Hype Cycle for Midsize Enterprises, 2021

Published 19 July 2021 - ID G00747565 - 137 min read

By Analyst(s): Mike Cisek, Paul Furtado, Nikhil Sood

Initiatives: Midsize Enterprise IT Leadership

Emerging technologies can cost-effectively and substantively augment the capabilities of midsize enterprises. This Hype Cycle is designed to help MSE CIOs identify and programmatically apply emerging technologies to accelerate business and IT outcomes.

Analysis

What You Need to Know

This Hype Cycle highlights technologies with potential wide-ranging impacts based on the characteristics that define midsize enterprises (MSEs). Two categories of technologies are featured. The first includes technologies broadly acknowledged as mature by the market, but that Gartner research indicates are often underutilized by MSEs. Conversely, leading MSEs are leveraging solutions in this category to improve both business performance and optimize IT operations. The second category highlights less-mature technologies that represent opportunities for disruption and innovation, including areas where MSEs can be first movers because of their size, agility and scale.

MSE CIOs should, therefore, focus on technologies that will have a high impact in their industry and company, but prioritize investments based on their technical feasibility, affordability and appetite for risk. Specific investment decisions should be informed by examining other relevant Hype Cycles and discussions with Gartner analysts who have in-depth subject matter expertise (see Understanding Gartner's Hype Cycles).

The Hype Cycle

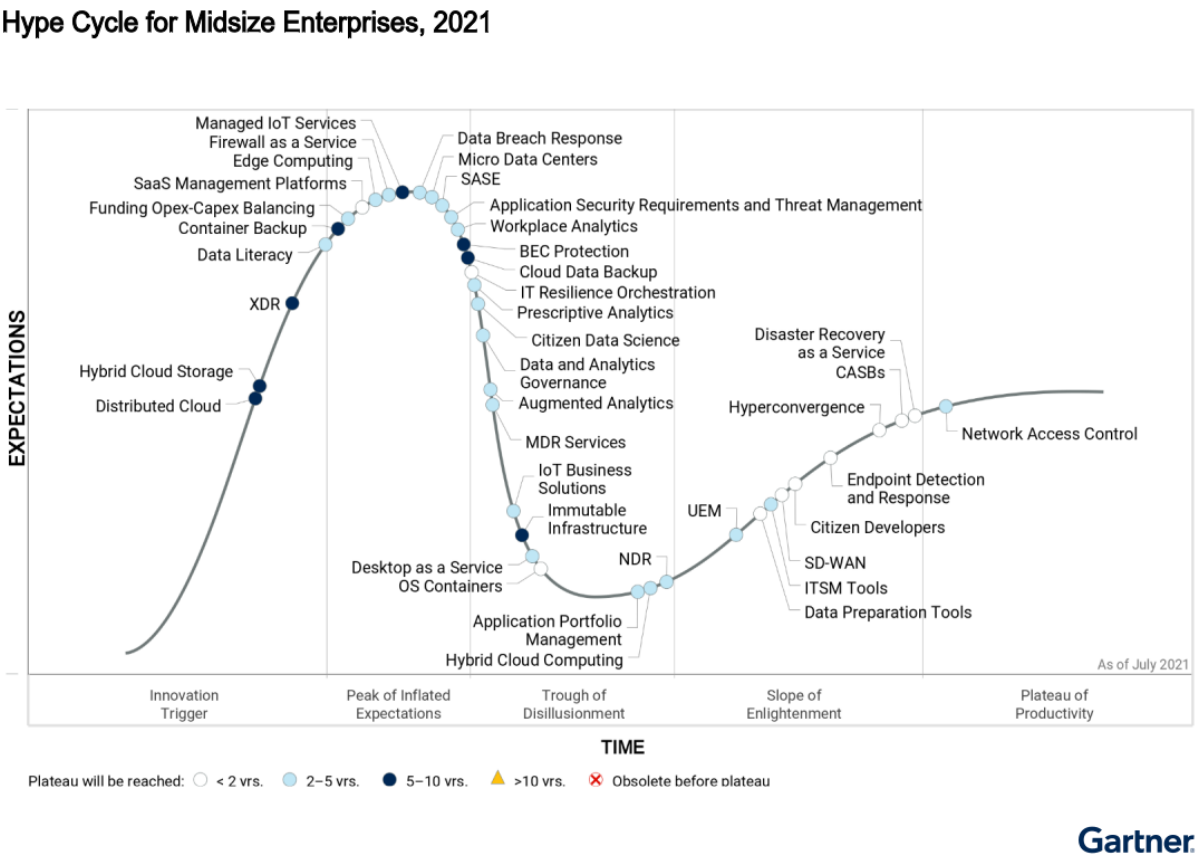
The economic, cultural and operational characteristics of MSEs strongly influence technology and business decision-making methodologies and processes. According to the 2021 Gartner CIO Survey, MSE CIOs were able to increase investment in IT tools, applications, infrastructure and legacy modernization (things that are normally difficult) as a direct result of the pandemic. Consequently, leading MSEs validated that the technologies cited in this Hype Cycle deliver on the promise of a high degree of benefit and applicability. The innovation profiles in this Hype Cycle will position MSEs to effectively plan and execute against business and IT priorities at scale, and support the three trends cited below:

- Data literacy and data-driven culture — Delivering and supporting the business capabilities, skills and competencies, and culture that acts on data and data-driven insights to deliver measurable outcomes
- Risk-based security — A practical, cost-effective approach to protecting the areas of greatest risk, while avoiding overspending on security tools
- Infrastructure utility — Easily managed software-defined solutions that support distributed workloads that securely transverse traditional on-premises and cloud-native architectures

This Hype Cycle is intended to help MSE IT leaders develop an effective vision and sound strategies to drive discussions with business leaders on how technology can improve current operational deficits and create new opportunities within their organizations. MSE CIOs must continually innovate and drive disruption to expand influence within the business by fostering an environment that encourages experimentation. Real-world experimentation will help MSE IT leaders quickly and effectively:

- Determine whether an alternative approach or emerging technology is a good fit for their organizations.
- Show business leaders what is possible before committing significant financial and human resources to full-scale implementation.

Figure 1. Hype Cycle for Midsize Enterprises, 2021



Source: Gartner

Downloadable graphic: Hype Cycle for Midsize Enterprises, 2021

The Priority Matrix

This Hype Cycle includes a disproportionate number of technologies with a benefit rating of transformational and high. This is deliberate, as our intention is to highlight technologies with a potential for high ROI. MSE CIOs should deliberately use rapid tests and proofs of concept to keep pace with the rapid rate of business and technology change and to fast-track innovation.

Table 1: Priority Matrix for Midsize Enterprises, 2021

(Enlarged table in Appendix)

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
Transformational	CASBs OS Containers	Augmented Analytics Citizen Data Science Edge Computing IoT Business Solutions Micro Data Centers SASE		
High	Citizen Developers Data Preparation Tools Endpoint Detection and Response Hyperconvergence SD-WAN	Application Portfolio Management Application Security Requirements and Threat Management Data and Analytics Governance Data Breach Response Data Literacy Desktop as a Service Funding Opex-Capex Balancing Hybrid Cloud Computing ITSM Tools MDR Services NDR Network Access Control Prescriptive Analytics UEM Workplace Analytics	BEC Protection Distributed Cloud Hybrid Cloud Storage Managed IoT Services XDR	
Moderate	Disaster Recovery as a Service IT Resilience Orchestration SaaS Management Platforms	Firewall as a Service	Cloud Data Backup Container Backup Immutable Infrastructure	
Low				

Source: Gartner (July 2021)

On the Rise

Distributed Cloud

Analysis By: David Smith, Daryl Plummer, Milind Govekar

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

"Distributed cloud" refers to the distribution of public cloud services to different physical locations, while operation, governance, updates and evolution of the services are the responsibility of the originating public cloud provider.

Why This Is Important

Distributed cloud enables organizations to use cloud computing wherever needed with consistency while the cloud service provider retains the burden and responsibility of managing the technology, implementation and evolution of the capabilities. It gives organizations the flexibility to support use cases that will benefit from the power of cloud services. Organizations can use distributed cloud to reimagine use cases where cloud computing is not currently feasible at the location desired.

Business Impact

A major notion of the distributed cloud concept is that the provider is responsible for all aspects of delivery. This restores cloud value propositions that are broken when customers are responsible for a part of the delivery, as is true in some hybrid cloud scenarios. The cloud provider must take responsibility for how the system is managed and maintained. Otherwise, the value proposition of distributed cloud is compromised.

Drivers

Distributed cloud computing is a style of cloud computing where the location of the cloud services is a critical component of the model. Historically, location has not been relevant to cloud computing definitions. In fact, the variations on cloud (e.g., public, private, hybrid) exist because location can vary. While many people may claim that private cloud or hybrid cloud requires on-premises computing, this is a misconception. Private and hybrid cloud do not require that the private components are in any specific location. With the advent of distributed cloud, location formally enters the definition of a style of cloud services.

Drivers include:

- In hyperscale public cloud implementations, the public cloud is the center of the universe. There has been distribution of cloud services through worldwide regions in public cloud practically since its inception. The major hyperscale cloud providers have different geographic regions around the world, and all are centrally controlled and managed, and provided by the public cloud provider.
- Distributed cloud supports tethered and untethered operation of like-for-like cloud services from the public cloud "distributed" out to specific and varied physical locations. This enables an important characteristic of distributed cloud operation — low-latency compute where the compute operations for the cloud services are closer to those that need the capabilities. This can deliver major improvements in performance as well as reduce the risk of global network-related outages.
- Data sovereignty and other regulatory issues.
- Perceived and real security and privacy concerns with off-premises applications and infrastructure.
- Latency needs of IoT/edge applications.
- Disconnected operations.

Obstacles

Customers can't abandon existing technologies in favor of complete and immediate migration to the public cloud. Sunk costs, latency requirements, regulatory and data residency requirements, and even the need for integration with noncloud, on-premises systems hold them back. Some obstacles include:

- Different approaches to distributed cloud have different value propositions (portability approach, software approach, appliance approach).
- Distributed services are a relatively small subset of the providers centralized services today and will take time to expand. They will never reach 100% parity.
- Distributed cloud running in your data center will inherently have limits to scale and elasticity that do not exist with the centralized public cloud.

- More-advanced approaches like distributed cloud embedded in networking or telecom equipment or delivered as metro area services are very immature.

User Recommendations

- Adopt distributed cloud by overcoming the fear of a single franchise controlling the public cloud and on-premises cloud estates.
- Use the distributed cloud model to prepare for the next generation of cloud computing by targeting location-dependent use cases (such as low latency, tethered scale and data residency) that are enhanced by using a distributed cloud model.
- Identify scenarios where distributed cloud use-case requirements can be met by evolution of a hybrid cloud model and where the requirements are substantially different.

Sample Vendors

Amazon Web Services; Google; IBM; Microsoft

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Distributed Cloud

'Distributed Cloud' Fixes What 'Hybrid Cloud' Breaks

The Cloud Strategy Cookbook, 2021

Hybrid Cloud Storage

Analysis By: Raj Bala, Julia Palmer

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Hybrid cloud storage aims to enable seamless data services among disparate data centers, edge and the public cloud infrastructure. It encompasses many deployment patterns with varying underlying technologies covering a variety of data types. Hybrid cloud storage solutions can be delivered by purpose-built hybrid cloud storage platforms, data transfer appliances, hyperconverged solutions, storage arrays, software-defined storage products or data management solutions.

Why This Is Important

The term “hybrid cloud storage” was first used in 2009 by vendors in the cloud storage gateway segment to describe their nascent offerings that treated public cloud storage as an archive tier for infrequently used, low-value data. But hybrid cloud storage is now used to transform high-value data using data services provided by public cloud infrastructure and platform services (CIPS).

Business Impact

- Tactical uses of hybrid cloud storage are often designed such that data is not easily readable in the public cloud due to the opaque storage formats used by vendors. As a result, these methods limit the full breadth of functionality that can be unlocked in the cloud.
- Strategic uses of hybrid cloud storage are often developed with modern approaches where vendors have taken care to ensure that data can not only be read in the public cloud, but also modified and synchronized back to its source.

Drivers

- Provides data disaster recovery and business continuity by snapshotting or copying structured or unstructured datasets from on-premises or edge storage to public cloud storage.
- Brings data closer to cloud compute and big data infrastructure for purposes of processing or analytics.
- Allows a single protocol or API on the front end to ingest the data, while on the back end, it supports multiple public cloud storage services for data storage.
- Standardizes the underlying storage platform for any deployment scenario (edge, core data center or public cloud infrastructure as a service [IaaS]) to improve the operational consistency of storage services.

Obstacles

- Complete disaster recovery requires coordination of more moving parts than hybrid cloud storage solutions often claim.
- There are far greater inefficiencies in moving data closer to the compute operations rather than moving compute operations closer to data; the latter is substantially more efficient.
- Capacity expansion of on-premises storage brings with it unexpected consequences when data is unintentionally recalled from the cloud or migration of data is required.
- The use cases for a common storage substrate across disparate environments are still nascent as the resulting benefits are not broadly applicable.
- Available bandwidth and large egress costs limit the continuous movement of data between the on-premises data center and the cloud.

User Recommendations

- Evaluate vendors of hybrid cloud storage across two imperatives: tactical uses and strategic uses. The tactical approach includes uses such as tiering aging data to the cloud. The strategic approach includes using public cloud compute and data services to transform data into actionable results.
- Walk through the mechanics of eventually dismantling hybrid cloud storage deployments, particularly ones that create lock-in scenarios due to proprietary vendor architecture and/or data gravity. The complexities involved may prevent you from deploying such solutions in the first place.
- Compare the total cost of ownership (TCO) of hybrid cloud storage solutions to traditional approaches and decide whether the savings, if any at all, are worth the resulting value gained. In certain instances, value derived may be marginal depending on use case and scope of the problem being solved.

Sample Vendors

Amazon Web Services (AWS); CTERA; Hammerspace; Microsoft; Nasuni; NetApp; Peer Software; Qumulo; Vcinity

Gartner Recommended Reading

Market Guide for Hybrid Cloud Storage

XDR

Analysis By: Peter Firstbrook

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Extended detection and response (XDR) is a vendor-specific threat detection and incident response tool that unifies multiple security products into a security operations system. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Why This Is Important

Extended detection and response (XDR) is similar in function to security information and event management (SIEM) and security orchestration, automation and response (SOAR). However, XDR is differentiated by its level of integration and automation, ease of use, and focus on threat detection and incident response. XDR solution providers must also provide multiple security controls such as EDR, CASB, Firewall, IAM, IDS, directly.

Business Impact

XDR products can reduce the total cost of managing security incidents, improve the productivity of the incident response team and reduce the overall cybersecurity risk posture of the organization.

Drivers

Midsize organizations are struggling to address the alerts generated from disparate security components. These alerts are often not correlated together to provide a full picture of the incident nor contextualized by other security control points. Although existing SIEM and SOAR tools can provide a similar function, the cost, complexity, and ongoing maintenance of these tools are too high for the midmarket enterprise. The people and skills required to integrate and maintain a best-of-breed portfolio of security tools is too high. XDR tools are primarily marketed by security solution providers that have a portfolio of infrastructure protection products, such as EDR, CASB, SWG, SEG and NDR. More advanced XDR tools are focusing up the stack by integrating with identity, data protection and application access.

Obstacles

Only a small list of vendors can truly offer an XDR product. Committing to an XDR approach could lead to overreliance on a single vendor. Large vendors that can provide an XDR product often execute much slower than the best-of-breed startups in addressing new threats. All XDR tools require some integration with security products from other vendors, however integration of most XDR products is still low. The efficacy of security products is still an important factor and some solutions in a portfolio may be less effective than the best-of-breed competition. There is also the potential dependency on a single source of the threat intelligence and detection content provided by the XDR vendor. XDR tools lower but do not eliminate the need for knowledgeable operators and 24/7 monitoring. Note that a primary differentiator between XDR and SIEM products is that XDR does not meet the needs for long-term log storage for use cases outside of incident response, such as compliance or operations.

User Recommendations

- Work with stakeholders to determine whether an XDR strategy is right for the organization.
- Base decision criteria on staffing and productivity levels, level of federation of IT, risk tolerance and security budget, as well as tolerance for a single-vendor lock in, and presence of existing XDR component tools.
- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, including when and why exceptions might be permissible.
- Plan future security purchases and technology retirements in-line with a long-term XDR architecture strategy.
- Seek security products that provide APIs for information sharing and automation with the XDR.

Gartner Recommended Reading

Innovation Insight for Extended Detection and Response

Market Guide for Security Orchestration, Automation and Response Solutions

At the Peak

Data Literacy

Analysis By: Alan D. Duncan, Sally Parker, Donna Medeiros

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data literacy is the ability to read, write and communicate data in context, with an understanding of the data sources and constructs, analytical methods and techniques applied. It is the ability to describe the use-case application and resulting business value or outcome.

Why This Is Important

Data and analytics are pervasive in all aspects of all businesses, in communities and in our personal lives. The ability to understand, interpret and act upon data — data literacy — is increasingly foundational to the digital economy and society. Data literacy helps explain to the board how data and analytics manifest in a company's use cases, explain how to identify, access, integrate and manage internal and external datasets, and describe advanced analytics techniques and enabling AI.

Business Impact

Data-driven enterprises require explicit and persistent organizational change to achieve measurable business outcomes. Employees know their organization is serious about change only when they see their leaders changing their own behavior. CDOs need to promote and orchestrate "leadership moments" where they act as role models, exemplifying new cultural traits at critical points. Central to success will be the ability to guide the workforce by addressing both data literacy and data-driven culture.

Drivers

- With the steady rise of the digital economy, and the need for businesses to be digitally literate, there is growing recognition of the role that employees' data literacy plays within an organization's overall digital dexterity.

