Hype Cycle for IT in GCC, 2018

Published: 13 July 2018 **ID:** G00338715

Analyst(s): Santhosh Rao, Bettina Tratz-Ryan

The Hype Cycle for IT in GCC presents a snapshot of technologies and services that CIOs should consider. The technologies and services included have direct impact on revenue generation, efficiency and/or quality improvement opportunities.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

The Gulf Cooperation Council (GCC) is an alliance of six Middle Eastern countries — Saudi Arabia, Kuwait, United Arab Emirates, Qatar, Bahrain and Oman. The Hype Cycle for GCC is targeted at CIOs, IT leaders and technical professionals. This Hype Cycle highlights a snapshot of technologies, processes and standards that have the maximum impact across organizations in the GCC region.

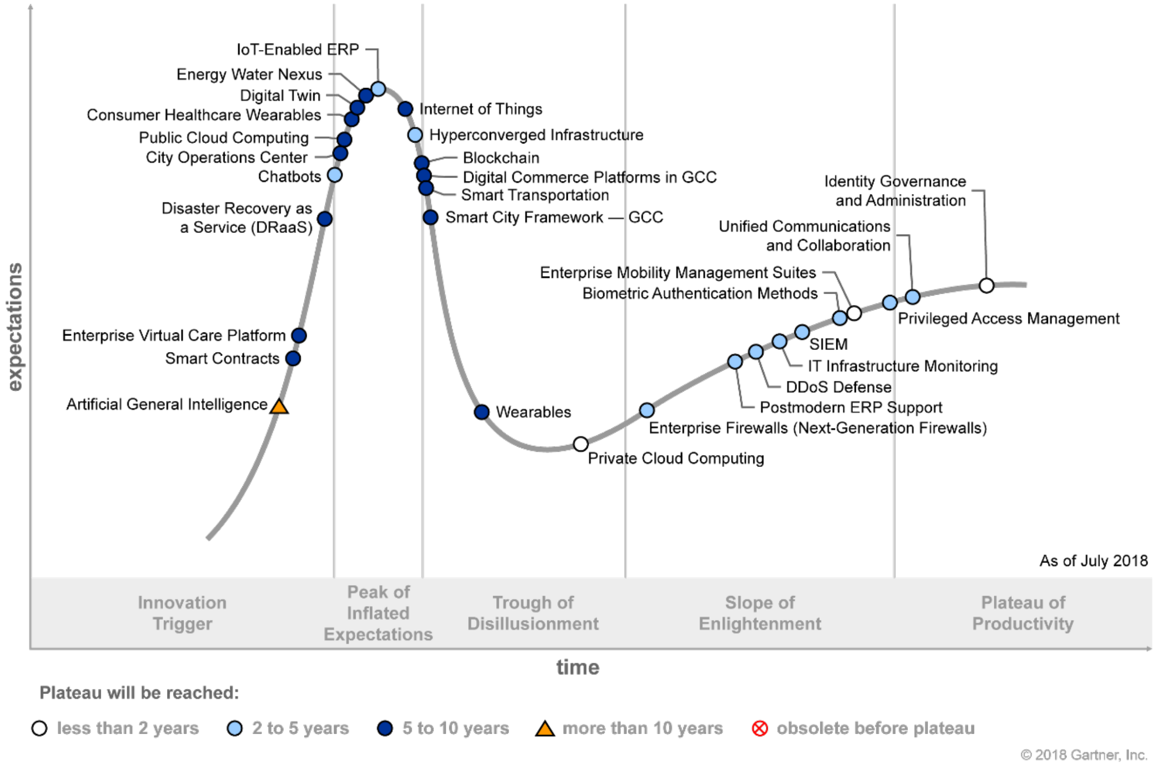
This Hype Cycle is intended as a starting point for developing IT strategies and technology roadmaps. Actual selection and deployment of any of these technologies should be augmented with input from other technology and industry Hype Cycles, relevant research, and communication with analysts who have in-depth knowledge of the products and vendors. This will help in identifying which is ideally suited for your environment (for example, rightsized, "good enough," cost-effective). Interested readers can refer to Gartner's broader collection of Hype Cycles for more detail on these and related technologies.

The Hype Cycle

As per "Gartner Market Databook, 1Q18 Update," the Middle East and North Africa annual IT spend in 2018 is expected to reach $155 billion, a 3.4% increase from 2017. The key verticals driving IT spending are banking, securities, insurance and retail verticals, which are primarily focused on digital business initiatives centered around blockchain, artificial intelligence and the Internet of Things. Enterprises and government entities in GCC countries realize that technology can be used as a key enabler to deliver services and create new business opportunities. This is reflected in the annual Gartner CIO Survey, which indicates that technology-related initiatives and improvements are the topmost business objective of enterprises in the region. The survey also indicates that BI/analytics, cloud services, ERP and security will be the top four areas to receive additional funding. It also indicates that the overall annual spending on data center infrastructure will decrease, as enterprises enter into cost optimization mode and look at alternative solutions such as infrastructure outsourcing and cloud services. The Hype Cycle for IT in GCC, 2018 assesses the technology maturity in areas such as digital business, IT infrastructure and security. It also covers specific technologies in the banking, healthcare, and oil and gas verticals.

In the last few years, all major governments in the GCC region have announced digitalization initiatives. The objectives for digitalization are several — delivering new services to citizens, optimizing existing processes, attracting foreign investors and skills, and identifying new revenue streams, thereby reducing dependency on oil and gas. Some of the country-specific initiatives include UAE Vision 2021, Saudi Vision 2030 and Qatar National Vision 2030. Availability of skill sets and high-technology providers continues to be a challenge in the GCC. However, countries such as UAE are beginning to address this by announcing long-term residential permits for expatriates, providing full ownership to foreign companies outside of free zones and creating innovation hubs in the region. On the supplier side, technology providers are also beginning to transform themselves. As margins from hardware and software continue to shrink, resellers and system integrators are undergoing transformation in order to position themselves as digital business enablers.

Figure 1. Hype Cycle for IT in GCC, 2018



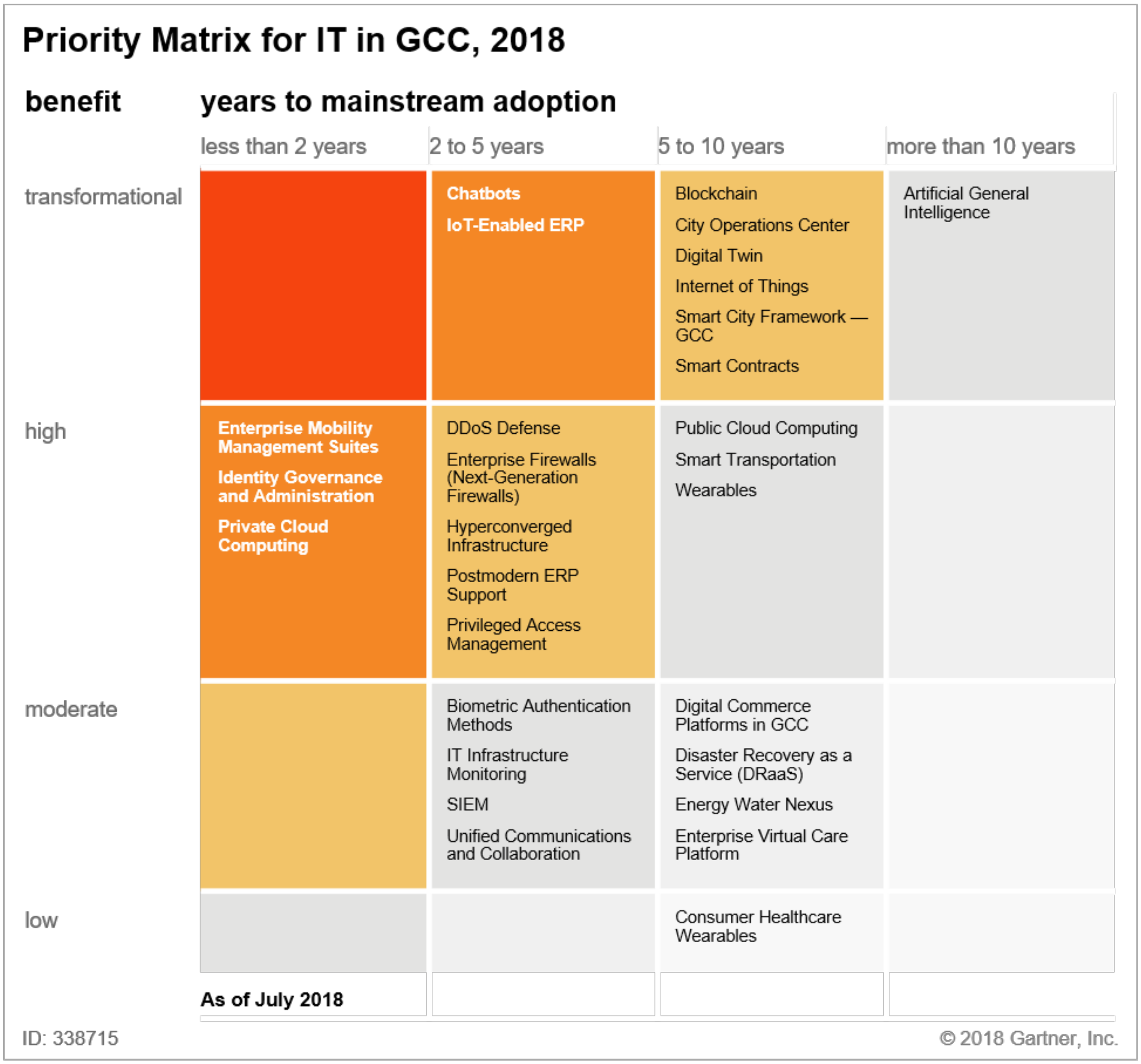
Source: Gartner (July 2018)

The Priority Matrix

The Priority Matrix maps the benefit rating for each technology against the length of time before Gartner expects it to reach mainstream adoption. This alternative perspective helps users determine how to prioritize their technology investments. In general, companies should begin in the upper-left section of the chart (transformational and less than two years), where the technologies have the most dramatic effects on business processes, revenue or cost-cutting efforts, and are available now or will be in the near future.

The Hype Cycle for IT in GCC constitutes a mix of technologies at various stages of maturity and varying degrees of impact — from low to transformational. Technologies such as blockchain, IoT and digital twins are transformational in nature and are expected to become mainstream in five to 10 years, owing to the increase in the number of digitalization projects currently underway. Oil and gas and manufacturing companies are expected to use IoT and digital twins for asset performance management and streamlining processes. Blockchain has received significant interest from government and financial institutions in the region as they look for innovative ways to streamline records management and integrate with existing financial systems. Interest in technologies such as hyperconverged systems and next-generation enterprise firewalls are expected to become mainstream in the next two to five years, given the increased seriousness toward security and optimization of existing system infrastructure, reducing costs and driving efficiency.

Figure 2. Priority Matrix for IT in GCC, 2018



Priority Matrix for IT in GCC, 2018

benefit	years to mainstream adoption less than 2 years	2 to 5 years	5 to 10 years	more than 10 years
transformational		**Chatbots** **IoT-Enabled ERP**	Blockchain City Operations Center Digital Twin Internet of Things Smart City Framework — GCC Smart Contracts	Artificial General Intelligence
high	**Enterprise Mobility Management Suites** **Identity Governance and Administration** **Private Cloud Computing**	DDoS Defense Enterprise Firewalls (Next-Generation Firewalls) Hyperconverged Infrastructure Postmodern ERP Support Privileged Access Management	Public Cloud Computing Smart Transportation Wearables	
moderate		Biometric Authentication Methods IT Infrastructure Monitoring SIEM Unified Communications and Collaboration	Digital Commerce Platforms in GCC Disaster Recovery as a Service (DRaaS) Energy Water Nexus Enterprise Virtual Care Platform	
low			Consumer Healthcare Wearables	

As of July 2018

ID: 338715

© 2018 Gartner, Inc.

Source: Gartner (July 2018)

Off the Hype Cycle

The following technologies no longer appear on this Hype Cycle, because they have matured, been replaced by a technology more relevant to the GCC market, become obsolete or do not fit within the technology domains that this Hype Cycle covers:

- Omnichannel apps
- Digital experience platforms

- Digital business consulting services
- Field mobility
- Open microcredentials
- Cloud office
- Production surveillance systems
- Virtual desktop infrastructure

On the Rise

Artificial General Intelligence

Analysis By: Tom Austin

Definition: Artificial general intelligence (AGI) — also known as "strong AI" and "general-purpose machine intelligence" — would handle a very broad range of use cases, if it existed. It does not, though it is a popular subject of science fiction. Current AI technologies do not deliver AGI. Despite appearing to have human-like powers of learning, reasoning and adapting, they lack commonsense, intelligence, and extensive means of self-maintenance and reproduction. Special-purpose AI — "weak AI" — does exist, but only for specific, narrow use cases.

Position and Adoption Speed Justification: Tangible progress on AI has been limited to weak AI. AGI's position and adoption speed on this Hype Cycle therefore remain unchanged. (We changed this entry's name from "general-purpose machine intelligence" in 2017 to reflect the popularity of the term "AGI.")

Today's AI technology cannot be proven to possess the equivalent of human intelligence (the lack of agreement about a test to prove such intelligence is itself a problem). It may, at some point, be possible to build a machine that approximates human cognitive capabilities, but we are likely decades away from completing the necessary research and engineering.

The subject of AGI often arises in discussions of "cognitive computing" — a term that means different things to different people. For some it denotes a set of AI capabilities, for others a specialized type of hardware (as in neuromorphic or other highly parallel, short propagation path processors). It can also describe the use of information and communication technology to enhance human cognition, which is how Gartner uses the term.

User Advice: Focus on business results enabled by applications that exploit special-purpose AI technologies, both leading-edge and older.

Leading-edge AI is enabling what are currently considered "amazing innovations," including deep-learning tools and related natural-language processing capabilities. These innovations are doing what we previously thought technology could not do. They are, however, typically research tools that are only just emerging from research labs, undergoing turbulent changes in direction, and not fully understood in terms of engineering principles. Over time, we will learn their limitations and develop workable engineering guidelines. As the amazement wears off and ennui sets in, we will treat them as "aging innovations."

Look for business results enabled by applications that exploit aging innovations (including expert systems and other symbolic AI approaches, as well as simpler forms of machine learning), amazing innovations (typically more powerful but less understood technologies), or both. Examples of such applications include autonomous means of transportation, smart advisors and virtual assistants focused on various goals (such as improved wealth management) and responsibilities (such as sales or budget management). Most use both amazing and aging innovations.

Special-purpose AI will have a huge and disruptive impact on business and personal life. End-user organizations should ignore AGI, however, until researchers and advocates demonstrate significant progress. Until then, ignore any suppliers' claims that their offerings have AGI or artificial human intelligence — these are generally illusions created by programmers.

Business Impact: AGI is unlikely to emerge in the next 10 years, although research will continue. When it does finally appear, it will probably be the result of a combination of many special-purpose AI technologies. Its benefits are likely to be enormous. But some of the economic, social and political implications will be disruptive — and probably not all positive.

