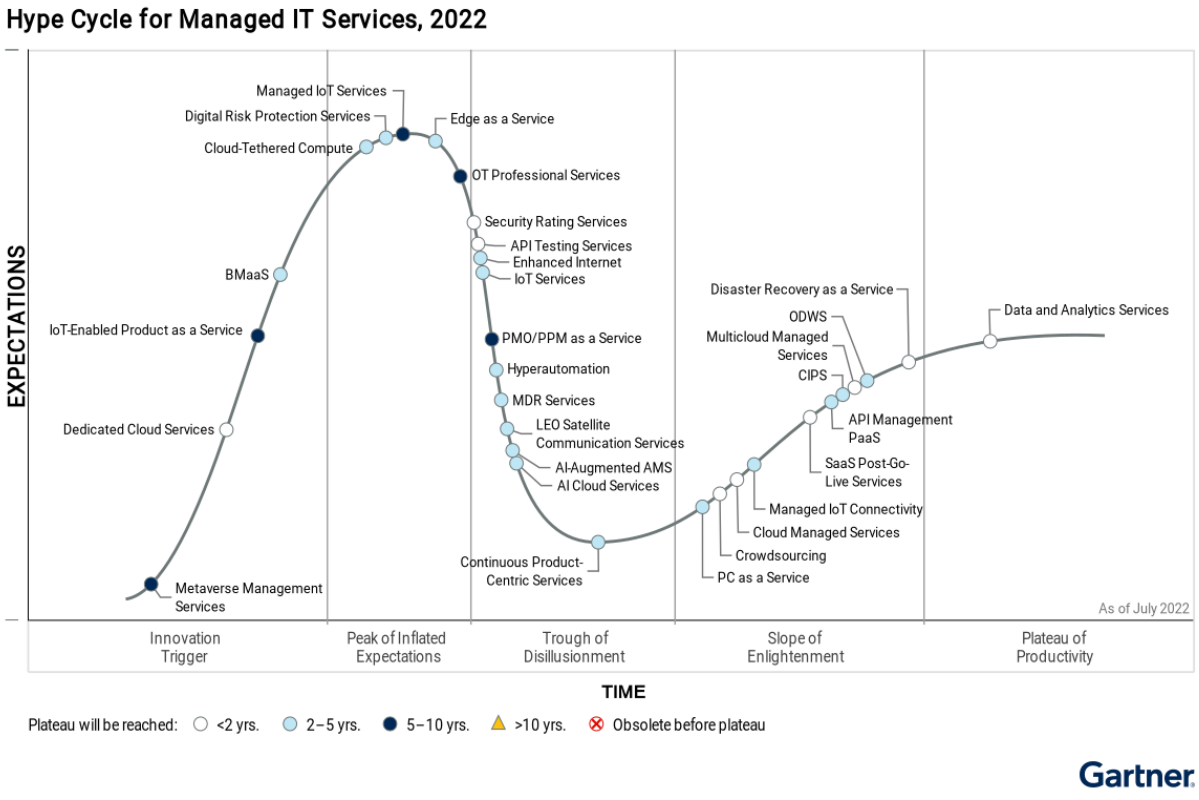
1. Delivering traditional services, but in a more innovative way
2. Establishing a new way to deliver platform components on an organization's behalf
3. Establishing new ways to deliver outcomes on an organization's behalf

The platform and outcome delivery are where the hype is strong. As organizations modernize their technology platforms, more and more offerings from third parties will emerge to provide the components and ongoing services needed. Some will become mainstream very quickly, and some will be superseded or aggregated with other offerings well before hitting their peak.

Similarly, technologies such as hyperautomation and artificial general intelligence [2] will combine, enhancing, optimizing or supplementing existing services. These technology combinations will also generate new autonomous services, which may radically transform service delivery or rapidly fizzle out when the hype dies.

Sourcing, procurement and vendor management (SPVM) leaders must understand the extent to which IT services can affect and guide their service sourcing strategy [3] and investment decisions, as services offer varied delivery options and contract structures. To cut through the hype, IT leaders should use this research to guide their strategic planning for managed IT services.

Figure 1: Hype Cycle for Managed IT Services, 2022



Source: Gartner (July 2022)

The Priority Matrix

The Priority Matrix shows managed IT services, by impact, against a timeline for the number of years until mainstream adoption. It is useful for ranking which services an organization should examine first based on maturity and potential business impact. With the continued drive to modernize technology platforms, it is no surprise that dedicated cloud services, metaverse management services and IoT-enabled product as a service are transformational.

Organizations already undergoing modernization initiatives should focus on maximizing the impact and outcomes of those decisions with services such as managed IoT services, PC as a service and AI-augmented AMS. While modernized services stabilize, organizations should plan to deploy more proven services, such as ODWS, CIPS and continuous product-centric services, to continue the momentum.

Gartner continues to observe the intersection of maturing and new services, especially in the areas of scalability and operational efficiency, with mainstream adoption of many significant services expected over the next two to five years. Services such as AI cloud services and edge as a service are being viewed as highly beneficial within the same time frame. Similarly, managed IT services will see moderate to high impact from API testing services, cloud managed services and SaaS post-go-live services.

Table 1: Priority Matrix for Managed IT Services, 2022

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	Dedicated Cloud Services		IoT-Enabled Product as a Service Metaverse Management Services	
High	API Testing Services Cloud Managed Services Data and Analytics Services Multicloud Managed Services	AI-Augmented AMS AI Cloud Services BMaaS CIPS Continuous Product-Centric Services Digital Risk Protection Services Edge as a Service Hyperautomation IoT Services LEO Satellite Communication Services Managed IoT Connectivity MDR Services ODWS PC as a Service	Managed IoT Services OT Professional Services PMO/PPM as a Service	
Moderate	Crowdsourcing Disaster Recovery as a Service SaaS Post-Go-Live Services Security Rating Services	API Management PaaS Cloud-Tethered Compute Enhanced Internet		
Low				

Source: Gartner (July 2022)

On the Rise

Metaverse Management Services

Analysis By: Brett Sparks

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Embryonic

Definition:

Metaverse services are composed of the technologies and disciplines required to design, build, operate and sustain an organization's virtual world where they and their trusted citizens from other metaverses collaborate, co-create and invent safely and under agreed mutual laws. Not unlike physical security and facilities services, metaverse managed services provide the critical function of making sure the ideas, data or IP shared is protected and workplace violence or harassment is nonexistent.

Why This Is Important

As awareness of the metaverse has leapt into corporate culture, more companies are utilizing these capabilities and developing their own virtual spaces to increase customer engagement/interest, drive employee retention or host virtual hands-on training. While these services are mainly in the hands of a few solution/service providers (Rooom, Teams, Virbela, etc.), organizations will look to have their own virtual real estate complete with landscaping architects (branding) and janitorial services (social monitoring).

Business Impact

Potential impacts on brand, clients, growth and revenue are enormous, both positively and negatively. Metaverse services must be taken seriously, as potential business impacts can include:

- Brand awareness and management for consumer-facing applications, such as support, sales and marketing, e-commerce, XR and/or gaming platforms.
- Employee experience and productivity for internal-facing applications, such as virtual meetings, collaboration tools and training.
- IT cost of ownership and ops, such as compute instances, storage and connectivity, procurement and management of XR devices for employees.

- Finance, revenue management and business models, such as adoption of digital currencies and NFTs.

Drivers

- As the COVID-19 pandemic pushed toward remote work, the metaverse now pushes us farther into augmented 3D digital worlds of the future.
- In line with the concept of Anywhere Services, metaverse managed services look to provide highly immersive and interactive environments for conferences, storefronts, labs and creative workplaces like manufacturing, pharmaceutical, gaming, construction and travel and hospitality.
- Unlike the point-in-time, singular-event virtual meetings of today, gatherings in metaverse spaces will require sound governance and maintenance in addition to the deep data and analytics for organizationwide scale.
- Like most large initiatives, engagement from almost every layer of the organization will need to be engaged and educated on the new benefits and risks. From HR leaders and corporate counsel to CISOs and IT operations, this will be a new frontier.

Obstacles

- Maturity and wide adoption of IoT, Edge computing and augmented/virtual reality (AR/VR) has been slow moving in many organizations. Without these core technologies, employment of a metaverse is not possible.
- Though blockchain is essential in the metaverse, over 75% of organizations are still researching its usefulness, with only 11% having fully deployed this technology.
- Self-sovereign identities (SSIs) are elemental for traversing between metaverses and critical to the success of play-to earn (P2E) commercial aspirations. While critical, standardization and adoption of a unified SSI model is a work in progress, and therefore, so are privacy concerns.
- Organizations are new to the application of their ESG policies for metaverse solutions (e.g., immersive meetings, collaborations or training) and will require further POCs and trials to iterate requirements for management services required.

User Recommendations

- Work with business areas interested in the metaverse to selectively invest in emerging technologies, innovation and specific intellectual property (IP) by choosing the ones that are most aligned with product and service roadmaps for the next 36 to 48 months.
- Choose providers that can understand your organization's midterm product and services roadmaps and develop capabilities that are persistent, decentralized, collaborative and interoperable, as they are the key aspects of a complete metaverse.
- Help set and manage executive expectations for timelines on creating and employing a complete metaverse and the cost of maintaining virtual worlds.

Sample Vendors

Accenture; Globant; Oodles Technologies; QReal; Tech Mahindra

Gartner Recommended Reading

Emerging Technologies: The Future of the Metaverse

Emerging Technologies: Critical Insights on Metaverse

Dedicated Cloud Services

Analysis By: Tobi Bet

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Dedicated cloud services can be viewed as a subset of distributed cloud. They include the installation and management of a locally placed cloud (via appliance) on the edge within the clients control plane encompassing all data points including metadata. While these services perform at less than public cloud scale, they can deliver a solid economic edge option demonstrating better performance than an on-premises solution.

Why This Is Important

With nationalism, weather instability and the recession on the rise, organizations will be looking for more creative ways to meet their business needs. War, the pandemic, ransomware, latency, legal and legacy issues will drive different behaviors in the next decade. This service will have a transformational impact with the introduction of this type of cloud, potentially increasing from its current status as a niche service to reaching 5% market share by 2025.

Business Impact

Concerns stemming from latency or legacy issues will need to be considered by Gartner's estimated 54% of global organizations still running legacy applications.

Drivers

- Sovereignty and national regulations will perpetuate the need for new and lesser used existing ways to deliver cloud services regionally.
- Socioeconomic factors such as the pandemic and Russia's Invasion of Ukraine are pushing the need for a cloud like service organizations can control.
- Rising security concerns including ransomware, web bot attacks and malware will have a direct impact on organizations wanting better performance but wary of relinquishing their data off-site.

Obstacles

- Oracle Dedicated Region Cloud@Customer/Exadata Cloud@Customer, Google Anthos, Microsoft Azure Stack, Hewlett Packard Enterprise (HPE) and a few others offer a version of an appliance/cloud service, but none are widely used at this time.
- If external factors continue to push the cloud back to a more "private" environment, a supply chain issue could develop if the demand increases quickly.
- Many such systems require a long-term commitment and physical space for the appliance placement.
- The options are sparse and dissimilar, requiring clients to be very specific about what each service can and cannot do.

User Recommendations

- Get acquainted with dedicated cloud services and edge options as a viable alternative to the public cloud if one of the above issues is of major importance to the success of the business.
- Some dedicated cloud services eliminate technical debt through a lease option while others may not. It's important to understand each vendor's capabilities and differences.
- Ask your cloud center of excellence (CCOE) or vendors' CCOE to review all the options including dedicated cloud.
- Clarify and document where the boundaries exist between the responsibilities of the supplier and IT team — elements such as data backup and application security may be the end user's responsibility.

Sample Vendors

Accenture; Atos; Amazon Web Services Proserve; Birlasoft; Cintra; Centroid; Deloitte; Hitachi Vantara; Oracle OCS/ACS; Taos

Gartner Recommended Reading

Is Oracle Cloud Infrastructure Ready for Use in Your Multicloud Strategy?

Market Guide for Oracle Cloud Infrastructure Professional and Managed Services

Forecast Alert: IT Spending, Worldwide, 1Q22 Update

IoT-Enabled Product as a Service

Analysis By: Eric Goodness, Scot Kim

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

IoT-enabled product as a service is a commercial model where businesses acquire “servitized” operational assets as recurring operating charges. Agreements define fitness for purpose and guaranteed outcomes based on asset performance, availability and quality of output. Embedded IoT provides users, manufacturers and financial intermediaries asset data required to audit asset usage, effectiveness and to mediate remedies for nonperformance.

Why This Is Important

Leasing contracts are well-established in select industries. However, selling equipment and products as a service, based on usage-based fee without terms and revenue commitments, is nascent. Redefining non-IT assets as a flexible operating expense with conditions for performance, scale and availability is transformational for enterprises. This business model reduces impediments for purchase or where margins from consumables offset selling equipment at cost or near cost.

Business Impact

IoT-enabled product as a service transforms how manufacturers sell products and services, and how enterprises consume them in terms of flexibility for usage and the ability to ramp up and scale down usage. A good model for IoT-enabled product as a service requires an end-to-end IoT distributed architecture that supports a usage-based business asset with contracted guarantees for reliable business outcomes that span asset performance and effectiveness. Such a model reduces the risk of asset investment and performance, and provides clarity to the cost of operations.

Drivers

Drivers that lead enterprises to consider IoT-enabled product as a service include the following:

- Increasingly, the technologies needed to implement the IoT-enabled product as a service business model are readily available at costs that continue to decrease year over year. Key to the reduction in costs is the use of open-source technologies, and the increasing presence of off-the-shelf capabilities to integrate into various IT and OT systems that reduce the costs of development and integration.
- IoT-enabled product as a service speaks to a strong overall business trend to shift business costs from asset ownership and capital expenditure (capex) to asset subscription and operating expenditure (opex).