- The role of the data and analytics function has changed. It is now at the core of an organization's business model and digital platforms.
- CDOs can emulate their higher-performing peers by putting much more emphasis, energy and effort into meeting the change management requirements of their data and analytics strategies.
- Defining what data-driven behaviors are expected, using a "From/To/Because" approach, is central to employee development plans. It ensures that creators, consumers and intermediaries have the necessary data and analytics skills, knowledge and competencies.
- CDOs need to take immediate action to create and sustain data literacy. Quick wins build momentum, but lasting and meaningful change takes time because it requires people to learn new skills and behave in new ways.

Obstacles

- Lack of common data literacy models/frameworks/standards
- A piecemeal approach to training and certification
- Aversion to change
- Lack of talent and poor data literacy
- Lack of initiatives to address cultural and data literacy challenges within strategies and programs
- "Data literacy" means different things to different providers: from enhanced data visualization skills to fostering curiosity about data more broadly
- Overall adoption will still take years

User Recommendations

- Create a strong narrative vision of desired business outcomes, particularly with respect to innovation. Raise awareness through storytelling.
- Call out examples of "good" and "bad" data literacy to promote desired behaviors.
- Work with stakeholders who have enthusiasm and appetite, and who recognize that improved data literacy is a factor for success.

- Partner with HR and business leaders to identify the level of data literacy, learning goals and outcomes for various job roles and personas. Use data literacy assessments to evaluate current data literacy levels and desire to participate.
- Go beyond vendor product training to focus on people's other role-related skills. Use a mix of training delivery methods (classroom, online, community, on the job) to improve overall learning effectiveness.
- Align training and self-service solutions with a broader data literacy portfolio to meet the data literacy needs of both data consumers and creators.

Sample Vendors

Avado; Coursera; Data To The People; Gartner Consulting; Pluralsight; Skillsoft; The Center of Applied Data Science (CADS); The Data Lodge; Udacity; Udemy

Gartner Recommended Reading

Roadmap for Data Literacy and Data-Driven Business Transformation: A Gartner Trend Insight Report

Tool: Communicating the Need for Data Literacy Improvement

Chief Data Officers Must Address Both 'Skill' and 'Will' to Deliver Data-Driven Business Change

Tool: Data Literacy Personas

Data Literacy Providers Will Accelerate the Time to Value for Data-Driven Enterprises

Container Backup

Analysis By: Jerry Rozeman, Nik Simpson, Santhosh Rao

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Container backup helps back up persistent volumes of containerized application data and Kubernetes configuration data such as K8S objects. Container backup solutions are offered either as part of a traditional backup solution, as part of the primary storage solution or as a containerized application.

Why This Is Important

Container backup is an emerging technology that protects organizations against data and configuration loss in a containerized environment. Container backup is largely nascent. It is different from a physical or virtual machine (VM) backup as there is no direct mapping between the application and the underlying storage.

Business Impact

Container backup can help:

- Business owners responsible for application data in addressing the data and application configuration loss risk associated with containerized application environments, as such protection is not available by default.
- Platform and application engineering teams in protecting their data as they become the new owners responsible for containerized application data protection.

Drivers

- Containerized application adoption will increase at a rapid pace during the next few years primarily driven by the rapid growth of cloud adoption, application modernization leveraging containerization and the need for application mobility. This will in turn fuel the need to protect data in these environments.
- DevOps processes requiring the need for multiple copies of data are continuously looking for tools to simplify development. Container backup solutions can deliver on this need by delivering copy data management features.

Obstacles

- Data protection of new workloads has always been an afterthought and that especially applies to container-based applications.
- While container technology seems like the next evolution of server virtualization, the technology and operating model are completely different compared to operating VMs and hypervisors. Moreover, container technology requires new buyers in application or DevOps teams who do not see backup to be as high a priority as the infrastructure team does.
- It will still take a long time for the majority of organizations to move away from traditional hypervisors and VMs to container technology in production. This limits the growth potential of container technology and as such it will limit the growth of data protection in containerized environments.
- The current ecosystem for container backup is quite immature.

User Recommendations

- Evaluate the need for container backup based on application criticality as not every container app requires backup.
- Invest in container knowledge to understand the need for backing up Kubernetes objects like namespaces, secrets, keys, configuration maps, etc., in addition to just persistent volumes.
- Align container backup with the organizational structure as, unlike traditional infrastructure, container backup operations will be performed by the platform or application engineering teams.
- Dedicate budget for protecting containers as it requires additional investments in backup infrastructure.
- Adopt a strategy for container backup just as with every other data source in your enterprise.
- Select specialized container backup solutions first while traditional backup solution capabilities mature over time.

Sample Vendors

Appranix; Arpio; Cohesity; Commvault; Dell Technologies; IBM; Portworx by Pure Storage (Portworx); Rubrik; Trilio; Veeam (Kasten)

Gartner Recommended Reading

Magic Quadrant for Data Center Backup and Recovery Solutions

Critical Capabilities for Data Center Backup and Recovery Solutions

Funding Opex-Capex Balancing

Analysis By: Kevin Ji, Michael Warrilow

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

With the increasing adoption of public cloud service, IT leaders are struggling to comprehend and determine the implications for their infrastructure budgets since consumption-based pricing models have greater variability, and this requires new spend management disciplines to be introduced. IT leaders should work with the finance function to determine and communicate how the shift to the cloud affects their organizations' operating budgets.

Why This Is Important

Enterprise infrastructure and applications are increasingly cloud-based, creating an escalating shift away from more-traditional, predictable capital-based models of IT expenditure. The resultant shift from capital expenditure (capex) to operating expenditure (opex) causes budgetary and cost management pressures in many organizations.

Business Impact

IT leaders are struggling to comprehend and determine the implications of funding opex/capex balancing on their operations, projects and budgets. The finance function, possibly wedded to more-traditional capitalization-oriented models of purchase/lease and depreciate, is challenged by the changes. They are being forced to update their policies, processes and procedures, as well as anticipate and plan for changes in the funding models.

Drivers

- In the public cloud service model, the customer contracts to pay a service fee in exchange for a right to use the cloud provider's services for a specified term.
- Cloud usage tends to increase over time, leading to new applications coming online and increases in associated resources (including network egress, storage, management and automation).
- Organizations have changed and balanced the funding from the traditional procurement process since cloud expenditure cannot be capitalized under applicable accounting standards.

Obstacles

- It is often unclear exactly what cloud services an organization will consume or what the full financial implications are. Executives may not know the impact on the radically different pricing structures and associated nuances of variability that can arise from consumption-based demand.
- When doing cost comparisons, IT leaders cannot simply calculate the difference between buying and amortizing hardware over a specific period and procuring those same resources in cloud IaaS.

User Recommendations

- Analyze your current infrastructure vendor agreements and related spend to fully budget for the true impact of "as a service" payment on your total operating costs.
- Determine your accounting options by working with the finance team, including tax advisors.
- Prepare and maintain an opex-capex impact assessment to communicate to the finance team by investigating pricing and related commercial options for public IaaS/PaaS cloud services.
- Establish the appropriate accounting treatment for all of your enterprise cloud costs. Ensure your approach complies with defined cloud migration principles and maximizes your ability to secure funding for your budget.

Gartner Recommended Reading

The Impact of Public Cloud on Operating Budgets

SaaS Management Platforms

Analysis By: Chris Silva, Dan Wilson

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Gartner defines SMPs as stand-alone tools that can discover, manage and secure multiple SaaS applications from a central admin dashboard, delivered as a turnkey service. The market for SMP consists of both pure-play SaaS-only management tools and SAM tools that have extended their software license and operational management to SaaS-based applications.

Why This Is Important

IT administrators lack a central dashboard to view utilization and entitlements or to centrally automate administrative tasks across the portfolio.

The market for SaaS management platforms (SMPs) has matured, with core capabilities to:

- Discover usage of SaaS applications.
- Track uptake, ongoing usage and automate workflows.
- Establish consistent identity, access and data governance controls across the SaaS estate.

Business Impact

As SMPs expand to address more SaaS applications, they will emerge as a key source of analytics data, with some vendors offering analysis of collaboration patterns among workers and across tools. This will act as a trigger to workflows in other systems and contribute to broader user experience measurement activities.

Drivers

As organizations' SaaS portfolios grow, so does the need for a single orchestration point for visibility and control. Client interest began to grow in late 2019, and Gartner has witnessed its continued modest growth in 2020. This growth is driven by:

- Continued investment in SaaS applications, which means exponential growth in admin overhead when conducted on a per-app basis. Each incoming SaaS app adds a new admin console to the mix, and with it a need to add skills unique to that application.
- Maturity of SMP tools. The portfolio of SaaS applications SMPs can manage is growing, but not every SMP will offer coverage across 100% of the SaaS estate, especially when niche or vertically-specific SaaS apps are in the mix.
- As the portfolio of managed apps grows, it is important to note that not all integrations are the same. In some cases, the SMP may be able to read information from the SaaS environment, while in other areas the SMP can both read information from, and write changes to, the SaaS environment. In almost all cases, this distinction will vary across supported SaaS apps.

Buyer awareness and product maturity have been positively impacted by recent rounds of investment into the SMP market. These range from small seed investments to eight- and 10-figure funding commitments to vendors raising capital in later-stage rounds. Despite this growth in capital, which has driven maturity and awareness of SMPs, many organizations still seek security-specific posturing tools (SSPM) to solve subsets of the SMP mandate. Others seek to gain the advantages of visibility and control over SaaS apps using CASB or WAFS functionality.

Obstacles

The growth in awareness of this class of tool is still growing. Despite an uptick in interest over the course of 2020-21 relative to established technologies, Gartner sees interest in SMPs in its early to intermediate stages of growth. Its position on the Hype Cycle and adoption reflect this.

Three forces can impact the SMP market:

- **Hybrid environments:** The reality of the app mix in many businesses requires a tool that can span management of traditional and SaaS apps, a differentiator touted by the SAM vendors making investments in SMP features.

- **Increased competition:** Infusions of investor capital have provided many (but not all) SMP vendors with resources to drive product differentiation, as well as brand and product awareness.
- **Distributed pain:** While large enterprises have begun to express interest in these tools, the distributed ownership of SaaS apps also means distributed management operations, often hiding the aggregate operational costs of the entire SaaS portfolio.

User Recommendations

Organizations looking to an SMP for better visibility of the SaaS estate must choose a tool that:

- Offers discovery capabilities that discover usage at multiple points (e.g., expense system for paid apps, identity system for apps using SSO or at the network or client level to identify traffic) in order to identify SaaS apps in use.
- Avoid acquiring incomplete solutions by reviewing the depth of integrations for each supported SaaS app. Not all SMPs will offer both read and write (bidirectional) functionality with all SaaS apps, meaning that some integrations are likely to only provide basic reporting of usage metrics.
- No SMP at this stage of the market is likely to address 100% of a large and diversified, or conversely vertically-specific SaaS application portfolio. Review whether support for key SaaS tools is present in the SMP being chosen.

Sample Vendors

AvePoint; BetterCloud; CloudM; CoreView; Intello; Productiv; Quest-Quadrotech; Torii; Zluri; Zylo

Gartner Recommended Reading

Market Guide for SaaS Management Platforms

Predicts 2021: Crisis Will Force Changes to Software and Cloud SaaS Contract Negotiation

Optimize Cost and Risk as These Software and SaaS Pricing Metrics Emerge to Enable Digital Business

Edge Computing

Analysis By: Bob Gill, Philip Dawson

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Edge computing describes a distributed computing topology in which data storage and processing are placed in an optimal location relative to the location of data creation and use. Edge computing locates data and workloads to optimize for latency, bandwidth, autonomy and regulatory/security considerations. Edge-computing locations extend along a continuum between the absolute edge, where physical sensors and digital systems converge, to the "core," usually the cloud or a centralized data center.

Why This Is Important

Edge computing has quickly become the decentralized complement to the largely centralized implementation of hyperscale public cloud. Edge computing solves many pressing issues, such as unacceptable latency and bandwidth requirements, given the massive increase in edge-located data. The edge-computing topology enables the specifics of the Internet of Things (IoT), digital business and distributed IT solutions, as a foundational element of next-generation applications.

Business Impact

Edge computing improves efficiency and cost control through processing close to the edge (e.g., better automation and quality control), and more business opportunities and growth (e.g., customer experience and new real-time business interactions). Early implementations have succeeded in enterprises that rely on operational systems and data outside core IT, such as the retail and industrial sectors.

Drivers

Drivers to the adoption and implementation of edge computing include:

- Growth in cloud adoption has exposed the disadvantages of extreme centralization. Latency, bandwidth requirements, the need for autonomy, and data sovereignty or location requirements may be optimized by placing workloads closer to the edge and data produced at the edge, rather than centralizing in a hyperscale data center.
- Data growth from interactive applications and systems may not be economically funneled into the cloud.
- Applications featuring customer engagement and analysis favor local processing for speed and autonomy.
- IoT use cases are expanding from the industrial sector to other verticals, driving a move toward a hierarchical and distributed model.

Obstacles

- Extreme diversity of devices and application types amplify complexity issues
- Widespread application of the topology and explicit application and networking architectures are not yet common outside vertical applications, such as retail and manufacturing
- Lack of understanding of benefits/use cases
- Lack of standards
- Although the physical infrastructure for edge is maturing rapidly, the overall management and orchestration challenges of distributed applications are beyond vendor-supplied, component management offerings. The tasks of managing, securing, maintaining and updating the physical infrastructure, software and data requires considerable development before management and orchestration can be considered mature.

User Recommendations

- Create and follow an enterprise edge strategy by focusing first on business benefit and holistic systems, not solely pointing to technical solutions or products.
- Establish a modular, extensible edge approach through the use of emerging edge frameworks and architectures, which allow for the mixing and matching of technologies based on enterprise direction, not simply “what comes with the vendor solution.”
- Accelerate time-to-benefit and derisk technical decisions through the use of vertically aligned system integrators (SIs) and independent software vendors (ISVs) that demonstrate an understanding of and ability to implement and manage the full orchestration stack from top to bottom.
- Evaluate the deployment of “edge as a service” options, which promise to deliver “business-outcome-based solutions” that adhere to specific SLAs, while shifting deployment, complexity and obsolescence risk to the provider.

Gartner Recommended Reading

2021 Strategic Roadmap for Edge Computing

Cool Vendors in Edge Computing, 2021

Firewall as a Service

Analysis By: Adam Hils, Rajpreet Kaur

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

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

Why This Is Important

The uptick in remote work, and growing adoption of SD-WAN and hybrid WAN architectures are increasing interest in using FWaaS. We anticipate that this trend will continue. FWaaS offerings are of varying levels of maturity. Organizations considering FWaaS should conduct extensive proofs of concept or limit the scope of an initial production deployment.

Business Impact

The main business impacts are:

- FWaaS offers a significantly different architecture for branches or even single-site organizations. It offers greater visibility through centralized policy, increased flexibility and reduced capital costs associated with using a fully or partially hosted security workload.
- As with other as a service (aaS) security offerings, FWaaS changes budgetary considerations as organizations move from capital to operational spending.
- Organizations with workforces that may stay remote will find that FWaaS helps them work securely in a widely-distributed network.

Drivers

- Organizations rearchitecting their networks by implementing SD-WAN often want FWaaS to secure outbound network traffic.
- Firewall as a Service is a core component of the security access service edge (SASE) framework often offered as part of a larger SASE security service.
- FWaaS can decrypt outbound traffic for inspection at scale. Alternative branch firewalls often lack the performance to do this.
- The move toward remote work in 2020 and 2021 necessitates bringing security services closer to the workers to minimize latency.

Obstacles

- Network firewall appliances comprise the largest security equipment market in security and risk. The appliance approach has been predominant for decades, and many organizations use them effectively and efficiently.
- Security and risk leaders find some FWaaS solutions difficult to implement and manage.
- Over 75% of outbound traffic in organizations is HTTP and HTTPS traffic. Cloud-based secure web gateway (SWG) services can protect and inspect this traffic at scale to offload existing hardware-based firewalls. This makes it much easier to extend investments in existing firewall hardware without completely rearchitecting the edge to forward all traffic to a FWaaS.
- FWaaS licensing is based on per user per year subscription pricing. This can be more expensive for large organizations with high user counts compared to hardware-based solutions, which may have lower subscription costs and can be deployed and used beyond their capital depreciation life span.

User Recommendations

- Verify that the additional hop to the FWaaS infrastructure does not create unacceptable latency for some of your sites and look at business models that limit initial investment until limited latency is proven. The appeal of simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance.
- Determine whether your organization is ready to move the entire security workload into the cloud, or if you need thicker local devices to address privacy concerns and perform some on-premises computation (such as segmentation or VLAN trunking).
- Assess how FWaaS might impact your branch architecture, especially your ability to maintain and easily manage multiple network segments. Current FWaaS offerings are mostly outbound security for now, or they are targeted at protecting mobile workers or companies whose applications are primarily cloud-hosted with no branch dependency on headquarters for applications.
- Evaluate the strength of the cloud service on three key aspects — data center locations, points of presence and SLA. Ensure that the FWaaS provider has sufficient points of presence for your remote workforce. Ensure that they have data centers close to branch offices and a strong SLA for availability and latency (e.g., 99.999% uptime and no more than 100ms of latency).
- Conduct an individual assessment of each key as-a-service security component that you plan to deploy and determine whether FWaaS provides unique security features, such as shared threat intelligence gathered from similar client organizations.
- Include the possibility of failure in the centralized FWaaS infrastructure in business continuity plans.

Sample Vendors

Aryaka; Barracuda; Cato; Check Point Software Technologies; Cisco; Palo Alto Networks; Versa; Zscaler

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Select the Right Strategy for Securing Web Access

Managed IoT Services

Analysis By: Eric Goodness

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

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

Why This Is Important

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

Business Impact

There is increasing demand for IoT-enabled business benefits, such as improved customer experience, creating new "servitized" products, and new value creation such as revenue and insights from data. An enterprise deploys managed IoT services to substantially reduce the time to value of deploying IoT and to contractually shift the risk of IoT success to external providers to ensure planned benefits and outcomes associated with digital business.