There are currently no vendors of systems that exhibit AGI, but many companies are engaged in basic research. Examples are DeepMind (owned by Google), OpenAI and Vicarious.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Recommended Reading: "Smart Machines See Major Breakthroughs After Decades of Failure"

"How to Define and Use Smart Machine Terms Effectively"

Smart Contracts

Analysis By: Adrian Leow; Avivah Litan; Nigel Montgomery

Definition: A smart contract is a computer program or protocol, typically running on a blockchain-based technology platform, which facilitates, verifies or executes business processes that could be triggered by events, on-chain and off-chain transactions or interactions with other smart contracts. Rules are defined in the smart contract relating to an agreement that automatically enforces those rules by allowing the performance of a transaction without third parties, making a smart contract a self-executory contract.

Position and Adoption Speed Justification: As they emerge, smart contracts will be used to automate contract clause execution, offering fine-grained contract specifications with built-in enforcement (mediated by the underlying technology foundation or platform). Smart contracts can function at varying levels of scope: from a single transaction to an organizational unit, to an ecosystem. Smart contracts are designed to record evidence that the requirements of particular conditions, such as certain specific payment terms, have been met — thereby potentially lowering the cost of fraud or arbitration.

Smart contracts are the least mature subsystem of blockchain technology, which is itself still very immature. The word "smart" is something of a misnomer. The computer code is prescriptive and has no inherent artificial intelligence (AI) or self-learning capabilities, although it is expected that AI will be used (outside the blockchain) to process large volumes of data and provide feeds to the prescriptive code.

As used today, the term "smart contracts" refers to code written in blockchain-based languages (such as the Ethereum Solidity language) that govern how transactions are processed on a blockchain platform. The future vision of smart contracts includes a potential replacement for complex legal documents, but there are many obstacles to be overcome, which will take many years.

Smart contract scripting languages, tools, frameworks and methodologies are all currently at an early stage of development. The need for a secure scripting language that is "Turing complete," as well as enabling easy smart contract creation that is provably correct, is still an unsolved problem in the industry. The capability to automate complex agreements and, for a trustless runtime environment, to provide a deterministic programming language, are key technical challenges that are five to 10 years away. Smart contracts also imply multiple contractual executions within the same interaction process, as opposed to the need to have "one contract" covering all aspects of the interaction. This places greater emphasis on the performance of each component. The platform's ability to scale sufficiently to provide a seamless user experience — as monolithic contracts are replaced by granular agreements — will be a crucial factor in the adoption of smart contracts. In the future, possibly five to 10 years from now, smart contracts are likely to offer regulators and lawyers an opportunity for enforcement via evidentiary audit trails of actions being performed, thereby enhancing existing traditional contractual law.

User Advice: Enterprise architecture and technology innovation leaders looking at developing a strategy to deploy smart contracts should:

- Research the embryonic maturity of the platforms, technology, tools and frameworks to determine the amount of time and resources intended for investment in smart contract development.
- Develop a clear understanding of the different smart contract platforms, programming models, tools, frameworks and ecosystems, and their limitations and challenges.
- Identify use cases that can derive significant benefit from the core value promised by smart contracts. This includes being aware that the term "smart contract" is already being misused and its imminent "safe" use exaggerated.
- Examine whether business goals for smart contracts can be achieved through traditional contracting processes.

- Identify integration points with existing processes to determine their impact on core industry and ecosystem value propositions. Assess the implications for your information management architecture, legal compliance policies, payment systems and customer service processes.
- Determine policies with respect to contractual enforcement and smart contract use. Familiarity with the technology will also be required by all participants for transactions to succeed.

Business Impact: As stated, smart contracts will develop in different forms and with differing levels of impact. Many will simply replace existing transactional tracking mechanisms and execution systems as blockchain emerges as a platform for supply chain management. As such, smart contracts will be impactful. However, only when truly secure and proven smart contracts develop will smart contracts have the potential to transform commercial relationships through granular obligation recognition and secure value transference.

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Sample Vendors: Attores; Augur; Ethereum; Gnosis; Hyperledger; Monax; Oraclize; R3; RSK; SmartContract

Recommended Reading: "Be Careful What You Wish for When Engaging Smart Contracts to Support Your Digital Business"

"Top 10 Strategic Technology Trends for 2018: Blockchain"

"Invest in Technologies That Enhance Digital Trust to Boost Digital Value at Scale"

"Blockchain Status 2018: Market Adoption Reality"

"Market Guide for Blockchain Platforms"

Enterprise Virtual Care Platform

Analysis By: Mike Jones

Definition: An enterprise virtual care platform enables healthcare delivery organizations (HDOs) to augment certain elements of conventional face-to-face care delivery with virtual capabilities such as wearable and monitoring device integration, video services, clinical encounter automation, real-time scheduling, queuing or virtual waiting rooms. It also supports the integration with telemedicine equipment as required. Vendors providing these platforms often bundle managed services for telemedicine carts, peripherals along with implementation services.

Position and Adoption Speed Justification: In the past several years, there has been a significant increase in interest in virtual care and telemedicine, along with recognition of the technical challenges that need to be addressed. In the last 12 months, Gartner has reviewed an increasing number of RFIs or RFPs for procurement of enterprise-level virtual care solutions indicating a shift toward scale among HDOs and regional health bodies.

This has spawned the rise of virtual care platform solutions. Enterprise virtual care platforms enable HDOs to provide a broad range of virtual care services to enhance patient experience, branch into new populations and service lines, and transform service delivery efficiency under alternative payment models. Current platforms offer a functionality that is not available in existing EHR/ megasuite offerings, and EHR integration is a key success factor. A number of EHR vendors are now offering APIs to enable integration with alternative vendor platforms for virtual care in recognition of customer needs and demands for integration (e.g., integration for video capability).

The technical need for an enterprise platform to help enable the delivery of virtual care and telemedicine at scale is clear. Today, there are multiple large and small vendors competing in this relatively nascent market with a wide array of functionality. Our expectation is that over time, there will be a coalescence of both vendors and functionality, and in 2018, we have seen industry announcements that fit with this prediction (e.g., American Well's intention to acquire Avizia). We have adjusted our prediction of time to plateau to 5 to 10 years although we expect this to be closer to the five-year mark.

The main barriers to adoption are clinician cultural norms, agreement on payment models, in addition to regulatory and to a lesser degree information governance concerns regarding cloud services which are changing as cloud platforms become more established in healthcare. Another factor affecting time to mainstream adoption is the risk appetite for HDOs in changing or expanding service models to explore new markets.

User Advice: HDOs considering expanding their business capabilities across a range of care settings should:

- Develop a vision and roadmap for enterprise telehealth in their organization with a supporting strategic case that looks at the whole clinical service portfolio.
- Review and determine use cases including ones in which any existing HDO telehealth offerings can be migrated or integrated into an enterprise platform.
- Consult with the clinical leaders to understand their perspectives of how this can improve care, and address change issues at an organizational and specialty level before implementing the platform. Work through how the platform will be used to facilitate improvements in efficiency, quality, safety and experience.
- Ensure sufficient resources are given to change management, EMR interoperability and workflow integration, addressing each specialty on its own merits.
- Discuss virtual care/telehealth plans with their main payers to ensure coverage in terms of payment.
- Request comprehensive API capabilities from the EHR vendor with regards to integration of data and functionality for scheduling virtual care visits, calling video and other device integration functionality, and bidirectional handling of patient-related clinical and administrative data.

- Review the capabilities and preferred reseller/vendor endpoints in terms of commercial terms and conditions, quality of peripherals offered, and existing infrastructure that may be compatible or needs replacement over time. Ensure compatibility with existing medical device integration and network policies to help with value for money and minimize implementation costs and risks.

Business Impact: The target audience for these platforms includes HDOs that provide a range of care offerings in a range of settings (such as an accountable care organization) or are looking to expand into new business lines in response to market opportunities or customer expectations. The expected impact is on frontline care delivery across a range of clinical specialties and care settings (home, clinic, hospital). From a clinician's perspective, it offers opportunities for improved productivity and revenue. For HDOs, it offers opportunities in new markets, improved customer engagement and satisfaction, and improved care outcomes. For patients, it offers a more flexible model of seeking and receiving better care experience, and better health and well-being outcomes.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: American Well; Avizia; Cisco; Global Telehealth Services; GlobalMed; InTouch Health; Royal Philips; Visiba Care

Recommended Reading: "Master These Proof Points to Create a Sustainable Virtual Care Roadmap"

"Extending the Reach of Healthcare Delivery With Virtual Care"

"Adopt This Decision Framework for Virtual Healthcare Delivery"

"Your Virtual Care Strategy Needs an Update: Leverage Your EHR as the Primary Technology Foundation"

Disaster Recovery as a Service (DRaaS)

Analysis By: John P Morency; Santhosh Rao

Definition: Disaster recovery as a service (DRaaS) is a cloud-based recovery service in which the service provider is responsible for managing virtual machine (VM) replication, VM activation and recovery exercise orchestration. Increasingly, in addition to service offerings that just recover VMs, a growing number of service providers are now offering managed hosting services for hybrid recovery configurations that are composed of both physical and virtual servers.

Position and Adoption Speed Justification: The number of providers offering DRaaS now exceeds 500. DRaaS growth will be strongest in areas where customers have limited public cloud options in highly regulated industries (such as finance and healthcare), or where business processes are supported by IT systems beyond virtualized x86 environments (such as bare-metal servers, as well as legacy UNIX platforms for those providers that support it).

Initially, small organizations with less than 100 employees were DRaaS early adopters. The reason for the service uptake in smaller organizations was because they often lacked the recovery data center, experienced IT staff and specialized skill sets needed to manage a disaster recovery (DR) program on their own. This made managed recovery in the cloud an extremely attractive option. However, since the beginning of 2014, many large enterprises (with 1,000 to 5,000 employees) and very large enterprises (with more than 5,000 employees) have also begun initial piloting or have moved beyond the piloting stage to full production.

User Advice: Clients should not assume that use of cloud-based recovery services will subsume use of traditional DR providers or self-managed DR any time in the near future. The key reasons for this are computing-platform-specific recovery requirements, security concerns, data sovereignty constraints, active-active operations requirements, software licensing and cost advantages of noncloud alternatives, among others. In addition, a new class of software (IT resilience assurance or ITRA) supports the means by which product customers can orchestrate their own recovery using a hyperscale cloud service. Therefore, it is important to look at DRaaS as just one possible alternative for addressing in-house recovery and continuity requirements.

Consider cloud infrastructure when:

- You need DR capabilities for either existing Windows- or Linux-based production applications
- Formally managed recovery service levels are required
- The alternative to a cloud-based recovery approach is acquisition of additional servers and storage equipment for building out a dedicated recovery site

Additionally, because public cloud services continue to rapidly evolve, carefully weigh the cost benefits against the service management risks as an integral part of your DR sourcing decision making.

Business Impact: The business impact is moderate today. The actual benefits will vary, depending on the diversity of computing platforms that require recovery support and the extent to which service customers can orchestrate recurring recovery exercises that need to be performed. An additional consideration is the extent to which the customer can transparently and efficiently use same-provider cloud storage for ongoing data backup, replication and archival. The key challenge is ensuring that these services can be securely, reliably and economically used to complement or supplant the use of more traditional equipment subscription-based services or dedicated facilities. In addition, given that no service, including DRaaS, is immune to scope creep, it is incumbent on service users to ensure that providers consistently deliver on committed recovery time and availability service levels, especially as the size of the in-scope configuration increases and the in-scope data center configuration becomes more heterogeneous.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: BIOS; du; Etisalat; IBM Resiliency Services; Injazat Data Systems; Mobily; Oman Data Park

Recommended Reading: "Survey Analysis: IT Disaster Recovery in 2017"

Chatbots

Analysis By: Magnus Revang; Anthony Mullen; Brian Manusama

Definition: A chatbot is a stand-alone conversational interface that uses an app, messaging platform, social network or chat solution for its conversations. Chatbots vary in sophistication, from simple, decision-tree-based marketing stunts, to implementations built on feature-rich platforms. They are always narrow in scope. A chatbot can be text- or voice-based, or a combination of both.

Position and Adoption Speed Justification: Chatbots have really increased in hype over the last couple of years. But still, only 4% of enterprises have deployed conversational interfaces, which includes chatbots. However, 38% of enterprises are planning or actively experimenting, according to the Gartner 2018 CIO Survey. This sets chatbots up for tremendous growth over the next few years, but also sets it up for a large backlash once it reaches the top of the Hype Cycle.

Chatbots in social media, service desk, HR or commerce, as enterprise software front ends, and for self-service, are all growing rapidly. Still, the vast majority of chatbots are simple, relying on scripted responses in a decision tree and relatively few intents. Related to chatbots are virtual agents, which are broader in scope and sophistication, require more infrastructure and staffing to maintain, and are designed for a longer relationship with its users outside of single interactions. Users will interact with hundreds of chatbots, but few virtual agents.

Enterprises with successful chatbot installations are already looking at the challenge of managing multiple chatbots from different vendors performing different use cases. It is likely that more enterprises will seek out platform offerings and middleware offerings as the space matures. The space is currently oversaturated with companies and offerings, the vast majority of which will not manage to keep up with the pace of innovation as alternatives to decision trees, such as fact extraction and process mapping, become more common — and voice and multimodality become more viable. Looking at the investments, attention and research by big software companies in this space, we are looking at a rapid evolution until we reach productivity in about four years.

User Advice:

- Start proofs of concept for chatbots today — the window of opportunity for experimentation is still here, but will likely close by the end of 2018. The lessons from those experimental projects will be invaluable as the technology evolves.
- Treat vendors as tactical, not strategic — acknowledge that you'll most likely want to switch vendors two to three years from now.
- Focus on vendors offering platforms that can support multiple chatbots

Business Impact: Chatbots are the face of artificial intelligence and will impact all areas where there is communication between humans today. Customer service is a huge area in which chatbots are already impacting. Indeed, it will have a great impact on the number of service agents employed by an enterprise, and how customer service itself is conducted. For chatbots as application interfaces, the change from "the user having to learn the interface" to "the chatbot is learning what the user wants" has great implications for onboarding, training, productivity and efficiency inside the workplace. To summarize, chatbots will have a transformational impact on how we interact with technology.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Amazon; Facebook; Google; Gupshup; iFLYTEK; IBM; Microsoft; OneReach; Oracle; Rulai

Recommended Reading: "Architecture of Conversational Platforms"

"Market Insight: How to Collaborate and Compete in the Emerging VPA, VCA, VEA and Chatbot Ecosystems"

"Conversational AI to Shake Up Your Technical and Business Worlds"

At the Peak

City Operations Center

Analysis By: Bettina Tratz-Ryan

Definition: A city operations center refers to a platform that helps government officials manage smart city environments with a city solution encompassing a comprehensive and holistic viewpoint. The solution delivers operational insights to optimize the city operations' efficiency and quality of citizen life through visualization.