- There are increasing numbers of financial intermediaries willing to finance large, expensive assets in the IoT-enabled product-as-a-service model. This relieves OEMs from owning the very assets they manufacture.
- Additionally, a growing class of IT and OT system integrators have embraced IoT-enabled product as a service as a new revenue stream. These vendors bundle assets with life cycle services that price assets as a service; the model also eliminates the user need to staff for the maintenance and support of the asset.
- IoT and “connectedness” provide an improved approach to ongoing over-the-air (OTA) software release and change management for software updates, patches and fixes.

Obstacles

- The adoption of IoT-enabled product as a service includes the complexity of engaging in due diligence for a service that is concept not well-known by many sourcing and vendor management personnel. Users must consider a host of business considerations ahead of procurement, such as hours or coverage for service and support, SLAs and time to cure for business impacting events, determinants for penalties and termination for nonperformance.
- IoT-enabled product as a service requires input from IT and OT executives and operations management. Operations managers must support the performance management approaches and practices of the provider offering revenue-generating assets as a service. The IT organization is key to ensuring the support systems that enable the “servitization” of assets conform with the architecture, systems and security of the buying organization.

User Recommendations

- Perform your own multiyear total cost of ownership analysis to validate the benefits of an IoT-enabled product as a service.
- Work to determine if the manufacturer engages with financial intermediaries to operationalize the as-a-service offerings. Determine if P&C coverage is available to mitigate the risks of engaging in such a model.
- Negotiate agreements that clearly establish mutually agreed SLAs and OLAs for IoT-enabled product-as-a-service performance and reliability.
- Factor in all nonrecurring and recurring charges, terms of agreement and penalties into your IoT-enabled product-as-a-service business model.
- Secure the rights to IoT-enabled product-as-a-service data, including mutual agreements on exactly which data and the methods are required for accessing it.
- Determine which other entities will have access to your data and how your data is monetized by the supporting ecosystem.

Sample Vendors

Atlas Copco; Caterpillar; Cy.Pag.; Danfoss; Michelin; Philips; Toshiba; Xylem

Gartner Recommended Reading

Asset-Intensive Manufacturing CIOs Must Invest in Gartner's 2022 Top Strategic Tech Trend — Total Experience

Market Trends: Consumption-Based Pricing for On-Premises Infrastructure Is Evolving to an as-a-Service Model

Guide Contract Management With the EaaS Customer Bill of Rights

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) provides physical infrastructure such as 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 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 can run workloads without restrictions based on hypervisor or OS compatibility, or performance concerns for client workloads. This results in faster and more agile "physical" infrastructure deployment, and efficiency in meeting elasticity and scalability demands. BMaaS is often selected over virtualized public cloud infrastructure to conform to legacy software licensing requirements based on permanent deploying onto fixed physical hosts (e.g., Oracle).

Business Impact

BMaaS offers:

- The advantages of dedicated infrastructure (predictability, security, performance) with the elasticity, scalability and agility of IaaS.
- A cloudlike experience in a data center location better suited to customer needs for low network latency and data residency, for example.
- 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

BMaaS is not an entirely new concept, but it is gaining momentum again, not as a complete replacement for on-premises equipment or the cloud, but as an augmentation. Drivers include:

- The ability 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 — is attractive.
- There is interest in cloud-native technologies as a path toward cloud independence and to reduce lock-in.

- Bare metal may solve the issue of physical workload location addressing the concerns that highly centralized offerings may pose, either due to latency concerns, enterprise control, or data sovereignty and regulations.
- Bare metal offers the speed and agility of public cloud, with far greater control over workload and data placement.
- Noncontinuous use of bare metal can be less costly than physical infrastructure, does not tie up capital expenditure (capex) and is faster to deploy operationally as operating expenditure (opex).

Obstacles

- 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, or integration of multiple, network offerings may be required.
- 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

- Identify target candidates for BMaaS by evaluating IaaS-bound applications and determining whether the attributes of BMaaS are a better fit.
- Build BMaaS into cloud assessment models by identifying those attributes that can only be addressed through the software licensing compatibility, hypervisor independence and 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 whose licensing terms are 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

At the Peak

Cloud-Tethered Compute

Analysis By: Tony Harvey, David Wright

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Cloud-tethered compute is an approach to edge-in systems management in which servers are designed to be deployed across a wide range of locations, but centrally administered from a vendor-provided console located in the public cloud. The cloud connection may be permanent or intermittent. It can deliver Bare metal as a service (BMaaS), Infrastructure as a service, PaaS or a combination of these solutions — typically, but not exclusively in a subscription based model.

Why This Is Important

Edge-in solutions and hybrid infrastructures that use both on-premises and cloud-based compute need to be managed from a single console that can deploy, update and monitor at scale. Cloud tethering provides an ideal way to do this with a cloud based management platform that provides easy connectivity and can scale as needed.

Business Impact

Cloud-tethered compute systems will affect businesses across IT, finance and procurement:

- IT teams will see a reduced need for local administration and maintenance, freeing them up for higher-value activities.
- New skills will be required in the business for contractual analysis, security and spend management for these systems.
- The IT and finance resource budget may cycle to a services-based delivery model.
- IT operations will be more flexible and aligned with business demands.

Drivers

- The ease and capabilities of a SaaS-based solution for managing devices at scale, especially when devices have intermittent connectivity.
- IT teams are being tasked with delivering differentiated IT services to the business. Avoiding local administration using a cloud-tethered compute system enables the IT to focus on these higher level services in a self-service automated fashion without having to involve a traditional IT outsourcer.
- For “born in the cloud” companies that have no capability or desire to build on-premises solutions, cloud-tethered compute systems enable them to meet data sovereignty or latency requirements.
- Promise of “evergreen” technology refresh solutions that keep systems up-to-date with the latest technology, removing the need for IT to manage infrastructure refreshes.
- More realistic products that do not promise a complete cloud experience, but a cloud-managed experience with access to cloud services.

Obstacles

- Risk of insufficient agility: current three year agreements and fixed hardware investments are at odds with the dynamic and changing nature of the edge infrastructure markets.
- Limitations on service availability that do not match the customer expectations. What services customers actually want and what the various providers are able to deliver have not yet to date matched up fully.
- Differences in deployment models between IT-based solutions that deploy into data centers and cloud-tethered solutions that are being deployed into environments more traditionally associated with Operational Technologies.
- In many cases, the vendor expertise in support of and maintenance of field solutions is new and untested.

User Recommendations

- Identify scenarios in which the tethered compute model provides clear business value, versus a more-traditional IT solution.
- Ensure that field maintenance operations and SLAs are well-documented and -understood.

- Use pilot programs to evaluate vendor capabilities and any necessary updates to I&O procedures, processes and skill sets.
- Organize a joint team that includes I&O, OT, vendor management and finance to evaluate all proposed cloud-tethered compute solutions.
- Assess the economics and requirements against a range of vendor solutions and consumption models; each vendor will have very different capabilities.
- Ensure that contract terms and SLAs meet the requirements of the finance and IT teams, and that end-of-term options (or lack thereof) are fully understood.
- Clarify and document where the boundaries exist between the responsibilities of the supplier and IT team — elements such as data backup and application security are likely to be the end user's responsibility.

Sample Vendors

Avassa; EDJX; Hivecell; Microsoft Azure ARC; Pratexo; Spectro Cloud; Sunlight.io

Gartner Recommended Reading

Distributed Cloud: Does the Hype Live Up to Reality?

Quick Answer: How Executive Leaders Should Understand and Address Public Cloud Risk

Top Strategic Technology Trends for 2022: Cloud-Native Platforms

Cool Vendors in Edge Computing

Digital Risk Protection Services

Analysis By: Mitchell Schneider

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Digital risk protection services (DRPS) are delivered via a combination of technology and services to protect critical digital assets and data from external threats, and enable attack surface reduction. These solutions provide visibility into the open (surface) web, social media, dark web and deep web sources to identify potential threats to critical assets and provide contextual information on threat actors, their tactics and processes for conducting malicious activities.

Why This Is Important

During the past few years, attacks (e.g., credential theft) have become more complex, voluminous and targeted, and they are continuously disrupting business operations for organizations worldwide. The relevance of digital risk is not limited to security operations, but also other business functions, such as marketing, legal and fraud. Furthermore, DRPS is a highly outsourced function because the need is often driven by the fact that many organizations do not have the necessary in-house skills.

Business Impact

DRPS proactively identifies exposed digital assets at risk, collects and performs analysis of mapped data with prioritization of risks, and offers alerting and reporting capabilities providing actionable intelligence. Furthermore, it enhances business resilience, using people, process and technology (e.g., taking down an active threat and remediating on misconfigured environments) and improves security posture, which can prevent future threats and business operational impact.

Drivers

- The continued interest in DRPS — in terms of more vendor offerings and adoption — has been driven by its ability to support a broad range of use cases and user roles. Example use cases include digital footprinting (e.g., mapping internal/external assets and identifying shadow IT); brand protection (e.g., impersonations, doxing and misinformation); account takeover (e.g., credential theft, lookalike domains and phishing sites); data leakage detection (e.g., protection of intellectual property and PII of employees and customers, as well as credit card data); and high-value target monitoring (e.g., VIP/executive monitoring).
- Complexities in the management of risks are key reasons organizations benefit from DRPS. These complexities include an expanding attack surface, due to a more mobile workforce; higher reliance on e-commerce, regulatory compliance, cloud assets, digital business transformation; and the magnitude of information derived from monitored risk and security activities.
- Demand for DRPS has also been driven by the accessibility of such an offering for small or midsize businesses (SMBs) that originally couldn't benefit from threat intelligence (TI), due to lack of specialized skills and resources on security. This is because of the less technical and more accessible nature of the intelligence made available by many DRPS providers, as well as the availability of a managed service type of offering.

Obstacles

- The DRPS space is growing with more than 50 vendors aligned with this market. The vendor capabilities vary and may be limited in their ability to provide a comprehensive solution. Some vendors have a best-of-breed approach, whereby they focus heavily on niche DRPS use cases (e.g., VIP/executive monitoring), whereas many vendors have expanded to support more than one use case, including external attack surface management (EASM) — the latter natively or via acquisition.
- Market consolidation is accelerating and increasingly overlaps with complementary markets, such as TI, endpoint protection platforms (EPPs), managed security service providers (MSSPs)/managed detection and response (MDR) providers, as well as EASM. These markets are experiencing increased competition.

User Recommendations

- Evaluate the capabilities and features of DRPS offerings and match them to the needs of users' security programs and business risks. Ask vendors what threats they cover and whether they focus on a specific use case or many (e.g., phishing, dark/deep web monitoring, digital footprinting, data leakage and/or social media protection).
- Prioritize best-of-breed solutions to meet specific urgent needs, depending on the urgency and importance of the core use case. One example would be threats arising from consistent look-alike domains and phishing domains requiring takedown services. Assess vendors based on takedown success rates and ability to work with internet service providers (ISPs) and registrars in foreign locations.
- Prioritize solutions that include managed services in their offerings (especially if there are resource constraints), that can predict and prevent issues from occurring in the first place, and have service-level agreements (SLAs) that ensure the fastest remediation time.

Sample Vendors

BlueVoyant; CloudSEK; CybelAngel; Cyberint; Digital Shadows; HelpSystems; Microsoft; Rapid7; Recorded Future; ZeroFOX

Gartner Recommended Reading

Market Guide for Security Threat Intelligence Products and Services

Competitive Landscape: Digital Risk Protection Services

Quick Answer: What Is the Difference Between EASM, DRPS and SRS?

Innovation Insight for Attack Surface Management

Managed IoT Services

Analysis By: Eric Goodness, Emil Berthelsen

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Managed IoT services are third-party services that support part or all of the production of an IoT solution by an end user on an ongoing basis. Delivery of managed IoT services is most often enabled by cloud-based tools and skilled personnel observing structured processes in an operations center. However, there is a demand for on-premises delivery, especially where IoT integrates with a certain class of OT systems.

Why This Is Important

Managed IoT services integrate and aggregate a range of technologies included within the categories of edge devices, IoT platforms and IoT-enabled applications. Overall, managed IoT services converge IT and OT through integration, and offload the day-to-day monitoring, management and related analytics of IoT systems that contribute to business outcomes. Additionally, the service addresses a significant lack of skills to design, build and run IoT solutions.

Business Impact

There is an increasing demand for IoT-enabled business benefits, such as improved customer experience, creating new servitized products, and new revenue and insights from data. Enterprises are investing in managed IoT services to reduce the time to value of deploying IoT and shift the risk of IoT success to external providers to guarantee outcomes associated with digital business. Perhaps the fastest-growing use of managed IoT services lies with manufacturers creating smart connected products.

Drivers

Managed IoT services moved further toward the Peak of Inflated Expectations on the Hype Cycle. The move is based on the increase in IT-centric and IoT service providers now offering managed IoT services, and the use-case examples being shared with Gartner. Enterprises recognize the need to offload the management of their IoT solutions for a number of reasons, including:

- Cost reductions
- Access to skills that do not exist within the company
- Improved user experience, such as the use of predictive maintenance
- Too large scope and scale of the deployed solution to create a platform and organization dedicated to effective monitoring and management to guarantee a certain level of availability and performance

- Security

Obstacles

- A lack of end-user experience for upfront planning and strategy development for these services
- An inability to focus on simply scoped use cases, such as condition-based monitoring of a non-IT asset, which are generally more successful than broader, far-reaching digital transformation projects
- A lack of experience to identify and define remedies for nonperformance based on business impact
- A lack of service providers with deep expertise and experience across a wide range of use cases

User Recommendations

Align managed service provider (MSP) attributes and capabilities within your sourcing selection criteria, including foundational elements, such as:

- Expertise in creating and managing complex multisourcing agreements that span the technologies, service delivery, and outcomes and SLAs
- Professional services for the integration of devices and platforms, and pushing sensor data to enterprise applications
- Alignment of your key performance indicators (KPIs) with the SLAs of the managed services proposed

Sample Vendors

Accenture; Atos; Cognizant; Insight; Orange Business Services; Tata Consultancy Services (TCS); Wipro

Gartner Recommended Reading

Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2021-2031, 1Q22 Update

3 Areas to Drive IoT Differentiation Beyond Functions and Features

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 of 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 implementation challenging for even the most tech-savvy enterprises, while the potential for selecting a technical “dead end” is high. Edge as a service features a delivery model for edge computing in which a system integrator, independent software vendor and/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

- Most enterprises do not possess the skills or experience to build and manage complex, distributed systems incorporating a diversity of end systems and software stacks.
- EaaS delivers and maintains prebuilt solutions with a primary focus on meeting service-level agreements (SLAs) 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 vendor selection a nearly impossible task.
- Enterprises looking to limit risk find EaaS to be a safe and defensible choice. 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.