Drivers

Enterprises recognize the need to offload the management of their IoT solutions for a number of reasons, including:

- Cost reductions
- Access to skills that do not exist within the company

- Improved user experience, such as the use of predictive maintenance
- Effective monitoring and management to guarantee a certain level of availability and performance
- Security

Managed IoT services moved further toward the Peak of Inflated Expectations on the Hype Cycle. The move is based on the increase in IT-centric and IoT service providers now offering managed IoT services and the use-case examples being shared with Gartner. Perhaps the fastest-growing use of managed IoT services lies with discrete manufacturers creating smart connected products.

Obstacles

Obstacles for success with managed IoT services include:

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

User Recommendations

Align MSP attributes and capabilities within your sourcing selection criteria, including foundational elements, such as:

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

Sample Vendors

Accenture; Atos; Cognizant; Insight Enterprises; Orange Business Services; TCS; Wipro

Gartner Recommended Reading

Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2020-2030, 1Q21 Update

Service Provider Insight: IoT Market Size by Sector

3 Areas to Drive IoT Differentiation Beyond Functions and Features

Survey Analysis: Focus on Practical Outcomes for IoT Projects

Data Breach Response

Analysis By: Nader Henein, Bernard Woo

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Adolescent

Definition:

Data breach response, augmentation and the associated disclosure are the set of activities required to assess and potentially notify regulatory authorities and — depending on impact — affected individuals when personal data is compromised. Today, disclosure is mandated by omnibus laws such as the European Union's GDPR or subject/region specific laws as is the case with individual U.S. state breach notification legislation.

Why This Is Important

Appropriate management of a breach impacting personal data can substantially reduce fines (as Gartner has observed on multiple occasions), and potentially strengthen ties with affected consumers by demonstrating that the organization is proactively taking ownership of the situation. Inversely, delayed response, limited transparency and overly legal-language based communications often elicit regulatory investigations and is paired with reputational damage and customer loss.

Business Impact

Data breach response can have a critical impact on the resilience of an organization. Breaches will create significant chaos as key members of the executive team pivot from preexisting priorities to address the reputational, regulatory and likely financial impact of the breach. Taking the process one step further, newer legislation in some regions imposes statutory sentences on company directors for egregious or negligent handling of personal data.

Drivers

- Modern privacy regulations have raised the bar on data breach notification impacting personal information, many of which require disclosure to the supervisory authority within days of discovery.
- In the U.S., not only do all 50 states have breach notification laws in place, some, such as New York, have amended their laws in the past two years. Amendments typically both expand the data in scope and requirements surrounding the protection of that data.
- The regulatory evolution illustrates the need for organizational commitment and resource allocation.
- An ongoing process to align the technical and operational elements of incident response with new legal and regulatory requirements.
- Elevating the capacity to disclose a data breach (to regulators and affected individuals) in a time frame is something many organizations are not prepared for today.
- Worth noting that though many organizations are driven by fine avoidance, incidents will happen, and a well-developed response program can pay back in dividends with fine reductions more than 50%.
- An emerging trend is rapid consumer mobilization following an incident. Often marshalled through social media, the impact of mass customer exodus will often dwarf regulatory fines and does not offer the organization the option of an appeal through the courts.
- Data breach response requires a combination of technical acumen (forensics analysis as to how the breach took place, the number and type of records involved, and appropriate remediation) paired with coordinated organizational processes. For further details see the Market Guide for Digital Forensics and Incident Response Services.

Obstacles

- Establishment and testing of a data breach program is an expense without an immediate return, in the sense that it will pay only if something has gone wrong. This often causes the program to be deprioritized in-lieu of more pressing or revenue generating tasks.
- Data breach service retainers are also not commonly available because of the variability and uncertainty of the type of breach, data involved and number of records making each breach scenario unique.
- Even with a strong program in place, the time-to-discover an incident can be measured in months and sometimes years, though this trend is improving.

User Recommendations

- Assess whether an incident will trigger any regulatory actions and meet the threshold for a privacy violation.
- Record and maintain the details about incidents (not just violations) as some jurisdictions have stringent record-keeping requirements.
- View data breach response as a multidisciplinary process that involves having documented procedures, and simulated drills, like table-top exercises, to ensure that tasks are well-defined, and responsibilities are clear. The process should also involve coordination and transparency between the various teams, and integration into the larger incident response training to provide for breach disclosure and rapid response requirements.
- Augment your organization's ability to address data breaches in an efficient and timely manner to address regulatory and data subject disclosure requirements.

Sample Vendors

BigID; OneTrust; RadarFirst; Securiti

Gartner Recommended Reading

Data Breach Response in an Era of Heightened Expectations

Data Breach Response Plan Toolkit

Market Guide for Digital Forensics and Incident Response Services

Micro Data Centers

Analysis By: David Cappuccio, Philip Dawson

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

A micro data center is modular and smaller than a computer room — usually no more than a rack of equipment or less. All required facilities and IT functionalities (such as uninterruptible power supply, servers, storage, networking, cooling and monitoring) are contained in the micro data center. It is designed for specific needs (for example, accumulating sensor data or small remote office support) at distributed locations, and it is typically managed remotely as part of a broader infrastructure.

Why This Is Important

Localized or micro data centers are a fact of life, and their use cases in edge and IoT environments are increasing. By applying a self-contained, scalable, and remotely managed solution and process, CIOs can reduce costs, improve agility, and introduce new levels of compliance and service continuity.

Business Impact

Creating micro data centers is something companies have done for years but often in an ad hoc manner. By partnering with vendors and creating a consistent and standardized architecture, enterprises can regain control of these critical assets and increase the ability to rapidly introduce site-specific services, while reducing risks and operational costs and improving service levels.

Drivers

- Consistency: For organizations with a large number of sites, consistency in the IT and networking architecture, consistency in the installation of said architecture, and consistency in the operational procedures to maintain, update and manage the environment will enhance the ability to deploy site-specific workloads quickly using a standardized toolset. By creating a consistent environment, the overall costs can be reduced through standardization of vendors, architecture and software. Implementation and operational costs can also be reduced by creating a repeatable and easy-to-implement solution for local building managers.
- Control: Whether on manufacturing plant floors, IoT installations, or in retail outlets or professional office areas, control of remote IT assets is extremely complex. A micro data center implementation provides greater control of the assets through remote tools, while also allowing standardized methods for releasing new applications, software upgrades, maintenance patches and equipment upgrades.
- Continuity of service: Micro data centers must be able to operate independently, regardless of what happens at the home office. If a primary data center goes down for any reason, remote sites still have a business to run, and the ability to provide continuous operations independently for short periods of time is a critical design criterion. Point-of-sale systems still need to operate, inventories still need to be updated (or drawn from), and security and access control systems must continue.
- Compliance: Adherence to regulatory issues, audit, data location, latency and localized business requirements is key. In addition, the deployment of well-defined operations controls that can be effectively applied to support related compliance requirements is crucial. By creating a standardized, controlled environment at each site, you can increase the level of compliance, while decreasing the level of risk to the business.

Obstacles

- Local control of business at remote sites has often dictated how and why specific technologies were deployed, and changing that mindset will be a challenge.
- Implementation of a consistent operating methodology (purchase, deployment, monitoring, management) across many sites will be required.
- Vendor selection, but more importantly vendor strategy, must align with IT strategy to create a consistent, repeatable deployment model.

User Recommendations

- Focus on maximizing operational independence, while minimizing IT skills and risks at remote sites.
- Design micro data centers to run autonomously but to be controlled centrally.
- Create a standard, self-contained micro data center solution designed for easy deployment, simple replacement, and remote monitoring and management.

SASE

Analysis By: Joe Skorupa, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Secure access service edge (SASE) delivers multiple converged network and security as a service capabilities, such as SD-WAN, SWG, CASB, NGFW and zero trust network access (ZTNA). SASE supports branch office, remote worker and on-premises general internet security use cases. SASE is delivered as a service and enables zero trust access based on the identity of the device or entity, combined with real-time context and security and compliance policies.

Why This Is Important

SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered applications. It increases visibility, agility, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and network security services mainly via a cloud-delivered model. SASE can reduce the number of vendors required for secure access from four to six today to one to two over the next several years.

Business Impact

SASE enables:

- New digital business use cases (such as digital ecosystem and mobile workforce enablement) with increased ease of use, while reducing costs and complexity via vendor consolidation and dedicated circuit offload
- Infrastructure and operations and security teams to deliver a rich set of networking and network security services in a consistent and integrated manner to support the needs of digital business transformation, edge computing and work from anywhere

Drivers

- SASE is driven by enterprise digital business transformation: the adoption of cloud-based services by distributed and mobile workforces, edge computing and business continuity plans that must include flexible, anywhere, anytime, secure remote access and use of the internet and cloud services.
- The need to flexibly support digital business transformation efforts with a zero trust security architecture while keeping complexity manageable is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service (see The Future of Network Security Is in the Cloud). The COVID-19 pandemic accelerated these trends.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices as well as reduce attack surface and shorten remediation times by as much as 95%.
- Network security models based on data center perimeter security are ill-suited to address the dynamic needs of a modern digital business and its distributed digital workforce. This is forcing a transformation of the legacy perimeter into a set of cloud-based, converged capabilities created when and where an enterprise needs them — that is, a dynamically created, policy-based secure access service edge, or SASE.

Obstacles

- **Organizational silos, existing investments and skills gaps:** A full SASE implementation requires a coordinated and cohesive approach across network security and networking teams.
- **Organizational bias and regulatory requirements that drive continued on-premises deployment:** Some customers have an aversion to the cloud and want to maintain control.
- **Global coverage.** SASE depends upon cloud-delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Russia and the Middle East, where vendors may have limited cloud presence.
- **SASE security services maturity:** For the next several years, SASE capabilities will vary widely. Sensitive-data visibility and control is often a high-priority capability, but it is difficult for most SASE vendors to address. Your preferred vendor may lack the capabilities you require but two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the CISO and network architect when evaluating offerings and roadmaps from incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN refresh or SD-WAN to update network and network security architectures.
- Strive for not more than two vendors for all core services to minimize complexity and improve performance.
- Identify required capabilities for networking and security, including latency, throughput, geographic coverage and endpoint types to develop evaluation criteria.
- Focus on vendors that include CASB if DLP is a priority. They have the most experience in this area.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the numbers of vendors required. Deploy ZTNA to augment or replace legacy VPN to limit investment in legacy technology.
- Consolidate vendors to cut complexity and cost as contracts renew.
- Leverage branch office transformation and MPLS offload to adopt SASE for security services.

Sample Vendors

Cato Networks; Fortinet; Palo Alto Networks; Versa Networks; VMware; Zscaler

Gartner Recommended Reading

2021 Strategic Roadmap for SASE Convergence

Market Guide for Zero Trust Network Access

The Future of Network Security Is in the Cloud

Magic Quadrant for WAN Edge Infrastructure

Magic Quadrant for Cloud Access Security Brokers

Market Guide for Zero Trust Network Access

Market Trends: How to Win as WAN Edge and Security Converge Into the Secure Access Service Edge

Application Security Requirements and Threat Management

Analysis By: Dale Gardner

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Application security requirements and threat management (ASRTM) tools automate the creation of security requirements and threat models. ASRTM can integrate with SDLC tools to manage requirements and perform validation. Tool updates are derived from changes to regulations, platforms, frameworks, and evolving threats. ASRTM dynamically highlights potential security ramifications of functional requirements and recommends appropriate secure coding practices or architectural counter measures.

Why This Is Important

Threat modeling and security requirements creation are essential in the effort to create secure applications. ASRTM tools facilitate these processes by shifting security even further left, beyond the start of the SDLC. While ASRTM does not secure code, it eases the task of creating secure code and application architectures. It also helps ensure appropriate security requirements, in contrast to broad standards that inadequately secure high-risk apps, while over-burdening low risk projects.

Business Impact

Automated ASRTM tools significantly decrease the effort to create and maintain threat models, security requirements, and risk assessments. This ensures security specifications that are specific to individual projects can be defined early, while costs and risks are low — rather than after. This offers significant benefits to multiple parts of the organization, including architects, developers, security teams and even business stakeholders.

Drivers

- Threat modeling is a best practice in application development. Despite this, adoption has been restrained by the generally manual nature of the task, and the need to involve multiple individuals. The time and complexity required deter the effort for all but the most critical applications.
- The ready availability and increasing sophistication of ASRTM tools enable individuals or a small group to carry out threat modeling and requirements generation with a fraction of the time and effort typically required. They can also make the task much more approachable for architectural and development staff that may lack training in application security concepts and requirements.
- Organizations of all kinds continue to struggle to create secure applications. Issues include both the creation — and, hopefully, detection and elimination — of inadvertent vulnerabilities, as well as essential design flaws leaving an application susceptible to attack. ASRTM can assist with both problems. With relatively limited effort — especially as compared to manual approaches — the tools can generate relevant security-related requirements aligned to the threat model and attack surface of a given application. The data generated in the process can also guide triage and assessment of vulnerabilities discovered, based on their potential impact.
- ASRTM tools can also be integrated into a variety of SDLC tools, as well as with integrated risk management systems. In the first case, this can ensure the simplified transfer of functional requirements and user stories to developers for inclusion on development activities. Links to testing frameworks can also help ensure that security requirements have been fully and properly implemented. In the latter case, links to risk management aid in reporting on the specific risks associated with an application, and elevate visibility to management.

Obstacles

- Capabilities vary. Free and open source tools enable easy adoption, but fall short when representing complex systems. That prompts consideration of commercial tools, although limitations constrain suitability for advanced users.
- Another challenge is awareness. In the face of demands for improved application security, most organizations continue to focus on application security testing tools. While an essential element of a program, such tools fail at identifying design flaws, and produce more output than can be effectively managed in rapidly moving DevOps environments.
- Currency — the ability to accurately represent a rapidly changing application — remains an Achilles heel for tools. A threat model is only so good as its ability to provide an accurate representation of a system — and the bulk of tools today require effort to update models as applications change, leading to abandonment of the effort. Tool vendors have begun to link systems directly to cloud platforms, ensuring changes are reflected automatically in the model, producing updated guidance.

User Recommendations

- Treat threat modeling, security requirements generation and enforcement as best practices within a secure software development life cycle model. These tools can be leveraged to help automate these tasks while incorporating content knowledge from the tool vendors on emerging threats and security requirements.
- Use a risk-based approach, which the tools help enable, to align the level of effort in threat modeling with the risk posed by the application.
- Leverage ASRTM tools to automate what are otherwise manual or overlooked efforts, in order to ensure threat modeling and security requirements generation activities are incorporated into their software development life cycle process and development workflow.
- Train development, engineering, operations, and architectural staff and the use, and value, of the tools and encourage their use early, and continuously, in the development process and post deployment (to validate application threat protection efforts).

Sample Vendors

foreseeti; IriusRisk; Microsoft; OWASP Foundation; Security Compass; we45

Gartner Recommended Reading

12 Things to Get Right for Successful DevSecOps

Use Threat Modeling to Teach Secure Design (ADP)

5 Ways EA Can Help the Organization Focus on Security

Workplace Analytics

Analysis By: Dan Wilson, Stuart Downes

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Aggregated insights derived from technology performance data and organizational context are used to improve technology performance and adoption as well as influence employee experience, collaboration and productivity. Data is commonly collected through agents, sensors, graphs or APIs.

Why This Is Important

While many organizations are making significant investments in digital workplace and digital transformation initiatives, most are not collecting data on or are unable to effectively measure the impact of their efforts. Without data and analytics, digital workplace leaders are unable to justify additional investments required to scale new technology. This is especially important given the financial pressure that organizations are under and increased demands to improve employee experience.

Business Impact

Workplace analytics (WPA) provide digital workplace leaders visibility into the impact on digital and organizational change management, including:

- Transparency into technology performance and usage.
- Application of organizational context data.

- Derived insights, which help uncover ways to drive adoption and enhance experience, identify productivity inhibitors, and help improve technology and business alignment.
- The ability to feed data into or include nudge engines to reinforce best practices.

Drivers

- Overall employee experience is now heavily influenced by the technology experience as the majority of interactions with peers, vendors and customers are exclusively through technology. IT leaders are looking for data to baseline and measure the progress of improving the stability, availability and performance of the devices and systems they deliver, especially as changes are made.
- Digital transformation requires visibility into what technology employees depend on, and how well they can use technology to improve work and improve productivity.
- The increased threat of cyberattacks requires IT and security teams to understand what devices and technology are being used and from where they are being used so appropriate measures can be implemented to reduce risk. This includes use of unmanaged devices (BYOD or BYOPC) or public conferencing technology to conduct internal or confidential classified business.
- Remote work has limited a leader's ability to see and adjust collaborative behaviors and patterns, as they could in the office. The patterns themselves have also changed to be less timebound, requiring leaders to adjust accordingly.
- Organizations are also looking for data to inform the return to the office as a collaboration hub by prioritizing those that are struggling with remote work and for insights into potential employee engagement and wellness issues.
- WIth all of this data and advanced analytics, organizations can also look to identify and promote best practices.

Obstacles

- The inability of IT, HR and business leaders to agree on requirements and use cases.
- The tendency to use dashboards before defining the questions leaders seek to answer.
- Union workers or legal/regulatory limitations on data collection due to privacy concerns within some organizations.
- The threat that leaders with trust issues may misuse data for employee surveillance.
- The failure of change-averse teams to adopt processes focused on delivering change based on analytics-derived insights that, instead, continue to use historic precedence.
- The cost of several tools or capabilities to aggregate data and insights from other digital workplace technology management tools.
- Paying too much attention to experience scores and benchmarking inside analytics tools, which can misclassify efforts due to algorithms lacking context or sophistication.
- A delta between what organizations want from WPA and what can actually be done with the data collected.

User Recommendations

Hype has passed the Peak of Inflated Expectations as more organizations are using WPA, but some are struggling with the need to use multiple tools or aggregate several data sources to maximize value. Gartner recommends:

- Consolidate requirements and align collective goals to corporate objectives by collaborating with shared services and line of business peers.
- Ensure policy and legal compliance by partnering with HR and Legal.
- Avoid tool sprawl by reviewing existing capabilities or potential upgrades before buying new.
- Minimize risk by training managers on appropriate use before granting access and ensuring that employees understand the intent and use of WPA.