Position and Adoption Speed Justification: In smart city environments, speedy and seamless data exchange and information for city issues — such as traffic congestion, air pollution, energy and water consumption, safety and security conditions, and natural disasters — are required between different sectors and processes. It connects different data sources and orchestrates user- or citizen-facing engagements and the ideal view of situational awareness. A city operations center enables smart city officials and leaders to:

- Integrate data from various sectors and agencies
- Manage resources
- Connect with citizens and address their concerns

- Realize transparency and accountability for city operations
- Optimize city growth and operations

A city operations center also practices open government principles of transparency and accountability by sharing data about city operations with the public. The level of adoption varies by the technical and data requirements of local governments to consolidate multiple management platforms. Very often, operations centers work together in systems approaches to align processes for emergency response, resilience, mobility management and many other objectives.

User Advice: City government CIOs and urban planners need to define the operations center as a platform for management decisions for specific environments that include multiple business units and data streams. Traffic control, public safety and policing as well as critical infrastructure have their own departmental operating platforms. In a smart city strategy, different datasets from various operating management platforms and systems across government entities, districts and neighborhoods are now joined. CIOs have to consider the orchestration of IoT implementations and in-use data to extract value for operations control and city management. This way, they can deliver KPIs for optimization of maintenance routes, asset wear and tear and real-time decision making. As the analytics in operating platform also involve event and situational data, CIOs will support decisions in operations centers and urban platforms that offer the ability to manage and orchestrate infrastructure alignment and user experiences in real time to apply KPIs such as ISO37120 and SLAs.

CIOs should provide solid data fusion and visualization for benefits resulting from smart operations and urban management, as they have direct impacts on fiscal control of city government and provide transparency (with contextualized information) to citizens.

CIOs of local governments should leverage a city operations center to both address current issues and craft a medium-city strategy, which should include development of the local economy and disaster countermeasures. The data in a city operations center is consolidated to understand such city trends as traffic volume and flow and demographic changes.

Business Impact: The purpose of a smart city is to optimize city operations — not to build infrastructure. Domain technology and knowledge will play important roles in the city operations center because they help city governments make quality judgments based on data.

The primary functions (business impact areas) of a city operations center are:

- Routine operations management, resource monitoring and optimization, automated decision making, dashboard reporting and data sharing
- Emergency response hub, situation awareness and escalated decision making by humans
- Data resources for future smart city planning

In this regard, operations centers will morph from a decision-making perspective into urban platforms that create an interactive engine for application development and data visualization. In addition to control and command centers, for instance, FIWARE standards provide a framework environment that allows an urban open source migration path for standardized service, data and process management.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Cisco; Hitachi; Huawei; IBM; Microsoft; NEC; Oracle

Recommended Reading: "Digital Business Success Depends on Civilization Infrastructure: A Gartner Trend Insight Report"

"Market Guide for Government Open Data Management Platforms"

"Innovation Insight: Smart City Aligns Technology Innovation to Citizen Expectations"

Public Cloud Computing

Analysis By: Santhosh Rao

Definition: Public cloud computing is a style of computing in which scalable and elastic, IT-enabled capabilities are provided as a service to external customers, using internet technologies — i.e., public cloud computing uses cloud computing technologies to support customers external to the provider's organization.

Position and Adoption Speed Justification: Public cloud adoption in the Gulf Cooperation Council (GCC) is low, but will accelerate during the next two years. This is mainly driven by global hyperscalers, such as Amazon Web Services (AWS), Microsoft Azure, SAP and Oracle announcing data centers in the region. Furthermore, during the past two years, local hosters and telecommunication providers have been transforming themselves to deliver cloud services. End-user spending on public cloud computing in the Middle East and North Africa (MENA) region will reach $1.49 billion in 2018. Early adopters of the public cloud include midsize enterprises, e-commerce startups that are typically "born in the cloud" and large enterprises that are beginning to deploy noncritical applications on the public cloud to leverage the agility and elasticity that the hyperscalers offer.

User Advice: CIOs and IT leaders in the GCC region should begin formulating a cloud strategy. CIOs must identify an owner who is responsible for orchestrating the organization's enterprisewide cloud strategy and work with functional leads who are responsible for helping scope the various business and technical requirements. They must take a bimodal approach toward cloud adoption, by balancing risk and due diligence with rapid acquisition and deployment of cloud services. New initiatives centered around Internet of Things (IoT), artificial intelligence (AI) and machine learning can leverage the agility and pay per use nature of public cloud computing. Decision on migrating existing applications to the cloud must be based on a thorough analysis of pros and cons of moving these applications to the cloud.

Regulatory requirements on data locality are unclear, and government policy toward cloud computing is not yet formulated in most countries in the GCC. Therefore, CIOs are advised to work with risk and compliance teams to determine the impact of moving applications to the public cloud, particularly when leveraging public cloud data centers hosted outside the region. For scenarios in which enterprises lack in-house skills to move and manage applications in the cloud, we recommend that they leverage the services of managed service providers that can take responsibility for migrating and managing applications in the public cloud.

Business Impact: Public cloud services generate economies of scale and sharing of resources that can increase agility and choices of technologies. For enterprises, the cloud has the potential to become the foundation that enables businesses to transform, differentiate and gain a competitive advantage. Cloud computing can accelerate time to market and help organizations build capabilities rapidly on initiatives such as data and analytics, the IoT and AI.

Such projects often have uncertain business outcomes and require a fail fast approach. Attributes such as agility, elasticity and pay-per-use make cloud computing a compelling solution for such Mode-2 projects. Enterprises can also leverage the elastic nature of the cloud for application-bursting scenarios in which the computing capabilities of public cloud are leveraged as an extension to on-premises resources when required. Infrastructure services such as disaster recovery and backup/archive are also potential use cases for which the cloud can be beneficial.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Adolescent

Sample Vendors: Amazon Web Services; BIOS ME; du; Etisalat; IBM; Injazat; Microsoft Azure; Mobily; Oman Data Park

Recommended Reading: "2018 Planning Guide for Cloud Computing"

"Designing a Cloud Strategy Document"

"Solution Path for Developing a Public Cloud Strategy"

"Designing a Public Cloud Exit Strategy"

Consumer Healthcare Wearables

Analysis By: Mike Jones

Definition: Consumer healthcare wearables refer to the use of consumer-grade devices as recommended by a clinician to inform and track compliance with a prescribed treatment plan. It is separate from the use of medical grade devices (typically approved by FDA or equivalent) for the purposes of clinical diagnosis, treatment and monitoring.

Position and Adoption Speed Justification: Wearable electronic devices are designed to sense the human body or the environment around the wearer. Most can wirelessly send information to a smartphone or computer, but it could also be sent to the cloud or connected to an Internet of Things (IoT) platform. They have embedded intelligence such as a microcontroller or digital signal processor.

Healthcare delivery organization's (HDO's) use of lower cost consumer wearables is expected to grow alongside that of medical grade remote monitoring devices for the following reasons:

- They offer a means of engaging with patients to help drive self-management and compliance with HDO-prescribed lifestyle regimens.
- They are offered at an affordable price point.
- They can help differentiate the HDO through improved patient engagement and experience.
- They can provide an additional source of data for case managers to check in with patients to see how they are coping with their treatment regimens or to respond to periods of inactivity.
- They can provide an incentive to patients to change behaviors.

The speed of adoption will depend on proof of effectiveness and the cost and ease of integration of such devices into clinical workflow and analytics capabilities. Platforms in this space now offer a means for HDOs, insurers, pharma/life sciences companies, government agencies and the vendors of EHRs and enterprise virtual care clinical platforms to offload the complexity and risk of managing numerous device types and protocols.

There is a range of wearables available in this space at different levels of maturity and application by the HDO. These include:

- Wristband style devices (e.g., Garmin, Fitbit, Apple Watch, Samsung) for measuring exercise patterns and intensity
- Consumer-grade blood pressure (BP) monitoring devices
- Sleep monitoring and brainwave monitoring
- Clothing that senses blood flow and respiratory rates

We do not see this type of data being fully integrated into an EHR in the same way in which medical devices would. However, the general observations and findings of the physician when observing behavioral trends in the use of the devices could be captured as a part of clinical documentation.

Apple's recent announcement that they are working with Stanford Health Care to determine if Apple Watch can detect irregularities with the heart's rhythm is an example of how this technology would be used in primary and secondary prevention, possibly under new health delivery models by digital giants.

User Advice: CIOs should:

- Evaluate the application and effectiveness through peer-reviewed case studies, focusing on applications for lifestyle, rehabilitation and patient engagement and retention.
- Discuss the potential and socialize the concept of use of these devices within clinical practice through the chief medical informatics officer/chief nursing informatics officer (CMIO/CNIO) so as to determine the most appropriate forms of monitoring and tracking.
- Ensure piloting takes place in a tightly scoped project with clear metrics for measuring clinical and patient feasibility and do not neglect to consider issue of ownership of data and consent to collect and use data.
- Be aware of security/data protection requirements of your region where this information is traversing the cloud environment of the vendor platform that aggregates and presents the information.

Business Impact: Consumer-grade wearables offer HDOs the opportunity to use lower cost wearables as a complement to medical grade remote monitoring devices. This will lower the costs of monitoring patients, while improving clinical outcomes through the additional data generated by the devices.

The expected benefits of wearables for digital care delivery for the HDO include:

- Greater compliance with prescribed lifestyle regimens.
- Differentiation in the market because of focus on services that deliver better user experience and increased customer intimacy.
- An ability to monitor effectiveness of their prescribed lifestyle and exercise regimen at a relatively low cost per user when compared to medical grade monitoring equipment.

We have assessed benefit rating as medium/low as these are yet to be proven in terms of clinical- and cost-effectiveness in the way that medical grade remote medical monitoring devices have been.

Benefit Rating: Low

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Apple; Fitbit; Garmin; iHealth; OMRON; Panasonic; Samsung; Validic

Recommended Reading: "Master These Proof Points to Create a Sustainable Virtual Care Roadmap"

"Extending the Reach of Healthcare Delivery With Virtual Care"

"Adopt This Decision Framework for Virtual Healthcare Delivery"

"Business Drivers of Technology Decisions for Healthcare Providers, 2018"

"Your Virtual Care Strategy Needs an Update: Leverage Your EHR as the Primary Technology Foundation"

Digital Twin

Analysis By: Alfonso Velosa; Marc Halpern; Benoit J. Lheureux

Definition: A digital twin is a virtual representation of a real object. Digital twins are designed to optimize the operation of assets or business decisions about them, including improved maintenance, upgrades, repairs and operation of the actual object. Digital twins include the model, data, a one-to-one association to the object and the ability to monitor it.

Position and Adoption Speed Justification: The idea of modeling the operational behavior of things and processes continues to gain traction:

- For operators of assets (aircraft, buildings, power plants, windmills), digital twins are starting to gain adoption. Their primary near-term use is lowering maintenance costs and increasing asset uptime.
- For product OEMs, digital twins are beginning to proliferate for connected products (cars, lights, stereos). The primary near-term use of digital twins is differentiation and to help the enterprise manage warranty costs, support channel partners and better understand customer experiences.

Hundreds of millions of things will have digital twins within five years.

The digital twin profile has moved closer to the Peak of Inflated Expectations, in part due to heavy promotion by technology and service providers. Although about 5% of enterprises have started implementing digital twins, less than 1% of assets have digital twins.

User Advice: CIOs should identify and prioritize opportunities to use digital twins for business outcomes. To do this, consider the following:

- Business outcomes: Determine with business leaders the outcomes (financial, innovation, productivity) they hope to realize by exploiting digital twins. Leverage design thinking to identify potential business models.
- Objectives: Work with IoT teams to review your strategy and establish an IT vision for digital twins. Align it with the enterprise's digital transformation strategy.
- Technology: Start with asset models based on key business uses. Build the system representation, applying physics and function features as appropriate. Determine what data is necessary to "feed" the models and the types of analytics needed. Use standards where possible, but don't let their dearth limit innovation.
- Stakeholder engagement: Engage the business unit to build their business twin strategy. This may require discussions on the nature of digital twins, their value, and issues such as the cost of software asset life cycle management. Use design thinking exercises to help develop the models and user experience.

- Digital ethics: Work with business and legal teams to establish a policy on ownership of the digital twin models and data, as well as who may participate. Ensure this digital ethics policy helps engage partners and customers about what data may be shared and monetized.
- Business case: Align with business objectives, to identify a portfolio of digital twin initiatives that provide short (~1 year) and midrange (~5 year) paybacks.
- Risk analysis: Create a threat and opportunity analysis of the current business ecosystem, incorporating digital twin development by competitors or partners.

Business Impact: Digital twins are transformational as they enable business to optimize or transform their current business models. In the next decade, digital twins will become the dominant design pattern for solutions.

For example, they enable superior asset utilization, service optimization and improved customer experience. They create new ways to operate, such as consumption of physical outcomes instead of the capital expenditure acquisition of industrial assets. And they will open up new ways to monetize data.

Digital twins will challenge most enterprises to change their thinking from a hardware-centric to a hardware-plus-software-centric perspective. This includes the implications on operating business models, product management costs, and risks on unethical data use.

Finally, digital twins' impact will extend beyond assets. People within the supply chain are currently being modeled and analyzed. The digital twin of organizations has been used to optimize the business decisions for customer experience, cost optimization and portfolio management.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: ANSYS; Cognite; Dassault Systèmes; Flutura Decision Sciences and Analytics; GE Digital; IBM; Microsoft; Particle; PTC; Siemens PLM Software

Recommended Reading: "Five Approaches for Integrating IoT Digital Twins"

"Exploiting Digital Twins to Drive Ecosystem Strategies"

"Four Best Practices to Avoid Digital Twin Failures"

"Digital Twins Will Impact Economic and Business Models"

"Innovation Insight for Digital Twins — Driving Better IoT-Fueled Decisions"

"Top 10 Strategic Technology Trends for 2018: Digital Twins"

Energy Water Nexus

Analysis By: Bettina Tratz-Ryan

Definition: The nexus between energy production and water availability is directly intertwined. The nexus contributes to main industries and urban development. Innovative technologies utilizing data to project the impact on different industries and urban areas are key to managing water supply and demand relative to energy and water consumption and its production cycle.

Position and Adoption Speed Justification: According to the UN-Water directive, by 2020, half the world's population will be living in countries with water-supply shortages. Factors include:

1. Water is critical to energy, such as hydrothermal, but also to nuclear power plants.
2. 70% of freshwater globally is used for agricultural, 22% for industrial and 8% for residential uses.
3. The biggest loss of water is in transport and distribution.
4. Although there are new technologies on desalination (removing the saline from saltwater to turn it into freshwater), the process consumes high amounts of energy (approx. 15 kWh to 17.1 kWh per 1,000 gallons of water produced).
5. Water is integral to shale gas production.

Regions and countries with increasing droughts and the shifts in water allocation are challenged in their economic and industrial performances, especially with those highly dependent on oil and gas. The uncontrollable increase of population and rapid industrialization in developing countries are also major contributors.