Edge as a service solves for:

- Lack of skills and experience in building and operating edge computing solutions.
- Exposure to technology obsolescence.
- The business unit preference for business-outcome-based solutions rather than technology.
- Unpredictable costs when the number of sites is either growing or shrinking.

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 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 (targeted, specific application set versus a more general, distributed infrastructure platform).
- Examine EaaS 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

2021 Strategic Roadmap for Edge Computing

OT Professional Services

Analysis By: Kristian Steenstrup

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Operational technology (OT) professional services encompass professional services delivered by consulting companies with engineering capabilities and engineering services, OT system integrators, and OT system OEMs. The services focus on data collection and management of equipment (integration), such as heavy machinery as well as OT cybersecurity, product management tools and processes. Providers supporting these services typically offer industry-specific or product-specific OT system knowledge.

Why This Is Important

Asset-Intensive industries will need help aligning and integrating IT and OT domains so should consider OT professional services. The market is split between OT vendors offering professional services, OT focused service providers and industrial IoT-focused companies. The rise of IoT means that IT-centric service providers may disrupt the OT professional services market. The conservative and risk-averse nature of the market creates slower growth than we would see in an IT-oriented market. 44% of clients surveyed use external OT services in some form.

Business Impact

Businesses are impacted in two major ways:

- CIOs can accelerate their transformation by utilizing OT professional services in coordination with internal IT resources.
- OT professional services can support industries to deploy digital solutions for business initiatives that drive key outcomes — such as cybersecurity, asset optimization and operational efficiency — and provide operational cost reductions and savings.

Drivers

- While IT is responsible for OT in many companies their lack of experience will be aided by outside expertise.
- Business initiatives driven by the proliferation of digital business and Industrie 4.0 continue to increase enterprise spending on OT professional services.
- There is interest in integrating industrial IoT into OT platforms that could be quicker to unlock with professional services help.
- Many clients (24%) will look to their OT vendors to provide these services because they are most familiar with the equipment and OT systems deployed.
- OT professional services providers bring deep vertical knowledge, equipment knowledge and updated strategies to manage and leverage OT environments.
- Shortage of required skills in end-user organizations.

Obstacles

- The position of this innovation profile is moving slowly. The use of OT professional services struggles to gain traction with businesses who take a DIY approach.
- Providers struggle with marketing their value and contribution to tip the balance.
- OT services are more industry- and equipment-specific than IT services, and therefore more specialized and fragmented.
- Risks exist if the OT service provider does not have sufficient experience in a client's specific technology platforms and industry.
- Overall rarity of experienced resources in the OT service providers' organization.

User Recommendations

Industrial companies with OT requirements are moving forward in the deployment of digital solutions, which increases the need for OT expertise in support of these digital solutions. OT professional services innovation is an inherently verticalized function.

- Seek providers that support your industry locally with domain-specific operations knowledge. These providers should have an understanding of the OT systems (design and function), data processing and analytics methods, operational data flows, the level of integration required between IT and OT, and the opportunity to leverage OT data for business gain.
- Create a capability assessment that defines your internal OT expertise, as well evaluation criteria to identify and select the best-fit OT professional services provider.
- Partner with OT professional services providers that are aware of the more-prevalent IoT-industry-focused standards, regulations and consortia not only within your industry but your geography.

Sample Vendors

Atos; Black & Veatch; Hitachi; NTT DATA; Rockwell Automation; Wipro

Gartner Recommended Reading

Quick Answer: What Are IT/OT Alignment and IT/OT Integration?

Manufacturing Insight: How to Position Hybrid IT/OT Offerings

Sliding into the Trough

Security Rating Services

Analysis By: Christopher Ambrose, Sam Olyaei

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Security rating services for cybersecurity provide continuous, independent scoring and rating for enterprises with a visible presence on the internet. They gather data from public and private sources via nonintrusive means, analyze the data and rate security using proprietary scoring methodologies. These tools are used for internal security, cyberinsurance underwriting, due diligence in mergers and acquisitions, and third-party/vendor cybersecurity assessments and monitoring.

Why This Is Important

The increasing focus on cybersecurity threats and data privacy regulations and the reliance on third parties — especially (but not exclusively) cloud service providers — have created a growing need to understand internal and external threats and security postures. The traditional approaches for assessing third-party security controls are stressed and have limitations, especially when hundreds or even thousands of external parties are involved.

Business Impact

SRM leaders can obtain an objective, yet passive, and therefore incomplete evaluation of a company's cybersecurity posture for a relatively low cost. SRS has been used to engage corporate boards and senior leadership in facilitating ongoing security investments. SRS findings can be used to supplement data derived from security assessments and business impact analysis; however, a "rating score" without context provides limited value for business executives and board members.

Drivers

There are many drivers to why an organization may consider using an SRS:

- Third-party security assessments or certifications provide point-in-time snapshots, but are not always available or shared by third parties.
- Relying on vendor-completed security questionnaires is also point-in-time, and is highly subjective, labor-intensive and inefficient for infosec departments and the vendors asked to complete the assessments.
- Some clients are under increased pressure to provide cybersecurity posture measures to senior management and to their customers, ideally in comparison with peers and competitors.
- Increasingly, enterprises struggle to translate cybersecurity metrics into quantifiable measures of risk.
- Vendors can use SRS to support sales and marketing by demonstrating that they practice good security.
- SRS represents an independent source of data to support a number of use cases.
- Some buyers are looking for more than a security rating, and that's driving SRS vendors to alter their product strategies, expanding capabilities to include other solutions and services (e.g., security assessment questionnaires, managed services) at lower price points than traditional GRC or IT Vendor Risk Management solutions.

While the use cases for these solutions are documented here, Gartner expects that additional use cases will emerge to address the growing demands for measuring and monitoring cybersecurity controls. Additionally, Gartner expects to see more mergers and acquisitions in this market, which continues to expand with limited differentiation among new entrants.

Obstacles

- While providing some useful metrics of an entity's cybersecurity posture, these services don't provide a complete assessment of security controls, as their information is primarily publicly sourced (from accessing internet IP addresses, for example).
- The market for SRS continues to evolve with some SRSs adding capabilities to supplement their "outside-in" passive internet scanning models with assessment data that they or their customers collect. This is done through the use of automated assessment survey tools that let the user request information on third-party cybercontrols, policies and standards.

- No service or solution has matured to provide consistently time-tested ratings, and some may not have full visibility in cloud environments, especially SaaS.
- Although we see these services as important innovations in improving an enterprise's ability to assess and monitor the potential for cybersecurity vulnerabilities, they are not a replacement for due diligence and assessment of internal or third-party controls.

User Recommendations

SRM leaders can use SRS to:

- Evaluate the security posture and possible control inadequacies of a third party.
- Monitor and receive alerts on the security status of key vendors and service providers.
- Provide leadership with an independent assessment of their own security posture, and compare that to peers or competitors.
- Provide leadership and internal stakeholders with a rudimentary quantification of a vendor or other third party's risk to an enterprise.
- Demonstrate their security posture to prospects and customers by sharing scores.
- Evaluate an organization's security posture in support of cyberinsurance underwriting processes.
- Inform merger and acquisition (M&A) decisions.

Sample Vendors

BitSight Technologies; Black Kite; Panorays; RiskRecon; SecurityScorecard; UpGuard

Gartner Recommended Reading

Innovation Insight for Security Rating Services

Navigating the Vendor Risk Management Solution Market

API Testing Services

Analysis By: Jaideep Thyagarajan

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

API testing services refers to a set of testing activities that is performed directly and as part of integration testing to validate if the programming interfaces meet expectations for quality, functionality, reliability, performance and security. Focusing mainly on the business logic layer of the software architecture, API testing involves using software to send calls to the API, receive output and validate the system's response.

Why This Is Important

Defective APIs directly impact digital experiences, such as mobile apps and reactive web applications, meaning that API quality is critical. Poor-quality APIs impact developer experience, which is increasingly important as organizations use APIs internally and build external developer communities. Therefore, API testing services are an important consideration to mitigate business risk and to ensure seamless integration of applications with other services.

Business Impact

APIs have emerged as a critical tool for building modern applications, as evidenced in the surge in organizationwide API strategies. An API that fails to deliver the expected level of quality, security, reliability and performance can thus have tremendous business impacts, both to the organization producing it and to those consuming it. Risks associated with application failure have broader business impacts; hence, the quality of the APIs produced and consumed is now more important than ever.

Drivers

- Many organizations have created API platform teams composed of API center of excellence (COE) team members with a mandate to deliver high-quality, reliable APIs.
- Organizations increasingly rely on APIs as part of their daily operations, such as logistics APIs for retail deliveries, and APIs into systems of record. These APIs must be reliable and well-designed.
- APIs are treated more like products than code. They are designed for consumption for specific audiences (e.g., mobile developers), they are documented, and they are versioned in a way that users can have certain expectations of their maintenance and life cycle. Because of better standardization, they have a much stronger discipline for security and governance, as well as being monitored and managed for performance and scale, thereby amplifying the importance of testing them.
- API testing services offer an opportunity to test the core functionality of the app without having to interact with a potentially disparate system. This helps in early bug detection, instead of bugs becoming larger issues during GUI testing, and thereby protects the application from malicious code and breakage.
- APIs have become a primary attack surface for many systems. These attacks have resulted in an endless stream of data breaches and other security incidents, yielding significant damage to organizations and individuals. As a consequence, sourcing, procurement and vendor management (SPVM) teams — along with the business leaders whose applications APIs support — express significantly increased interest in API testing and security.
- Traditional testing skills and team culture do not apply naturally to APIs, because APIs are used by other systems — not directly by end users. API testing calls for a different set of skills that involves the ability to understand the business logic of the service in addition to scripting and coding skills. Therefore, seeking specialized API testing services is becoming a matter of priority for many SPVM teams.

Obstacles

- APIs present challenges like broader attack surface area, higher potential for unexpected misuse and unpredictable demand, among others. These challenges translate to specific testing ramifications that require strong consulting skills to factor in all of the API test scenarios, which some providers may struggle with.
- API testing includes tasks like preparing the environment on which the API will exist, updating the API testing requests scheme, deciding on the sequence of API calls and validating parameters, among others. These activities often call for a strong involvement of client-side resources, as well.
- Incumbent vendors offering traditional testing services may not have strong API testing skills. So, the selection criteria need to factor in API-testing-specific key capabilities. These can include the ability to understand basic rules of creating good APIs, to design tests that are relevant for APIs, to use API testing tools, to understand business logic of service and to locate real user scenarios.

User Recommendations

- Begin evaluation and selection efforts by assessing the overall role that APIs play in your application portfolio, their criticality to the organization, and the security and business risk — and technical requirements — they pose.
- Give preference to API testing services that are underpinned with intelligent test creation and automated validation. Because testing a broad range of conditions and corner cases is critical with APIs, automation must come to the forefront.
- Ramp up the scope for extensive performance testing as part of services. Considering the highly exposed nature of APIs, there is a strong potential for unpredictable and volatile traffic volumes. Therefore, it is critical to determine whether your APIs satisfy SLAs in the event of surging demand.
- Examine the testing capabilities provided by existing tools in your application testing portfolio, including full-life-cycle API management platforms, which may include API testing. Tools are a key component of API testing services.

Sample Vendors

APImetrics; Applause; Cigniti; Infosys; Postman; SmartBear; Stoplight; TCS; Tricentis; Wipro

Gartner Recommended Reading

How to Deliver Sustainable APIs

How to Successfully Implement API-First Integration

The Evolving Role of the API Product Manager in Digital Product Management

Enhanced Internet

Analysis By: Mark Fabbi, Bjarne Munch

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Adolescent

Definition:

Enhanced internet is a collection of internet-based service offerings to improve the reliability and performance of internet-based traffic and applications. Enhanced internet is offered as over-the-top services and include features such as telemetry-based routing and performance optimization. Enhanced internet services may be sourced by enterprise customers or built into SaaS services, and are increasingly relevant due to growing cloud adoption.

Why This Is Important

As enterprises increase the use of cloud services, the internet becomes the mission-critical component of the WAN. While internet services have become more reliable over time, they do not come with the same service levels and consistency found in business-class WAN services, especially on a global basis. Enhanced internet services attempt to bridge the gap using lower cost business-class internet transport .

Business Impact

Enhanced internet enables enterprises to provide a more assured, reliable and high performance network for cloud-resident applications. It is particularly relevant for organizations using multiple cloud services with a global or panregion footprint and for apps that are impacted by performance variations, such as real-time traffic. Distributed midsize enterprises moving to an all-internet-based network should consider enhanced internet for a more assured experience with lower price points.

Drivers

- Interest in enhanced internet services is increasing as a growing proportion of enterprise applications are deployed in the cloud and rely on internet services for access.
- A growing number of SD-WAN, SASE and MSP vendors have integrated Enhanced internet capabilities to differentiate their offerings.
- Traditional MPLS services are often expensive and inflexible.
- New startups and associated venture capital financial investments are focused on stand-alone market and integrating enhanced internet into SD-WAN solutions.
- Enhanced internet capabilities and the requirements for a more assured internet service, with more secure and predictable performance, are becoming a talking point with a growing range of vendors in the industry.
- The internet is not good enough in all regions or for all applications. Therefore, a need exists for a more assured, consistent internet experience.