- Avoid irrelevant comparisons to other companies by using tool-provided experience scores to baseline and measure your own progress.

Sample Vendors

ActivTrak; Avanade; Humanyze; Microsoft; Sapience; Scalable Software; Worklytics

Gartner Recommended Reading

Enhance Digital Workplace Operations With Machine Learning and Automation

Adapt the IT Operating Model to Deliver Indispensable Digital Workplace Services

Top Strategic Technology Trends for 2021: Anywhere Operations

Optimize End-User Services Through Segmentation of Work Settings

Enablement Mindset Is the Missing IT Ingredient to Improve Workforce Digital Dexterity and the Employee Experience

BEC Protection

Analysis By: Mark Harris

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Business email compromise (BEC) protection detects and filters malicious emails that fraudulently impersonate business associates with the aim of misdirecting funds or data.

Why This Is Important

BEC messages typically do not include malicious links or attachments, and are often sent from legitimate mail servers, which makes them very difficult to identify. Attackers are often well-informed by publicly available information (e.g., that on LinkedIn) in order to increase their effectiveness. BEC attacks can result in significant financial loss and reputational damage.

Business Impact

BEC attacks pose a significant risk to all industries. They accounted for 43% of cybercrime losses in 2020. These attacks are often relatively low-tech and targeted at valuable individuals, such as members of the accounts payable team or the CFO. BEC attacks are often combined with email account takeover attacks.

Fraudulent invoices are the most common form of BEC attack. They can undermine trust in a relationship and cause financial loss.

Drivers

Adoption of BEC protection technology is increasing because:

- Traditional techniques for detecting malicious attachments or links are ineffective against BEC attacks.
- Reputation-based detection techniques are relatively ineffective because these attacks often come from legitimate email accounts with good reputations.
- Spoofed emails to customers are difficult to detect because they do not involve the corporate email system organization.
- Losses from BEC attacks can be significant — they sometimes amount to millions of dollars.
- All financial transactions, including requests to change payroll details, are at risk.
- BEC attacks often go unnoticed initially — it is often only when the intended recipient notices a payment has not been made that the fraud is detected.
- Compromised email accounts enable attackers to use real email conversations to redirect funds. These account takeover attacks are indistinguishable from legitimate emails.

Obstacles

- BEC protection involves not just the use of BEC solutions but also: (1) user education, both of staff within an organization and of external suppliers (and others), in order to identify BEC attacks; (2) a move away from email as a means of processing high-risk financial transactions. Changes to other processes and procedures, or the introduction of procure-to-pay solutions, can also help.
- Even the most effective solutions are not 100% effective, and, as attackers' techniques evolve, solutions focused on BEC may lose sight of the latest techniques being used.
- Solutions that rely on APIs provided by cloud email providers are limited to what those APIs provide and their continued support by Microsoft and Google.
- BEC protection capability is likely to be absorbed into broad email security solutions before reaching the plateau.

User Recommendations

- Complement the use of email security solutions with increased user awareness by educating users about BEC phishing techniques and the limitations of email as an authentication factor in high-risk transactions.
- Implement standard operating procedures to authenticate email requests for financial or data transactions, and move high-risk ad hoc transactions from email to more authenticated systems.
- Upgrade or supplement email security solutions with advanced phishing protection, including natural language processing, natural language understanding, computer vision and machine-learning-based social graph analysis.
- Implement Domain-Based Message Authentication, Reporting and Conformance (DMARC) to authenticate email domains and minimize domain abuse.
- Implement multifactor authentication for email to protect against account takeover.

Sample Vendors

Abnormal; Armorblox; Mimecast; Proofpoint

Gartner Recommended Reading

Protecting Against Business Email Compromise Phishing

Market Guide for Email Security

How to Build an Effective Email Security Architecture

Cloud Data Backup

Analysis By: Jerry Rozeman, Michael Hoeck, Chandra Mukhyala

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Cloud data backup tools back up and restore production data generated in the cloud. Data can be generated by SaaS tools (e.g., Microsoft Office 365); platform as a service (PaaS) tools (e.g., Amazon Relational Database Service [RDS]); or infrastructure as a service (IaaS) tools (e.g., Amazon Elastic Compute Cloud [EC2]). Backup copies can be stored in the same or a different cloud location, or on-premises in the data center, where restore granularity/recovery location options should be offered.

Why This Is Important

SaaS, PaaS and IaaS providers typically offer infrastructure resiliency and availability to protect their systems from server, site or region failures but do not take responsibility for the data. When data is lost due to infrastructure failure, user or admin errors, software corruption, or malicious attacks, user organizations are fully responsible. Cloud data backup tools address these deficiencies.

Business Impact

Adopting cloud data backup tools will require significant investments in software, infrastructure, knowledge and processes, which often are not a part of the cloud business cases. However, as many of the tools can be delivered as a SaaS functionality, complexity can be significantly reduced.

Drivers

- As more production workloads migrate to the cloud (in the form of SaaS, PaaS or IaaS), it has become critical to protect data generated natively in the cloud.
- Cloud providers focus on infrastructure high availability and disaster recovery but are not responsible for application or user data loss.
- Most SaaS applications' natively included data protection capabilities are not true backup, and lack secure access control and consistent recovery points to recover from internal and external threats.
- As Microsoft Office 365 gains momentum, the need for better protection is growing rapidly, which is especially driven by Microsoft's inconsistent and incomplete use of recycle bins, requirement of retention policies, and lack of intuitive recovery processes.
- Backup of Salesforce data is the second-most-addressed workload by these vendors mainly driven by Salesforce complex and incomplete recovery of data.
- IaaS and PaaS data backup is a more nascent area that caters to organizations' need to back up production data generated in the IaaS or PaaS cloud.
- Native backup of IaaS and PaaS data usually resorts to snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation.

Obstacles

- Deploying data protection for cloud-based workloads is an additional investment; however, this is often an afterthought, because it is not a part of the business case.
- In-depth review of each cloud vendor's SLAs is another obstacle that customers have to overcome as it limits them in their speed of cloud adoption.
- The outcome of the SLA review might block the cloud service adoption as the SLA might not meet company requirements.

User Recommendations

- Evaluate and thoroughly understand cloud-native backup and recovery capabilities, and compare them with your situations before migrating applications to SaaS, PaaS or IaaS data backup solutions.
- Ensure that contracts with cloud providers clearly specify the capabilities and costs associated with the backup solution, and understand the limitations of such solutions.
- Factor in additional backup costs into the total cost of ownership calculation before migrating to the cloud.
- Focus on ease of deployment, ease of management, data mobility, storage efficiency and flexible options in terms of backup/recovery granularity and location when selecting third-party backup tools.

Sample Vendors

AvePoint; Cohesity; Commvault; Druva; Rubrik; Veeam

Gartner Recommended Reading

Magic Quadrant for Data Center Backup and Recovery Solutions

Critical Capabilities for Data Center Backup and Recovery Solutions

Market Guide for Backup as a Service

IT Resilience Orchestration

Analysis By: Ron Blair

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

ITRO solutions are chiefly aimed at helping to improve the reliability, speed and granularity of workload recovery due to unplanned outages by automating disaster recovery (DR) processes while lowering the costs of application dependency mapping, DR run book creation, exercise efforts and reporting.

Why This Is Important

Ensuring smooth and predictable recovery operations is an ongoing challenge for organizations, especially when large volumes and multiple types of systems, applications and databases are involved. For many organizations, the preferred approach is to manage application failover by using ITRO tools.

Business Impact

Particularly beneficial for organizations with 150 or more server images, ITRO tools provide improved IT application recovery through automation of application workload failover and failback. They also improve configuration integrity and consistency between production and recovery sites, which may be an internal data center, a colocation site or a public cloud. These tools ease the burden of DR exercises, allowing for more frequent exercises, thus resulting in greater recovery confidence.

Drivers

Per the 2021 Gartner Security and Risk survey, 32% of respondents fully use and 78% use ITRO tools in some shape or form today, with only 5% stating they have no plans to be using them within the next 12 months. Some drivers include:

- Increased awareness of the importance of recovery and thus greater budgets. In fact, per the same survey referenced above, 59% expect budget increases in 2021.
- Greater access to ITRO as a number of different products are encapsulating ITRO capabilities into product sets. For example, backup products continue to improve both replication and automated recovery capabilities, and hyperscale cloud providers have built or acquired capabilities from former independent software providers.
- Hybrid cloud inherently needs these high levels of orchestration for disaster recovery capabilities.
- Large, highly regulated industries with relatively heterogeneous environments find themselves needing an orchestrator of many different platforms and replication tools.

- Heightened cybersecurity concerns were expressed in the 1Q21 Emerging Risk survey, where enterprise assurance personnel (such as those in enterprise risk management and internal audit) rated cybersecurity control failures as the most important emerging risk by potential impact and probability.

Obstacles

Many ITRO products' focus is on orchestrating only the workloads they replicate. Others focus less on replication and rather on orchestrating other replication tools, backup products, and platforms, providing prefabricated libraries and playbooks.

As a result, there are common obstacles with varying relevance:

- Both hyperconverged solutions and cloud providers increasingly include both ITRO characteristics and add-on DR options.
- As more workloads are containerized, the advent of container orchestration solutions come into play.
- Cloud deployments and organizations with embedded automation teams typically leverage a combination of cloud-native or third-party cloud orchestration and configuration automation software.

User Recommendations

- Gain agreement for need and potential value by asking questions such as: Do we need to improve our RTO? Are we performing DR exercises as often and as granular as we should? Are we confident we could recover from actual disasters without key personnel?
- Narrow down ITRO types by asking questions such as: Would we potentially derive value from a tool that provides both replication and orchestration? Do we have a relatively heterogeneous environment where we need an orchestrator of many different platforms and replication tools?
- Ensure strategic alignment by asking questions such as: Have we already invested in platforms or backup/replication products that may have some or all the functionality embedded? What strategic bets have we made at the macro level in terms of investments in automation teams, platforms and tooling (for example, IT service management [ITSM], cloud management and automation)? And what is the appetite to leverage those resources for DR automation?

Gartner Recommended Reading

Market Guide for IT Resilience Orchestration

IT Resilience — 7 Tips for Improving Reliability, Tolerability and Disaster Recovery

Prescriptive Analytics

Analysis By: Carlie Idoine, Peter Krensky

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Prescriptive analytics is a set of capabilities that specify a preferred course of action to meet a predefined objective. The most common types of prescriptive analytics are optimization methods, a combination of predictive analytics and rules, heuristics, and decision analysis methods. Prescriptive analytics differs from descriptive, diagnostic and predictive analytics in that the technology explores multiple outcomes and provides a recommended (and sometimes automated) action.

Why This Is Important

Prescriptive analytics provides capabilities to further automate/augment decision making to improve business responsiveness and more optimal outcomes. From a “purist” perspective, the term “prescriptive analytics” is a broad category with little hype, encompassing components with varying positions across the Hype Cycle and various levels of maturity. Such components include optimization, rules combined with predictive techniques and decision intelligence.

Business Impact

Prescriptive techniques support:

- Strategic, tactical and operational decisions to reduce risk, maximize profits, minimize costs, or more efficiently allocate scarce or competing resources.
- Recommendations for a course of action that best manages the trade-offs among conflicting constraints and goals.

- Exploration of multiple scenarios and comparison of recommended courses of action.
- Strategic and tactical time horizons as well as real-time or near-real-time decision making.

Drivers

- Maturing and expanding data science initiatives, better algorithms, more cost-effective cloud-based computing power and a substantial increase in available data.
- With improvement in analytics solutions, data quality, skills and broader use of predictive analytics, prescriptive analytics will continue to advance.
- In addition, the increasing popularity of graph techniques provides a great substrate for prescriptive analytics techniques, highlighting early signals for actions, causality links and forward paths of actions, facilitating the implementations of decisions and actions.
- The post COVID-19 reset with a focus on optimization and other advanced techniques with an emphasis on prioritizing actionable, proactive insight — as opposed to the more traditional reactive reporting.
- AI platforms and decision management tools increasingly include prescriptive techniques, driving user acceptance and potential value to the organization.
- Prescriptive analytics ranges from relatively straightforward rule processing to complex simulation and optimization systems.
- Prescriptive analytics continues to evolve, responding to ever greater complexity in business, with more need for more advanced prescriptive analytics and composite AI, e.g., combining rules/decision management with machine learning or optimization techniques.
- Organizations continue to improve and optimize their decision making, by applying decision intelligence and decision modeling to support, augment or automate decisions more effectively. Prescriptive analytics is a key enabler of this approach.

Obstacles

- Lack of expertise for how and where to apply prescriptive techniques.
- Lack of formal operationalization methods and best practices.
- Historic requirement for separate advanced analytics software that specializes in prescriptive techniques with little cohesion across the analytic capability continuum from descriptive to diagnostic to predictive to prescriptive.
- Even established use cases can fall victim to common data science challenges such as data quality, bias and talent shortages.
- Although it is a necessary competence, prescriptive analytics does not automatically result in better decision making.

User Recommendations

- Start with a business problem or decision where there are complicated trade-offs to be made, multiple considerations and multiple objectives.
- Understand the breadth of prescriptive analytics' approaches and decision models available, and which best cater to the nature of your specific business problems and skills.
- Look for packaged applications that provide specific vertical or functional solutions, and service providers with the necessary skills.
- Gain buy-in and willingness from stakeholders — ranging from senior executives to front line workers carrying out the recommended actions — to rely on analytic recommendations.
- Ensure that your organizational structure and governance will enable the company to implement and maintain functional, as well as cross-functional, prescriptive analytics recommendations.

Sample Vendors

AIMMS; Decision Lens; FICO; Frontline Systems; Gurobi; IBM; River Logic; SAS; Sparkling Logic; Veriluma

Gartner Recommended Reading

When and How to Combine Predictive and Prescriptive Techniques to Solve Business Problems

Predicts 2021: Analytics, BI and Data Science Solutions — Pervasive, Democratized and Composable

Worlds Collide as Augmented Analytics Draws Analytics, BI and Data Science Together

Effective Use of Supply Chain Analytics to Mitigate Business Disruptions

Sliding into the Trough

Citizen Data Science

Analysis By: Carlie Idoine, Shubhangi Vashisth, Rita Sallam

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Citizen data science is a set of capabilities and practices that allow users to extract advanced analytic insights from data without the need for extensive data science expertise. This provides responsive insights and faster time to insight for driving business decisions.

Why This Is Important

Innovations in augmented analytics tools enable those without expert data science knowledge and experience to be productive in applying data science and machine learning (DSML) methods within their analyses. Citizen data science helps unlock new insights beyond use of basic descriptive and diagnostic capabilities, enabling democratization of analytics capabilities as well as an upskilling path and new opportunities for business analysts and developers.

Business Impact

Citizen data science forms the foundation of next-generation analytics and can be leveraged to:

- Make insights from DSML more accessible and pervasive.
- Narrow the DSML talent gap due to the shortage and high cost of data scientists.
- Bring extensive domain expertise and increase efficiency of expert data scientists.
- Perform specific phases of the analytics life cycle (such as feature generation and selection, and algorithm selection) to scale and focus use of expertise where needed.

Drivers

- Historically, building DSML models required expert data scientists who are difficult and expensive to hire and retain. Citizen data science helps overcome such limitations.
- Central to citizen data science is the availability of augmented analytics capabilities. These include automated, streamlined data access and data engineering; augmented user insight through automated data visualization and exploration; modeling and pattern detection including feature engineering, model selection and validation; automated deployment and operationalization; and capabilities to support collaboration and sharing.
- Citizen data science will be a key driver of analytics adoption for the foreseeable future. Many business users want to upskill their analytics knowledge and expertise and may already be doing so. This population has become so prevalent that tools and features have been designed specifically for their use.

Obstacles

- Upskilling in advanced DSML techniques and approaches is important to derive value from citizen data science. Classroom learning provides a foundation but must be supported by on-the-job learning and experimentation.
- Tools with augmented analytics capabilities and additional processes to manage creation and sharing of models will be required to support citizen data science.
- There is still a need to (statistically) validate results of citizen data science by expert data scientists.
- Expert data scientists often resist or underestimate the effectiveness of citizen data science approaches.
- Citizen data science is often deemed to be just a preliminary, elementary step and not a fully functional DSML approach.
- Citizen data science leveraged in silos with no oversight or collaboration among experts and others with a vested interest in DSML success could lead to duplication of data engineering and analytic effort, lack of operationalization and limited visibility and standards.

User Recommendations

- Scan opportunities for citizen data science to complement existing analytics and expert data science initiatives across the data science life cycle.

- Define the citizen data scientist as a formal persona. Define its “fit” relative to other roles, and identify those who fit the citizen data scientist profile.
- Track the capabilities (technology) and roadmaps of existing business intelligence (BI) and data science platforms and emerging startups for support of augmented features.
- Educate business leaders and decision makers about the potential impact of a broader range of users leveraging DSML to gain leadership support.
- Acknowledge that you still need specialist data scientists to validate and operationalize models, findings and applications.
- Provision augmented analytics tools (including but not limited to citizen data science tools), platforms and processes to support and encourage collaboration between business users, application developers and data science teams.

Sample Vendors

Aible; Alteryx; BigSquid AI; Dataiku; DataRobot; dotData; H2O.ai; SAS; SparkBeyond; Tellius

Gartner Recommended Reading

Worlds Collide as Augmented Analytics Draws Analytics, BI and Data Science Together

Build a Comprehensive Ecosystem for Citizen Data Scientists to Drive Impactful Analytics

Pursue Citizen Data Science to Expand Analytics Use Cases

The 5 Myths of Citizen Data Science

Best Practices to Avoid Citizen Data Science Failure

Data and Analytics Governance

Analysis By: Saul Judah, Debra Logan, Andrew White

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Data and analytics governance is the specification of decision rights and an accountability framework to ensure the appropriate behavior in the valuation, creation, consumption and control of data and analytics. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of data and analytics in enabling an organization to achieve its goals.