User Advice: CIOs in different water-intensive industries need to build water management, the critical factor of price volatility of energy, and water supply into their IT procurement models and need to work with city leaders to make those conservations visible.

IT leaders in the industry need to track volatility in real time by analyzing data through smart city, water- and energy-management platforms and boards. End users need to look to involve new energy sourcing that includes waste to energy, circular economy to generate energy and broader energy-generation models in microgrids and distributed grids.

CIOs in emerging economies should apply or evaluate technology solutions such as sensors, IoT and analytics together with modeling and simulation for energy use. They should also network with solutions that create water sustainability and quality of water harvesting and management as they are key concerns for developed markets as well.

Business Impact: Business is greatly impacted by the availability and cost of energy and water as well as by the competing sources for other industries such as agriculture and food production in addition to urban centers. Cost of operations to produce water as well as energy based on competitive uses presents significant issues, and the potential stigma of using water for industrial uses instead of civic uses could prove a reputational issue. Transparency and public relations have to be shown to disperse the concerns for depletion or risk relative to operations. For example, the fracking industry in the Southern U.S. is using water from urban centers to bring it to the fracking locations, causing discussions about droughts and water availability in the community. In different industries, the energy-water nexus has caused businesses to change their business processes. The textile industry is dyeing without water, saving the water and, in addition, also energy as the textiles do not need to be dried.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: ABB; Accenture; Adasa; Black & Veatch; Deloitte; Fujitsu; GE Energy Connections; Hitachi; Siemens; thinkstep

Recommended Reading: "Innovation Insight: Smart City Aligns Technology Innovation to Citizen Expectations"

"Digital Business Success Depends on Civilization Infrastructure: A Gartner Trend Insight Report"

IoT-Enabled ERP

Analysis By: Duy D Nguyen; Denise Ganly

Definition: IoT-enabled ERP leverages advancing IoT technologies alongside postmodern ERP strategies to enable businesses to adopt and develop new business models and revenue streams.

Position and Adoption Speed Justification: As organizations begin to recognize the potential business value and the digital transformation benefits IoT brings, focus is shifting from the technology itself to business innovation. The short term to midterm impact of IoT on ERP will depend on an organization's postmodern ERP strategy and its business model. In manufacturing and supply chain operational scenarios, IoT is already enabling faster decision making and eradicating inefficiencies through the introduction of things like self-monitoring components predicting potential failure and alerting the need for maintenance. As IoT becomes pervasive, pressure will mount on the ERP systems supporting business processes to accommodate more IoT platforms.

ERP could fast become the bottleneck of the digital business. At a point unique to each organization, organizations will need to renovate or replace current ERP and related systems that don't allow IoT integration to ensure that they can provide sufficient real-time automated responses to IoT requests. This means additional interfaces to IoT front-end systems. Hence, in three to five years, IoT will enable new ways of streamlining ERP operational processes. IoT, particularly when augmented with emerging cloud services to capture, store and analyze vast amounts of big data, will be transformational for ERP.

User Advice: IoT will put increased pressure on ERP-related systems through increased integration requirements, data volumes, and speed of business process innovation. Organizations will need to renovate or replace the systems currently supporting their business through adoption of a postmodern ERP strategy, if they haven't done so already. Where ERP renovation is not viable, many organizations will need to upgrade their systems with capabilities to enable connection and information processing via new and varied types of front-end IoT systems and platforms. They will need additional processing capacity and high reliability. Evaluate these needs now. Organizations must ensure new systems can support real-time business decision making and that they are culturally equipped to make support real-time decision making. Organizations will also likely need to seek new industry-specific IoT-experienced service providers. Enablers such as in-memory computing are already providing some palliative respite, enabling some organizations to delay potential ERP replacement.

The criticality to act to accommodate IoT might seem far off. However, early action may yield long-term competitive advantage if you can build a compelling business case for innovation based on IoT. Ensure you have determined, documented and revised your postmodern ERP strategy. Establish where IoT could improve your ERP operational processes, as well as support new innovative processes. Upgrade your ERP system to a version that offers the required IoT functionality or interfaces. Create pilot project using Gartner's IoT reference architecture to analyze business objectives and technical requirements to implement these initiatives.

Business Impact: As a silent weapon, the business impact of IoT for some organizations will be immense and increased as a disruptive force for the next two to five years. Major industrial and business software vendors' solution portfolio will provide various IoT platforms and business-focused applications that equip application leaders to deliver a range of industry-specific capabilities, visible only through increased and sustained business competitiveness. However, this will be accompanied by the cost of ERP modernization or replacement. For some organizations, the business impact of not gearing your business for the impact of IoT on your ERP strategy and the systems that support it could be catastrophic. Impact is already being seen related to business analytics, predictive analysis, shop-floor monitoring, asset maintenance and retail (or, more precisely, customer-facing systems).

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Aptean; Epicor Software; IFS; Infor; Microsoft; Plex; QAD; SAP; Unit4

Recommended Reading: "Forecast: The Business Value of Artificial Intelligence, Worldwide, 2017-2025"

"Top 10 IoT Technologies for Digital Business in 2018 and 2019"

"IoT's Challenges and Opportunities in 2017: A Gartner Trend Insight Report"

"Seize the Moment by Maximizing Value With Event-Driven ERP Architecture"

"How to Renovate Your ERP to Provide a Digital-Ready Core"

"Architect IoT Using the Gartner Reference Model"

Internet of Things

Analysis By: Alfonso Velosa; Benoit J. Lheureux; Nathan Nuttall

Definition: The Internet of Things (IoT) is the network of dedicated physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment. IoT comprises an ecosystem that includes assets and products, communication protocols, applications, and data and analytics. IoT is a core building block for digital business and digital platforms.

Position and Adoption Speed Justification: Although enterprises vary in their IoT adoption, ranging from those with limited experience with IoT to organizations that are digitally transforming with IoT (a minority of companies). Gartner's 2018 CIO survey indicates that 12% of enterprises have deployed IoT and 24% are actively experimenting. Use cases range from incremental benefits (for example, asset optimization) to transformative benefits (for example, product as a service). The more developed use cases are typically found in fleet management and the industrial markets, where ROI is calculated from cost optimization such as reducing maintenance and fuel.

While the hype continues, we only moved the profile's position a slightly past the peak, as enterprises in the Middle East face increasing cost, complexity and scaling challenges implementing IoT solutions that deliver value. Challenges include immature IoT solutions, security concerns, end-to-end integration complexity, and an excess number of vendors that will not all survive the trough.

User Advice: IoT projects touch many roles in the organization. Use the following recommendations to guide your actions:

- Ensure you align your IoT strategy to your enterprise's digital transformation goals or its strategic objectives. But start small, experiment, and look to other industries and ecosystem partners for ideas.
- Build business cases with project payback of less than 24 months to account for implementation uncertainty.
- Focus on culture and process change instead of technology for operators of assets. This requires looking at the business priorities and engaging stakeholders with business projects with short-term outcomes.
- Ensure the architecture teams are ready to incorporate IoT across the IT and operational technology portfolio. Develop a platform architectural approach that enables you to manage a multivendor ecosystem to mitigate the damage from the inevitable shakeout of vendors.
- Budget to invest in skills to support IoT platforms, data integration, analytics and security solutions.
- Select your technology and service providers based on their technology stack, their focus on business results, and their ecosystem of partners.

- Ensure the end-to-end compliance of your IoT solution to relevant legislative and vertical-specific standardization bodies for global scalability and business model design.
- Establish your enterprise's digital ethics policies — for example, who has the rights to monetize IoT data, what form of right-to-repair issues you'll support, and so forth.
- Build a team to scan for threats from enterprises in your ecosystem who may use IoT capabilities to damage or limit your differentiation and competitiveness.

Business Impact: IoT has business transformation and evolutionary impact for most enterprises. IoT projects will impact most enterprises' competitive position, product development strategies and internal operations. Connected things will help drive revenue, lower costs, and improve enterprise processes and asset utilization in one, or a mix, of these usage scenarios:

- Improve operations: Better productivity; increased efficiency, logistics and coordination
- Optimize assets: Asset utilization, health monitoring, reliability, predictive maintenance and asset performance management
- Generate revenue: Improved products, usage-based pricing and monetizing IoT data
- Increase engagement: Improved experiences of consumers, citizens and others in order to improve loyalty and increase customer lifetime value
- Improve well-being: Wellness, longevity and care delivery for a better quality of life
- Conserve resources: Energy efficiency and pollution reduction

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: ABB; Deloitte; Ericsson; Eutech Cybernetic; Fujitsu; Huawei; SAP; Tata Consultancy Services (TCS); Telefónica; Vodafone

Recommended Reading: "Internet of Things Primer for 2018"

"Digital Disruption Profile: IoT Drives Rethinking Business Models, Processes and Skills"

"Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2017 Update"

"How an IoT Center of Excellence Can Help CIOs Deliver Better IoT Solutions"

"IoT: Think Big, Start Small, Move Fast"

"Implementing and Executing Your Internet of Things Strategy: A Gartner Trend Insight Report"

Hyperconverged Infrastructure

Analysis By: John McArthur; Philip Dawson

Definition: Hyperconverged infrastructure (HCI) is scale-out software-integrated infrastructure with a building block approach to compute, network and storage on standard hardware under unified management. HCI vendors build appliances using off-the-shelf infrastructure, engage with systems vendors that package the HCI software as an appliance or sell software for use in a reference architecture. HCI may also be delivered as a service or in a public cloud.

Position and Adoption Speed Justification: Hyperconverged infrastructure adoption has accelerated, as vendors now have offerings, either through direct development, OEM partnerships or via the acquisition of startups. VMware VSAN, introduced in 2014, enabled the global installed base of VMware ESXi customers to implement HCI, as did Storage Spaces Direct in 2016, for Microsoft Windows Server 2016 Data Center Edition customers. Meanwhile, Nutanix, an early innovator in HCIS appliances, has established multiple OEM relationships and developed reference architectures for other systems vendors, and Cisco, HPE and Pivot3 made important acquisitions. Initially used for test and development and targeted applications, HCI vendors enhanced offerings with improved networking and storage performance, supporting more general-purpose and mixed workloads, including some mission-critical applications and, increasingly, edge deployments. Users gain the benefits of simplified management, greater agility and granular scaling, although the modular building block approach that links storage and compute can result in over-provisioning of compute or storage, and some have scaling limits.

User Advice: Implement HCI when agility and management simplicity are of critical importance. While scaling increments may be smaller than integrated infrastructure systems or traditional general purpose disk arrays and servers, the total acquisition cost of HCI may be higher. Expect infrastructure management to be simpler, but HCI requires consolidation of operations and capacity planning roles and retraining in organizations that operate in technology silos of compute, storage and networking. HCI also requires the consolidation of budgets, and may require the alignment and shortening of technology refresh cycles, especially in organizations that have different refresh cycles for compute, storage and networking. Run proofs of concept before adopting HCI, especially for edge deployments and mission-critical workloads, and test performance under a variety of failure scenarios, as solutions vary greatly in performance under failure, their time to return to a fully protected state and the number of failures they can tolerate. Avoid starting with mission-critical workloads, but rather become knowledgeable in lower-risk deployments (such as test and development). Give preference to vendors that enable independent scaling of storage and avoidance of additional operating system, application, database software and hypervisor license costs. Vendors may claim support for large clusters, but consider multiple clusters when the node count is greater than 12. While servers are perceived as commodities, they differ greatly in terms of power, cooling and floor space requirements, and performance. Hardware can represent up to 80% of the total solution cost, so evaluate HCI software on a variety of hardware platforms for lowest TCO and best performance.

Business Impact: The business impact of HCI is greatest in dynamic organizations with short business planning cycles and long IT planning cycles. HCI enables IT leaders to be responsive to new business requirements in a modular, small-increment fashion, avoiding large-scale over provisioning and the big-increment upgrades typically found in three-tier infrastructure architectures. HCI's simplified management decreases the pressure to hire hard-to-find specialists and will, over time, lead to lower operating costs, especially as HCI supports a greater share of the compute and storage requirements of the data center. During the period of transition, however, HCI will be another silo to manage, and could represent a short-term increase in management complexity. HCI is of particular value to midsize enterprises and remote sites needing cloud-like management efficiency with on-premises or edge-driven infrastructure. As more vendors support public cloud deployments, HCI will also be a stepping stone toward public cloud agility.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Sample Vendors: Cisco; Dell; HPE (SimpliVity); Microsoft; Nutanix; Pivot3; Scale Computing; Stratoscale; VMware

Recommended Reading: "Magic Quadrant for Hyperconverged Infrastructure"

"Critical Capabilities for Hyperconverged Infrastructure"

"Charting the Shifting Trends in Hyperconvergence: From HCIS to HCI (and Back Again?)"

"How Midsize Enterprises Can Overcome Organizational Opposition to Hyperconvergence"

Blockchain

Analysis By: David Furlonger; Rajesh Kandaswamy; Fabio Chesini

Definition: A blockchain is an expanding list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Each record contains a time stamp and reference links to previous transactions. With this information, anyone with access rights can trace back a transactional event, at any point in its history, belonging to any participant. A blockchain is one architectural design of the broader concept of distributed ledgers.

Position and Adoption Speed Justification: Blockchain has become the de facto term that commentators use to describe all things relating to its original Bitcoin Protocol construct as well as multiple other aspects of ledger and token technologies and subjects. This is unfortunate as it creates significant misunderstandings concerning the various value propositions and capabilities of both the original model as well as how the first concepts have evolved over the last 10 years.

In reality, core developers have evolved the original block and chain ledger architecture into a wide variety of different information management and transaction execution models using multiple varieties of consensus algorithms, data and network governance models, token creation and distribution, and use cases.

Over the past decade enterprise executives have come to realize the inadequacies of implementing the original concept in terms of scalability, programmability, etc. Significant hype remains about the value of blockchain and distributed ledgers. It is not yet clear whether the general public will readily accept nonintermediated information management and transaction execution models and decentralized governance. It is also less than clear whether enterprises and vendors will relinquish control. During the next five to 10 years, convergence in architectural deployment styles is as likely as platform offerings converge. Distributed ledgers will gain similar functional characteristics (e.g., Zero-knowledge proofs, tokens, privacy controls, APIs, secure wallets, etc.). Market differentiation in ledger varieties will lie in the inherent capabilities to solve particular business problems. In the medium term, unless and until more standards, interoperability, viable and secure economic models, flexible quality user interfaces and enterprise scale capabilities are developed and adoptable in a mission-critical context, widespread acceptance of blockchain (beyond its current format) and distributed ledgers will remain problematic.

User Advice: Blockchain introduces challenges to enterprise and government operating models by introducing decentralized data/transaction management and governance. This negates the need for expensive intermediation. The use of a cryptographic token as a form of value also destabilizes the operation of financial systems raising questions about pricing, risk management, competitive positioning, funding, etc. Open source and the distributed nature of programming and applications threatens the centralized control that traditional technology vendors have had over the market. These issues have led to the evolution of multiple other forms of ledger constructs under the broader term of distributed ledger, which blockchains now fall under. These newer distributed ledger varieties often do not use tokens, nor do they offer the same kind of decentralized operating models that the original construct promised. As distributed ledgers have gained more momentum, they are superseding the initial blockchain concept via the use of executable programs allowing customized applications to be developed on top of the ledger protocol.