Obstacles

- Enterprise organizations lack awareness.
- Integrating additional components from new, unknown suppliers can complicate and add risk to enterprise cloud transitions.
- Some SaaS providers integrate enhanced internet into their services, and we have seen increased adoption by SD-WAN and SASE vendors to integrate enhanced internet into their offerings resulting in enhanced internet being absorbed into other offerings.
- Enhanced internet must fit into a narrow financial window to ensure they remain less expensive than traditional MPLS services.
- Enhanced Internet may be subsumed by SaaS, SASE and/or SD-WAN markets and solutions as part of OTT service consolidation. There is a clear need for a more assured and optimized delivery of internet-based applications, but enhanced internet services may be better served as an integrated component in SaaS, SASE and/or SD-WAN solutions.

User Recommendations

- Evaluate OTT enhanced internet services when looking for more assured, high-performance internet-based connectivity, at least for those locations and applications that need additional assurance and performance. Any migration of WAN architecture or evaluation of the end-to-end network security architecture is an ideal time to consider enhanced internet services requirements as part of a larger evaluation.
- Include enhanced internet features in the evaluation of SASE or SD-WAN technologies. Enhanced internet capabilities can provide differentiation.

Sample Vendors

Alkira; Anapaya; Cloudflare; Syntropy; Teridion

Gartner Recommended Reading

Cool Vendors in Cloud Computing

IoT Services

Analysis By: Eric Goodness, Emil Berthelsen

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

IoT services encompass support, maintenance and professional services to provide a range of business and technical expertise in support of initiatives where IoT is used to enable targeted outcomes. Various frameworks, methodologies and assets are within scope for IoT services. IoT services must be viewed within the broader remit of “digital services.” The core outcomes of IoT services lie in the data acquisition and the data contribution to value achievement and digital strategy execution.

Why This Is Important

A lack of internal resources skilled in IoT technologies and how to operationalize the integration of IT, OT and IoT drives the demand for IoT services. Growth in demand is strong across all sectors, with the overall market for IoT services growing to $25 billion in 2022 at an annual growth rate of 28% from 2021. The availability of a broad and deep pool of providers that can balance technical expertise with sector-specific acumen is key for successful IoT adoption for digital business impact.

Business Impact

Buyers seek IoT services to:

- Improve the processes related to strategy development and vendor due diligence relating to IoT technologies and business design patterns
- Accelerate the time to solution to recognize internal (operations, processes) and external (market, customers) benefits from digital optimization and digital transformation
- Reduce noncore resources and mitigate the risks of deployment, integration and support

Drivers

- The use of external service providers (ESPs) offers the skills and expertise not found in most enterprises. The emerging market for IoT solutions has created a unique market landscape for IoT services because the most common service providers for IoT hardware and software are OEMs and ISVs, respectively. In fact, ISVs are responsible for integrating at least 60% of the IoT platforms in the market.
- The use of ESPs offers enterprises a way to derisk the deployment, integration and implementation of IoT-centric products in the enterprise. Users are able to hold providers to various SLAs to ensure proper functionality and outcomes from the IoT solutions. Risk mitigation is also extended to cost control for project deployment.
- A fast-growing market of suppliers of IoT services spans industrial equipment OEMs, traditional IT ISVs, IT and OT systems integrators, and niche IoT providers (hardware and software) offering a catalog of IoT services that span design, build and run services. Most importantly, the growing pool of providers is not only able to address technology challenges, but also increasingly able to factor in business acumen relating to sector-specific and regulatory requirements of customers.

Obstacles

- Determining the suitability of providers is challenging for many users. The market for providers is fragmented, and expertise is distributed unevenly, usually by technology segments, IoT devices, middleware and applications.
- User preference for purchasing IoT development and integration services from their existing IoT platform vendors, who can be small, restricts the scale of service scope and spend.
- The market has yet to see a broad pool of third-party maintainers for IoT products. This means maintenance and support services are mostly awarded to device OEMs and middleware vendors. Most of these providers are immature or small, and customer service is often not at the same level that users experience with larger IT companies.

User Recommendations

- Engage service providers early to accelerate successful IoT adoption by clearly defining the activities and success metrics to support the transition of IoT POCs to field trials and into production systems and services. Service fees charged ahead of the acceptance of production systems and services may be returned/credited back to the user organization.
- Create a plan to identify where your business will provide services, augment partnered services or source services entirely to external providers by auditing and aligning internal resources to IoT project phases and success requirements.
- Ensure access to the best resources across the service life cycle by abandoning legacy vendor management choices. Vendor size and legacy have little to do with the successful design, building and operation of IoT solutions. The IoT market is fueled by smaller, nontraditional service providers and models, such as build-operate-manage-transfer, and revenue sharing for connected products.

Sample Vendors

Accenture; Atos; Cognizant; Hitachi; Insight; KORE Software; Vodafone

Gartner Recommended Reading

Tech Providers 2025: MSPs Must Lead the Adoption of Emerging Tech Services for Digital Businesses

Forecast: IT Services for IoT, Worldwide, 2019-2025

3 Areas to Drive IoT Differentiation Beyond Functions and Features

PMO/PPM as a Service

Analysis By: Anthony Henderson, Jim Longwood

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

PMO/PPM as a service (PPMaaS) includes PPM consulting, implementation and operational project services contracted to service providers for a fixed or variable and scalable program of work. PPM is an aggregate of all aspects of project, program, product and portfolio management. This includes PMOs, enterprise PMOs (EPMOs) and major IT initiatives for program operation and governance. It excludes offerings purely focused on staff augmentation or training services.

Why This Is Important

In today's highly disruptive environment, enterprises must possess the ability to pause or stop unnecessary work and/or reallocate resources and funds in response to shifting priorities to deliver continuous value. Many organizations cannot retain full-time staff with the necessary skills and experience to address all aspects of project, program and portfolio management. One way to address these capability gaps is to contract for PPMaaS from specialty external managed service providers.

Business Impact

Using PPMaaS helps organizations:

- Access experienced project and program managers, scaling up more quickly to meet variable demands, with a scalable pool of skilled resources bringing best-practice processes.
- Create an opportunity to develop, mentor and grow internal skills and capabilities.

- Focus attention on delivering the business outcomes in a more timely fashion without being distracted by developing inexperienced contractor resources.
- Provide another option for addressing skills and resource attrition.

Drivers

- The acceleration of digital investments amid an environment characterized by increasing disruption and uncertainty will require enterprises to shift to adaptive and product-based practices. Organizations are seeking flexibility, cost control, skills, experience and more dynamic capacity improvements to meet these requirements. This shift is driving an increased usage of on-demand short- and long-term specialist PPM resources and services.
- Workforce planning and availability is a significant driver of enterprise success in the delivery of projects, programs and products. Many organizations are challenged by the lack of existing resource capacity and the inability to secure skilled independent contractors.
- Organizations need to keep pace with the varying demands and business fluctuations that are the norm in today's digital environment. To meet variable demand requirements, PPMaaS offerings range from traditional time and materials (T&M) to project-based and prepackaged PMO-managed services using a scalable catalog of PPM-related services.
- Enterprises also wish to focus their existing resources on identifying candidate digital technologies and related agile/DevOps implementation services, often on a product-based approach. Using external PPMaaS providers frees up their key resources to focus on these new initiatives to reduce costs and improve productivity.

Obstacles

- While leveraging PPMaaS can also drive efficiencies and reductions in costs, establishing internally or externally sourced PPM activities introduces new costs and risks. Often, externally provided PPMaaS requires assistance from sourcing, procurement and vendor management (SPVM) leaders. SPVM groups need to increase their insight and experience in going to market, establishing and managing short- and long-term PPM contracts for these services.
- Elements such as contracting a provider whose resources are culturally compatible with your internal staff and understanding the nuances of delivering project resources in your industry can be obstacles to the successful use of PPMaaS. Poor management of attrition rates of the PPMaaS provider can also reduce the efficiency of using these offerings.

User Recommendations

- Define short- and long-term objectives and conduct a needs assessment to determine what levels of services and experience make sense.
- Ensure that the PPMaaS offerings provide flexible and scalable access to talent when needed, with or without long-term commitment or extra permanent hires. Many providers offer it as an on-demand resource or as an add-on to existing implementation services.
- Ensure knowledge transfer provisions are included in the contract to reduce long-term dependency and promote development of the retained organization skills when services are complete.

Sample Vendors

Capgemini; Core Consulting Group; CUPE International; EY; DXC Technology; Gibbs Hybrid; Infosys; PM Solutions; TCS; Tech Mahindra Business Services

Gartner Recommended Reading

Market Guide for Providers of PPM as a Service

Effective Strategic Portfolio Management Drives Better Business Outcomes

Hyperautomation

Analysis By: Stephanie Stoudt-Hansen, David Groombridge, Frances Karamouzis

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Business-driven hyperautomation is a disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible. Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms to achieve business results. These include, but are not limited to, AI, machine learning, event-driven software architecture, robotic process automation (RPA), iPaaS, packaged software, and process/task automation tools.

Why This Is Important

The primary reason that hyperautomation is critical is the unrelenting demand for accelerated growth through business model innovation or disruption, coupled with the underlying foundation of operational excellence across processes and functions. 2021 Gartner research shows that CEOs (over 50%) and boards of directors (69%) demand a path to accelerated growth and operational excellence (see Future of Work Trends: Hyperautomation Growth Initiatives Delivered by High-Performance Fusion Teams). Hyperautomation initiatives are a critical path toward achieving desired business outcomes.

Business Impact

Hyperautomation initiatives focus on digitizing documents and artifacts to ensure that their business and IT process workflows have the least amount of friction. This task-level digitization is the foundation for process-level and cross-functional enablement of decision making for business agility and resiliency. Well-architected hyperautomation initiatives demand standardization of processes, which enables improved quality and cycle time. Additionally, digitalization enables accessibility and transparency, which catalyze workers (both human and digital).

Drivers

Over the past 15 years, the business value drivers underlying hyperautomation can be captured in three eras that were spearheaded by various constituencies (IT teams, business units or fusion teams):

- **The labor arbitrage era** is characterized by an IT-led approach. It predominantly focuses on “cheaper” as the primary business driver: Do more with less to deliver cost savings. Gartner estimates that 90% of all global enterprises include some type of labor arbitrage approach in their current strategies (volumes and locations vary).
- **The automation arbitrage era** is characterized by a business-unit-led approach. It primarily focuses on faster cycle time. A quintessential example includes using a virtual worker (“bot”) to shift something from six hours to 60 minutes.
- **The business model disruption era** is upon us, and is characterized by fusion-team-led approaches. It focuses on better, higher-quality business processes. The previous eras were focused on changing “levers of effort” (i.e., cost of labor) while this new era is focused on results (outcomes rather than inputs).

Obstacles

- **“Siloed” approach:** The ubiquity of hyperautomation has led to an incredible volume and velocity of adoption across functions. Unfortunately, the concurrent nature across business functions has been executed via “siloed” or diffuse purchases of technology tools, solutions and platforms. Gartner estimates that more than 56% of organizations have an average of four or more concurrent hyperautomation initiatives underway.
- **Lack of planning for total cost of ownership (TCO) or governance:** The explosion of projects, coupled with the need for speed, often leaves unaddressed the all-important planning for post-production-managed operations and governance structures.
- **Technology confusion and overspend:** The zeal for hyperautomation has driven more vendor offerings, overlapping functionality and inconsistent pricing structures, rendering technology strategy, architecture and integration a dizzying and difficult process. The result is overspending on more vendors that are not always orchestrated across the enterprise.

User Recommendations

- Architect and plan for multiple concurrent hyperautomation initiatives. Continue to automate everything that can and should be automated. Ensure appropriate investment in vendor management and risk competencies due to the volume of services and technologies involved.
- Establish and curate an adaptive governance structure with the goal to manage risk, driving operational resiliency and agility while optimizing total cost of ownership.
- Focus on the use of high-performance fusion teams to drive growth and create scalable, resilient business models that work as force multipliers for accelerating digital business.
- Define shared ownership and metrics of the hyperautomation initiatives on the following business outcomes: higher-quality, more resilient processes; higher usage due to employee and customer-centric experiences; speed (time to market, cycle time reduction and quicker adoption); and intelligent, data-driven decision making at scale.

Sample Vendors

Accenture; Appian; Celonis; EPAM; Microsoft; ServiceNow; UiPath; WorkFusion

Gartner Recommended Reading

Future of Work Trends: Hyperautomation Growth Initiatives Delivered by High-Performance Fusion Teams

Predicts 2022: Hyperautomation Demands Adaptive Governance

Infographic: Boost the Value and Success of Business-Driven Hyperautomation Initiatives

Driving Efficiency and Reliability With Hyperautomation

A Counterintuitive Way to Preempt Resistance to Hyperautomation: Promote the Plans

MDR Services

Analysis By: Andrew Davies

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Managed detection and response (MDR) services provide customers with remotely delivered modern security operations center (MSOC) functions. These allow organizations to rapidly detect, analyze, investigate and respond through threat mitigation and containment. MDR providers offer a human-driven, turnkey experience, using a predefined technology stack that commonly covers endpoint, network, logs and cloud. This telemetry is analyzed within the provider's platform using a range of techniques.

Why This Is Important

The cyberthreat landscape is more volatile, and the number of attacks against organizations are increasing. Most organizations lack the resources, budget or appetite to build and run their own 24/7 SOC function, which is required to help them protect and defend against attacks that increasingly cause more impact and damage to operations. MDR services enable organizations to procure modern SOC capabilities to address this need, and fill gaps in their threat detection and response coverage.

Business Impact

Organizations that have not invested in threat detection and response capabilities are at risk from the impact of cyber incidents. The challenge of finding, acquiring and retaining the necessary expertise — and the right tools — makes building an adequate internal capability unappealing. MDR services combine people process and technology, translating security issues into business focused impacts and outcomes, reducing cost and complexity and allowing increased maturity through turnkey adoption.