Why This Is Important

Data and analytics governance allows organizations the oversight to drive better behaviors relating to information assets in the enterprise, enabling better business outcomes. Data and analytics leaders need good governance practices to enable key business outcomes, such as market growth, cost optimization and merger and acquisition scenarios.

Business Impact

Data and analytics leaders should anticipate the following impacts:

- Better governance oversight, accountability and understanding of decision rights relating to data and analytics across the enterprise and within business areas
- Increased levels of business collaboration, engagement and innovation to drive mission critical priorities in the enterprise
- Increased levels of data literacy and cultural change enabled by better governance

Drivers

- Since the initial outbreak and response to the COVID-19 pandemic, many markets have rallied, with organizations now increasing investment in data and analytics to accelerate their digital business optimization and transformation initiatives. As a result, their effort to establish governance has gained momentum, which in turn drives hype. Gartner-client call volume has increased by more than 40% year over year for data and analytics governance.
- Investment in data and analytics is widespread across enterprises, with business functions spending as much on these initiatives as central IT teams, causing proliferation of information silos. The need for effective governance capabilities has therefore become an increasing concern for data and analytics leaders, as a framework for enabling the connected enterprise, while addressing the local information needs of business functions.
- Organizations with higher information maturity increasingly recognize that taking a data *and* analytics governance approach — rather than one focusing on individual information asset types (e.g., data governance) — yields better business results. Elsewhere, we have seen organizations recognize the urgent need to establish governance "to get the ball rolling," even if it is for only data governance or analytics governance. This significant increase in effort and hype relating to data and analytics governance is being seen in all industries, geographies, organization types and maturity levels.
- Hype and interest are also growing in many areas related to data analytics and governance, such as AI model governance, analytics governance in data warehouses and data lakes, trust-based governance, IoT data governance, and ethics as a discrete policy.

Obstacles

- Data and analytics governance is complex, organizationally challenging and politically sensitive. It is often difficult to get executive-level consensus for data and analytics governance programs, and as a result they are led by IT, with a view to "bringing in the business later." Because these initiatives are not business-outcome-based, they typically result in failure.
- Despite the diversity and complexity of business scenarios, most organizations continue to take a one-size-fits-all, command-and-control approach to their data and analytics governance. Furthermore, most organizations have a poor understanding of executive leader accountability and decision rights for information. Establishing an effective governance for data and analytics is therefore difficult to achieve. As organizations' expectations of what can realistically be achieved through data and analytics governance decline, we see its position on the Hype Cycle descend into the Trough of Disillusionment.

User Recommendations

- Identify critical business outcomes that need good data and analytics to be successful. Focus your governance work here to maximize your investment, developing a business case if needed.
- Engage key business stakeholders in sponsoring and driving the initiative, alongside the CDO, to enable information culture change.
- Focus on the least amount of data with the maximum business impact, while managing your risk to embed data and analytics governance in the full business context.
- Clearly define the scope of work related to data and analytics governance: policy evaluation and setting, policy interpretation and enforcement, and policy execution. The first two must be led by business; the latter can be enabled by IT.
- Consider how data standards and metadata management can be used to implement data and analytics governance in the enterprise. Though business leaders may not fully understand their importance, an industrial governance capability needs enterprise-scale data and analytics capabilities.

Gartner Recommended Reading

The State of Data and Analytics Governance Is Worse Than You Think

Next Best Actions to Improve Your Data and Analytics Governance

7 Must-Have Foundations for Modern Data and Analytics Governance

Deploying Effective Data and Analytics Governance: 3 Companies That Got It Right

Adaptive Data and Analytics Governance to Achieve Digital Business Success

Augmented Analytics

Analysis By: Rita Sallam

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Augmented analytics uses AI and ML techniques to automate data preparation, insight discovery, data science, and machine learning model development and insight sharing for a broad range of business users, operational workers and citizen data scientists.

Why This Is Important

Many of the activities associated with preparing data, finding patterns in data, building models on complex combinations of data, and sharing insights with others, remain highly manual. This limits user adoption and potential business impact.

Business Impact

- Augmented analytics is transforming how and where users interact with analytics content as it has become a core component of most analytics and BI and data science platforms.
- Insights from advanced analytics — once available only to skilled analysts, citizen data scientists and data science specialists — are now in the hands of business analysts and a broad range of decision makers and operational workers across the enterprise — the augmented consumer — driving new sources of business value.

Drivers

- Organizations increasingly want to analyze more complex datasets combining diverse data from across the enterprise as well as from external sources. With an increasing number of variables to explore in data harmonized from many diverse datasets, it is practically impossible for users to explore every possible pattern combination, and even more difficult to determine whether their findings are the most relevant, significant and actionable. Expanding use of augmented analytics will reduce the time users spend on exploring data, while giving them more time to act on the most relevant insights.
- Augmented analytics capabilities are increasingly mainstream features of data preparation, analytics and BI platforms and data science and machine learning tools. They are also being embedded in enterprise applications and domain and industry specific solutions. This is delivering insights most relevant to a broad set of application users to improve decision-making and actions.
- Dynamic data stories are an example of a combination of augmented analytics features used to automate insights. This combines augmented analytics with natural language query (NLQ), natural language generation (NLG) and anomaly detection into dynamically generated data stories delivered to users in their context. This type of user experience will reduce the use of predefined dashboards for monitoring and analysis and increase the use of augmented analytics.

Obstacles

- Trust in autogenerated models. Organizations must ensure that the augmented approach is transparent and auditable for accuracy and bias, and that there is a process to review and certify analyses created.
- Training. With more automation comes greater user responsibility and the need for more, but different user training.
- Collaboration. Establishing a collaborative environment, pairing expert data scientists with nonexperts across the analytic life cycle will be essential to capitalize on the skills of all parties.
- User outreach. Using augmented analytics not only to support new and less expert analytic users, but also to shorten time to insight for more expert users.
- Ecosystem. It will be critical to build an ecosystem that includes not only tools but also data, people and processes to support the use of augmented analytics.

User Recommendations

Data and analytics leaders looking to make analytics more pervasive should:

- Identify the personas that will benefit most from augmented analytics capabilities.
- Ensure users can get value from new augmented analytics features by providing targeted and context-specific training. Invest in data literacy to ensure responsible adoption.
- Focus on explainability as a key feature to build trust in autogenerated models.
- Assess the augmented analytics capabilities and roadmaps of analytics and BI, data science, data preparation platforms, and startups as they mature. Look for upfront setup and data preparation required, the types of data and range of algorithms supported, integration with existing tools, explainability of models and the accuracy of the findings. Also evaluate emerging dynamic data storytelling capabilities.
- Provide incentives for citizen data scientists to collaborate with, and be coached by, specialist data scientists who still need to validate models, findings and applications.

Sample Vendors

Microsoft (Power BI); Oracle (Analytics Cloud); Qlik; SAP Analytics Cloud; SAS; Tableau; Tellius; ThoughtSpot; AnswerRocket; Igenius; Conversight.ai; TIBCO Spotfire

Gartner Recommended Reading

Magic Quadrant for Analytics and Business Intelligence Platforms

Critical Capabilities for Analytics and Business Intelligence Platforms

Tool: Visual Guide to Analytics and Business Intelligence Platform Capabilities

Top Trends in Data and Analytics for 2021

How Augmented Analytics Will Transform Your Organization: A Gartner Trend Insight Report

MDR Services

Analysis By: Toby Bussa

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Managed detection and response (MDR) services leverage a combination of technologies at the host, the network and, increasingly, the cloud layer, as well as advanced analytics, threat intelligence, and human expertise to deliver 24/7 threat monitoring, detection and response. MDR providers undertake incident validation and investigation, and response actions to disruption, and they contain threats.

Why This Is Important

Attacks against organizations are relentless and increasing. Most organizations lack the resources, budget or appetite to build and run their own 24/7 modern security operations center (SOC) function, which is required to help them protect and defend themselves against attacks that increasingly cause more impact and damage to operations. MDR services enable organizations to procure modern SOC services to address this need and fill gaps in their threat detection and response coverage.

Business Impact

Organizations of all sizes that have not invested in threat detection and response capabilities are at risk, due to increasingly hostile external threats. This situation, combined with the challenge of finding, acquiring and retaining the necessary expertise and the right tools, makes building an adequate internal capability challenging. MDR services reduce the complexity of identifying the right mix of people, process and technology by enabling buyers to buy capabilities directly from service providers.

Drivers

- MDR services continue to expand beyond the traditional “turnkey” approach whereby the provider brings a predefined, or highly curated and supported, set of technologies. The expansion to supporting a broader set of log, data and alert sources has been well received by organizations that want more say over what is monitored, but it also puts pressure on providers to adapt and scale how they deliver their services, while delivering high-fidelity threat detection.
- Active responses by MDR providers are being required by buyers, especially in North America, and this challenges both parties to ensure responses are made in a coordinated and reliable way.
- In response to customer demand, MDR providers are adding foundational security operation capabilities, such as vulnerability management, log management and risk management, to their offerings.
- Cloud-native security operations solutions like security information and event management (SIEM), security orchestration, analytics and reporting (SOAR) and extended detection and response (XDR) with multitenant capability, MDR-friendly programs, and SOCaaS or “SOC in a box” offerings are enabling new MDR service providers.

Obstacles

- The number of MDR service providers continues to grow, with new ones becoming visible to Gartner at least weekly. This makes it more difficult for buyers to identify the best provider for their needs.
- Gartner hears of performance issues with MDR service providers and failed engagements due to misaligned expectations.
- Technology vendors with XDR solutions, which already offered managed endpoint detection and response (EDR) as a form of MDR, have started positioning their MDR services as managed XDR, which will likely increase buyers’ confusion.
- Managed security service providers (MSSPs) have added MDR offerings to their portfolios to address buyer demand and compete better — a development that further complicates buyers’ decision-making process.

User Recommendations

- MDR buyers should focus on outcomes, not technologies. Organizations underinvested in technologies like EDR and network detection and response (NDR) should favor an approach in which a vendor provides the tools and delivers the desired outcomes.
- Buyers lacking the staff and expertise to handle incident response activities once a threat has been identified, or that want to add threat-hunting capabilities, should assess MDR services.
- If there are existing investments in threat detection technologies, such as EDR, NDR and SIEM, MDR services that deploy their own technologies may be inappropriate. Consider services that can use existing technologies, and augment them to fill gaps.
- If technology management, compliance monitoring and reporting, and other managed security services are required, consider MSSPs, especially those that offer MDR-type services.
- Buy MDR services that offer transparency, that encourage engagement through modern user interfaces, and that have open communication channels with analysts and delivery teams.

Sample Vendors

Arctic Wolf; CrowdStrike; eSentire; Expel; F-Secure; FireEye; Rapid7; Red Canary; Secureworks; Trustwave

Gartner Recommended Reading

Market Guide for Managed Detection and Response Services

IoT Business Solutions

Analysis By: DD Mishra

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

IoT business solutions are often implemented by integrating IoT devices, IoT data, IoT platforms and IoT applications — combined with IT assets (business applications, legacy data, mobile, and SaaS) — to work together toward desired business outcomes.

Why This Is Important

IoT adoption is rapidly increasing; the enterprise IoT platform market will grow to $7.6 billion in 2024 with a 31% CAGR. Companies are investing in a wide range of diverse IoT technologies and integrating them into different applications in order to drive different business outcomes. To succeed in IoT implementations, application leaders must thoroughly examine and understand the full scope of end-to-end IoT business solutions and the functional role of IoT platforms within them.

Business Impact

IoT Business solutions are widely used in different verticals such as Pharmaceuticals, Healthcare, Energy, Transportation among others, with use cases ranging from plant and process automations, smart contract solutions, asset tracking, inventory management, resource utilization and energy conservation.

Drivers

- The potential benefits and drivers vary from organization to organization, but we see the demand for asset tracking, predictive maintenance, productivity and process, and power optimization as the key driver for growth and adoption of IoT.

Obstacles

- IoT Implementations often encounter bottlenecks and hurdles across businesses. The inhibitors of growth include technical complexity, security and privacy challenges, integration challenges and skill gaps.

User Recommendations

- Analyze your desired business outcomes. While limited IoT point solutions themselves can deliver some business value, more complete IoT business solutions can achieve expanded outcomes via automated business responses.
- Plan what your end-to-end IoT business solution should look like, clearly identifying and prioritizing which IoT-enabled business outcomes you desire and create a roadmap.
- Commission an IoT center of excellence (COE) to explore the potential business value of IoT solutions and their potential impact on existing business units, IT infrastructure and your business processes and applications.

Gartner Recommended Reading

Predicts 2020: As IoT Use Proliferates, So Do Signs of Its Increasing Maturity and Growing Pains

Use the IoT Platform Solution Reference Model to Help Design Your End-to-End IoT Business Solutions

Immutable Infrastructure

Analysis By: Neil MacDonald, Tony Harvey

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Immutable infrastructure is a process pattern (not a technology) in which the system and application infrastructure, once deployed into production, is never updated in place. Instead, when changes are required, the infrastructure and applications are simply replaced from the development pipeline.

Why This Is Important

Immutable infrastructure ensures the system and application environment is accurately deployed and remains in a predictable, known-good-configuration state. It simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security and simplifies troubleshooting. It also enables rapid replication of environments for disaster recovery, geographic redundancy or testing. This approach is easier to adopt and often applied with cloud-native applications.

Business Impact

Taking an immutable approach to workload and application management simplifies automated problem resolution by reducing the options for corrective action to, essentially, one — repair the application or image in the development pipeline and re-release into production. The result is an improved security posture with fewer vulnerabilities and faster time to remediate when new issues are identified.

Drivers

- Linux containers and Kubernetes are being widely adopted. Containers improve the practicality of implementing immutable infrastructure and will drive greater adoption.
- Interest in zero trust and other advanced security postures where immutable infrastructure can be used to proactively regenerate workloads in production from a known good state (assuming compromise), a concept referred to as “systematic workload reprovisioning.”
- For cloud native application development projects, immutable infrastructure simplifies change management, supports faster and safer upgrades, reduces operational errors, improves security and simplifies troubleshooting.

Obstacles

- The use of immutable infrastructure requires a strict operational discipline that many organizations haven't yet achieved, or have achieved for only a subset of applications.
- IT administrators are reluctant to give up the ability to modify or patch runtime systems.
- Although immutable infrastructure may appear simple, embracing it requires a mature automation framework, up-to-date blueprints and bills of materials, and confidence in your ability to arbitrarily recreate components without negative effects on user experience or loss of state.
- Many application stacks have elements that are deployed in the form of virtual machine images. VM replacement is slower and requires greater coordination than other workload components such as containers.

User Recommendations

- Reduce or eliminate configuration drift by establishing a policy that no software, including the OS, is ever patched in production. Updates must be made to the individual components, versioned in a source-code-control repository, then redeployed for consistency.
- Prevent unauthorized change by turning off all normal administrative access to production compute resources — for example, by not permitting SSH or RDP access.
- Adopt immutable infrastructure principles with cloud-native applications first. Cloud-native workloads are more suitable for immutable infrastructure architecture than traditional on-premises workloads.
- Treat scripts, recipes and other code used for infrastructure automation similarly to the application source code itself, which mandates good software engineering discipline.

Sample Vendors

Amazon Web Services; Ansible; Chef; Fugue; Google; HashiCorp; Microsoft; Puppet; SaltStack; Turbot

Gartner Recommended Reading

How to Make Cloud More Secure Than Your Own Data Center

Top 10 Technologies That Will Drive the Future of Infrastructure and Operations

Programmable Infrastructure Is Foundational to Infrastructure-Led Disruption

Adapting Vulnerability Management to the Modern IT World of Containers and DevOps

Desktop as a Service

Analysis By: Stuart Downes, Mark Margevicius, Tony Harvey

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Desktop as a service (DaaS) solutions provide a virtualized desktop experience to workers, entirely from a remote hosted location such as the public cloud. DaaS eliminates the need for businesses to purchase the physical infrastructure associated with desktop virtualization, instead functioning through subscription- and usage-based payment structures. DaaS includes provisioning, patching and maintenance of the management plane and resources to host workloads.

Why This Is Important

DaaS provides secure remote access to applications and desktops using a network connection. No data resides on the endpoint, offering a solution that can increase security, redundancy, bursting and performance for remote workers. DaaS offers scalable services, allowing clients to appropriately size and consume their environments hour by hour, day by day, and month by month; however, not all have such granular billing options.

Business Impact

The pandemic highlighted the requirement to deliver secure desktop and application experiences to users in any location:

- Revenues grew by 98% in 2020 compared to 2019 as clients adopted DaaS to secure work-from-home experiences.
- DaaS enables business continuity and anywhere operations for home-based and hybrid home-office operations.

- DaaS enhances security for BYOPC use cases reducing risks for businesses.

Drivers

- Improve security and compliance — centralize data, minimize exposure on notebook PCs.
- Support remote work with no data residing on the endpoint.
- Endpoint computing models that allow any device models and bring your own PC (BYOPC) endpoints.
- Simplified end-user computing operations that are performed in the cloud, especially evident with a highly distributed workforce.
- Business continuity, the main driver for DaaS growth in 2020.
- On-demand desktops.
- A financial model that allows scaling of cloud resources and an opex model.
- Scaling to meet the needs of short-term employees, such as seasonal workers.
- Securely extend services to external contractors, including IT developers and business process outsourcing (BPO).
- Enabling rapid access to systems during mergers, acquisitions and divestitures.
- Rich graphics use cases like engineering, games development, fashion and geographic information systems (GIS) benefit from GPU-enabled workstation class virtual desktops and applications.
- Where supply of devices, or high attrition rates, makes the provision of a physical device difficult.
- Eliminates the need for complex virtual desktop infrastructure (VDI) implementations.
- Enables business expansion to new regions without the need to deploy data centers.

Obstacles

- Cost — In many cases, direct infrastructure cost comparisons show higher IT costs for DaaS compared to VDI or desktop PCs, usually the business case turns positive only when business and users costs are included.
- Multimedia streaming, web meetings and video call performance in DaaS are not equivalent to that of a physical endpoint.
- Applications and data that are landlocked in on-premises data centers that have, or are perceived to have, network-related performance issues when the desktop or application is hosted in the cloud.
- Some DaaS solutions require complex configuration, which, although simpler than VDI, can in some cases require careful configuration and selection of appropriate storage services to ensure a performant DaaS experience.