Use clear language and definitions for internal discussions about the nature of the technology, the ledger being developed and the business intention. Ensure that nontechnical executives understand the differences in business outcomes (for example, from both an operational risk and an ecosystem perspective) that each variety of ledger enables. Closely monitor distributed ledger developments and platforms, including related initiatives in areas such as consensus mechanism development, data management (e.g., sharding, channels, sidechains, etc.), authentication, governance models and decentralized applications (dapps).

If resources permit, consider distributed ledgers for proof of concept (POC) experimentation, but make sure your team has both the technical and business skills to understand the problem to be solved. Identify integration points with existing infrastructures (e.g., digital wallets, core systems of record, etc.) to determine future investment plans. Evaluate the total cost of ownership, especially against existing database systems and be very cautious about vendor lock in and merely replatforming the enterprise.

Business Impact: Blockchains continue to have high visibility, not least due to the wildly speculative volatility in the underlying tokens and the unclear nature of the participants. Block and chain architectures will likely not be suitable for many enterprise activities, especially taking into account the aspects of decentralization, risk, governance, etc. Presupposing the technical and business challenges of the broader concept of distributed ledgers can be overcome enterprises are most likely to gravitate instead toward experimentation with more multiuse architectural varieties. However, startups may continue to seek disruptive opportunities using the original block and chain concept and enterprise executives should undertake scenario planning accordingly.

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Bitcoin; Dash; Ethereum; Litecoin; Zcash

Recommended Reading: "The Future of Money Is the Programmable Economy, Not Just Bitcoin"

"Maverick* Research: In a Post-Bitcoin World, Metacoin Platforms Enable the Programmable Economy"

"Hype Cycle for the Future of Money, 2014"

"The Bitcoin Blockchain: The Magic and the Myths"

Digital Commerce Platforms in GCC

Analysis By: Yanna Dharmasthira

Definition: Digital commerce platforms facilitate purchasing transactions over the web. They support the creation and continuing development of online relationships with consumers and business customers across multiple retail, wholesale, mobile, direct and indirect sales, call center and digital sales channels. Core digital commerce platforms build digital B2B, B2C and B2B2C commerce sites.

The digital commerce platforms discussed here exclude online marketplaces.

Position and Adoption Speed Justification: Digital commerce platform software has a later penetration in GCC compared to other regions due to culture and entrenched establishment of malls and brick-and-mortar shops. The region, however, has a large potential for growth due to strong consumer spending power, strong infrastructure (including internet) and e-government initiatives.

Both domestic investors and (increasingly) foreign investors, however, prefer to direct their funding to online marketplaces (which compete with digital commerce platform software). For example, Amazon acquired Dubai-based Souq.com in 2017.

Digital commerce platform software growth is generated by high-end retailers and mature retailers in fashion, electronics and health/beauty. Its growth is triggered by multinational organizations expanding to GCC with their own online sites to build customer and brand loyalty. Online SMBs targeting working, younger generation and more-price-sensitive market segments help drive market growth.

Challenges include entrenched shopping mall culture, preference of COD, inadequate postal address systems in some areas, preference of same-gender interaction for delivery service and less established digital customer behavior. B2C is currently more dominant in driving the adoption of digital commerce platform software.

User Advice:

- Define your digital commerce objectives, such as expanding reach to more customers, improving customer experience or reducing distribution cost.
- Since physical stores are important, integrate in-store and online customer experience. Differentiate by increasing the number of points of interaction and gradually incentivizing users to shop online, for example, by enabling them to reserve and buy online and then pick up and pay in the store.
- Include mobile channels, online marketplaces and retail stores as part of your multichannel customer experience strategy and ensure a consistent experience throughout the customer journey. Polish your fulfillment and last-mile delivery strategy.
- Operate the online marketplaces yourself by opening up to third-party sellers. This helps to enrich your product offering and makes it more attractive to shoppers.
- Evaluate the product localization capabilities and ability of vendors to address GCC customers in Arabic and other local languages.

Business Impact: CIOs of end-user organizations in GCC are challenged to develop digital commerce experiences that can connect both online and offline while also improving customer experience and increasing loyalty. In addition, they need to reduce their overall cost of operations and are fending off increased competition from global players interested in the strong purchasing power of the GCC region. Organizations can leverage digital commerce platform software and technology as they face these challenges.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: CS-Cart; IBM; Magento Commerce; Oracle; Salesforce; SAP; ShopGo

Recommended Reading: "Market Trends: Digital Commerce Platforms in Growth Mode, Worldwide"

"Magic Quadrant for Digital Commerce"

Smart Transportation

Analysis By: Venecia K Liu; Nathan Nuttall; Bettina Tratz-Ryan

Definition: Smart transportation is a framework describing the movement of people and assets by modes that include vehicles, planes, trains, ships and bikes. It leverages information and environmental data to move passengers or assets. This involves real-time, context-aware data exchange and service offerings between conveyances, operators, passengers, assets, routes, timing and traffic patterns for both consumer and industrial applications.

Position and Adoption Speed Justification: Smart transportation is a strategic framework to support the sustainable economic and environmental development of cities and urban corridors. Over the next 10 years, it is morphing into the support mobility as a service concept, where data from all modes of transportation are ported into a single application platform to provide travelers with journey mapping. Smart transportation is a demand-based mobility concept that optimizes modes of transportation in the most efficient, sustainable and autonomous ways possible. While smart transportation covers all types of transport regardless of geography (e.g., seaports, airports, train infrastructure and roadways), much of the focus of smart transportation is in the context of smart cities initiatives.

Operational technologies and IT converge in the smart transportation framework, where intelligence is embedded into sensors on the transport asset. Smart cities illustrate compelling transportation benefits by leveraging contextual information about residents, businesses and mobility needs mapped against real-time data. Examples of this data are time of day, number of vehicles and travelers, pricing of road traffic per time of day and user, and environmental impacts (e.g., pollution, noise, productivity and perceptions of environmental quality).

Transportation CIOs in local government are starting to combine big data analytics, computer vision and machine learning to monitor traffic flow and automatically adjust traffic signals to improve congestion and traffic flow. Local governments are also working with several providers to build on the mobility as a service concept. They are partnering with transportation network intermediaries that provide platforms where multiple modes of transport data are used. Routes, schedules, availability, operations times and location-based data are combined with mapping data, traffic congestion data, geographical information systems data and, in some cases, a universal payment platform across all modes of transportation in real time. These services enable travelers to have ease of travel, safety and convenience.

Smart transportation is post the Peak of Inflated Expectations, as many cities have recognized the benefits of having a smart transportation framework and are applying data analytics to traffic flow patterns to adjust traffic signals based on congestion.

User Advice: Public transport CIOs should adopt smart transportation as part of an overarching mobility as a service concept with a multimodal approach. Internet of Things (IoT) sensors on smart transportation assets and infrastructure can provide valuable data that can be shared to a wider ecosystem (such as auto manufacturers, logistics firms, car-sharing operators and travel planning agents). As part of the overall planning, data ownership, data governance, privacy and security should be discussed among constituents. Smart cities agencies and transport authorities should look at the overall goal of journey mapping individual use cases across roadways, rail lines, foot and bike traffic, and signaling infrastructure. They must offer real-time transportation options and journey recommendations given the current state of congestion, user context and location-based events.

CIOs in public transport and traffic agencies need to support an operations platform for many different suboperations of public transport and traffic management to enable control and management processes.

CIOs of industrial organizations should evaluate the productivity gains leading to improved fuel efficiency, route/schedule optimization, lower CO_2 emissions and the reduction of fleet maintenance. These organizations can include logistics and supply chain, fleet management and logistics centers close to urban environments, such as airports, industrial parks and harbors.

Business Impact: Smart transportation impacts every industry, from users to producers, and anyone needing people or cargo transport. This biggest impact is on the industry itself (rail, road, maritime, aviation, buses, subways and taxis), but also to auto manufacturers and those requiring the distribution of goods as a requirement for their business. Smart transportation will broadly impact efficiency and effectiveness, mobility options, economic development, safety, security, population urbanization, the proximity of people's homes to work, and climate change initiatives. Autonomous vehicles and artificial intelligence will have a significant impact in the development of this sector.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: CVIC Software Engineering; Fujitsu; Hitachi; IBM; Reply; Siemens Mobility; Streetline; Tecsidel; Worldsensing

Recommended Reading: "Innovation Insight: Smart City Aligns Technology Innovation to Citizen Expectations"

"Transportation Network Intermediaries Will Disrupt Smart Mobility"

Sliding Into the Trough

Smart City Framework — GCC

Analysis By: Bettina Tratz-Ryan

Definition: Smart city in the GCC is the ability of the life cycle approach on urban governance to improve its citizens' life, stimulate its economy, and protect its environment. The strategy development, as well as its execution, is driven by a group of public sector and citizen stakeholders. They define and measure the impact of technology through data and analytics to create a user-focused and contextualized experience.

Position and Adoption Speed Justification: Smart cities have been embedded in national and local government strategies in the GCC to create economic diversification and improve the economic, social and environmental infrastructure of GCC countries. With their growing population, cities are the center of societal development and citizen comfort, which is expressed and measured in citizen happiness.

Compared with other regions and countries, in GCC countries, the satisfaction of the population with governmental services, as well as the usage of infrastructure and services, is a cornerstone of smart city strategies. The speed is accelerating from the development of free zones, new trading centers and new "greenfield" neighborhoods that are being developed in conjunction with real estate developers, business partners and leisure industry as investors. Smart city investments are closely linked to digital government strategies, with United Arab Emirates (UAE) leading the efforts in Dubai and Masdar City in Abu Dhabi.

User Advice:

- CIOs and IT leaders need to restructure their performance indicators for infrastructure and data architecture investments in terms of the ability to show KPIs that include citizen impact. Therefore, CIOs and IT leaders for the local government have to understand the business impact of smart city strategies, whether it is greenfield developments of housing developments Ajman or citizen satisfaction for public services in Dubai.
- CIOs in local government and ecosystems need to apply technology solutions and analytics of operational, IoT and user data to create an understanding of the urban environment. This also includes the development and the support of open data portals to encourage application development, creating the platforms to offer innovative experiences.
- CIOs of real estate developers and industrial zones, like Dubai Design District, or Lusail City in Qatar or Sharjah Smart City Map, need to understand technology solutions that create smart services to drive competitive experiences for users and citizens. That includes smart building and operational management solutions, as well as infrastructures for creating a digital urban environment.
- Public safety, visual analytics, as well as safe city strategies linked to smart city are critical for CIOs and IT leaders as they require an understanding of a control-and-command environment that will understand, operate and predict security, resilience and safety issues while creating an ambient living environment.

Business Impact: Real-time data created from IoT and social community data will need to be orchestrated to become high-quality data to be able to service contextualized services that will create citizen impact and satisfaction, or citizen happiness. Therefore, data management and governance become a critical tool for a CIO to develop a sustainable pipeline for internal government services, as well as citizen engagement. Smart Dubai has developed a happiness impact in which all the smart city investments and applications are mapped to the citizen satisfaction of government services. The business acceleration through blockchain and financial data sharing are key for the sustainable interaction between stakeholders in government and industry, especially with big events like Expo 2020 in Dubai.

Enterprises are mandated to report the satisfaction of their customers which is driving the integration of rating and feedback loop in business applications. There will be a reputational and business risk if customers and users cannot provide the feedback in a user-friendly way.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Accenture; Cisco; Deloitte; Hitachi; IBM; Siemens

Recommended Reading: "Innovation Insight: Smart City Aligns Technology Innovation to Citizen Expectations"

Wearables

Analysis By: Alan Antin

Definition: Wearable electronic devices are designed foremost to be worn and to sense the human body or the environment around the wearer. Most can wirelessly interface with cloud services or connect to the Internet of Things (IoT), typically through smartphone apps. They have computing intelligence built in, such as a microcontroller or digital signal processor. Examples include smartwatches, head-mounted displays (HMDs), body-worn cameras, Bluetooth headsets, wristbands, smart garments, sports watches and other fitness trackers.

Position and Adoption Speed Justification: Wearable devices moved closer to the Trough of Disillusionment because smartwatches, fitness trackers and immersive technologies are not living up to the hype that they would quickly be as popular as smartphones. Data must be integrated with that of other software platforms and with the IoT to deliver accurate insights, remote control and monitoring. Artificial intelligence is needed to more fully interpret input from wearable sensors and to deliver actionable advice as it is needed. New value must be created through services that are personalized to the preferences of consumers and the needs of businesses using contextual information and biodata gathered through wearable electronics.

Interest in wearables remains high due to Apple, Samsung, Google and others fostering ecosystems expected to gain traction. Different types of wearables have their own pace of development and adoption depending on their use case. Wearable products today are still early versions of what will be possible with sensors and analytics in the 10 year time frame.

User Advice: Invest in deployments or pilots for wearable user interfaces in the enterprise. Start with wearables for mobile workers who cannot conveniently put aside what they have in their hands to use a phone or tablet, or who need to keep their heads up or to hold on for safety. Workers can update the information management systems in factories with voice commands or video through head-mounted displays. Evaluate wearables to improve worker safety, such as environmental monitoring, detecting bodily injuries or contacting help in case of an emergency.

Choose use cases for wearables that make tasks more convenient and evaluate security and manageability requirements. Enterprise mobility management software options are becoming available for smartwatches that can serve as user interfaces to enterprise platforms such as Salesforce.

Enable people to be healthier through participation in employer wellness programs, healthcare providers and insurance companies that include incentives for sharing data through wearable fitness trackers. The general health of the consumer or employee can be measured with wearables, including body temperature, exercise, heart rate and heart rate variability (stress). Update and communicate policies for protecting personal data privacy.

Where time-motion and ergonomic efficiency is essential to productivity, such as in call centers and logistics organizations, employers are investigating wearables, such as head tracking through audio headsets and showing workflow tasks on HMDs. Provide remote expert help through wearable cameras for training. Conduct a cost-benefit analysis, especially before developing custom solutions for lower-paid workers in cost-sensitive roles.