Drivers

- The use of an MDR service helps organizations focus on their risks and outcomes that will directly impact their business objectives by ensuring that they have the needed threat monitoring and detection in place, rather than wide-scale collection of data and generic security logs.
- The expansion of an organization's IT infrastructure and digital footprint, moving into a broader set of providers and technologies, puts pressure on them to maintain visibility across an ever broader set of attack surfaces. MDR providers offer high-fidelity threat detection and coverage of a wide range of data sources, technologies and SaaS platforms.
- MDR customers are increasingly looking for vendors that will initiate measures for active containment or disruption of a threat. This is now a core requirement for buyers when selecting a provider. However, the level of autonomy granted to vendors varies according to the trust level. With the improved access to MDR service providers portals, clients can have the ability to see the response that will be executed for a scenario, and possibly execute it, if needed.
- MDR providers are expanding capabilities to include exposure management, incident response and risk management. The combination of these, with a traditional detection and response capability, offers a wide field of vision for a variety of risk-based issues that organizations face.
- Buyers increasingly require fast adoption of mature capabilities that would otherwise have taken a long time to build or buy, and have been prohibitively expensive. MDR delivers a turnkey solution for those who have no desire to build and maintain internal capability or require capability quickly.

Obstacles

- A lack of understanding of risks for the organization makes it more difficult for buyers to identify the best provider for their specific needs.
- Technology vendors with solutions in the detection and response market offer closely named, but often more light-touch overlay services, such as managed endpoint detection and response (MEDR), managed security information and event management (MSIEM) and managed extended detection and response (MXDR), which increases buyers' confusion.
- Performance issues with MDR service providers and failed engagements are often due to misaligned expectations. Buyers should clearly outline what they require the services to deliver, rather than focus on the technology or data that they want monitored.
- Not having staff assigned to services as the point of contact can cause challenges. Segmentation of operational responsibilities between internal contacts and an external partner, if not defined effectively, usually leads to dissatisfaction with services.

User Recommendations

- Focus on outcomes, not technologies, for MDR buyers. Organizations underinvested in technologies like EDR and network detection and response (NDR) should favor an approach in which a vendor provides the tools and delivers the desired outcomes.
- Assess MDR services if buyers are lacking staff and expertise to handle incident response activities once a threat has been identified, or want to add threat-hunting capabilities.
- Examine compatibility as a requirement if there are existing investments in threat detection technologies, such as EDR and SIEM, MDR services that only deploy their own technologies, as this may be costly and disruptive.
- Examine MSSPs if technology management, compliance monitoring and other managed security services are required — especially those that offer MDR-type services.
- Buy MDR services that offer transparency, encourage engagement through modern user interfaces and have open communication channels with analysts and delivery teams.

Sample Vendors

Ackcent; Cybereason; Deepwatch; eSentire; Expel; Kudelski Security; Open Systems; Rapid7; Red Canary; WithSecure

Gartner Recommended Reading

Market Guide for Managed Detection and Response Services

Quick Answer: What Key Questions Should I Ask When Selecting an MDR Provider?

Quick Answer: How Do I Manage the Risks Associated With Outsourcing to an MDR Provider?

LEO Satellite Communication Services

Analysis By: Bill Ray

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Low earth orbit (LEO) extends to around 1,300 km, less than 4% of the distance of a traditional communication satellite. Connecting to satellites in LEO uses significantly less power, supporting low latency and faster data. However, coverage requires a large number of satellites, most of which will have a limited life span (around five years). Several companies have launched LEO services for broadband internet access and low-speed IoT connectivity.

Why This Is Important

Companies such as Amazon and SpaceX have invested in satellite services intended to provide internet access to consumers and enterprises. Innovations from the smartphone industry have reduced the price and weight of satellites, combining with lower launch costs to make these constellations appear economically viable. As of 2Q22, Starlink is providing internet access to quarter of a million customers, and OneWeb still hopes to provide an enterprise service globally before the end of 2022.

Business Impact

LEO services will make broadband internet, and IoT data, globally available. Companies and employees can assume that internet access will always be available, removing network access as a limit on locations to work or live. Geography will cease to be a factor in connectivity available to remote offices, and home workers will be able to live where they like. This connectivity will extend to include airplanes, ships and sea platforms, creating a ubiquitous internet (and corporate intranet).

Drivers

- LEO satellite constellations are being launched to address two distinct markets: broadband internet access, and low-power IoT connectivity. These markets are being addressed by different companies using different constellations, as the requirements are quite distinct.
- Despite the wide-scale deployment of terrestrial wired and wireless services, there are still millions of homes and businesses that lack sufficient internet access, even in developed markets. Satellite broadband is relatively expensive (SpaceX's Starlink is charging $99 per month plus $499 installation) and won't compete with already installed fiber to the cabinet or home. However, we have calculated that there are enough homes without connectivity within the current coverage areas to sustain the Starlink service with reasonable penetration.
- Other customers include airlines, ships and the military. LEO satellites can also provide backhaul for cellular services — a single satellite uplink can provide connectivity to a cell tower providing 5G, 4G, Wi-Fi or any other local access technologies. This reduces the cost of network deployment for cellular operators, extending coverage into areas that have previously been economically impossible.
- Starlink is the first mover, with more than 2,000 satellites deployed by 2Q22. However, it will need to compete with offerings from Amazon's Project Kuiper network as well as competing projects such as OneWeb, Telesat, SatNet.
- IoT connectivity is a different market, focusing on low cost and low power to provide global asset monitoring and tracking. Companies such as Myriota already offer a sensor with a five-year battery life and satellite connectivity, while Lacuna Space uses chips and radios conforming to the existing LoRa standard, reducing the cost of a satellite-connected IoT sensor to a few dollars. Asset tracking remains the primary application, but condition and environmental monitoring will also be an important use case.

Obstacles

- To provide oceanic and remote region coverage (needed by military customers), satellite-to-satellite links are required. Only the Iridium narrowband constellation currently has such links.
- Customer equipment currently costs more than $1,000, and subscription costs will vary widely between providers. Developments in antenna design and mass production should reduce that cost, which needs to be below $500 for widespread adoption.
- Maintaining 30,000 satellites, with a life of five years, requires 500 new satellites per month. Current launch vehicles, such as the SpaceX Falcon 9, can launch 60 satellites at a time. This will not be sufficient, so larger launch vehicles (such as the SpaceX Starship or Blue Origin's New Glenn) will be needed.
- Satellite operators are required to avoid interfering with incumbent deployments, limiting the radio spectrum they can use. We expect that radio spectrum access will become a key point of negotiation, and perhaps litigation, in the next five years.

User Recommendations

- Exploit the rapid development of LEO services by adding satellite connectivity into future and strategic planning.
- Check the location of teleports to predict early-service availability; early services will only be available within 500 km of a teleport (earth station).
- Prepare for international availability by liaising with local regulators and resellers. LEO services are inherently global, so will spread internationally as quickly as regulators will allow.
- Protect investment by validating the technical and financial ability of your provider to launch and maintain its constellation.

Sample Vendors

Astrocast; Myriota; OneWeb; Starlink

Gartner Recommended Reading

Maverick* Research: LEO Satellites Will Trigger the Revolution That 5G Has Failed to Deliver

AI Cloud Services

Analysis By: Van Baker, Bern Elliot

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Artificial intelligence (AI) cloud services provide AI model building tools, APIs for prebuilt services and associated middleware that enable the building/training, deployment and consumption of machine learning (ML) models running on prebuilt infrastructure as cloud services. These services include vision and language services and automated machine learning to create new models and customize prebuilt models.

Why This Is Important

The use of AI cloud services continues to increase, with vendors competing to become the platform of choice for developers and citizen data scientists. Applications will increasingly use AI cloud services in language, vision and machine learning in applications to help automate and accelerate achievement of business objectives. Developers are aware of these offerings and are using both prebuilt and customized ML models in applications. The adoption of these services is rapidly accelerating.

Business Impact

The impact of AI will extend to the applications that enable business, allowing developers and data scientists to enhance the functionality of these applications. With the incorporation of forecasts, next best actions and other capabilities, including automation of many workflows that are currently handled manually, these AI cloud services will enable advanced machine-learning-enabled applications that improve business performance.

Drivers

- **Opportunities to capitalize on new insights.** The explosion of data from both internal and third-party sources enables insight that has previously been unavailable to the business.
- **Support demand for conversational AI.** The need for human-to-machine interactions that are based on conversational capabilities is increasing.
- **To meet business key performance indicators (KPIs).** There is a mandate for businesses to automate processes to improve accuracy, improve responsiveness and reduce costs by deploying both AI and machine learning models.
- **Reduced barriers of entry.** The ability to do one shot or few shot learning has reduced need for large quantities of data to train models and accessibility for developers and citizen data scientists to AI and machine learning services due to the availability of API callable cloud-hosted services will expand the use of AI.
- **Relevance for key use cases.** There are multiple use cases that span language, vision and automated machine learning services.
- **AutoML as an enabler for custom development.** Use of automated machine learning to tailor the off-the-shelf services to more precisely address the specific needs of the business is increasing.
- **A wide range of AI cloud services.** AI cloud services from hyperscaler cloud providers as well as specialized providers in the market including orchestration layers to streamline deployment of solutions are available.
- **Increasing deployments of sensor networks.** Sensor networks in IoT-based solutions that facilitate data use to drive model development and facilitate proactive response to changes in the data rather than reactive responses are increasingly deployed.
- **Emerging AI model marketplaces.** New marketplaces should help developers adopt these techniques through AI cloud services.

Obstacles

- **Lack of understanding** by developers and citizen data scientists about these services and how they can be applied to specific business use cases.
- **Pricing models** for AI cloud services that make it challenging for businesses to determine the costs associated with use of these services.
- **Lack of guidance** for solutions that utilize multiple services to address specific use cases for developers and citizen data scientists including guidance on how to use automated machine learning to supplement and enhance the standard language and vision services.
- **Minimal marketplaces** for prebuilt machine learning models that could be used by developers and citizen data scientists.
- **Serious lack of ModelOps** capabilities that contribute to challenges in integration of AI into applications.

User Recommendations

- Choose AI cloud services over building custom models to address a broader range of use cases and for quicker deployment and built-in scalability.
- Improve the chances of success of your AI strategy by experimenting with different AI techniques and AI cloud services providers, using the exact same dataset and then selecting one that best addresses your requirements. Consider using an A/B testing approach.
- Use AI cloud services to build less complex models, giving the enterprise the benefit of more productive AI while freeing up your data science assets for higher-priority projects.
- Empower non-data-science users with automated features. Use features like automated algorithm selection, dataset cleansing and preparation, and feature engineering for project elements, and leverage existing expertise on operating cloud services. This will assist technical professional teams with little to no data science expertise.

Sample Vendors

Amazon Web Services; Clarify; Dataiku; Google; H2O.ai; IBM; Microsoft

Gartner Recommended Reading

Critical Capabilities for Cloud AI Developer Services

Magic Quadrant for Cloud AI Developer Services

AI-Augmented AMS

Analysis By: Gunjan Gupta, Brett Sparks

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

AI-augmented application management services (AMS) use machine learning, artificial intelligence for IT operations, natural language processing and other AI technologies to automate the support, maintenance and enhancement of a portfolio of business applications.

Why This Is Important

AMS providers are increasingly leveraging AI technologies to improve IT service delivery for clients. AI-augmented AMS may employ AI, ML, NLP and/or RPA to:

- Proactively filter, prioritize and diagnose errors prior to incidents
- Automate email, ticket or phone requests, including correct routing and proposal of common solutions
- Predict defects, generate test data and optimize tests
- Preserve privacy while data is accessed and processed

Business Impact

AI-augmented AMS offers multiple potential benefits:

- Improved customer satisfaction and UX
- Long-term stability of clients' application landscapes

- Better predictability and continuous self-improvement of application support activities
- Improved delivery cycle times
- Potential delivery cost reductions of up to 50%, depending on how many incidents can be prevented or resolved by automation
- Easy scale-up of bot and ML capabilities, freeing development teams to concentrate on higher-value efforts

Drivers

- Due to market demand, AMS providers are using AI platforms to improve the quality and price competitiveness of service delivery. They're applying AI mostly to transactional tasks, such as test execution, application operations and incident resolution.
- Large service providers have built their own platforms for intelligent automation. Examples include IBM's Watson; Accenture's myWizard and AIP+; Digitate's ignio; Wipro's Holmes; Infosys' Nia; Cognizant's Automation Center; HCL Technologies' DRYiCE; Capgemini's Intelligent Automation Platform; and Atos' SyntBots. Small and midsize service providers are building platforms with software partners such as Amelia, arago and Resolve.
- Clients are also asking for improved reliability of their existing business applications. They're seeking service provider support to enhance system maintenance using AI capabilities.
- As clients move toward standardized (i.e., "keep the core clean") versus customized ERP implementations, the opportunities for AI-driven AMS increase.

Obstacles

- The intelligence of current solutions does not seem to increase at the same speed as the complexity of client application and infrastructure architectures. However, the providers continue to invest in new bots and use cases for their offerings.
- Investment in automation tools is expensive, and often, the benefits do not become clear until after implementation. Success with these tools depends on the data volume, the data quality and the sophistication of the learning algorithms. Vendors find it hard to commit to benefits before they have seen the client's data.
- Most of the use cases focus on reducing run and operational issues, not on facilitating high-value tasks such as identifying business needs and preventing incidents.

User Recommendations

- Expand your evaluation of competitive bids for managed services by accounting for commitments that service providers are willing to make using their automation platforms.
- Ensure that incident log data or repetitive workload tasks are comprehensive, clear and complete — not brief, terse or ambiguous — because AI systems will learn by reading these incident logs and identifying patterns in them.
- Work closely with providers to identify how you can adopt AI-augmented AMS by quantifying the value delivered. The value delivered should be reduced effort, higher quality and cost savings — not just the addition of a new technology to the ecosystem.
- Differentiate between AI-augmented AMS platforms and the service being offered, if lock-in to a particular platform is a concern.
- Ensure your contracts have sufficient flexibility to anticipate the unknown. The contract must incentivize the provider to address any unknown use cases in the future.