User Recommendations

DaaS will continue to mature and increase in adoption through 2025. DaaS is yet to move through the Trough of Disillusionment onto the Slope of Enlightenment. Clients should:

- Understand the three DaaS market segments and select a vendor from the appropriate segment: (1) Client-defined DaaS: Clients configure their DaaS experience and manage their workloads. This requires less skill than VDI; *2) Vendor-defined DaaS: The vendor configures the DaaS experience and clients manage their workloads; and (3) Managed DaaS: The vendor configures the DaaS experience and the vendor manages the workloads.
- Choose a DaaS vendor whose services best align to your requirements; even within each segment, there are differences between the services vendors offer.
- Optimize multimedia streaming, web meetings and video calls.
- Select a DaaS vendor that offers billing granularity that you require; some are granular hour by hour, others day by day or month by month.

Sample Vendors

Amazon Web Services; Citrix; Evolve IP; Microsoft; SACA; SimpleCloud; VMware; Workspot

Gartner Recommended Reading

Market Guide for Desktop as a Service

Microsoft's Restrictions for Licensing Windows and Office 365 for VDI/DaaS on AWS and Other Hyperscale Clouds Require Attention

Physical, Virtual and Cloud Desktops: Is a Hybrid Approach Inevitable?

How to Build a Successful Business Case for Desktop Virtualization

OS Containers

Analysis By: Thomas Bittman

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

OS containers are a shared OS virtualization technology that enables multiple applications to share an OS kernel without conflicting. This is enabled by what is usually called a "container daemon," which provides logical isolation of processes. This enables several applications to share an OS kernel, while maintaining their own copies of specific OS libraries.

Why This Is Important

Containers were used for years to increase the density of lightly used workloads (e.g., Oracle Solaris Zones, Virtuozzo and FreeBSD jails), focused on infrastructure management. Now containers are focused on developer requirements, for agile development, rapid provisioning and real-time horizontal scaling — especially for microservices architecture applications and cloud computing.

Business Impact

Container technologies are part of a development architecture that will help enterprises become more agile, with applications that can change quickly, scale rapidly to demand, and improve the density of capacity use. In production, containers will be used strategically for new applications designed for agile development, rather than existing, monolithic application architectures. However, for developer ease of use, containers will also be used as wrappers for traditional workloads.

Drivers

- Lightweight overhead for small applications (improving capacity utilization and density).
- Ease of use and reuse by application developers.
- Aligns to microservices architecture and agile development.

Obstacles

- Reliance on operating system for application isolation creates security concerns, especially in multitenant environments.
- Unlike with hypervisors, existing applications require redesign to take full advantage and leverage the benefits of containers.
- Container use is constrained by tools and operations immaturity and complexity — especially in security, monitoring, data management and networking.
- Developing the right operational model for Kubernetes deployments is difficult, and requires organizational evolution and new skills.

User Recommendations

- Use containers when security and manageability concerns are easily mitigated.
- Combine containers with VMs to separate developer concerns from capacity management, and when the performance overhead of VMs is an acceptable trade-off.

Sample Vendors

Canonical; Docker; Microsoft; Oracle; Red Hat; Virtuozzo; VMware

Gartner Recommended Reading

Best Practices for Running Containers and Kubernetes in Production

Application Portfolio Management

Analysis By: Stefan Van Der Zijden

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Application portfolio management (APM) is an IT discipline that profiles an organization's business applications and products — evaluating business and technical fitness together with cost — to identify and prioritize activities for improvement. APM informs application portfolio rationalization and modernization by categorizing applications into tolerate, invest, migrate or eliminate strategies.

Why This Is Important

APM leads to more conscious management of application assets and investments. Benefits are realized when the analytics lead to agreement with business, financial and IT stakeholders on application strategies and roadmaps that optimize capabilities for the resources available.

Organizations dealing with IT modernization or, more broadly, with the evolution of business processes and technology portfolios, benefit from the adoption of APM.

Business Impact

Business perceptions of IT are often hurt by spiraling maintenance costs and poor responsiveness due to legacy systems with high levels of technical debt. Effective APM will identify and prioritize improvement opportunities to remove business obstacles and impediments. It will result in a simpler portfolio, well-managed portfolio risk, lower and more predictable recurring costs, and a higher percentage of the IT budget being directed toward growth or transformative initiatives.

Drivers

- Application portfolio is an important business asset, and its health, composition and life cycle must be carefully managed.
- The need to increase the business fit, business value and agility of applications, and to reduce their cost, complexity and risk is one of the major drivers behind APM.
- APM helps redirect the overall budget to achieve desired business outcomes.

Obstacles

Companies are slow to adopt APM because:

- Organizations underestimate the value of applications as business assets, and the cost, risk and complexity they carry.
- Getting business engaged and to support the change in applications is difficult.
- The value of APM is not well-understood and is often seen as a bookkeeping exercise.
- The responsibility of monitoring and reporting application portfolio fitness is not assigned or fragmented.
- APM loses out when competing with other initiatives.
- APM is often seen as an ad hoc or one-off activity instead of an ongoing discipline. APM is typically started as a response to a major business event. This can be a merger or an acquisition, or a major business transformation initiative forcing a reevaluation of the entire portfolio. APM is also started when a tipping point is reached and the current state is no longer tolerable for the organization. Examples are a security breach, compliance risk, high cost or poor stability.

User Recommendations

- Peak performers should undertake APM regularly to fuel continuous improvement of the application portfolio and to identify ways of increasing its operational advantages.
- Lagging organizations should undertake APM to help allocate limited resources to the most critical gaps from business stakeholders' lens, to drive adoption of better practices across lines of business and to move toward more efficient support of business services.
- For other organizations, adoption is triggered by a business event or tipping point — a significant event that highlights portfolio inefficiencies/issues and triggers an APM initiative.

Gartner Recommended Reading

Managing a Portfolio of Applications Demands More Than Application Portfolio Management

Use TIME to Engage the Business for Application and Product Portfolio Triage

How to Prioritize Application Inventory and Rationalization

Engage the Business by Developing an Application Strategy Together

Hybrid Cloud Computing

Analysis By: David Smith, Milind Govekar

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Hybrid cloud computing comprises one or more public and private cloud services that operate as separate entities, but ones that are integrated. A hybrid cloud computing service is automated, scalable and elastic. It has self-service interfaces and is delivered as a shared service using internet technologies. Hybrid cloud computing needs integration between the internal and external environments at the data, process, management or security layers.

Why This Is Important

Hybrid cloud theoretically offers enterprises the best of both worlds — the cost optimization, agility, flexibility, scalability and elasticity benefits of public cloud, in conjunction with the control, compliance, security and reliability of private cloud. As a result, virtually all enterprises have a desire to augment internal IT systems with external cloud services.

Business Impact

Hybrid cloud computing enables an enterprise to scale beyond its data centers to take advantage of the public cloud's elasticity. Therefore, it is transformational, because changing business requirements drive the optimum use of private and/or public cloud resources. This approach improves the economic model and agility. It also sets the stage for new ways for enterprises to work with suppliers and partners (B2B) as well as customers (B2C).

Drivers

- The key driver for hybrid cloud is a desire to evolve data centers to become more cloud-like and therefore have a private cloud that has cost and other characteristics that are more like a public cloud, while maintaining “in-house” infrastructure for key privacy, security, data residency or latency needs.
- As more providers deliver hybrid cloud offerings, they increasingly deliver a packaging of the concept. “Packaged hybrid” means you have a vendor-provided private cloud offering that is packaged and connected to a public cloud in a tethered way. Azure Stack from Microsoft is a good example of this packaging, but there is another approach as well. We call these two main approaches “like-for-like” hybrid and “layered technology” hybrid (spanning different technology bases). Packaged hybrid cloud is a key component of the distributed cloud concept.
- The solutions that hybrid cloud provides include service integration, availability/disaster recovery, cross-service security, policy-based workload placement and runtime optimization, and cloud service composition and dynamic execution (e.g., cloudbursting).
- Hybrid cloud computing is different from multicloud computing, which is the deliberate use of cloud services from multiple cloud providers for the same general class of IT service.
- Note that internally run, virtualized environments are often recast as “private clouds,” and then integrated with a public cloud environment and called a “hybrid cloud.” Hybrid cloud assumes that the internal environment is truly a private cloud. Otherwise, the environment is hybrid IT.

Obstacles

- Hybrid cloud computing complements multicloud computing. Although most organizations are integrating applications and services across service boundaries, we believe that few large enterprises have implemented hybrid cloud computing beyond this basic approach — and for relatively few services. Most companies will use some form of hybrid cloud computing during the next two years, but more advanced approaches lack maturity and suffer from significant setup and operational complexity.
- Hybrid cloud is different from hybrid IT, which is where IT organizations act as service brokers as part of a broader IT strategy, and may use hybrid cloud computing. Hybrid IT can also be enabled by service providers focused on delivering cloud service brokerage, multisourcing, service integration and management capabilities. These services are provided by vendors, such as Accenture, Wipro and TCS, and other service providers and system integrators.

User Recommendations

- When using hybrid cloud computing services, establish security, management, and governance guidelines and standards to coordinate the use of these services with public and private services.
- Approach sophisticated cloudbursting and dynamic execution cautiously, because these are the least mature and most problematic hybrid approaches.
- Create guidelines/policies on the appropriate use of the different hybrid cloud models to encourage experimentation and cost savings, and to prevent inappropriately risky implementations.
- Coordinate hybrid cloud services with noncloud applications and infrastructure to support a hybrid IT model.
- Consider cloud management platforms, which implement and enforce policies related to cloud services.
- Consider using hybrid cloud computing, if your organization implements hybrid IT, as the foundation for implementing a multicloud broker role and leveraging hybrid IT services and service providers to complement your own capabilities.

Gartner Recommended Reading

Top Strategic Technology Trends for 2021: Distributed Cloud

‘Distributed Cloud’ Fixes What ‘Hybrid Cloud’ Breaks

Predicts 2021: Building on Cloud Computing as the New Normal

NDR

Analysis By: Lawrence Orans, Jeremy D'Hoinne

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network detection and response (NDR) technology uses a combination of machine learning, rule-based detection and advanced analytics to detect suspicious activities on enterprise networks. NDR tools analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. NDR solutions monitor north-south and east-west traffic. These tools also provide threat hunting capabilities.

Why This Is Important

NDR is very effective in detecting suspicious traffic on networks, such as lateral movement or data exfiltration. It focuses on detecting abnormal behaviors, with less emphasis on more traditional signature-based controls, detecting known threats. NDR solutions also provide response capabilities. Responses can be automated (for example, sending commands to a firewall to drop packets) or manual (providing tools for incident responders to search through metadata for forensic analysis).

Business Impact

NDR solutions provide visibility into network traffic. The machine learning algorithms that are at the core of many NDR products help to detect anomalous traffic that is often missed by other detection techniques. The optional automated response capabilities help to offload some of the workload for incident responders. The threat hunting functionality provides valuable tools for incident responders.

Drivers

- **Low Risk — High Reward —** Implementing NDR tools is a low risk project, since the sensors are positioned out-of-band (they are not in the line of traffic, so they don't represent a point of failure or a "speed bump" for network traffic). Enterprises that implement NDR solutions as a proof of concept (POC) often report high degrees of satisfaction, because the tools provide much needed visibility into network traffic. The POC projects often result in the customer buying the solution, because they see value in the traffic visibility.

- **Encrypted Traffic Analysis —** As the volume of encrypted traffic grows, it becomes more challenging for traditional network security tools to analyze it. Multiple security research reports from leading vendors show growth in the frequency of instances where malware is delivered in an encrypted traffic stream. In the NDR market, vendors offer at least one of these three techniques for detecting anomalies in encrypted traffic. **JA3 signatures:** JA3 is a method of fingerprinting the handshake between a client and a server. By comparing handshakes in live traffic to the handshake patterns of commonly used applications, vendors can detect suspicious traffic. Nearly all NDR vendors support this technique. **Message lengths and time intervals between messages:** Monitoring this information is a proven technique for detecting suspicious traffic without decrypting it. Some vendors support this capability. **Traffic decryption:** Decrypting traffic so that it can be analyzed for malware is the most accurate technique, but only a few vendors support this capability.

- **Securing SaaS Applications —** Some NDR vendors offer the ability to monitor traffic destined for Microsoft 365 and other popular SaaS applications. These tools are good at detecting brute force login attempts and other suspicious behavior. Good CASB tools offer this functionality and more, but NDR vendors can add value where the customer does not already own CASB technology.

Obstacles

- NDR competes for budget with endpoint detection and response (EDR), increasingly extended detection and response (XDR) and sometimes user analytics, depending on the threat vectors that the prospective customers try to mitigate.
- Enterprises with a lower maturity security operation program might struggle to justify the expense for a technology that cannot simply be evaluated by counting the number of alerts it triggers.
- The response features of the NDR products are more recent and still evolving.
- Smaller organizations do not have the staff to support and operate a detection-only tool, but struggle to accept a fully automated response.
- False positives — they are inevitable with any behavioral-based detection tool. But NDR tools, once tuned, do not exhibit a chronic problem in this area and tend to trigger a relatively low volume of alerts.

User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific protocol patterns in your enterprise network to gain maximum value from NDR.
- Carefully plan sensor deployment so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important.
- Tune out false positives in the implementation phase (false positives may be triggered by vulnerability scanners, shadow IT applications, and other factors that may be specific to your environment).
- Select sensors that are sized appropriately for your network. Some vendors offer sensors that support up to 100 Gbps of line rate capture, whereas other vendors' sensors can only scale up to 10 Gbps.

Sample Vendors

Arista Networks; Cisco; Darktrace; ExtraHop; Fidelis Cybersecurity; FireEye; Gigamon; Plixer; Vectra; VMware

Gartner Recommended Reading

Market Guide for Network Detection and Response

Climbing the Slope

UEM

Analysis By: Dan Wilson, Chris Silva

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Unified endpoint management (UEM) tools provide agent-based and agentless management of computers and mobile devices through an employee-centric view of endpoint devices running Windows 10, Google Android and Chrome OS, Apple macOS, iPadOS, and iOS. UEM tools apply data protection, device configuration and usage policies using telemetry from identities, apps, connectivity and devices. They also integrate with identity, security and remote access tools to support zero trust.

Why This Is Important

UEM simplifies endpoint management by consolidating disparate tools and streamlining processes across devices and operating systems. UEM has expanded beyond management to offer deeper integration with identity, security and remote access tooling to support a zero-trust security model that enables the anywhere workforce. Leading UEM tools are also using analytics and machine learning to enable intelligence-driven experience automation (IDEA) to reduce IT overhead and improve employee experience.

Business Impact

By adopting UEM, I&O leaders can streamline operations and improve endpoint management. Specific impacts include:

- Location-agnostic endpoint management and patching, enabling the anywhere workforce.
- Reduced total cost of ownership (TCO) of managing endpoint devices by simplifying device management and support processes.
- Reduced security risk through support for more device types and OSs, better policy management, and integration with identity, security, and remote access tools.

Drivers

- The anywhere workforce demands tools that extend beyond a single platform or require devices to be on a specific network to function.
- IT looks to simplify and streamline endpoint deployment, management and patching to enable provisioning of new devices for remote employees, improve device performance and reliability as well as visibility across the endpoint estate, and reduce security risk.
- Increasing emphasis on employee experience requires greater visibility into performance, reliability and consistency of endpoints is supported by new UEM tool analytics and automation capabilities.

Obstacles

Though they are reducing as tools mature, obstacles to UEM adoption include:

- Legacy organization models where the responsibility for mobile and PC management, remote access, and security is distributed across several IT teams.
- Gaps in IT's skill set around modern endpoint management, or too much focus on maintaining heavily customized and controlled device configurations.
- Costs can be a concern for organizations that do not currently use mobile device or client management tools.
- Organizations with thousands of group policy objects (GPOs) with little awareness of what each does will struggle to rationalize them in order to migrate to configuration service provider (CSP) profiles.
- Highly complex environments with multiple Active Directory forests or domains, network segmentation, and/or autonomous subsidiaries or business units can also struggle with the centralized nature of cloud-native UEM tools.

User Recommendations

Hype has advanced beyond the trough toward the Slope of Enlightenment as UEM tools have matured and adoption has increased. Some organizations still struggle with the human change management that is required to adapt processes and refocus IT staff on simplifying and modernizing endpoint management.

Gartner recommends:

- Capitalize on pandemic-induced momentum and the need to enable the anywhere workforce to replace disparate MDM and CMT tools and consolidate to UEM as well as embrace modern OS management for Windows 10 and macOS.
- Review IT policies and procedures to identify and eliminate unnecessary references to or dependence on MDM, CMT or location-specific technologies. This will help avoid common inertia, limitations and excuses related to something being against policy.
- Upskill or replace IT engineers and support staff to increase the use of UEM, modern management and automation capabilities.

Gartner Recommended Reading

Magic Quadrant for Unified Endpoint Management

Critical Capabilities for Unified Endpoint Management Tools

Security Best Practices for Work-From-Home Scenarios

Embrace Windows 10 Modern Management to Enable a Highly Distributed Digital Workplace

Predicts 2021: Digital Workplace Infrastructure and Operations

Innovation Insight for Unified Endpoint Security

Data Preparation Tools

Analysis By: Ehtisham Zaidi, Sharat Menon

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Data preparation is an iterative and agile process for cleaning and transforming raw data into curated datasets for data integration, data science/ML and analytics/BI. Data preparation tools promise faster data delivery time by letting business users integrate datasets for their use cases. They allow users to identify anomalies and patterns, and review their findings in a repeatable fashion. Some tools embed machine learning algorithms that automate and augment repeatable data preparation tasks.

Why This Is Important

Data preparation tools are important because they allow less-skilled business analysts, citizen integrators and LOB users to find, enrich and transform their data with minimal coding and data management knowledge. These tools enable self-service data management and integration and use automation to reduce the manual (and often error-prone) interventions needed by business teams before they can make their data fit for purpose prior to analysis in their analytics/BI or data science tools.