Business Impact: Wearables have the potential to provide new efficiencies, improve quality and compliance, and enable new revenue opportunities. Early industries to adopt wearable electronics are aerospace and the police, followed by sports, manufacturing, materials handling, field service, architecture and retail. Wearable cameras are ready for deployment now for use cases such as for police/security, firemen and other first responders as well as inspections. Field service and manufacturing are streaming videos to an expert who sees what the wearer sees, reducing time to repair. Sports is using wearables on players for an "in-the-game" perspective in tracking the performance of athletes. VR headsets are used to coordinate designs of buildings with architectural firm clients and the construction trades. Augmented reality solutions on HMDs can increase productivity by providing part labels, checklists, maps and instructions superimposed on real-world views. The healthcare market stands to benefit from wearable user interfaces that enable mobile health monitoring, especially for self-care and management of chronic conditions.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Apple; Epson; Fitbit; Google; Microsoft; Plantronics; Qualcomm; Samsung; Sony; Vuzix

Recommended Reading: "Cool Vendors in Health Wearables"

"Cool Vendors in Enterprise Wearable and Immersive Technologies, 2017"

"Market Insight: Wearables in Healthcare Ecosystems Get Rolling in 2018"

"Improve Customer Experience for Wearables With Artificial Intelligence"

"Semiconductor Forecast Database, Worldwide, 1Q18 Update"

"User Survey Analysis: Wearables Need to Be More Useful"

Private Cloud Computing

Analysis By: Thomas J. Bittman

Definition: Private cloud computing is a form of cloud computing used by only one organization, or one that ensures an organization is completely isolated from others. As a form of cloud computing, it has full self-service, full automation behind self-service and usage metering. It does not have to be on-premises, or owned or managed by the enterprise.

Position and Adoption Speed Justification: Private and public cloud computing are at opposite ends of the "isolation" spectrum. As public cloud providers have offered virtual private cloud, dedicated instances, and dedicated hosts, the gap between private and public has become a spectrum of isolation choices.

Organizations that build a private cloud service are emulating public cloud computing providers to acquire similar benefits — mainly agility, mainly for new cloud-native applications, mainly for business value and growth. This can be for infrastructure as a service (virtual machines or containers), platform as a service, or in some situations, software as a service.

The use of third parties for cloud computing (private and public) has been growing rapidly. The ongoing cost and complexity of building a true private cloud can be extreme, and the rationale for building your own has been declining.

This term is also used to describe a very different trend, where traditional infrastructures that are being modernized with virtualization, some automation, and some self-service — leveraging only some valuable attributes of cloud computing, but applying them to existing applications with traditional infrastructure requirements. However, because these are different trends, Gartner does not include this form of modernization in our definition of private cloud. But when the goal is IT efficiency or modernization for existing applications, these "just enough cloud" architectures can be beneficial (but that's not covered in this profile).

User Advice:

- Evaluate third-party options first. These include hosted private cloud, managed services, virtual private cloud alternatives, or public cloud.
- Choose your private cloud strategy based on the necessary return on investment or business goals: If business growth or business value for new applications, consider a true cloud architecture; if IT efficiency or IT modernization for existing applications, choose cloud-inspired technologies and methods to implement surgically. Just-enough cloud is often enough.
- Focus on business and application needs first, don't start with the technology. One technology architecture and operational model cannot support all of the application needs of a typical enterprise. Either build multiple architectures and operational models, or leverage third-parties.
- Focus on services that fit the cloud model — standard, high-volume and self-service; those that require agility, horizontal scalability; and usages that might be short-lived.

- Consider the long-term roadmap for your private cloud services. Build with the potential to integrate, interoperate or migrate to public cloud alternatives at the appropriate time.
- Manage the scope of work — start small, and broaden based on the business case.
- Build expertise in managing multiple architectural and operational models, and multicloud — this is more valuable to an enterprise than expertise in building a single cloud architecture.

Business Impact: Cloud computing enables agility that an enterprise can use to react quickly to business requirements in functionality or scale. Due to economies of scale, cloud computing can also improve efficiency and lower costs. However, because leveraging a true cloud computing architecture requires applications and operational models designed for cloud computing, the cost of transformation for existing applications does not always justify the investment.

True private cloud computing is used when enterprises aren't able to find cloud services that meet their needs in terms of regulatory requirements, functionality or intellectual property protection. True private cloud computing is almost always purpose-built for a specific set of new applications, and their success can be measured in revenue or market share.

When the primary goal of a private cloud is IT efficiency, businesses can reduce costs and improve overall operational efficiency for their existing application portfolios by leveraging cloud technologies where appropriate, and adding manual or custom intervention, or customized changes as needed to support those applications.

However, enterprises need to recognize that these are two different goals, with different architectures, and trying to do them in a single architecture usually achieves none of the goals well. Being bimodal, based on business and application needs makes the most business sense.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Apprenda; BMC; Hewlett Packard Enterprise; IBM; Microsoft; Pivotal; Red Hat; VMware

Recommended Reading: "When Private Cloud Infrastructure Isn't Cloud, and Why That's Okay"

Climbing the Slope

Enterprise Firewalls (Next-Generation Firewalls)

Analysis By: Adam Hils

Definition: Enterprise firewalls (sometimes called NGFW) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, identity awareness and intrusion prevention, using intelligence from outside the firewall. These extra firewall intelligence services include cloud-based advanced threat detection (ATD) and threat intelligence

(TI). An enterprise firewall should not be confused with a stand-alone network IPS or SMB multifunction firewalls (unified threat management [UTM]).

Position and Adoption Speed Justification: Enterprise firewalls are achieving a very large market size, and capabilities continue to improve. This technology has advanced greatly and has supplanted the preceding technology of stateful firewalls in most enterprise perimeters. The time to plateau has been adjusted to a longer time in reflection of the increased number of services — such as recent integrations with cloud access security brokers (CASBs) — being added to the firewall, and the disruptive effects of public and private cloud-native firewalls providing competition within the data center. To be relevant in IaaS deployments, enterprise firewalls must show smoother integration with the IaaS environments and better policy automation. In addition, the rise of encrypted traffic is forcing enterprise firewall vendors to enhance decryption capacity and performance with hardware and software enhancements.

User Advice: Consider enterprise firewalls for your shortlist if you're replacing or upgrading a legacy stateful network firewall at the network edge and you don't have a significant investment in a stand-alone IPS. However, if you have such an IPS investment, ensure that any selected firewall has strong IPS functionality, so that, when the IPS needs to be replaced, you'll have the option to move to an enterprise firewall that includes IPS with the least amount of disruption. Enterprise firewalls rarely include slower inspection mechanisms, such as antivirus or physical anti-malware sandboxes, as these can introduce unacceptable latency. Although not housed in the same appliance, better firewall vendors now have "good enough or better" cloud-based sandboxes, or connections to local sandboxes from the same or a partnered vendor providing a single console view. A difficulty for any cloud-based sandbox is the limited adoption and efficiency of TLS decryption on firewalls, which reduces the visibility of encrypted traffic; leaving encrypted traffic unavailable for IPS or sandbox inspection.

Business Impact: The modern enterprise firewall closely integrates the capabilities of enterprise firewalls with network intrusion prevention and other services.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Check Point Software Technologies; Cisco; Forcepoint; Fortinet; Hillstone Networks; Huawei; Juniper Networks; NSFOCUS; Palo Alto Networks

Recommended Reading: "Magic Quadrant for Enterprise Network Firewalls"

"Next-Generation Firewall Hype Has Become an Obstacle for Enterprises"

"How to Maximize Value in Firewall Contract Negotiations"

Postmodern ERP Support

Analysis By: Duy D Nguyen

Definition: Postmodern ERP support refers to a shift in ERP support to align with the evolution of ERP architecture from a single, all-encompassing megasuite to a more federated environment composed of loosely coupled cloud and on-premises applications. As ERP suite technology advances and business functions move to the cloud, the role of the ERP support organization must evolve.

Position and Adoption Speed Justification: Pressure to restructure how ERP support is delivered is increasing. Enterprises must adapt quickly to adopt and institutionalize the organizational changes necessary to support the increasing shift of ERP capabilities to the cloud.

Many ERP and business application vendors already provide domain capabilities in the cloud (Workday for human capital management, for example). Recent Gartner surveys show that over 80% of enterprises have already adopted a hybrid ERP scenario. Although many enterprises have extended their ERP portfolio to include cloud solutions, postmodern ERP support's position on the Hype Cycle reflects our view that fewer enterprises have worked out how to support hybrid ERP solutions effectively. Better leveraging customer success offerings from the ERP vendors and promoting a continuous standardization mindset are still challenges to be overcome by companies adopting hybrid ERP environments.

User Advice: As more ERP functionality is moved to the cloud, managing a hybrid ERP solution through its life cycle becomes more complex. ERP leaders must develop new approaches to identifying and resolving application issues and responding to new service requests that incorporate the concept of cloud services. Particular areas that must be addressed include service management, integration management and governance for changes initiated outside the enterprise by the cloud vendor.

In addition, application leaders responsible for ERP should:

- Redefine the ERP competence center to support postmodern ERP scenarios.
- Develop ERP competence center skills and resources to support cloud services.
- Adjust the enterprise's application change governance processes to reflect cloud service providers' delivery models and limitations.
- Revise the application change control group's approval process to incorporate cloud service factors.
- Expand application support processes to include working with the cloud service provider's resources, processes and constraints.
- Redefine roles and responsibilities between the business and IT to provide support.

Business Impact: Postmodern ERP demands a change to the status quo of the IT organization's roles and responsibilities. Cloud services can either simplify or add an extra layer of complexity to application support efforts, because much of the cloud service's life cycle is out of the control of the

IT organization and the ERP leader. Failure to recognize the shift in required organizational structure, resources, skills, governance, methods and processes will hurt the IT organization's ability to support the business. Supporting postmodern ERP requires service relationship management capability — skills in procurement, contract management and service management, for example — which will require the IT organization to change.

Postmodern ERP also changes the relationship between the ERP support organization and business stakeholders and users, because cloud solutions and services shift more control to the business.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Recommended Reading: "Seize the Moment by Maximizing Value With Event-Driven ERP Architecture"

"Deciding to Buy or Build in the Postmodern ERP Era"

"Identify When ERP Replacement Is Required to Enable Digital Business Transformation"

"2018 Strategic Roadmap for Postmodern ERP"

"Toolkit: ERP Competency Center Resources Allocation Model"

"What ERP Application Leaders Must Do to Succeed With Mode 2"

"Invest in the Superuser Role to Improve ERP Support"

DDoS Defense

Analysis By: Lawrence Orans; Claudio Neiva

Definition: Distributed denial of service (DDoS) attacks use multiple techniques to disrupt business use of the internet or to extort payment from businesses to stop the attacks. DDoS defense products and services detect and mitigate such attacks.

Position and Adoption Speed Justification: This year, the positioning of DDoS defense moved slightly to the left again, due to the continuing innovation from DDoS attackers that results in challenges to enterprises. For example, in March 2018, the largest ever DDoS attack (1.3 Tbps) ever recorded was launched against GitHub. The attackers used Memcached servers to amplify the DDoS attack. In late February 2018, a vulnerability with Memcache was disclosed and the issue was quickly fixed. However, before the update could be applied to the approximately 100,000 Memcached servers, the attack was successfully executed.

User Advice: DDoS mitigation services should be a standard part of business continuity/disaster recovery planning, and they should be included in all internet service procurements when the business depends on the availability of internet connectivity. Most enterprises should look at detection and mitigation services that are available from CSPs, hosters or DDoS security-as-a-service specialists (for example, "scrubbing center" providers). To defend against complex, application-based attacks, a mix of local protection (on-premises DDoS appliances) and cloud-based mitigation services is a strong option. The content delivery network (CDN) approach to DDoS protection is also a valid approach, particularly when the organization is already using a CDN for content distribution to improve the performance of its website. However, the CDN approach only protects websites. It does not protect against attacks aimed at nonweb targets (for example, corporate firewalls, VPN servers and email servers). Another option for DDoS mitigation services comes from the IaaS providers. The leading IaaS providers (AWS, Microsoft Azure and Google Cloud) all offer basic and advanced (fee-based) DDoS mitigation services.

Because of the increased awareness of DDoS attacks, more communications service providers (CSPs) and hosters have entered the market for DDoS mitigation services. Some have built their own infrastructure, whereas others have partnered with specialty DDoS mitigation service providers. Still others have actually been offering services over many years, which has enabled them to develop strong expertise. Prospective customers should gauge the level of experience of CSPs and make sure that the price of their services reflects their level of experience. Also, we still hear that some CSPs are "blackholing" traffic, when they have been unable to mitigate an attack against a customer. This technique protects the CSP's other customers from collateral damage, but it completely removes the targeted customer from the internet. Enterprises considering ISP-based DDoS mitigation services should request clauses that their traffic will not be dropped.

The increased competition in the DDoS mitigation market has also led to more competitive pricing and pricing models. Many providers now offer packages that are more cost-effective because they include a fixed number of mitigations per year (as opposed to an unlimited mitigation model). Enterprises that are at less risk of being attacked frequently are good candidates for these new pricing models with a fixed number of mitigations.

Business Impact: Any website can be targeted by DDoS attackers. Attackers will sometimes target nonweb resources (such as firewalls) to disrupt users' access to the internet. DDoS mitigation services are highly effective in mitigating these attacks. For example, a good DDoS mitigation provider will restore access to a company's website, even during a large-scale attack. Enterprises that lack DDoS mitigation services could face heavy financial losses in the event of an attack. Also, if the enterprise does not defend itself properly during an attack, its reputation could be negatively impacted. Thus, DDoS mitigation services are a highly valuable investment for every enterprise that needs to protect its website and its access to the internet.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: Akamai; F5; Imperva; Link11; Neustar; Nexusguard; NETSCOUT (Arbor); Oracle (Dyn); Radware; Verisign

Recommended Reading: "Market Guide for DDoS Mitigation Services"

"Best Practices to Defend Your Organization Against DDoS Attacks in India"

"Defining Cloud Web Application and API Protection Services"

IT Infrastructure Monitoring

Analysis By: Pankaj Prasad

Definition: ITIM tools capture the performance and availability of IT infrastructure components that reside in a data center or are hosted in the cloud as infrastructure as a service (IaaS). These tools monitor and collate the availability and resource utilization metrics of servers, networks, database instances, hypervisors and storage. It is common for these tools to collect metrics in real time and perform historical data analysis of the elements they monitor.

Position and Adoption Speed Justification: Infrastructure component monitoring tools have been available for decades, supporting IT infrastructure components across all primary domain groups (such as, servers, networks, storage, database). These are usually the first set of tools in which enterprises invest to monitor availability and to enable the ability to troubleshoot in a reactive manner.

Changes in IT architectures mean ITIM tool vendors have to be quick in responding to and addressing new requirements. As an example, with increasing adoption of container technologies, some ITIM vendors are addressing the need to monitor containers at a more granular level rather than treating containers like a regular OS-level process. Toward this goal, some vendors are rearchitecting their monitoring tools for more granular data collection.

Vendors are also focusing heavily on the visual aspects to provide relevant information through interactive dashboards and the ability to dynamically drill down to component levels in the infrastructure. The improvement in user interface (UI) is being combined with advanced analytics to provide relevant insights for IT and non-IT personas, with the focus clearly on insights rather than raw data. Some vendors are aiming for a one-stop solution by including APM metrics either through acquisitions, partnerships or through organically deploying some application monitoring features within existing portfolio.

Many of these tools offer log parsing or aggregation, combined with analytics capability. Analytics is further leveraged to enable dynamic thresholds, and in some cases, for topology and dependency maps. The combination of metrics and logs with analytics can be used for context, cause-and-effect correlation and enable easier and faster troubleshooting capability, resulting in better MTTR.