Gartner Recommended Reading

How Agile, Digital and Automation Drive the Increase in Nearshore IT and Business Services and What to Do About It

Market Guide for AI-Augmented Software Testing Tools

Optimize Application Testing Quality and Speed With Embedded Intelligent Automation Services

Infographic: Artificial Intelligence Use-Case Prism for Software Development and Testing

Emerging Technologies: Critical Insights Into AI-Augmented Software Development

Continuous Product-Centric Services

Analysis By: Alan Stanley

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Continuous product-centric services are those delivered by an external service provider under a long-term contract to supply a multidisciplinary team that builds, deploys and supports software using agile and DevOps approaches.

Why This Is Important

The post-COVID-19 digital surge is accelerating the speed at which organizations are using agile, DevOps and cloud. This is causing buyers of IT consulting and outsourcing to negotiate commercial models which are very different from the implementation statements of work (SOWs) and managed service contracts of the waterfall era.

Business Impact

- Purchasing continuous product-centric services helps organizations achieve the rapid time to market offered by agile and DevOps using global delivery models.
- The services are ideal for cloud-native software development projects, making use of self-service provisioning, automated testing and frequent automated deployment of changes.

Drivers

- One of the underlying principles of DevOps is to eliminate delays and waste.
- However, functional outsourcing creates delays in the handoff from one supplier to another of tasks such as provisioning, releases to production and incident escalation.
- This tension has been exacerbated by the recent growth of product-centric models.

Obstacles

- Buyers of custom software development services prefer contracts where suppliers are accountable and manage delivery risk. Vendor accountability is very hard in an agile environment when the developers come from one supplier, the testers from another, and production support from a third.
- Buyers are therefore now sourcing an integrated multidisciplinary squad or pod, in which everyone on the team except the product owner comes from the same supplier. Gartner terms this “continuous product-centric services.”
- On smaller contracts to build digital business cloud-hosted customer-facing applications, continuous product-centric services are widespread and normal. Recently, buyers of large outsourcing contracts have turned away from outsourcing IT functions in favor of the continuous product-centric model. See Case Study: The Estée Lauder Companies Is Transforming Its IT Services Sourcing for Digital Delivery.

User Recommendations

Sourcing and vendor managers of multiyear IT outsourcing contracts must:

- Evolve the scope of their contracts. Move away from contracts based on functional silos such as consulting, development, testing or operational support.
- Make contract changes to add new continuous product-centric services in order to better use their DevOps capabilities.
- Plan to change over time from the consumption of functional outsourcing services to continuous product-centric services.

Sample Vendors

Accenture; Cognizant; EPAM; HCL Technologies; Infosys; Tata Consultancy Services (TCS); Wipro

Gartner Recommended Reading

Market Insight: Grow DevOps Services Into Continuous Product-Centric Services

5 Metrics to Demonstrate High-Performance Agile Development Services

The Future of DevOps Toolchains Will Involve Maximizing Flow in IT Value Streams

Climbing the Slope

PC as a Service

Analysis By: Stephen Kleynhans, Autumn Stanish

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 a monthly fee per device for a configured, supported PC. It builds on a combination of leasing, configuration and management support, and a range of services, but promises more flexibility than traditional leasing and an opex model. PCaaS is distinct from desktop as a service (DaaS), which is an as-a-service model for delivery of virtual desktops from the cloud.

Why This Is Important

Pressure to transform IT delivery services to support and add value to new business initiatives is causing enterprises to examine alternatives to traditional PC acquisition and management practices. PCaaS is available from several providers (including PC makers, value added resellers and Outsourced Digital Workplace Service providers). Offerings typically build on standard PC leasing agreements and bundle basic life cycle services with some process management for a monthly per-seat fee.

Business Impact

PCaaS can relieve IT departments of tedious device management processes, provide a predictable financial model, and scale to support a remote workforce:

- 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 Autopilot, to automatically enroll new devices to distributed employees potentially providing improved user experience.

Drivers

- Hardware supply chain issues and chip shortages have created long lead times for end-user devices. Sourcing and procurement are actively looking for alternative delivery models to traditional company-owned PC procurement.
- 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 is still a number of custom deals, there is overall less confusion for customers about what PCaaS offers. We expect that offerings will continue to evolve through 2024, as customers become more familiar with the concept and vendors expand services to cover hybrid work scenarios.
- Vendors continue to grapple with building attractive, profitable and affordable solutions by expanding their services while ensuring their internal capabilities are matured 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 their deals more attractive, leaving customers with unmet delivery expectations as providers attempt to balance growing their service offerings while maturing their own internal capabilities.
- Current supply chain challenges and operational changes resulting from remote work, have impacted the ability of providers to meet previously made commitments.
- 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.
- 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; 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

Crowdsourcing

Analysis By: Jaideep Thyagarajan

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Crowdsourcing is the use of communities of people who have signed up to a company's community platform. Crowdsourcing can be performed by either vetted or unvetted resources, and services may include application design, coding, development, testing, support and project management.

Why This Is Important

Crowdsourcing provides access to innovation and resources at scale by using vetted and unvetted communities. Through the pandemic it is established that, with appropriate safeguards and governance, remote work and service delivery function well. More organizations are willing to try out crowdsourcing as an alternate option. And with the "Great Resignation," demand is expected to further grow.

Business Impact

Sourcing, procurement and vendor management (SPVM) leaders facing pressure from CEOs and CIOs to lower costs, optimize resources and provide innovative solutions can quickly leverage crowdsourcing communities. The solutions help to lower operational and personnel costs because they approach tasks and staffing as needed. They also require less onboarding, limited provisioning, no ongoing salary and no overhead costs (such as office space), and clients can set up more flexible pricing models.

Drivers

- Organizations are seeing increased demand for quickly developing and testing applications to meet requirements for speed after a period of rapidly accelerating digital business transformations.
- In light of shifting needs in terms of COVID-19, the crowdsourcing model can address resourcing needs and gaps, especially around new technologies, flexibility and improved price points. It can also provide delivery diversification to reduce risk.
- Crowdsourcing allows for competition to come up with the best new idea by capitalizing on the collective knowledge of a known community of experts.
- Organizations can fill targeted needs by choosing the best qualified personnel or the optimal solution from a vetted pool of resources and submissions.
- Organizations can use crowdsourcing for validating ideas and products and for consumers of any kind by using a larger pool of potential users.
- The talent crunch, which has impacted organizations across the globe with surging attrition and labor rates, has resulted in SPVM leaders needing to consider alternative sourcing options to source a steady flow of supplemental talent.

Obstacles

- Crowdsourcing is not likely to completely replace the use of internal resources or external service providers. It should be evaluated as a complement to outsourcing delivery methods for application services or for enterprise projects seeking innovative solutions.
- Lack of clarity on which tasks/activities should be crowdsourced. SPVM leaders facing business demands for innovation, flexibility or cost-efficiency should create internal criteria to select projects suitable for crowdsourcing, and then start with proofs of concept and/or trials.
- Lack of transparency on members on the crowdsourcing platform. SPVM leaders must check the reputation of each crowdsourced community and of any crowdsourcing firm.
- Risk of IP contamination, loss of sensitive data and confidentiality associated concerns may discourage some organizations while considering crowdsourcing.

User Recommendations

- Evaluate crowdsourcing as a complement to outsourcing delivery methods for application services or for enterprise projects seeking innovative solutions.
- Select between delivery of crowdsourcing through pure-play companies, as well as through “managed application services communities.” These communities refer to service and product providers’ commercial use of crowdsourcing to deliver application design, testing, and development services to end-user organizations.
- Assign internal roles and responsibilities to examine the use of crowdsourcing when using crowdsourcing companies directly. Typical related roles are that of a project manager and a crowd curator.
- Create mitigation plans for risks to avoid potential problems with quality, security, IP ownership and warranties, as well as the integration of externally developed solutions and/or resources. Mitigation plans can include using security scanning tools on “winning” solutions, providing masked data for sensitive projects, or verifying IP ownership and infringements rights.

Sample Vendors

Applause; CrowdWorx; Gigwalk; HackerOne; Koder; Passbrains; Synack; Testbirds; Topcoder; Upwork

Gartner Recommended Reading

Market Guide for Application Testing Services

Cloud Managed Services

Analysis By: Craig Lowery

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud managed services are IT service offerings that provide for the day-to-day management of, and operational responsibility for, cloud service environments. A select set of professional services is typically offered and highly coordinated with the managed services to assist with cloud strategy, workload migration, solution architecture and ongoing transformation efforts. Cloud service brokerage is often delivered as a cloud managed service.

Why This Is Important

Cloud adoption is a critical strategic objective for most organizations, but most need help in achieving it. Cloud managed service providers (MSPs) deliver a mix of professional and managed services that guide their customers through typical cloud adoption patterns and into an ongoing, evolving operational state. This improves the organization's degree of success with a faster time to value.

Business Impact

Business benefits:

- The primary benefit of engaging a cloud MSP is to augment a cloud-adopting organization's expertise with certified, experienced personnel to provide advice and convey best practices.
- The secondary benefit is to provide the difficult-to-source tooling and day-to-day management of a highly dynamic operating environment.
- A long-term benefit of transformative outcomes occurs when organizations work with providers to unlock the disruptive potential possibilities of cloud computing.

Drivers

- As demand for public cloud services has grown steadily, so has the need for professional and managed services to successfully adopt those services.
- Organizations seeking to adopt public cloud lack the experience, skills, tools and staffing to successfully navigate key milestones: setting strategy, planning, implementation, optimization and ongoing evolution of cloud deployment.
- Strong cloud MSPs provide cloud capabilities aligned with hyperscale cloud infrastructure and platform services (CIPS) providers, unlocking technology innovations such as artificial intelligence, automation, data services and edge computing.
- The move to more cloud-native solutions and complex deployment scenarios such as hybrid cloud and multicloud have substantially emphasized the need for professional services expertise.

Obstacles

- Cloud MSPs have varying levels of capability based on the clouds they support, specific use cases, and the geographies and industries they target, as well as the technologies and personnel roles they use to deliver their services. This can make it difficult to choose the right MSP for an organization's purposes.
- Becoming heavily dependent on an MSP can make it difficult to leave it later. MSPs differentiate from each other in how they automate the delivery of their professional and managed services. They often create proprietary tools or trade secret integrations of open-source solutions on which a customer can become dependent.
- MSPs face the same challenges as end users in developing and retaining a skilled workforce. Although MSPs are generally better-positioned to attract and cultivate those resources, customers may have highly variable service delivery experiences from one interaction to the next or when compared with other customers.

User Recommendations

- Assess providers to ensure the provider has up-to-date expertise and a track record of success.
- Assess providers with capabilities across the adoption spectrum — from initial and ongoing advisory services (design) to implementation services (build) and managed services (run).
- Give first consideration to providers that demonstrate partnership status and accomplishments with the organization's primary public cloud provider.
- Assess providers' expertise and resources by industry, region and country.
- Plan for long-term value by choosing providers that can deliver innovations and support additional use cases and cloud providers as your needs change.
- Assess providers' ability to deliver to the organization's specific hybrid deployment patterns, which range from management of on-premises virtualization farms to distributed container and Kubernetes deployments to distributed public cloud solutions.

Sample Vendors

Accenture; Bespin Global; Capgemini; Cognizant; Deloitte; Logicworks; Rackspace Technology; SMX; TCS; Wipro

Gartner Recommended Reading

Magic Quadrant for Public Cloud IT Transformation Services

Critical Capabilities for Public Cloud IT Transformation Services

Managed IoT Connectivity

Analysis By: Pablo Arriandiaga

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Managed connectivity for IoT services encompass connectivity hardware, software, and network and IT services that are generally bundled and managed by a third-party provider. These services enable enterprises to connect, monitor, and control business assets and processes over a fixed or wireless connection. These services are key to informing and integrating purpose-built and stand-alone telematics systems, IoT platforms or legacy back-end IT and OT systems.

Why This Is Important

The market for cellular-based-managed IoT connectivity services, field-area networks (FANs) and satellite is mature, but enterprises are demanding capabilities that are still nascent in this market:

- NB-IoT and LTE-M
- eSIM and iSIM
- IoT Security standards as IoT SAFE.
- 5G technology and its role in edge computing
- Integration with hyperscalers
- Consumer or industrial connected products as most of managed connections are for connected commercial products
- Bring-your-own connectivity scenarios

Business Impact

Managed IoT Connectivity impacts businesses by:

- Simplifying IoT management by supporting the complexity of endpoints and connectivity types.
- Providing flexibility to the enterprise by supporting broader IoT initiatives. This is achieved by ensuring use of appropriate and rightsized solution components, including IoT hardware, connectivity to the cloud, flexibility to encompass a variety of connectivity providers in a seamless way through technologies such as eSIM.
- Helping enterprises to take more control of the IoT connectivity when it becomes a critical OT enabler.

Drivers

- NB-IoT and LTE-M: Gartner has observed adoption of NB-IoT and LTE-M starting to take off beyond China. These 3GPP IoT connectivity types have reduced the cost of the IoT connectivity and modules start to show affordable prices. Roaming agreements both for NB-IoT and LTE-M, have also grown significantly during this last year. Enterprises look for guarantees in terms of standard and broadly adopted connectivity versus nonstandard/proprietary technologies such as Sigfox or LoRa WAN, for devices and sensors that could have a lifetime of 10 years.
- Composable IoT Connectivity Platforms: Multinational companies where IoT connectivity is a critical element of their strategy for connecting their products and assets in a secure way require connectivity agnostic providers. These providers give them more flexibility for getting local IoT connectivity without impacting operations. This can be achieved with a sustainable managed IoT connectivity platform strategy that can be integrated with the rest of the IoT infrastructure and assets without the risk of changing the connectivity provider.
- Connected industrial products are starting to emerge with the convergence of IT/OT. Most of the vendors on the market are shifting priorities to serve the manufacturing industry beyond their traditional play in connected vehicles adding 5G and private mobile networks and edge compute to the managed IoT services proposition. Apart from traditional industry verticals in the managed IoT connectivity services market like transportation or utilities, other industry verticals like healthcare, insurance or retail that were underserved by this market are getting relevance. This is because they are accelerating their digital transformation.
- IoT Security with new standards as IoT SAFE that leverages a hardware secure element in the SIM, or “Root of Trust,” to establish end-to-end, chip-to-cloud security for IoT products and services.

Obstacles

- Lack of understanding of the benefits of 3GPP and non-3GPP LPWA networks by enterprises and its availability. Many times it is confused with 5G. 3GPP and non-3GPP LPWA networks provide low revenue for connectivity to vendors that have a lack of skills in industry verticals where these technologies could scale and don't promote it.
- 3GPP LPWAN global deployments still need to consolidate and enterprises still see a lack of prime contractors ensuring 3GPP LPWAN IoT connectivity across regions.
- eSIM costs remain high and architecture is complex to integrate so delaying eSIM adoption for IoT though composable IoT connectivity platforms are accelerating availability at scale as MNOs begrudgingly show more openness to integrate with 3rd parties through eSIM.
- Integration with hyperscalers and IoT platform providers is in very early stages, so enterprises can't access a seamless management of connectivity and devices under a single pane of glass or use the same vendor in most of the cases.

User Recommendations

- Identify vendors that could add more value on top of connectivity. Assess whether bundled solutions can be more cost-effective when including point solutions. Verticals that are well-served in this market are automotive, transportation and logistics, utilities or smart cities but increasingly manufacturing, retail and healthcare, as well.
- Evaluate cellular, LoRa and 3GPP LPWA capabilities by requesting specific agreements with local providers, global points of presence. This will avoid latency and flexibility through multi-IMSI, eSIM and iSIM to add third-party connectivity into vendors' managed IoT connectivity platforms (composable IoT connectivity platform).
- Assess the evolution of the vendors' roadmaps and ecosystem by ensuring they include edge and cloud integration, APIs availability natively integrated with hyperscalers, and roadmap for 5G, edge compute and private mobile networks.

Sample Vendors

AT&T; Deutsche Telekom; KORE; NTT; Orange Business Services; Telefonica; Telenor Group; Verizon; Vodafone; Wireless Logic

Gartner Recommended Reading

Magic Quadrant for Managed IoT Connectivity Services, Worldwide

2022 Critical Capabilities for Managed IoT Connectivity Services, Worldwide

Industry Insight: Composable IoT Connectivity Will Revolutionize Managed IoT Connectivity Business

Composable Solutions Are Main Drivers for CSPs Selling IoT and 5G to Enterprises

Quick Answer: Key Business KPIs for Benchmarking Managed IoT Connectivity Services

SaaS Post-Go-Live Services

Analysis By: Alan Stanley

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

After the implementation of a SaaS-based solution, the ongoing services needed to sustain and update the solution can be much less than the previous on-premises solutions but are not zero and are different in character from the dedicated managed services provided before. Service providers are updating their offerings to meet this requirement.

Why This Is Important

Software as a service (SaaS) is mainstream now for delivering standard business capabilities, but there are ongoing service elements from the SaaS provider, not just software. Many clients are confused as to where the provider obligations stop and how they will look after their installations. The new ongoing services model is usually less than with on-premises but is not zero and different in character. Many service providers are finding ways to address this change in demand.

Business Impact

Contracting for a predefined, dedicated capacity of services can:

- Lock the organization into an engagement that involves more service than necessary.
- Provide service that inadequately complements the base functionality support from the SaaS provider.
- Not handle the SaaS updates to common code that are vendor-driven automatically via scheduled releases.
- Lead to inability to use the new features or impact the current technical configuration.

Drivers

- Instead of the entire stack being managed at the client location, systems are assembled from components.
- The infrastructure and base application of these components is bundled with the SaaS provider.
- Organizations can use shared remote capacity to test system changes and manage the integrations and data flows between components.
- Business users can change or configure the more adaptable SaaS systems.
- IT services are moving to product-centric, business-aligned operations utilizing common core updates from the SaaS provider.

Obstacles

- Many IT staff and services providers have become very aligned to application managed services and application development, where all the work is customized to their environment and scaled accordingly.
- The move to SaaS needs both IT organizations and service providers to think more of continuously evolving the platform rather than building once, keeping safe and then upgrading.

User Recommendations

IT leaders engaged in implementing SaaS solutions for their enterprise, should:

- Identify the scale of support needed by discussing the ongoing services requirements with their business, IT team, implementation partner and what is provided by the SaaS provider.
- Ensure ongoing operation by contracting a “breakdown service” for the SaaS solutions to cover identified support gaps, and selecting a pricing option that allows for scalable, pay-for-use service options and committed service levels. Ensure the provider will meet obligations to provide capacity when needed and that any nondedicated (pooled) resources used know your configuration.
- Prepare for the regular changes by negotiating a service plan at a standard price, and put in place internal governance to allow the continuous integration of updates and ongoing communication on changes and benefits to the organization.

Sample Vendors

Accenture; CherryRoad; Deloitte; Evosys; IBM; Infosys; TCS; Wipro

API Management PaaS

Analysis By: Mark O'Neill

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

API management PaaS (APIM PaaS) takes an on-demand approach to the delivery of API management by providing an alternative to the purchase and installation of stand-alone, full life cycle API management software. APIM PaaS manages API access via provider-hosted API gateway services, with the option of on-premises API gateways, as well as providing an API developer portal. It is typically designed to be used with other PaaS services such as function PaaS (fPaaS) and integration PaaS (iPaaS).

Why This Is Important

Gartner's 2021 market share analysis shows that over 50% of API management is now delivered in the cloud. APIM PaaS takes full advantage of cloud benefits, such as autoscaling, resiliency and robust security. It also allows some vendors to offer per-API-call pricing. APIM PaaS may include the ability to deploy on-premises API gateways, to enable hybrid API management architecture with APIs on-premises and cloud-based API management.

Business Impact

APIM PaaS allows costs to scale with the business value of APIs, reducing the impact of a large outlay as an API program scales up. It enables APIs to be managed effectively when API traffic is unpredictable and potentially very large. APIM PaaS also brings business benefits when an APIM PaaS offering is provided as part of the PaaS platforms already in use by an organization, through unified procurement and billing.

Drivers

- APIM PaaS is driven by migration to and adoption of cloud platforms.
- SaaS adoption is also a driver, as organizations wish to use API management without needing to operate and maintain API management software.
- Serverless computing, including fPaaS, can act as a major driver for APIM PaaS. This is because fPaaS offerings can make use of API management on their associated cloud platforms. In some cases, they can automatically populate API gateways with endpoints so that fPaaS functions can be called via REST APIs.
- iPaaS and aPaaS are also drivers toward the need for API management provided by PaaS platforms.
- Since many organizations are building APIs in the cloud, APIM PaaS is also increasingly used in hybrid and multicloud scenarios.
- Automation is also a driver for APIM PaaS. This is because APIM PaaS also includes APIs in the API management platform itself. These are used to automate the creation and management of APIs, often as part of a DevOps pipeline, as well as for customizing the developer experience (DX) provided by an API developer portal.

Obstacles

- Perceptions of network latency can impact the uptake of APIM PaaS for managing on-premises APIs.
- APIM PaaS tends to focus on runtime (API gateway) capabilities, with limited support for life cycle management of APIs. This is not attractive for organizations that require enterprisewide API life cycle management.
- Data residency concerns, such as a storage of API payloads that may contain private information, are also an obstacle to the uptake of APIM PaaS for managing on-premises APIs.
- APIM PaaS can result in higher-than-expected pricing as API traffic grows.
- APIM PaaS solutions from cloud hyperscalers are generally tied to their larger PaaS platforms, and are not portable for use on other PaaS platforms.

User Recommendations

- Apply API mediation and prioritize the use of APIM PaaS to provide a cost-effective means of providing API management, even when your APIs are on-premises.
- Compare the pricing of APIM PaaS vendors, since not all provide consumption-based pricing.
- Include API PaaS as part of your API strategy, since it can accelerate time to market for mission-critical digital initiatives.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google (Apigee); IBM; Microsoft; Oracle; Postman; VMware

Gartner Recommended Reading

Magic Quadrant for Full Life Cycle API Management

Market Share: Application Infrastructure and Middleware, Worldwide, 2021

CIPS

Analysis By: Sid Nag

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

The cloud infrastructure and platform services (CIPS) market is where cloud providers offer IaaS and PaaS capabilities in an integrated manner. The degree of integration between IaaS and PaaS may vary, but it includes the use of a single self-service portal and catalog, shared identity and access management, a single integrated low-latency network, unified security, unified monitoring, and unified billing.

Why This Is Important

CIPS is important because:

- Customers are looking for integrated platforms to simplify development, deployment and operations.
- CIPS offerings are the most complete platforms in the industry, thereby driving significant market consolidation around these platforms.
- ISVs, SIs and MSPs have embraced the leading CIPS platforms, which makes them the foundation for most organizations' cloud operations.
- Workloads of today are complex. and cloud providers are addressing the problem by offering CIPS.

Business Impact

A well-functioning CIPS will offer enterprises a more natural, flexible and comprehensive cloud computing environment for their workloads, thereby addressing today's IT needs from an application perspective. Vendors also benefit from CIPS — those coming from IaaS and those specialized in PaaS increase their customer value proposition and ability to compete when covering the broader set of capabilities.

Drivers

- The appeal for CIPS is not necessarily in best-of-breed offerings, but in the unification and integration of platform capabilities across these services enabling broad support of workloads ranging from ERP to cloud-native.
- Most customers that use a hyperscale CIPS provider, such as Amazon Web Services or Microsoft Azure, have adopted a blend of the provider's IaaS and PaaS capabilities. Indeed, the availability of this broad portfolio of services is a key aspect of choosing a strategic cloud platform provider. Hyperscale CIPS providers deliver PaaS services with a direct dependency on their IaaS services. As a customer, whether you are using PaaS services or IaaS services, they are built on a common substrate. The combination of these services means you are making a strategic bet on the cloud provider.
- The complexity and level of investment required to offer a full, integrated portfolio of multifunctional PaaS and IaaS services will likely limit the vendor options in this market to a handful of hyperscalers. Some hyperscalers will form ecosystems, enabling smaller PaaS specialists to be included in this market. However, the maturity of this technology will be primarily dependent on the capabilities of the hyperscalers.

Obstacles

- Public CIPS markets are consolidating around the market leaders.
- IaaS-only or PaaS-only cloud providers will continue to exist, but only as secondary cloud providers compared with CIPS providers.
- This, in turn, could make it a market dominated by a handful of cloud providers, which could stifle competition and drive stand-alone cloud providers out of the market.

User Recommendations

- Use CIPS in both cloud-native and legacy migration projects to expand your design and deployment options. In some cases, this may involve using capabilities from multiple cloud providers.
- Prioritize consolidating systems on a hyperscaler CIPS offering when you are operating and governing fleets of applications at enterprise scale. This improves your economies of scale, skills and resources through standardization and consistency across your company and industry.
- Treat integrated CIPS providers as long-term application platforms. They should be managed as such, with appropriate attention to potential application portability issues.
- Do not assume that all services of the provider are of the same maturity, functional completeness or quality of service.
- Give extra credit to those that are multicloud, and therefore, can be colocated with multiple larger suites of CIPS capabilities, when considering a smaller specialist PaaS provider.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google Cloud Platform; Microsoft Azure

Gartner Recommended Reading

Magic Quadrant for Cloud Infrastructure and Platform Services

Critical Capabilities for Cloud Infrastructure and Platform Services

What Buyers Want From CIPS Providers

Risk and Opportunity Index: Cloud Infrastructure and Platform Services

Extending the CIPS Business to New Markets and Opportunities

Multicloud Managed Services

Analysis By: Sid Nag

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Multicloud managed services (MCMS), previously cloud service brokerage (CSB), is defined as an IT role and business activity in which a company or internal entity adds value to one or more (public or private) cloud services. This is done on behalf of one or more consumers of that service by providing an aggregation, integration, customization and/or governance role. MCMS enablers provide technology to support cloud service brokering activities.

Why This Is Important

With cloud being mainstream, especially the adoption of multicloud, MCMS will continue to increase. This has MCMS moving steadily toward the Plateau of Productivity. As organizations formulate their multicloud strategies, the role of IT as an MCMS provider has become an important function for many IT organizations. According to Gartner's cloud survey, more than 76% of organizations have adopted or plan to adopt multicloud.

Business Impact

Due to increased adoption of multicloud, IT has now widely embraced the "multicloud managed services" term. However, some external providers have used the "brokerage" label while offering the same functionality, and prefer terms such as "multicloud managed service provider." Meanwhile VARs, ISVs and OEMs are continuing to redefine their business models in context of the new cloud reality, but struggle to find the right business model for monetizing their value-added MCMS.

Drivers

- The area related to multicloud managed services that has grown the fastest over the last few years is the segment of third-party cloud managed service providers (MSPs).
- These MSPs offer value-added services for cloud migration and managed services on top of cloud infrastructure that are key to a successful multicloud adoption model.
- Providers come from a wide variety of backgrounds, including system integration, managed hosting and full-service outsourcing, which compete with pure-play startups.
- Providers of MCMS-enabling technologies include dedicated MCMS platforms, cloud management tooling (see Market Guide for Cloud Management Tooling) with embedded brokering capabilities and a wide variety of cloud management point solutions, all of which are part of the ecosystem of multicloud management.

Obstacles

- Providers tend to confuse combinations of siloed MSP practices for individual cloud providers as MCMS.
- There is also confusion around CMP platforms that have MCMS enablement being mistaken for MCMS.
- Many generic marketplace providers tend to cause confusion by calling themselves brokerage providers and by association tend to be perceived as MCMS players.
- Offering a truly integrated MCMS is very complex and expensive, and simplifying the problem through the use of CMP software limits flexibility.