Business Impact

Data preparation addresses a major challenge that most analysts, citizen integrators and line-of-business users face, i.e., the time, skills and effort needed to find, transform and deliver data for data and analytics use cases. Modern data preparation tools embed ML algorithms to significantly automate tedious data integration tasks. This allows business teams to prepare their data for faster time to analytics, and, therefore, spend more time doing high-value tasks such as data analysis.

Drivers

- The primary driver for data preparation tools is organizations' desire to improve speed, time to analytics, data sharing and user collaboration, and data science/ML and efficiency while producing trusted and integrated datasets ready for analysis.
- Data preparation tools allow less-skilled users such as citizen integrators, analysts and line-of-business users to perform last-mile data wrangling and transformation without any coding knowledge and minimal IT intervention before they can run analytics.
- Data preparation tools are necessary for data engineering teams to significantly reduce and even automate repetitive data preparation, integration and enrichment tasks so that they can focus on more strategic initiatives and allow business teams to prepare their own data for analysis. This greatly improves their productivity and allows them to focus on more important tasks such as assisting business teams with creating data products and focusing on automation.
- Data science teams demand tools that can significantly reduce the barriers to experimenting with new data sources and application data. Data preparation tools allow data scientists and data engineers to be more flexible with integrating and testing new data sources and targets for their experimental use cases, where data replication with ETL technology will lead to more costs and efforts to manage data pipelines and store data.
- Automating data preparation and integration is frequently cited as one of the major investment areas for data and analytics teams. Data preparation tools that embed AI/ML algorithms drive automation of various repetitive data engineering tasks, which thereby significantly reduces the efforts in integration and change management for data engineering teams.

Obstacles

- Data preparation tools have proved to be successful in enabling business teams to find and transform their own data, but most organizations struggle with "operationalization" of data preparation tasks, i.e., moving the prepared data from sandbox instances to production. This is because most data preparation tools don't provide the necessary capabilities to allow IT teams to regulate the prepared data on acceptable data quality and/or enforce data governance on the prepared data.
- Data preparation tools are sometimes wrongly marketed as a replacement to ETL tools. This leads to wrong expectations and less than optimal performance. Data preparation tools need to be used as a complement to data integration tools and not as a replacement.
- Some data preparation tools don't allow bidirectional exchange of metadata with traditional data management tools like data quality and metadata management tools. This leads to poor scaling of the models created with these tools or even governance chaos.

User Recommendations

- Evaluate data preparation tools that help analysts, data engineers, citizen integrators, data stewards and other analytics authors to enhance and streamline their data preparation time and effort.
- Evaluate data preparation tools for their ability to scale from self-service models to enterprise-level projects.
- Evaluate stand-alone data preparation tools when your use case is a general-purpose one, needing data integration for different analytics and data science tools. By contrast, evaluate the embedded data preparation capability of incumbent tools if you need data preparation only in the context of those tools.
- Give preference to tools that can coexist with other data management tools (such as data quality or data governance) and can capture, analyze and share metadata with them, to ensure governance and compliance.
- Deploy data preparation tools to complement traditional data integration approaches. Do not look to replace traditional data integration tools with data preparation tools.

Sample Vendors

Alteryx; DataRobot; IBM; Informatica; SAS; Talend; Trifacta

Gartner Recommended Reading

Market Guide for Data Preparation Tools

Tool: Evaluate Data Preparation Tools Across Key Capabilities

How to Build a Data Engineering Practice That Delivers Great Consumer Experiences

Magic Quadrant for Data Integration Tools

Critical Capabilities for Data Integration Tools

Toolkit: Job Description for the Role of a Data Engineer

ITSM Tools

Analysis By: Rich Doheny

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

IT service management (ITSM) tools help infrastructure and operations (I&O) organizations manage the consumption of IT services, the infrastructure that supports the IT services and the IT organization's responsibility in delivering business value with these services. These are used mainly by IT service desks and IT service delivery functions to support the tasks and workflows for such processes as incident, request, problem, change, service-level, knowledge and configuration management.

Why This Is Important

I&O leaders require robust ITSM tooling to drive business value in the services they provide. They enable I&O teams to track and report on its processes and workflows that can drive better accountability and support service improvement initiatives. As organizational needs mature, these tools provide insights into their environment to make better decisions, enable process automation and extend business consumer self and peer support capabilities.

Business Impact

ITSM tools are most heavily used by IT service support and IT service delivery functions in all industries to enable the tasks and workflows for processes including incident, request, problem, change, service-level, knowledge and configuration management.

Drivers

- The shift to a more distributed workforce puts pressure on I&O leaders to modernize their support practices and related tooling.
- ITSM vendors are investing in new capabilities supporting more federated and agile ITSM practices, workforce and process optimization, integration with development and collaboration tools, and omnichannel support, including virtual support agents and the use of automation technologies for IT service management (AITSM).
- The ITSM market landscape continues to evolve as significant vendors have consolidated their offerings during the past few years, through mergers and product retirement, and some traditionally midmarket-focused tools have shifted focus to establish upmarket momentum.

Obstacles

- More than 400 vendors offer ITSM products, but most are basic or intermediate tools that focus on IT service desk and ticketing functions targeted at lower-maturity I&O organizations. Despite the large number of participants, the enterprise market is dominated by a small number of vendors.
- With core process workflows built around common frameworks, many vendors in this market struggle to create meaningful differentiated messaging and help their customers justify the ROI.
- Vendors are increasingly concentrating product development on non-ITSM use cases (e.g., HR, facilities and project management) in search of margin and differentiation, as market saturation of basic and intermediate ITSM tools continues. If this continues, vendors investing across ITSM and non-ITSM workflows that lack significant R&D resources will see stagnation in their ITSM products. This will cause a broader functional gap between advanced and basic/intermediate tools.

User Recommendations

- Identify current ITSM needs along with what you can pragmatically deploy over an 18-month roadmap to avoid overspending. Organizations planning to achieve or retain basic to lower-intermediate I&O maturity should consider basic or intermediate tools.
- Avoid costly customization by prioritizing tools that provide advanced process support and AITSM, as well as integrate with broader ITOM solutions, specifically in IT asset management, discovery and IT process automation. This is especially true for high-maturity I&O organizations.
- I&O leaders pursuing DevOps and supporting agile methodologies should select tools that support adaptive process models and integration into their DevOps toolchains.
- I&O leaders must account for the total resource overhead associated with the product by factoring in licensing, cost and timing of implementation, ongoing maintenance, training required, and third-party products (e.g., automation or collaboration tools) to meet their base requirements.

Sample Vendors

Atlassian; BMC; EasyVista; Freshworks; Ivanti; ServiceNow

Gartner Recommended Reading

Magic Quadrant for IT Service Management Tools

Critical Capabilities for IT Service Management Tools

6 Smart Steps for ITSM Tool Selection Success

SD-WAN

Analysis By: Andrew Lerner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Software-defined wide-area network (SD-WAN) products replace traditional branch routers. They provide dynamic path selection based on business or application policy, centralized policy and management of appliances, VPN, and zero-touch configuration. SD-WAN products are WAN transport/carrier-agnostic, and can create secure paths across multiple WAN connections. SD-WAN products can be hardware- or software-based, and managed directly by enterprises or embedded in a managed service offering.

Why This Is Important

SD-WAN improves site availability, cost and performance for enterprise WANs, and is aligned with the broader shift of applications to public cloud workloads. There is high client interest in SD-WAN products, and we estimate that more than 50,000 customers have deployed SD-WAN products in production networks. Further, we expect continued rapid growth of SD-WAN deployments, and forecast vendor revenue to grow at a more than 20% compound annual growth rate (CAGR) for the next three years.

Business Impact

SD-WAN products create simpler and more cost-effective branch office WANs that map to modern application and cloud architectures. These products are significantly faster, easier to deploy and more manageable than traditional, router-based solutions. The benefits of an SD-WAN include reduced capital and operational expenditures (capex/opex) at the WAN edge, reduced device provisioning times, easier alignment with applications, and enhanced branch availability, compared with traditional routers.

Drivers

- Digitalization and cloud adoption are driving more applications out of private data centers and to public Internet, including SaaS and public cloud providers.
- In conjunction with hybrid or all-internet WAN topologies, SD-WAN improves availability, cost and performance for enterprise WANs.
- Organizations moving to hybrid or internet-only WAN transport are driven toward SD-WAN products because of their improved path-selection functionality and manageability.
- Several dozen vendors are competing in the market, including incumbent network and security vendors, startup vendors and smaller vendors with a regional or vertical focus. These vendors are aggressively pushing SD-WAN products and services to enterprises.

Obstacles

- Inability to get out of an existing equipment or service provider contract.
- WAN architecture is not hybrid and/or branch locations have only a single connection.
- Lack of budget.
- Closure of remote locations due to broader business reasons.
- Lack of cloud adoption, which reduces the benefits of hybrid WAN architectures.
- Limited need for increased branch availability.
- Inability to utilize the internet as transport, often due to compliance or security concerns, or lack of reliable connectivity.
- Existing WAN edge products (firewalls/routers) are good enough to meet business requirements.

User Recommendations

- Refresh your branch WAN equipment by implementing SD-WAN when you're migrating apps to the public cloud, building hybrid WANs, equipment is at end of life, or managed network service/MPLS contracts are renewing.
- Follow a thorough SD-WAN selection process by shortlisting a diverse set of vendors/providers and running a pilot.
- Include network security teams in the design, planning and implementation, because SD-WAN-enabled hybrid WANs directly affect placement of security controls, such as firewalls and secure web gateways (SWGs). SD-WAN should be designed in conjunction with a SASE architecture.

Sample Vendors

Cisco; Citrix; Fortinet; Hewlett Packard Enterprise (HPE); Palo Alto Networks; Versa Networks; VMware

Gartner Recommended Reading

Magic Quadrant for WAN Edge Infrastructure

Critical Capabilities for WAN Edge Infrastructure

Magic Quadrant for Network Services, Global

Toolkit: RFP Template for Managed and DIY SD-WAN Products and Services

2021 Strategic Roadmap for SASE Convergence

Citizen Developers

Analysis By: Jason Wong

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Citizen developers are employees not in the IT organization who create or extend application capabilities, mainly for internal consumption by teams or workgroups. They can use development tools and runtime environments sanctioned (or at least not actively forbidden) by corporate IT or the business units. A citizen developer is not a title, role or professional developer in the business unit, but rather a persona taken on by an employee.

Why This Is Important

Citizen development is part of the business-IT continuum and the democratization of technology trends. Business leaders are increasingly owning their departmental applications, as well as building an increasing number of applications themselves. The COVID-19 pandemic and remote working have accelerated the need for greater business agility and putting better tools in the hands of employees so they can more rapidly solve their problems with new apps and automation.

Business Impact

The long-term strategic impact of citizen development is enabling self-service business innovation within business units. Citizen developers are often aided by IT in some aspects of co-creation or technical support. They can generate new ideas leading to greater business agility, as well as increased workforce efficacy and efficiency. Citizen development hackathons are a great way to promote and foster citizen development, while enhancing digital dexterity across the enterprise.

Drivers

- According to a 2021 Gartner survey on Reimagining Technology Work, 41% of respondents can be classified as business technologists. These are employees who don't report into an enterprise or business unit IT function yet they use tools to produce some technology output, such as analytics reports, apps or automation. (Note: Some of these business technologists are professional developers, such as software engineers, working in a business unit like marketing, or research and development. These professionals are not citizen developers, but do work with citizen developers.)

- Employees have easier access to more tools than ever before, and it's only increasing. A citizen developer is not a full-time professional developer, nor a specific role, but rather a persona of a business technologist using these tools. They may have some job responsibility to develop a solution, or simply choose to engage in development activities to achieve some business outcome for the greater good. Gartner's 2021 Hyperautomation Survey found that business technologists working on business-driven automation initiatives use on average 2.7 tools (out of 21 tools shown).

- Citizen developers feel more empowered by powerful low-code development tools and "no code" tools that specifically cater to them. Many vendors now provide robust low-code development platforms making it easier for citizen developers to develop their own applications — even applications that once required professional development skills, such as building mobile apps or using AI automation services like chatbots.

- Citizen developers may also take on other citizen personas depending on their skills, ambition and scope of work. Gartner often sees citizen data scientist, citizen integrator and citizen automator personas in the digital workplace. Over time, some of these citizen developers have become part of fusion teams including business and IT collaboration and development.

Obstacles

- IT leaders often have a negative view of development outside of IT and label it as "shadow IT." Citizen development is not shadow IT. IT's resistance to recognizing business technologists' work and embracing citizen development results in missed opportunities to drive toward business and IT alignment.
- IT leaders also often fear losing control on account of increasing citizen development activities, making their teams less relevant or burdening IT with unmaintainable apps. However, the risks of citizen development are typically outweighed by the benefits. Risks to IT can be better managed by directly addressing inadequate tooling and disorganized support for a citizen development community, which are key factors leading to poor outcomes and risky apps.

User Recommendations

- Engage nonprofessional business technologists more actively to enlist and enable them to become citizen developers. Ignoring or attempting to prevent citizen development often carries more risks and limits enterprise innovation.
- Mitigate shadow IT risks by working with business unit leaders to enlist citizen developers to establish trust and define safe activity zones.
- Enable self-governing citizen development practices by fostering a community of practice (CoP) across business units and with IT.
- Improve outcomes for citizen-developed apps by joint (business and IT) selection of the right tools and enabling technologies.

Gartner Recommended Reading

How to Define and Guide Citizen Development Practices

Platform-Enabled Citizen Development (BP)

Democratize and Distribute Technology Work Across the Entire Enterprise to Accelerate Digital Business

Endpoint Detection and Response

Analysis By: Paul Webber, Jon Amato

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

EDR solutions can detect and investigate security events, contain attacks and produce remediation guidance. They must analyze user, process and system activity and device configuration. Reporting of user and device data is combined with direct intervention to detected events. Automated response and rollback of threats are desirable, integration and automation with other tools are key. Cloud hosting is predominant; some vendors can host on-premises for non-internet-connected systems.

Why This Is Important

All systems exposed to the internet, or attached to internal networks, are potentially at risk from attacks that often target vulnerable or unprotected systems. EDR is an essential part of the overall defense. It should be deployed to all managed systems in order to identify anomalous or malicious activity, reveal the tactics and techniques of advanced attacks and provide a means to respond to them.

Business Impact

- EDR is a must-have layer of protection for all industry sectors and should be applied to all devices and servers that connect to a network or handle corporate data.
- Early detection and rapid response are now vital, as prevention alone is not a viable way to approach contemporary threats and exploits.
- EDR is often stipulated as a mandatory security control in both internal and external policy.
- EDR provides the last means of defense when other layers fail to stop an exploit.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention and protection, and older EPP tools should be updated to have EDR functionality. Stealthy and state-sponsored adversaries, as seen in recent supply chain attacks, use advanced techniques to remain undetected and to bypass security controls.
- Remote work has accelerated the adoption of cloud-managed offerings, which now represent 60% of the install base and 95% of all new deployments.
- Fileless attacks are now a common component of all malware types, making the behavioral protection of EDR tools a critical capability to combat both advanced threats and an increasingly capable range of human-operated Ransomware campaigns.
- Advanced adversaries targeting an organization have shown they can disable protection solutions, making anti-tamper protection a critical facility. Comprehensive alerting and telemetry to facilitate early detection and fast response are also needed.
- As threats may target any system, EDR should now be a mandatory critical capability in the overall set of layered endpoint security controls, deployed to all managed endpoints and servers.
- The ability to rapidly respond in real time as incidents unfold is critical to containing the threat and stopping it from spreading.
- Augmenting existing vulnerability management programs and providing a means to reduce the attack surface is increasingly needed to ensure systems are not misconfigured and have no unpatched vulnerabilities.
- The collection of logs and events from EDR agents can also be used for retrospective threat detection and threat hunting.
- EDR tools often add the ability to manage adjacent risks such as the encryption of storage media, control of applications and internet activity.
- The increased stealth of advanced threats, human operated ransomware and state sponsored attacks, requires a new breed of security tools that work holistically together across all of the control areas of a complex attack.

Obstacles

- Adding detection and response features is now considered mainstream, though many organizations still lack the skills to use them.
- EDR adoption must be accompanied by investment in training responders, including “range” training that simulates real attacks.
- Organizations with few skilled staff should opt for managed detection and response services that provide monitoring, alerting and often triaging of alerts.
- Early definition-based agents needed frequent updates and used considerable amounts of system resources, leading to distrust of endpoint agents.
- Cloud-hosted workloads often have radically different “agile” deployment pipelines that preclude the use of traditional endpoint security tools. This usually results in a split environment, using separate tools for agile deployed workloads.
- Feature parity is not guaranteed for non-Windows systems. Consequently, endpoint security solutions for these systems lack the full EDR range of detection and response facilities.

User Recommendations

- Identify a single lightweight agent with remote deployment and low maintenance.
- Prefer cloud-hosted EDR solutions with faster time to value and vendors that provide automated processes.
- Target vendors that provide managed services themselves, including alerting, monitoring, incident response and managed detection and response.
- Favor vendors that can remove vulnerabilities and harden the endpoint against attack. They should provide direct access to endpoints to rapidly respond to issues.
- Look for third-party integrations with the ability to reuse existing investments like ITSM, authentication and threat intelligence.
- Specify tools with anti-tamper to ensure that agents are not disabled by attackers.
- Ensure data retention is adequate, uses archiving for cheaper storage and sends events and alerts to other security tools for longer retention.
- Seek ways to augment the solution with other security telemetry sources and integrated actions between tools, as provided by XDR systems.

Sample Vendors

Bitdefender; Cisco; CrowdStrike; Cybereason; FireEye; Microsoft; Palo Alto Networks; SentinelOne; Trend Micro; VMware Carbon Black

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy?

Hyperconvergence

Analysis By: Philip Dawson, Jeffrey Hewitt

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Hyperconvergence combines storage, computing and networking into a single system in an effort to reduce data center complexity and increase scalability. Multiple servers can be clustered together to create pools of shared compute and storage resources, designed for convenient consumption. Sales models included appliances and reference architectures using certified servers or delivered as a service or in a public cloud.

Why This Is Important

IT leaders seeking solutions that obviate the requirement for proprietary, external controller-based storage that permit a single management interface across silos of infrastructure and that can be cost-effective for certain use cases (e.g., VDI, edge/IOT, hybrid cloud) will consider hyperconvergence as a viable option.

Business Impact

Hyperconvergence enables IT leaders to be responsive to new business requirements in a modular, small-increment fashion, avoiding the large-increment upgrades typically found in three-tier infrastructure architectures.

Hyperconvergence is of particular value to midsize enterprises that can standardize on hyperconvergence and the remote sites of large organizations that need cloudlike management efficiency with on-premises edge infrastructure.

Drivers

- Hyperconvergence provides simplified management that decreases the pressure to hire hard-to-find specialists. Adoption is greatest in dynamic organizations with short business planning cycles and long IT planning cycles tied to hybrid cloud delivery. The HCI market is now trifurcating, centering around the data-center-led "hybrid cloud" cloud management use case, VDI use case and an "edge/IoT"' remote management use case.
- Hyperconvergence leads to lower operating costs, especially as it supports a greater share of the compute and storage requirements of the data center.
- VMware vSAN utilization among VMware ESXi customers, and Microsoft Azure HCI and Storage Spaces Direct utilization among Microsoft Windows Server 2016 and 2019 Datacenter edition customers, are on the rise.
- Larger clusters are now in use, and midsize organizations are beginning to consider hyperconvergence as the preferred alternative for on-premises infrastructure for block storage.
- Nutanix, an early innovator in HCIS appliances, has largely shifted to a software revenue model and continues to increase its number of OEM relationships and partners.
- Hyperconvergence vendors are achieving certification for more-demanding workloads, including Oracle and SAP, and end users are beginning to consider hyperconvergence as an alternative to integrated infrastructure systems for some workloads.
- As more vendors support hybrid and public cloud deployments, hyperconvergence will also be a stepping stone toward public cloud agility. Meanwhile, suppliers are expanding hybrid cloud deployment offerings.
- A growing number of hyperconvergence suppliers are delivering scale-down solutions to address the needs of remote office/branch office (ROBO) and edge environments typically addressed by niche vendors.

Obstacles

- Applications designed for scale-up architectures (as opposed to scale-out) are unlikely to meet cost/performance expectations when deployed on hyperconverged infrastructure.
- The acquisition cost of hyperconvergence may be higher and the resource utilization rate lower than for three-tier architectures.
- While HCI has somewhat matured from a hypervisor compute and storage function, networking is still split between hardware SDN and networking around SD-WAN driving edge deployments.
- For large organizations, hyperconverged deployments will remain another silo to manage.

User Recommendations

- Implement hyperconvergence for hybrid cloud infrastructure when agility, modular growth and management simplicity are of greatest importance.
- Establish that hyperconvergence requires alignment of compute, network and storage refresh cycles; consolidation of budgets; operations and capacity planning roles; and retraining for organizations still operating separate silos.
- Test the impact on DR and networking 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.
- Choose HCI appliance options to enable scale-down optimization of resources for high-volume edge deployments.
- Ensure that clusters are sufficiently large to meet performance and availability requirements during single and double node failures, and require proof-of-concept to reveal any performance anomalies.

Sample Vendors

Cisco; Dell EMC; Microsoft; Nutanix; Pivot3; VMware

Gartner Recommended Reading

Magic Quadrant for Hyperconverged Infrastructure Software

Critical Capabilities for Hyperconverged Infrastructure Software

Toolkit: Sample RFP for Hyperconverged Infrastructure

The Road to Intelligent Infrastructure and Beyond

CASBs

Analysis By: Craig Lawson, Neil MacDonald

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud access security brokers (CASBs) provide crucial cloud governance controls for visibility, compliance, data security and threat protection by consolidating multiple types of security policy enforcement into one place for SaaS, IaaS and PaaS. Examples include authorization, UEBA, adaptive access control, DLP, device profiling, object encryption, tokenization, logging, alerting and malware removal. Majority of CASB deployments are cloud-based; on-premises deployments are rare.

Why This Is Important

CASBs are critical for organizations to secure usage of business-critical cloud services. The four key areas — visibility, compliance, data security and threat protection — are the primary value propositions for the usage of CASBs.

Business Impact

CASBs enable consistent security policies and governance across cloud services. Unlike traditional security products, CASBs are designed to protect data stored in someone else's systems, are suitable for organizations of all sizes in all industries and can demonstrate cloud usage is well-governed. With continued feature expansion, ongoing convergence with SWG/ZTNA and relative ease of switching providers, favor one-year contract terms over lengthier ones when selecting CASBs.

Drivers

- End-user organizations need to secure use of business-critical, cloud-delivered applications and infrastructure; secure general internet to prevent threats to users, regardless of their location; and improve access to existing services while taking advantage of zero trust concepts. Today, CASB is converging with SWG and ZTNA to deliver this “three-legged stool” concept to support all these use cases.
- With SWG vendors enabling secure use of business-critical, cloud applications and infrastructure, and CASB vendors expanding functionality for general internet security and access to existing services, security leaders are now able to successfully deliver on the above-mentioned three capabilities from an increasing number of vendors providing all three.
- The COVID-19 pandemic has increased focus on two specific use cases that CASB technology directly helps with: the huge shift to remote working and the continuously increasing use of cloud services critical to business.

Obstacles

- Lack of a focus on DLP can lead to frustration with a CASB as organizations fail to build comprehensive policies and manage false-positive rates.
- A subset of controls are offered by CSPs themselves, for example, Office 365’s native security features and Salesforce Shield.
- Unclear organizational ownership of SaaS tenancy leads to a CASB implementation that fails to secure the SaaS adequately.
- Product consolidation failure in organizations where multiple CASBs exist through expanded licensing agreements.
- Overlapping CASB functionality from a number of vendors leads to duplication and confusion.

User Recommendations

- Examine vendor capabilities in four functionality areas: visibility, data protection, threat detection and compliance (see Magic Quadrant for Cloud Access Security Brokers for a more detailed analysis of these capabilities).
- Seek support for multiple modes of operation, namely forward proxy, reverse proxy (or RBI) and API for the best support of managed and unmanaged devices and cloud services via CASB.
- Aim to move to a single provider for CASB, SWG and ZTNA as these services are on strong convergence paths.

Sample Vendors

Bitglass; Broadcom (Symantec); Lookout (CipherCloud); McAfee; Microsoft; Netskope; Proofpoint

Gartner Recommended Reading

Magic Quadrant for Cloud Access Security Brokers

Critical Capabilities for Cloud Access Security Brokers

Magic Quadrant for Secure Web Gateways

2021 Strategic Roadmap for SASE Convergence

Market Guide for Zero Trust Network Access

Disaster Recovery as a Service

Analysis By: Ron Blair

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

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

Why This Is Important

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

Business Impact

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

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

Drivers

- Initially, DRaaS was primarily attractive to small or midsize businesses (SMBs). This was because DRaaS freed up the time of the IT staff in these businesses, and, in many cases, they lacked a secondary recovery data center and experienced support staff. As DRaaS has matured, it has become an attractive option for larger organizations that want to free up resources from managing routine operational tasks to focus on what they deem as more value-added activities. This has resulted in more complex and larger implementations. At one time, it was rare to find engagements larger than 250 server images; engagements now protect 1,000 or more server images.
- Due to COVID-19 and other recent events, organizations are reassessing other vulnerabilities. As a result, more focus is being placed on improving DR posture, as well as revisiting, and often accelerating, data center and cloud strategies.
- DRaaS vendors include a mix of service providers. For most, DRaaS is not their primary revenue-generating service. Some also support communications services, traditional subscription-based recovery services, colocation, managed hosting, infrastructure as a service (IaaS) and managed backup services. So, although the client's interest in DRaaS may be initially DR-oriented, DRaaS providers are often well-suited to meet related data center or IaaS needs as well.

Obstacles

Potential obstacles:

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

Leading DRaaS providers have several responses:

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

User Recommendations

DRaaS is ideal when:

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

When considering DRaaS providers:

- Become familiar with the DRaaS providers and types per the DRaaS Market Guide below.
- For more complex environments, consider DIY enablers such as those in the ITRO Market Guide below.
- Engage Gartner analysts to help determine fit and for assistance on approach and selection.
- Compare options via the downloadable spreadsheet in How to Determine If DRaaS Will Save Money.

Gartner Recommended Reading

Market Guide for Disaster Recovery as a Service

Market Guide for IT Resilience Orchestration

How to Determine If DRaaS Will Save Money

Entering the Plateau

Network Access Control

Analysis By: Claudio Neiva

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Network access control (NAC) enables organizations to implement policies and control access to corporate infrastructure by both user devices and cyber physical devices such as the Internet of Things (IoT) and operational technology (OT) devices. Policies may be based on authentication, endpoint configuration (posture) or users' role/identity. NAC can also implement postconnect policies based on integration with other security products.

Why This Is Important

Visibility and control for access to an organization's local IT infrastructure remain part of the protection strategy to reduce the attack surface. However, the cyber-physical system (CPS) for IoT and OT devices drives specific sectors, such as manufacturing, critical infrastructure and health, to consider CPS-centric security technologies to increase NAC.

Business Impact

The NAC market is considered mature with slow growth and acquisition of existing vendors (i.e., Pulse Secure and Inverse). In addition, the primary use case for implementing NAC is visibility and access control of equipment in the local infrastructure of the organization. NAC represents an important tool to apply segmentation and isolation of endpoints that may represent a risk to the entire infrastructure.

Drivers

- Preconnect or postconnect authentication approach. The preconnect authentication can be thought of as a "guilty until proven innocent" model ("default deny"); whereas postconnect authentication can be considered an "innocent until proven guilty" model ("default allow").

- Visibility into on-premises infrastructure connected devices with the goal of implementing access policies. This includes commonly used devices (such as a workstation, laptop, printer, IP phone, IP camera, access points and IoT devices like OT devices, medical devices and building automation).
- Management of corporate network access for different types of users and devices, such as employees, contractors, consultants and guests, using either corporate-owned or user-provided endpoints.
- Ability to analyze compliance with a minimum security posture at the endpoint and provision of a quarantine network for devices not in compliance via Change of Authorization (CoA). If not compliant, that device is only allowed access to a quarantine VLAN until those items are remediated.
- Interoperability with other security solutions. Integration with other solutions can happen in two ways: customization through open APIs or the use of built-in integration.

Obstacles

- NAC's focus is primarily as an on-premises control for devices and users, and can be expensive and difficult to implement at scale across an organization.
- NAC uniquely satisfies multiple security use cases for user and device security on the corporate network. However, depending on the organization's need, a combination of different solutions such as ZTNA, unified endpoint management (UEM) and CPS-specific security products might provide the same features and benefits as an NAC provider.
- Future security roadmaps may dictate implementation of a secure access service edge (SASE) framework that includes ZTNA products. ZTNA addresses some narrow NAC use cases for user-to-application segmentation and may influence the overall scope of an NAC implementation when considering both remote and on-premises security authentication and authorization policies for devices and users.

User Recommendations

- Focus on vendors that target organizations of your size and complexity and, in some instances, industry vertical or region. Because NAC is a mature market, many vendors are clearly aligned regarding small and midsize businesses and large-enterprise opportunities or specialize in certain industry verticals and regions such as Europe and Southeast Asia.

- Perform an initial network inventory before selecting an NAC vendor. This will influence your decision based on the capabilities of your network switches and routers, as well as help with budgeting since many NAC vendors license based on the number of IP addresses protected.
- Determine which UEM solutions are already installed on the network to identify providers that have direct integration with existing UEM solutions.
- Implement NAC to deliver visibility and control over your corporate network. Integrate with existing asset management solutions bidirectionally to help maintain an accurate list of devices connected to the organization.

Sample Vendors

Akamai; Auconet; Cisco; CommScope; Extreme; Forescout Technologies; Fortinet; Hewlett Packard Enterprise; InfoExpress; Ivanti; macmon secure; Open Cloud Factory; OPSWAT; Portnox

Gartner Recommended Reading

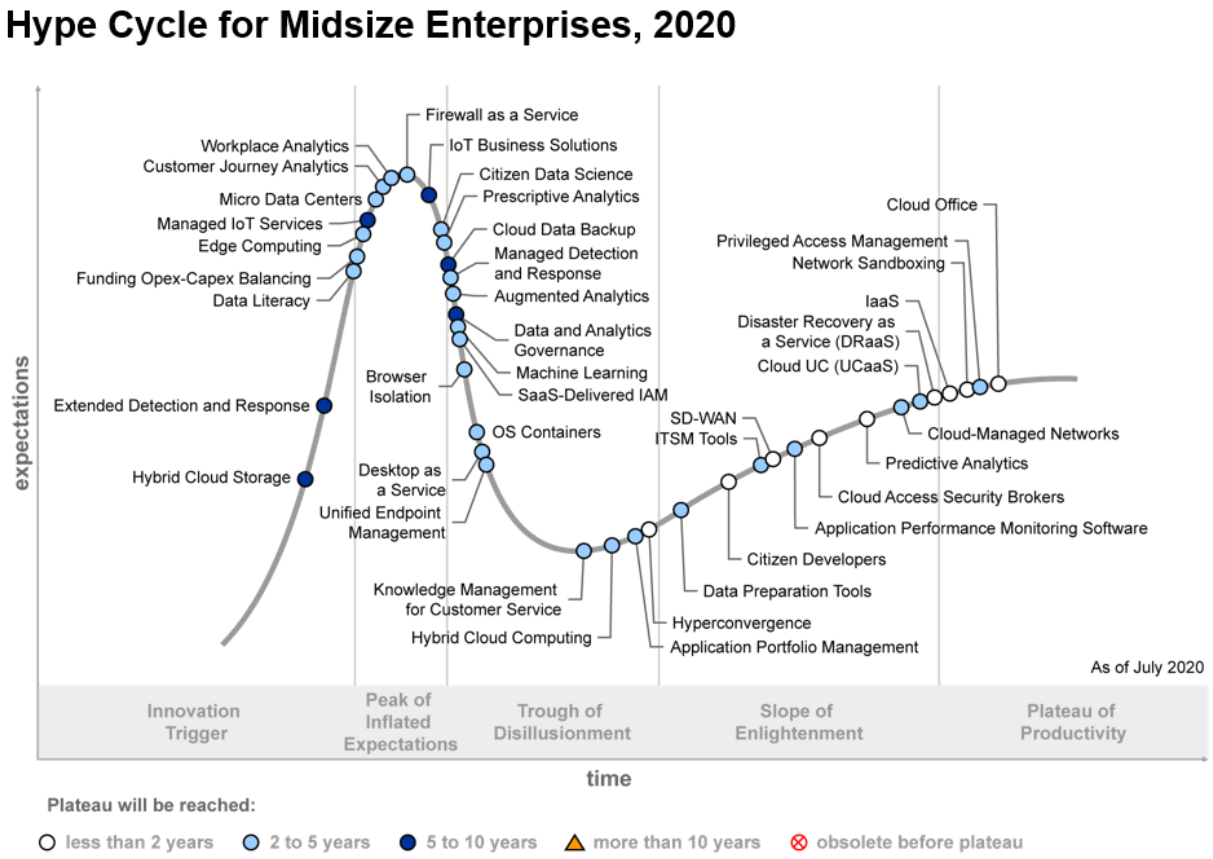
Market Guide for Network Access Control

Toolkit: Sample RFP for Network Access Control

Solution Path for Evolving to Next-Generation Enterprise Networks

Appendixes

Figure 2. Hype Cycle for Midsize Enterprises, 2020



Source: Gartner
ID: 448173

Gartner

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

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

Source: Gartner (July 2021)

Table 3: Benefit Ratings

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

Source: Gartner (July 2021)

Table 4: Maturity Levels

(Enlarged table in Appendix)

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

Source: Gartner (July 2021)

Document Revision History

Hype Cycle for Midsize Enterprises, 2020 - 30 July 2020

Recommended by the Authors

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

Leadership Vision for 2021: Midsize Enterprise Infrastructure and Operations

Using a Single IaaS Provider Ecosystem Is Sound Infrastructure Strategy for Midsize Enterprises

Strategies for Midsize Enterprises to Mitigate the Insider Threat

Quick Answer: Insourced, Hybrid or Outsourced? Find the Best Security Operations Center Approach for You

A Practical Data and Analytics Strategy and Operating Model for Midsize Enterprises

Answers for Midsize Enterprises Building a Data and Analytics Team

Table 1: Priority Matrix for Midsize Enterprises, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	CASBs OS Containers	Augmented Analytics Citizen Data Science Edge Computing IoT Business Solutions Micro Data Centers SASE		

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	*2 - 5 Years* ↓	*5 - 10 Years* ↓	*More Than 10 Years* ↓
High	Citizen Developers Data Preparation Tools Endpoint Detection and Response Hyperconvergence SD-WAN	Application Portfolio Management Application Security Requirements and Threat Management Data and Analytics Governance Data Breach Response Data Literacy Desktop as a Service Funding Opex-Capex Balancing Hybrid Cloud Computing ITSM Tools MDR Services NDR Network Access Control Prescriptive Analytics UEM Workplace Analytics	BEC Protection Distributed Cloud Hybrid Cloud Storage Managed IoT Services XDR	

Benefit ↓	*Years to Mainstream Adoption*			
	Less Than 2 Years ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Moderate	Disaster Recovery as a Service IT Resilience Orchestration SaaS Management Platforms	Firewall as a Service	Cloud Data Backup Container Backup Immutable Infrastructure	
Low				

Source: Gartner (July 2021)

Table 2: Hype Cycle Phases

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

Phase ↓	Definition ↓

Source: Gartner (July 2021)

Table 3: Benefit Ratings

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

Source: Gartner (July 2021)

Table 4: Maturity Levels

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

Source: Gartner (July 2021)