The ongoing pressure to reduce IT costs continues to fuel growing interest in open-source tools and SaaS delivery models. At the same time, the market is also seeing some SaaS offerings that leverage big data technologies for higher amounts of data ingestion and analytics for better insights. Most of the global enterprises have implemented these tools for their data center components as a minimum scope to capture availability and performance metrics.

ITIM tools market needs to keep pace with the rapid evolution of technology and IT architectures as end users rely on these tools for their diagnostic capability. As a result the ITIM market is lagging in maturity as it tries to rapidly evolve, for example, to provide visibility across cloud, containers and IoT.

User Advice: Enterprises must make investments in this area as their first step toward becoming more proactive in monitoring their infrastructure (from a performance analysis perspective). Organizations using point solutions such as separate monitoring solutions for Windows servers, UNIX servers and storage systems must consider investing in ITIM solutions to enable cross-domain visibility across their IT landscape and to ease event overload by leveraging the inbuilt ECA engine.

Most organizations can improve their monitoring capabilities simply by making more extensive use of the tools they have and then advance toward leveraging analytics capabilities for better insights, correlations and proactive capabilities.

Based on the current maturity level of the market, consider the following attributes when selecting ITIM tools:

- The scope of their footprint when collecting relevant metrics
- Ease of deployment
- Ability and ease of integration with other ITOM tools
- Ability to deal with data at speed and scale (IoT, microservices, containers)
- User interface and price

I&O leaders should look for the ability of the tools to parse logs and advanced analytics as additional features when assessing ITIM tools.

Organizations may extend their visibility into the application layer by deploying APM tools and also by leveraging AIOps platforms.

Business Impact: Infrastructure monitoring tools are used to monitor the quality of service of components and sections of the infrastructure, as well as help improve availability, lower risk and the total cost of ownership (TCO) of managing a large and complex infrastructure environment.

ITIM tools help derisk enterprises by making data available to other ITOM tools and processes such as capacity and performance management. This helps business ensure they do not overprovision or underprovision compute resources, which is especially important in virtual and cloud-based architectures. Additionally, they integrate or interchange data with third-party systems or across other toolsets in real time — for example, ITIM tools work with IT service management (ITSM) tools to open tickets for support.

ITIM also brings in efficiency and enhances productivity of IT operations teams by providing event correlation and analysis (ECA) capability. Postprocessing of events, policy-driven workflows and alert notifications help avoid event overload and workflows help avoid human error.

Increasingly, data from ITIM tools is being sent to algorithmic IT operations (AIOps) platforms for leveraging pattern recognition and machine learning capabilities, thereby easing the ability to assess impact of IT on customers.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Fata Informatica (SentiNet3); Galileo; NetApp; New Relic; OpsRamp; OP5; SolarWinds; Zabbix; Zenoss; Zoho (ManageEngine)

Recommended Reading: "Market Guide for IT Infrastructure Monitoring Tools"

"Modernize ECA With IT Infrastructure Monitoring Tools"

"Adopt a Data-Driven Approach to Consolidating Infrastructure Monitoring Tools"

"IT Infrastructure Monitoring Tools: Best of Breed or a Suite?"

"The Monitoring Metrics IT Operations Should Report On"

SIEM

Analysis By: Toby Bussa; Mitchell Schneider; Gorka Sadowski

Definition: Security information and event management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real-time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards and reporting).

Position and Adoption Speed Justification: Targeted attacks and broad-based malware infections resulting in breaches and data loss events have now caused threat detection to be the primary driver for purchasing SIEM technologies. New buyers and those with existing SIEM technology deployments seek earlier, more effective incident and breach detection through active security event monitoring. SIEM solutions continue to evolve to address a variety of persistent challenges — how to keep up with changing external and internal threats; increases in the volume, velocity and variety of data sources; and how to effectively implement, manage and use the solutions as expertise and resources become more constrained. New entrants have emerged from the user and entity behavior analytics (UEBA) space, and primarily emphasize a user-based approach to monitoring for threats, compared to the more traditional approach of event-based monitoring oriented around IP addresses and hostnames. Organizations looking to shorten the deployment cycle and transfer responsibility for managing a SIEM tool's platform are opting to leverage Software as a Service (SaaS) SIEM and hosted SIEM solution options, which are becoming more visible with buyers. However, the ability to integrate with many Infrastructure as a Service (IaaS) and SaaS environments via cloud connectors is still limited compared to the method of collecting log information from on-premises data sources.

SIEM vendors continue to develop and implement big data capabilities and advanced analytic functions in their own products, or through acquisitions of other security analytics technology vendors, and/or provide integrations with third-party technologies for these functions (e.g., UEBA). The result is improving security analytics capabilities ranging from basic capabilities (such as statistical baselining or trending that are included as part of core product functionality) to advanced, machine learning-oriented detections developed internally or provided by third-party solutions. SIEM technologies are also adopting more advanced incident response capabilities through the addition (either natively, via acquisition or integrations) of functions that add security orchestration, automation and response (SOAR) capabilities.

User Advice: Security and risk management leaders considering deploying a SIEM solution should first define their use cases, followed by the requirements for log management, threat monitoring, user and resource access monitoring, security incident response management, and compliance reporting. Other stakeholders in the organization (such as audit and compliance, network operations, server administration, database administration, and application support areas) may be required to provide assistance with defining the initial use cases and roadmap. It may also require the SIEM tool to integrate with other nonsecurity data sources that would provide additional business context for security event monitoring (such as user directories, configuration management databases [CMDBs] and vulnerability assessment products). Organizations should document their network and system topologies, and where security controls are deployed in the organization, along with future use cases that will affect the SIEM solution's expansion and evolution and analytic requirements. Estimates of log volume and event rate velocities, in addition to the number of log/data sources, should be documented for the initial use cases, as well as the future use cases that may be implemented within the next 12 to 24 months. Furthermore, considerations should also be made for how the SIEM technology will be administered, managed and operated, and whether an external service provider will be required to provide basic management of the solution and/or 24/7 security event monitoring and alerting.

Business Impact: SIEM solutions improve an organization's ability to quickly detect attacks and data breaches, and improve incident investigation and response capabilities. However, they require an ongoing investment in resources (budget, expertise and staffing) for both technology operations and security event monitoring to realize its true value. SIEM tools also support other use cases (such as the reporting needs for organizations with regulatory compliance obligations, as well as those subject to internal and external audits).

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: AlienVault; Dell Technologies (RSA); Exabeam; IBM; LogRhythm; McAfee; Micro Focus; Rapid7; Securonix; Splunk

Recommended Reading: "Magic Quadrant for Security Information and Event Management"

"Critical Capabilities for Security Information and Event Management"

"Establish Scope and Requirements for a Successful Security Information and Event Management Deployment"

"How to Deploy a Security Information and Event Management Solution Successfully"

"Overcoming Common Causes for SIEM Solution Deployment Failures"

Biometric Authentication Methods

Analysis By: Ant Allan

Definition: Biometric authentication methods use unique biological or behavioral traits to corroborate users' identities when they access endpoint devices; networks; or mobile, networked or web applications.

Across a wide range of use cases, any biometric authentication method may be used in one-to-one comparison mode (where there's an implicit or explicit claim of a specific identity) or one-to-many search mode (when the user simply presents his or her biometric trait and the system determines the user's identity from a range of candidates).

Position and Adoption Speed Justification: Biometric methods embrace many technologies and different use cases have different demands. The position and time to plateau of this technology represent optimal cases.

Improved user experience (UX) is a key driver, but the potential is not always fully realized. Usability and reliability issues have inhibited corporate adoption of fingerprint modes in particular, which still colors buyers' attitudes toward all modes.

Offerings that use existing inputs on endpoint devices for other modes (see the User Advice section) continue to mature. The lower cost and improved UX of these modes are appealing, and the UX benefits continue to drive adoption in mobile banking applications.

Although biometric specialists lead, mainstream authentication vendors continue to move biometric methods from roadmap to general availability. Vendors typically support one or more modes directly on one or more types of endpoints. Several vendors now exploit the user's phone as a capture device (or more) to support access from other endpoints (and in other channels).

Many vendors use Fast IDentity Online (FIDO) authentication protocols that can simplify implementation (among other benefits). W3C WebAuthn browser support will speed adoption and increase penetration over the next two years. The FIDO Alliance also plans a certification program that will give buyers greater confidence in FIDO-compliant biometric authentication solutions.

Client interest in using biometric methods for Windows PC and network login has been prompted by Microsoft's support for biometric methods in Windows Hello for Business. Where Hello falls short, client attention has turned to vendors that provide generic biometric solutions across multiple PC and mobile OSs. However, biometric authentication remains niche in this use case.

User Advice: Biometric methods with effective presentation attack detection (PAD), or liveness testing, are a viable alternative or adjunct to passwords and tokens across a variety of use cases. However, as with any authentication method, evaluate the potential benefits of specific biometric methods against the needs of each use case and choose among the options on the same basis. Biometric methods can provide greater individual accountability than alternatives and should be favored when this is paramount.

UX benefits are particularly relevant to all mobile use cases. Most modes can provide better UX for the majority of users than nonbiometric alternatives. Although banks commonly integrate device-embedded modes in mobile banking apps, third-party face and voice are emerging as the modes of choice, with some adoption of scleral vein and camera-based fingerprint modes. In general, active biometric modes that can make use of standard inputs (camera and microphone) offer UX, trust, accountability and other benefits over device-embedded methods. Consider options for people who cannot reliably use a particular method — but these might include alternative biometric modes.

Passive behavioral modes (keyboard, gesture and handling dynamics) can provide postlogin "continuous authentication" with minimal friction; these are best considered among other familiarity signals consumed by analytics, rather than as an orthodox authentication credential.

Consider migrating to biometric authentication for Windows PC and network access, but recognize the limitations of Hello for Business and evaluate proprietary solutions that offer broader endpoint support and choice of biometric modes.

Business Impact: Biometric methods with effective PAD can provide improved UX (although this varies by mode and, for some modes, by user) and increased trust and accountability (because biometric traits cannot be easily shared with others).

Biometric methods suit mobile use cases, where users — especially retail customers — resist having to use any kind of discrete token. Biometric methods may be integrated within mobile apps (as they are in mobile banking), enterprise mobility management solutions, apps for mobile push authentication and so on.

Biometric methods can be used for PC and network login. Proprietary solutions offer broader endpoint support and choice of biometric modes and are thus provide more value that device-embedded biometric methods, including those supported by Hello for Business.

Some biometric modes, such as face and gesture dynamics, can provide continuous authentication throughout a session, elevating trust and mitigating "walk away" risks, potentially eliminating the need to enforce timeouts, which users loathe. Face modes meet higher education needs for remote proctoring during online examinations. Passive behavioral modes add significant value to analytics-based tools, including OFD tools, elevating trust without degrading UX. In an OFD context, these modes can also provide bot detection.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: BehavioSec; BioID; BIO-key; FacePhi; HYPR; ImageWare Systems; Nuance; OneVisage; Veridium; Zoloz

Recommended Reading: "Best Practices for Selecting New User Authentication Methods"

"Technology Insight for Biometric Authentication"

"Market Guide for User Authentication"

"Don't Treat Your Customer Like a Criminal"

Enterprise Mobility Management Suites

Analysis By: Andrew Garver; Chris Silva

Definition: Enterprise mobility management (EMM) suites help organizations securely integrate mobile devices to their enterprise systems. EMM suites configure devices to comply with organizational policies, manage and secure applications, protect enterprise data, and increasingly provide contextual trust. Five core EMM technical categories help IT organizations perform these services: mobile device management (MDM), mobile application management (MAM), mobile content management (MCM), mobile identity and mobile containment.

Position and Adoption Speed Justification: EMM suites define a minimum security baseline by enforcing and executing basic policy actions across mobile operating systems. In addition, EMM suites are expanding their coverage from mobile to PC operating systems, such as macOS and Windows 10, with the aim of providing a consistent workflow through a common console. The continued decline of Windows applications, the impact of continuously updated OS platforms, and new bridge technologies such as Windows 10 co-management are leading organizations to rethink their PC management strategies. EMM is reaching maturity on the classic technology S-curve, having paved the way for both CMT and EMM tools to converge into unified endpoint management.

Even as EMM suites have gained adoption, organizations still confront end-user resistance to device management due to perceived loss of privacy. In addition, EMM suites have not been able to extend support to use cases that involve customer (B2C) ecosystems, and they have had limited success in B2B scenarios. Although EMM suites try to be platform-agnostic, Android fragmentation continues to be a problem in BYOD environments. MTD tools will increasingly complement EMM to fill the gaps in vulnerability detection and malware risks.

User Advice: Identify critical policy controls and the mobile use cases in your organization, and evaluate the EMM functions that are most critical in addressing those requirements. No EMM vendor excels in all functions because of the breadth of the products.

Use mobile apps as a catalyst to drive business mobility initiatives and increase adoption of EMM among your user base. Although MDM provides the plumbing to enforce policies, MAM provides opportunities for business enablement and quick wins.

Train your users at the time of deployment to increase overall user satisfaction and to reduce support overhead.

Integrate with IAM tools to provide conditional access to corporate resources by expanding the definition of trust to the user, app and device.

Identify the right use cases for managing PCs using EMM, such as bring your own PC (BYOPC). Investigate co-management for end-user systems that have a high number of legacy applications or complex granular control. Use native containerization approaches such as iOS-managed apps and Android management while avoiding vendor lock-in to EMM-specific SDKs.

Use EMM as an orchestration point to enforce policies in conjunction with other MTD tools.

Business Impact: EMM suites help mobilize business processes and workflows, so the business impact of EMM is tied to the impact of enterprise mobility itself. I&O leaders realize the growing importance of enterprise mobility as a meansEMM suites help mobilize business processes and workflows, so the business impact of EMM is tied to the impact of enterprise mobility itself. I&O leaders realize the growing importance of enterprise mobility as a means to gain competitive advantage. In that sense, EMM is used as a business enablement tool to fulfill two basic requirements: enabling general productivity (email, calendar and access to documents) and digital business initiatives (in-flight shopping, self-service kiosks and digital signage).

As organizations seek greater return on mobility investments, mobility management will involve delivering unified workspaces that encompass PCs, mobile devices, emerging form factors such as HMDs and wearables, and cloud-based services for app delivery and content storage. The ability to contextually deliver relevant content to mobile users by using the device and user context available through EMM tools will enable organizations to realize the value of digital business moments. The use of EMM data will go beyond security restrictions and will be harnessed to gain insights into app utilization and cost optimization.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: BlackBerry; Citrix; IBM; Matrix42; Microsoft; MobileIron; Sophos; SOTI; VMware (AirWatch)

Recommended Reading: "Use Analytics to Convert Enterprise Mobility Management Data Into Business Value"

"Unlock Mobile Digital Business Opportunities Using Enterprise Mobility Management Capabilities"

"Magic Quadrant for Enterprise Mobility Management Suites"

"Critical Capabilities for Enterprise Mobility Management Suites"

Privileged Access Management

Analysis By: Felix Gaehtgens

Definition: PAM tools offer one or more of these features:

- Control access to privileged accounts —for shared and emergency access.
- Randomize, manage and vault credentials (password, keys, etc.) for administrative, service and application accounts.
- Give single sign-on for privileged access to stop credentials being revealed.
- Control, filter and orchestrate privileged commands, actions and tasks.
- Manage and broker credentials to applications, services and containers to avoid exposure.
- Monitor, record and audit privileged access, sessions and actions.