User Recommendations

- Have a unified layer of consumption based on four pillars — aggregation, integration, customization and governance. In some cases, your organization can take on the role of an internal service broker to provide multicloud services to internal and external customers via an MCMS enablement platform. And for some other cases, your organization can turn to an external MCMS provider.
- Engage an external cloud MSP to perform the MCMS function if you lack the skills and capabilities or when an MSP can best meet your time-to-deployment or risk management requirements. Be sure to assess MCMS provider maturity at the commercial and technical level.
- Institute an internal MCMS role when brokering is perceived as a required internal core competency. Examples are when you want control over cloud consumption or you are responsible for delivering IT services across a hybrid cloud and multiclouds (public and private clouds). Colocate MCMS with your cloud center of excellence.

Sample Vendors

Accenture; Cognizant; Fujitsu; Kyndryl; NTT DATA

Gartner Recommended Reading

6 Best Practices to Create a Cloud Management Services Offering in the World of Multicloud and Hybrid Cloud

Market Insight: Top 10 Things 'To Do' to Seize the Cloud Service Brokerage Opportunity

ODWS

Analysis By: Daniel Barros, David Groombridge

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

Outsourced digital workplace services (ODWS; formerly known as managed workplace services [MWS]), is a subset of the IT outsourcing (ITO) market. ODWS focuses on delivering digital workplace capabilities to end users through a service provider that includes remote support, end-user device support and digital workplace enablement.

Why This Is Important

The objective of ODWS is to enhance employee digital experience by providing digital workplace services to enable new, more effective ways of working, raising employee engagement, and exploiting consumer-oriented styles and technologies. It aims to deliver a workspace that is intuitive, mobile-automated and collaborative. Technologies used in ODWS include intelligent automation, collaboration platforms, virtual assistance, ubiquitous access and flexible device support.

Business Impact

Most organizations today are challenged to expand their digital services and products, increase their workforce discretionary effort, and attract and retain the skills necessary for digital business transformation. In order to attract and retain the necessary talent, organizations must deliver a flexible and engaging digital workplace to its employees. ODWS takes a people- and business-centric approach to the workplace experience.

Drivers

- Employees expect their digital workplace experience to mimic the conveniences of the digital consumer world. However, outsourced legacy service desk and device support offerings are, in most cases, focused only on resolving incidents and service requests on a reactive basis.
- Legacy end-user services measure how fast tickets can be closed instead of focusing on the actual employee experience. The need to attract and retain talent, as well as to ensure that employees are as productive as possible, has created the demand for ODWS.
- Legacy end-user service-level metrics — such as speed to answer, average time to resolve and average handle time — are not effective metrics to measure employee experience.
- Organizations need to increase the utilization of workplace analytics to improve support effectiveness and resource efficiency. They also must measure the holistic employee experience through digital monitoring of IT systems and creation of user-centric XLAs.
- New digital workplace technologies (such as smart lockers, vending machines and IT support kiosks) allow service providers to deliver more agile and efficient ODWS to clients.

Obstacles

There are many obstacles to effective implementation of ODWS:

- From a buyer perspective, the biggest obstacle is approaching an ODWS deal as a cost play without considering the impact on employee satisfaction and retention and without a vision of how a digital workplace can deliver a business-level value by increasing productive user time.
- Excessive hype about “artificial intelligence,” “cognitive computing” or XLAs makes it difficult for client organizations to differentiate what results can be realistically achieved in their environment during the contract term.
- Providers are challenged in a competitive environment to continually invest in research and to measure and contract for outcomes. This environment challenges them to reduce costs and make analytics and machine learning services more effective.

User Recommendations

Client organizations sourcing ODWS must be diligent in understanding what is hype and what is real in this market. Clients contracting for ODWS must:

- Challenge the service provider to contract for end-user experience monitoring techniques that represent the actual digital workplace experience. Service agreements based on the end-user experience for ODWS are often referred to as experience-level agreements (or XLAs).
- Focus on the business value or the potential business outcome that can be related to the ODWS, and seek a service provider that is willing to contract for such outcomes.
- Reach out to references that have previously implemented such services to inquire about which results were effectively achieved.

Gartner Recommended Reading

Magic Quadrant for Outsourced Digital Workplace Services

Critical Capabilities for Outsourced Digital Workplace Services

Adapt the IT Operating Model to Deliver Indispensable Digital Workplace Services

5 Digital Workplace Myths That Impede Workforce Digital Dexterity

Disaster Recovery as a Service

Analysis By: Ron Blair

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

The disaster recovery as a service (DRaaS) market provides application recovery at a second location in the event of a disaster. At a minimum, it includes on-demand recovery cloud for planned exercises and declarations, server image and production data replication to the cloud, automated failover/failback between on-premises and the cloud, and recovery time service-level agreements (SLAs).

Why This Is Important

DRaaS is a great option for infrastructure and operations (I&O) leaders who want to improve their IT disaster recovery (DR) posture cost effectively when there aren't sufficient resources to fund improvements. It is compelling for organizations for which time-to-value is paramount for meeting compliance or regulatory requirements. The core value proposition is improved DR capabilities, better time to value, lower cost and lower risk than the organization could achieve on its own.

Business Impact

The business impact of DRaaS is moderate. Impact is pronounced among midsize organizations with fewer than 250 to 400 virtual machines (VMs) and in larger engagements in which there is close alignment across six fronts:

- Required timeline for improving DR capabilities
- The diversity of computing platforms
- Cost avoidance (e.g., data center, infrastructure, licensing, labor)
- Flexibility required (e.g., term/volume)
- Geographic or compliance needs
- Degree complementary to related strategic initiatives

Drivers

- Initially, DRaaS was primarily attractive to small or midsize businesses (SMBs). This was because DRaaS freed up the time of the IT staff in these businesses, and, in many cases, they lacked a secondary recovery data center and experienced support staff. As DRaaS has matured, it has become an attractive option for larger organizations that want to free up resources from managing routine operational tasks to focus on what they deem as more value-added activities. This has resulted in more complex and larger implementations. At one time, it was rare to find engagements larger than 250 server images; engagements now protect 1,000 or more server images.
- Due to the pandemic and other recent events, organizations are reassessing other vulnerabilities. As a result, more focus is being placed on improving DR posture (see 16 Tips to Enhance Your Disaster Recovery Program for guidance and downloadable 'quick-start' templates).
- DRaaS vendors include a mix of service providers. For most, DRaaS is not their primary revenue-generating service. Some also support communications services, traditional subscription-based recovery services, colocation, managed hosting, infrastructure as a service (IaaS) and managed backup services. So, although the client's interest in DRaaS may be initially DR-oriented, DRaaS providers are often well-suited to meet related data center or IaaS needs as well.

Obstacles

- The distributed nature of workloads and the use of multicloud has increased known and unknown recovery dependencies.
- "Larger engagements" typically translates into those with more staff on-hand and more-complex requirements — such as multinational, the use of DevOps teams, non-x86 workloads and a need for potentially hundreds of DR plans.
- The extent to which the above aspects are relevant and unaddressed for any given organization, other internal options will be examined.
- In addition, cloud providers themselves are baking more recovery and resilience options into their services.

Leading DRaaS providers have responded by augmenting offerings with:

- Higher-order services, such as hybrid cloud recovery, application recovery assurance and cyber resiliency
- Additional automation of front-end onboarding and change management
- Additional support for multiple platforms and more global reach

User Recommendations

Implement DRaas when:

- There is a mandate to improve DR capabilities quickly — whether internally charged, as a result of an audit or due to a business partner requirement.
- Your organization is bereft of resources that you can commit to DR, is lacking DR skill sets or would prefer to focus on other strategic initiatives.
- Colocation agreements used for DR or traditional subscription-based DR contracts are nearing the end of their terms.
- Significant investment will be needed during the next year for the existing DR infrastructure or the DR data center itself.

When considering DRaaS providers:

- Become familiar with the DRaaS providers and types per the DRaaS Market Guide below.
- Compare options via the downloadable spreadsheet in Tool: Identify and Evaluate Disaster Recovery as a Service Sourcing Options.
- Engage Gartner analysts to help determine fit and for assistance on approach and selection.

Gartner Recommended Reading

Market Guide for Disaster Recovery as a Service

Tool: Identify and Evaluate Disaster Recovery as a Service Sourcing Options

16 Tips to Enhance Your Disaster Recovery Program

Entering the Plateau

Data and Analytics Services

Analysis By: Jorgen Heizenberg, Twiggy Lo

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Data and analytics services are consulting implementation and managed services for the management and analysis of data to improve enterprise performance through more effective decision making. The core capabilities include D&A strategy, D&A governance, data management, analytics and BI, and AI.

Why This Is Important

Organizations are deploying D&A to support decision making and improving enterprise performance. D&A is becoming more strategic and expanding from the boardroom into business units with decentralized D&A communities. Most organizations lack the skills to execute on these D&A initiatives, and this is driving engagement with external service providers to fill in the skills gaps and deliver rapid time to transformation.

Business Impact

The following roles, in particular, can benefit from D&A services:

- **Chief Data Officer:** Gartner's seventh annual CDO Survey shows that skills and staff shortage is the No. 1 roadblock to the success of data and analytics.
- **Domain D&A Leaders:** Gartner's Survey Analysis: The Rise of Business-Domain-Led Data and Analytics Survey finds that leading organizations have shifted from traditional, centralized, IT-centric D&A teams to a model where domain D&A leaders share responsibility.

Drivers

- Organizations beginning their data-driven transformation, expanding D&A in their digital business strategies and becoming adept at maximizing the value of their D&A assets will see the greatest impact from external D&A services. Clients turn to service providers for their best practices, depth of (technical and business) expertise, improved time to market and faster value realization.
- Organizations moving to a more fact-based approach for decisions and/or business process transformation supported by D&A will need a life cycle of planning, building, managing, governing and optimizing D&A solutions delivered by external service providers.
- Organizations looking to scale and industrialize AI and machine learning technologies — beyond experimenting and innovating — will need support to improve accuracy, trustworthiness and speed of their pilots and prototypes as they move toward production.
- Service providers are rapidly adopting an “asset-based consulting” model that uses intellectual property assets for particular industries or business domains and prebuilt automation to accelerate delivery. These IP assets can include reusable code, frameworks, tools, methodologies, preconfigured solutions and platform-based business solutions. Automation ranges from basic macros and scripts to full-fledged AI, cognitive computing and machine learning.

Obstacles

- Many service providers are active in this market, and D&A leaders find it increasingly difficult to distinguish between them.
- Enterprises increasingly expect D&A service providers to drive organizational performance and guide digital business, act like a partner and deliver value beyond the project scope, but some lack the capabilities to do so.
- Offerings of external D&A service providers are generally mature, however, some areas, data monetization and data sharing still need skills improvement.
- External D&A service providers also need to build up skills for new approaches like DataOps, MLOps (aka XOps) and data fabric delivery.
- Other areas that would benefit from expansion of skills are D&A governance and ethics, and change management and data literacy.

User Recommendations

- Identify the D&A deficit (needed external support) based on the type of initiative, such as D&A strategy, data management, data governance or analytics programs.
- Collaborate with business stakeholders to prioritize requirements for external D&A skills, industry experience and technology support.
- Identify the types of smart automation and consulting assets, and change management capabilities required to embed D&A in the business processes and workflows of their organizations.
- Develop a set of D&A performance metrics, derived from the business stakeholder objectives, to measure the impact of the external services on the organization's business outcomes.

Sample Vendors

Accenture; Capgemini; Deloitte; EPAM; Fractal Analytics; LTI; McKinsey; SDG Group; Slalom; TheMathCompany

Gartner Recommended Reading

Magic Quadrant for Data and Analytics Service Providers

Critical Capabilities for Data and Analytics Service Providers

Tool: Vendor Identification for AI and Data and Analytics Service Providers

Market Guide for Artificial Intelligence Service Providers

Gartner Peer Insights 'Lessons Learned': How to Choose the Right Data and Analytics Service Providers

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 2022) (required)

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 2022) (required)

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 constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2022) (required)

Acronym Key and Glossary Terms

BMaaS	bare metal as a service
CIPS	cloud infrastructure and platform services
LEO	low earth orbit
MDR	managed detection and response
ODWS	outsourced digital workplace services
OT	operational technology

Evidence

[1] Quick Answer: How to Define Business Outcomes for Use in Consulting and Outsourcing Contracts.

[2] Augmenting Human Selves Through Artificial Agents — Lessons From the Brain, Frontiers in Computational Neuroscience.

[3] IT Services Strategic Sourcing Guide.

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

Create Your Own Hype Cycle With Gartner's Hype Cycle Builder 2021

Forecast: IT Services, Worldwide, 2020-2026, 2Q22 Update

Market Definitions and Methodology: IT Services

Magic Quadrant for Cloud Infrastructure and Platform Services

Market Guide for Digital Business Agencies, Consulting and Implementation Services

Infrastructure Services Sourcing Strategy: Practical Principles for Dynamic Insourcing Versus Outsourcing

Table 1: Priority Matrix for Managed IT Services, 2022

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	Dedicated Cloud Services		IoT-Enabled Product as a Service Metaverse Management Services	

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
High	API Testing Services Cloud Managed Services Data and Analytics Services Multicloud Managed Services	AI-Augmented AMS AI Cloud Services BMaaS CIPS Continuous Product-Centric Services Digital Risk Protection Services Edge as a Service Hyperautomation IoT Services LEO Satellite Communication Services Managed IoT Connectivity MDR Services ODWS PC as a Service	Managed IoT Services OT Professional Services PMO/PPM as a Service	
Moderate	Crowdsourcing Disaster Recovery as a Service SaaS Post-Go-Live Services Security Rating Services	API Management PaaS Cloud-Tethered Compute Enhanced Internet		

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Low				

Source: Gartner (July 2022)

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 2022) (required)

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 2022) (required)

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 constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2022) (required)