Position and Adoption Speed Justification: Interest in PAM tools remains high, driven by cybersecurity threats, regulations and the need for proper security hygiene that calls for greater control of privileged access. Vendors are starting to converge on bundled offerings, indicating a market rapidly maturing, but not yet commoditized. Thus, the position of PAM tools in this years' Hype Cycle advances. PAM tools are increasingly used to secure operational technology and industrial control systems. Securing privileged access to IaaS and PaaS is generating additional interest in those tools; however, PAM market growth is behind IaaS and PaaS market growth, indicating that privileged for many IaaS/PaaS assets are not properly protected — for now. Securing DevOps toolchains (continuous deployment/continuous integration) and management of credentials for containers is driving interest and intense product development activity by PAM vendors.

PAM tools broadly fall into two main categories: privileged account and session management (PASM), and privilege elevation and delegation management (PEDM; see "Market Guide for Privileged Access Management"). Some vendors offer alternative approaches, or focus on session recording and/or key management.

User Advice: Develop a leadership consensus of your security, regulatory, operational and cultural needs for managing privileged access before choosing a PAM toolset; established policies, practices and processes are usually ill-prepared to properly manage and govern privileged access. Getting agreement on any necessary changes to working practices is essential to successful deployment of PAM tools; without this, users will attempt to bypass or subvert the tools. Political boundaries and turf mentalities in organizations prevent comprehensive utilization and erode security.

Scrutinize offerings from multiple vendors; pricing for tools is converging into bundled offerings, but varies in licensing metrics (per user/per asset/per session). Tools from multiple vendors can often be integrated in a best-of-breed approach. Ensure that administrative accounts for network devices, hypervisors, IaaS, PaaS and SaaS are within scope as well. Several PAM vendors now offer their solutions as a service or offer deployment models in IaaS environments. Using hybrid approaches that mix on-premises with separate cloud-based options may work best for many organizations that have mixed infrastructures. Do not overlook service and software accounts — they are a considerable source of security and operational risk. Finally, failover planning is crucial for success; ensure that your solution is highly available.

Integrate PAM tools with change and incident management workflows (IT service management tools) for tighter access control in your operational environment. Also, try to automate privileged tasks as much as possible to eliminate the need for full operating-system-level privileged access by humans and to enable automated privileged tasks to be executed by lesser skilled personnel.

Business Impact: Privileged access is high risk and many breaches can be attributed to privileged access misuse, stolen privileged credentials or hijacked privileged accounts. PAM tools provide robust and granular control, transparency, and more accountability for privileged access than manual controls and custom or generic tools. Particularly, they offer the following benefits:

- Mitigate risks and achieve visibility of privileged operations and account use.
- Enable privileged access only when it is necessary — according to the principle of least privilege.
- Mitigate risks associated with malware targeting privileged accounts.
- Eliminate hard-coded passwords in application code, scripts and configuration files.
- Enable a forensic review of privileged access activity.
- Provide real-time monitoring, auditing and alerting of privileged activities.
- Manage credentials for DevOps toolchains and containers.
- Provide delegation for automated privileged tasks, which help significantly increase IT staff efficiency and reduce operating costs.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: ARCON; BeyondTrust; Bomgar; CA Technologies; Centrify; CyberArk; One Identity; Osirium; Thycotic; WALLIX Group

Recommended Reading: "Market Guide for Privileged Access Management"

" Best Practices for Privileged Access Management "

" Manage Service Accounts to Mitigate Security and Operational Risks"

Entering the Plateau

Unified Communications and Collaboration

Analysis By: Adam Preset

Definition: Unified communications and collaboration (UCC) is an enterprise approach to combining asynchronous and synchronous technologies, such as messaging, presence, voice, video and content collaboration. UCC solutions can be premises-based or cloud-based. Communications vendors penetrate new markets with messaging and content tools, while collaboration vendors enhance their platforms with real-time communication services.

Position and Adoption Speed Justification: UCC represents a vendor approach of delivering an integrated collective offering to address most worker communication and collaboration needs. Without UCC, enterprises have to blend portfolios of products from multiple vendors to provide capabilities without a unified experience. Workers expect to shift seamlessly from messaging to voice to video, and across physical spaces, platforms and devices, to reach internal and federated external collaborators. IT expects to manage the fewest products from a single vendor to satisfy the most workers. UCC is common, but seamless UCC remains an aspiration.

UCC merges formerly distinct markets. A vendor with heritage and strength in unified communications adds functionality to bolster collaboration, and vice versa. Feature overlap in different products is common. Strong traction for UCC depends on robust network and telephony infrastructure.

Cloud office collaboration vendors, such as Microsoft and Google, increasingly appeal to buyers with modest and simple UC needs, especially those de-emphasizing telephony. As UCC vendors invest in cloud offerings, new features and innovations lag behind in on-premises deployments.

User Advice: Gartner recommends that application leaders:

- Create a task force to develop a UCC strategy that is made up of line-of-business staff as well as communications and IT specialists, to reduce interdepartmental friction.
- Assess cloud options as seriously as on-premises solutions.
- Separate organizational and budget-related politics from the task of assessing the benefits of enhancing users' communication and collaboration capabilities.

A UCC project can produce both benefits and unintended drawbacks. In some cases, it could needlessly disrupt work practices, add complexity, and seem unnecessary, costly and a waste of resources. In other cases, it could improve communications, augment work performance, increase effectiveness, and help virtual teams to excel. Some employees may need rich unified communications, while others may require only "UC-lite," alongside collaboration tools. It is not an all-or-nothing proposition for every user.

Application leaders starting a UCC project should:

- Investigate needs in the context of specific use cases, before attempting to deliver a solution.
- Select solutions that integrate with, and support, critical business applications.
- Allow some degree of solution overlap, if it proves beneficial and sensitive to users' preferences and requirements; citizen IT deployments can help you understand these.
- Provide guidance about practices, if appropriate.
- Determine the right capabilities roadmap for various user segments.
- Look for user segments that already understand the potential benefits and business cases that present the clearest path to a measurable return.

Pilot projects can help build a case for more widespread deployment.

Business Impact: IT leaders expect integrated tools. Their expectations extend to the highest-value combination of interactive services — both inside and outside the firewall — and include both fixed and mobile devices. Presence services are vital unifying tools. Some vendors offer UCC capabilities as a complete stack. Standards-driven integrations make even more combinations possible. Large enterprises will likely need a harmonizing approach via a portfolio that covers "good enough for most" and "best-of-breed for a few" solutions.

Although there is generally an acceptance that UCC is necessary, organizations will struggle to quantify the benefits and calculate the ROI. Enterprises may need to eschew traditional ROI mechanisms and seek alternative, less quantifiable means to justify UCC investments. These include process cycle acceleration, faster problem remediation, increased information awareness, employee engagement and the inclusion of more internal and external resources as part of the planning process.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Alcatel-Lucent Enterprise; Atos; Avaya; Cisco; Google; Huawei; IBM; Microsoft; Mitel

Recommended Reading: "Digital Disruptions in the Unified Communications and Collaboration Market, 2017"

"Planning, Selecting and Deploying Unified Communications and Collaboration Primer for 2018"

"Digital Workplace Employees Need Enterprise Communications to Be More Harmonized Than Unified"

"Magic Quadrant for Unified Communications"

"Magic Quadrant for Unified Communications as a Service, Worldwide"

Identity Governance and Administration

Analysis By: Brian Iverson; Felix Gaehtgens

Definition: IGA solutions manage identity and access for users across multiple systems by aggregating and correlating disparate identity and entitlements data to enhance control over user access. This aggregated data serves as the basis for core IGA functions including: identity life cycle and entitlements management, access requests with approval workflows, access certification campaigns, role-based and policy-driven administration, fulfillment (direct provisioning and indirect fulfillment via service tickets), auditing, and reporting and analytics.

Position and Adoption Speed Justification: IGA tools are a cornerstone of organizations' IAM strategies, so IGA adoption has increased rapidly. Vendors are starting to address some concerns about complexity by offering more built-in functionality, deployment accelerators (such as preconfigured deployment scenarios) and preintegrated virtual appliances. Features such as support for identity analytics are also becoming mainstream. However, large organizations with mature governance, access request and fulfillment processes value the flexibility offered by many products that may be considered too complex for smaller organizations.

The IGA market has reached the point of maturity where mainstream products can fulfill all of the most common use cases. The basic functionality associated with core capabilities (identity life cycle, entitlements management, access requests with approval workflows, access certification campaigns, fulfillment and reporting) is delivered in a relatively consistent manner by products in the market. Most differentiation among products is focused on capabilities like role-based and policy-driven administration, provisioning to SaaS, auditing, and analytics.

User Advice: Overall user experience for end users is a top consideration for clients evaluating IGA solutions. Most vendors have adopted more business-friendly access request interfaces using familiar shopping cart paradigms. Vendors have also added mobile interfaces to their products to enable more modes of interaction with users for password management, access requests and approvals.

Organizations increasingly wish to use their ITSM tools for access requests, although ITSM tools do not yet provide an acceptable user experience for this purpose at most organizations. However, IGA tool vendors are providing integrations, and responsibility for handling access requests is expected to eventually shift from IGA to ITSM tools.

Organizations seeking IGA tools should focus most on the features and capabilities of immediate importance to them, paying most attention to fit and finish. Don't worry so much about the possibility of missing features that are not needed immediately — the market is driving vendors to adopt functionality that is most common, and gaps between products for base functionality have diminished. As such, the laundry-list RFP that lists every imaginable requirement should be eschewed in favor of RFPs that focus on the particular needs of the organization, so as to surface those products that will be the best fit.

Although the vast majority of IGA is still delivered as software, IGA-as-a-service is growing, as most vendors are working to provide options, especially for midsize to large enterprises.

Business Impact: IGA is the second-generation IAM solution for identity administration, governance and intelligence that consolidates functions in those areas into a single platform. IGA provides hands-on governance capabilities to the business owners of applications for direct accountability of access to their business information. It also provides transparency for audit and compliance (answering the question: Who has access to what?); granular control of that access through roles, entitlements, policies, access requests and periodic certifications; and targeted automation for fulfillment in a heterogeneous environment.

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: AlertEnterprise; CA Technologies; IBM; Micro Focus (NetIQ); Omada; One Identity; Oracle; SailPoint; Saviynt; SAP

Recommended Reading: "Definition: Identity Governance and Administration"

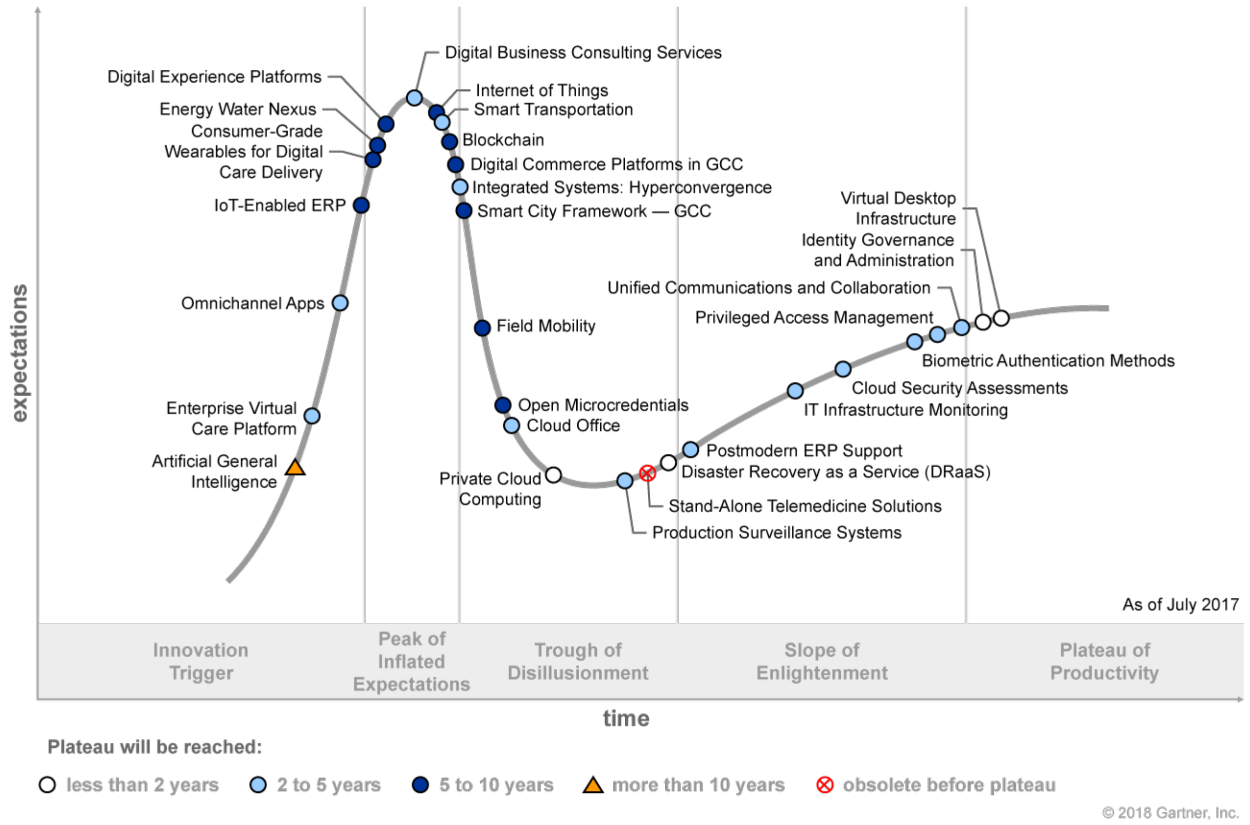
"Magic Quadrant for Identity Governance and Administration"

"Critical Capabilities for Identity Governance and Administration"

"Evaluation Criteria for Identity Governance and Administration"

Appendixes

Figure 3. Hype Cycle for IT in GCC, 2017



Source: Gartner (July 2017)

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant press 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 technology is pushed to its limits. The only enterprises making money are conference organizers and magazine publishers.
Trough of Disillusionment	Because the technology 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 technology'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 technology 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 technology to reach the Plateau of Productivity.

Source: Gartner (July 2018)

Table 2. 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 2018)

Table 3. Maturity Levels

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

Source: Gartner (July 2018)

Gartner Recommended Reading

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

"Understanding Gartner's Hype Cycles"

"Top 10 IoT Technologies for 2017 and 2018"

"Market Guide for IT Infrastructure Monitoring Tools"

"2017 CIO Agenda: A GCC Perspective"

Evidence

Industry-specific analyst inquiries and consulting engagements for GCC (e.g., government, healthcare) across GCC, GCC strategic plans and national policies.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity."