Gartner®

Hype Cycle for Business Continuity Management and IT Resilience, 2021

Published 12 July 2021 - ID G00747421 - 74 min read

By Analyst(s): David Gregory, Jerry Rozeman

Initiatives: Technology, Information and Resilience Risk

The COVID-19 pandemic, along with regulations, cyberattacks and increasing dependency upon digital systems, are driving organizations to embrace IT and business continuity management. Use this Hype Cycle to identify solutions that fulfill resilience, availability and recovery needs.

Analysis

What You Need to Know

Boards of directors and senior management are increasingly aware that business disruptions of any type are impactful and require an increased focus on business and operational resilience. With the move to digital business, any minor IT outage can have a major impact on revenue, costs and customer experiences. Participation in business ecosystems posits new revenue generation opportunities, as well as new risks and greater harm potential due to the increased interdependency and complexity.

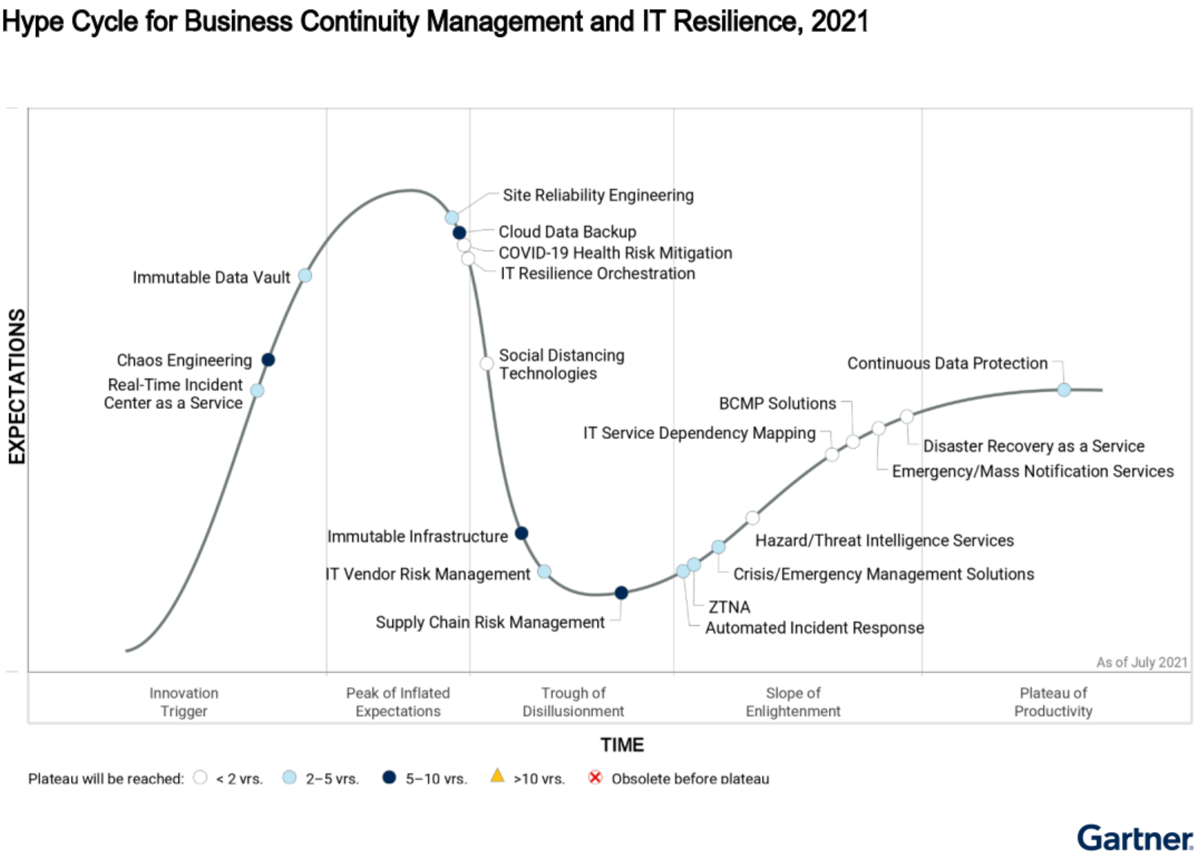
Security and risk management leaders and IT leaders responsible for IT resilience, disaster recovery and business continuity management (BCM) must work with the business to become innovative. They must create processes, practices and platforms to meet the “available 24/7 from anywhere” expectations of customers and the workforce. The cost of not being resilient can be severe, if not fatal for an organization. Therefore, resilience must be deliberately designed so that it is earned and learned by people, processes and technologies. This will ensure that resilience is adaptable, extensible, responsive, proactive and integrated.

The Hype Cycle

The purpose of BCM and IT resilience — both components of an organizational resilience program — is to increase an organization's capabilities for availability and recovery at all levels after facing a business disruption. Gartner believes that, while many organizations are starting to turn their attention to organizational resilience, it will still be five years or more before these practices become a holistic process across operational activities within the organization. Security and risk management leaders and IT leaders responsible for IT resilience, disaster recovery and BCM should be aware of the following changes to the 2021 Hype Cycle:

- A renewed focus on IT resilience innovations that proactively seek to improve operations abilities in order to prevent outages from occurring and recover faster.
- Resilience is a multipronged effort that spans infrastructure, and is also vital to build into the platform and applications that are being developed and deployed.
- Cybersecurity is vital in eliminating potential attack surfaces, while reducing the number of failure points and increasing IT resilience.
- Data backup, replication and storage practices continue to evolve and are vital for IT resilience efforts, as they serve as the backbone for recovery capabilities from both physical and logical failures.
- Cloud usage for production workloads and as a recovery location for on-premises environments is accelerating, necessitating the adoption of disaster recovery innovations that utilize or assist with those efforts.
- BCM practices are maturing, with fewer innovations appearing in the innovation region of the Hype Cycle. In fact, most are clearly on the Slope of Enlightenment, as they are being adopted by organizations growing the maturity of their response, recovery and restoration efforts.
- The resilience of IT systems and the overall continuity of business operations are paramount to serving customers and are increasingly becoming regulatory concerns. As more digital transformation occurs, this will only accelerate, requiring increased investment in the innovations listed here.

Figure 1: Hype Cycle for Business Continuity Management and IT Resilience, 2021



Source: Gartner (July 2021)

Downloadable graphic: Hype Cycle for Business Continuity Management and IT Resilience, 2021

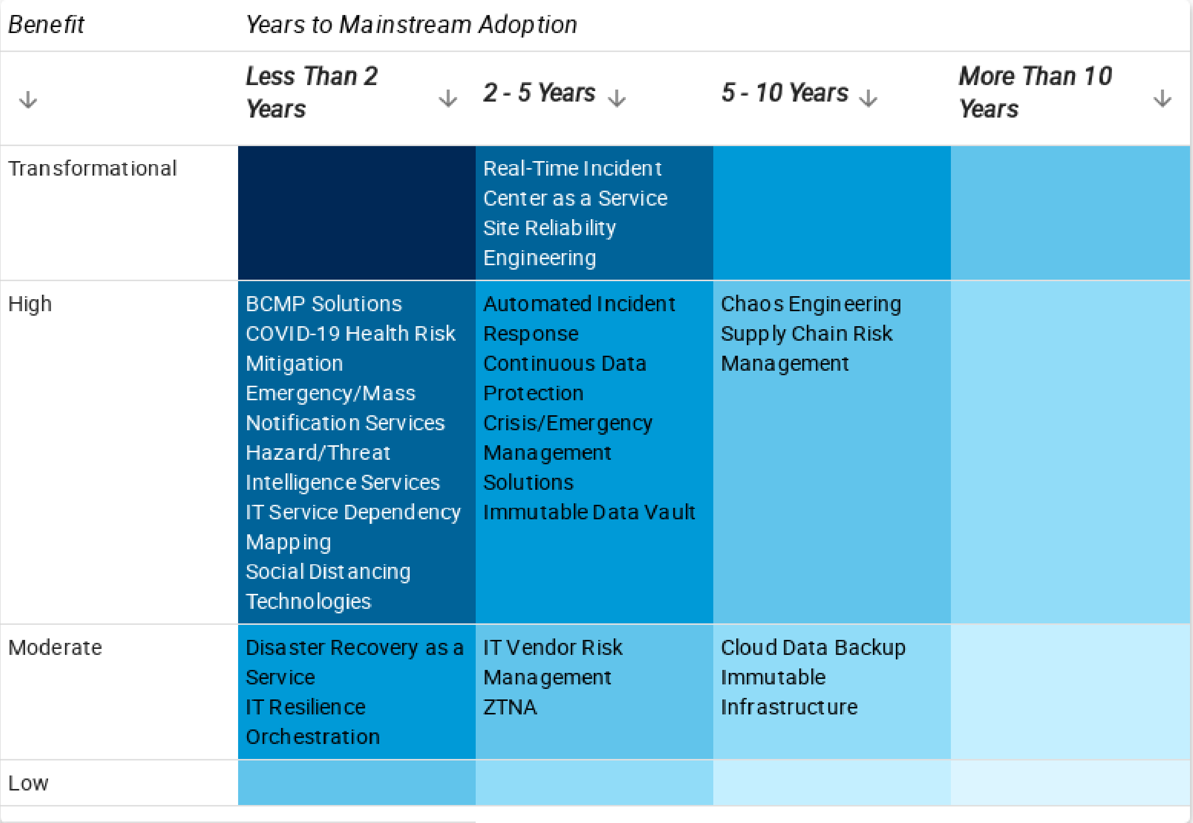
The Priority Matrix

The BCM and IT Resilience Priority Matrix shows the business benefit ratings of the continuity and recovery technologies on the 2021 Hype Cycle. The Priority Matrix maps the benefit rating of a process or technology against the length of time that Gartner expects it will take to reach the Plateau of Productivity.

This alternative, easy-to-read grid format helps users determine how to prioritize their IT resilience and BCM investments. In general, companies should begin in the upper-left quadrant of the chart, where the processes and technologies have the most dramatic impact on ensuring a strong ability to recover and restore business and IT operations after a business disruption. Organizations should continue to evaluate alternatives that are high impact, but further out on the timeline, as well as those that have less impact, but are closer in time to mainstream adoption.

Table 1: Priority Matrix for Business Continuity Management and IT Resilience, 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		Real-Time Incident Center as a Service Site Reliability Engineering		
High	BCMP Solutions COVID-19 Health Risk Mitigation Emergency/Mass Notification Services Hazard/Threat Intelligence Services IT Service Dependency Mapping Social Distancing Technologies	Automated Incident Response Continuous Data Protection Crisis/Emergency Management Solutions Immutable Data Vault	Chaos Engineering Supply Chain Risk Management	
Moderate	Disaster Recovery as a Service IT Resilience Orchestration	IT Vendor Risk Management ZTNA	Cloud Data Backup Immutable Infrastructure	
Low				

Source: Gartner (July 2021)

On the Rise

Real-Time Incident Center as a Service

Analysis By: Michael Brown

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A real-time incident command center fuses information from various sources and provides visualization to improve situational awareness capability. It is a type of command-and-control (C2) enabling service used by public safety agencies to coordinate responses to emergencies and other events. Typically created and managed by public safety organizations through integration of databases, sensor, video and communications systems, that outcome is becoming available in as-a-service form.

Why This Is Important

Information fusion and C2 are ubiquitous to public safety. Early examples include real-time crime centers. Full-spectrum incident management, enabled by information fusion and C2 technology, has emerged. Service providers now offer real-time incident management as a service. Jurisdictions with earlier crime-focused capabilities will seek next-generation full incident management capability. Jurisdictions lacking wherewithal for a command center now have opportunities with as-a-service offerings.

Business Impact

Public safety mission operators and their technology support organizations are primary stakeholders. Citizens are stakeholders regarding surveillance aspects such as video or license plate readers. Use of the technology can alter deployment and focus of resources. Improved citizen service through better emergency response is the leading advantage. With an as-a-service offering simplifying the creation of a real-time function, some agencies may gain capability where formerly unable.

Drivers

Real-time incident command center as a service is an outgrowth of earlier approaches and is enabled by supporting technology advancements:

- Next-generation real-time crime centers (RTCC) — RTCCs are the forerunner for real-time incident management. Earliest implementation of an RTCC dates to 2005 with many jurisdictions subsequently adopting some form of information fusion and C2 technology. The growth has been driven by citizen expectations to achieve crime reduction and government budget constraints that demand efficient use of public safety resources. While law enforcement was the initial use of information fusion and C2 to improve situational awareness and deployment of limited resources, more generalized use cases demand the same approach. Wildfire management, natural disasters, special events and pandemic response are some nonpolicing examples where real-time incident management is necessary.

- IP-enabled everything — The IP enablement of much of the communications, sensor and surveillance capabilities of public safety fosters integration. Bringing together information assets like databases, radio, video, IoT, mass notification, geographic information systems, license plate readers and geolocation tracking cannot be trivialized, but with each of these sources being digitized, the integration problem is made more simple. The lower cost of integration, IoT and SaaS delivery model is enabling and driving the ability for public safety jurisdictions to have a more sophisticated, near-military-level operational picture and C2 capability.

Obstacles

- Interagency cooperation — The information fusion aspect and unified C2 of real-time incident management inherently means sharing. The information assets will be owned by multiple agencies. For regional cooperative approaches, the information assets will not even reside in a single jurisdiction.

- Cost — This will limit deployment to larger jurisdictions or entail cooperative relationships among smaller jurisdictions. Grants or other forms of capital investment often used for new public safety capabilities will not address recurring cost of incident management center staffing and technology subscription or maintenance fees.

- Citizen privacy concerns — Civil liberties advocates may have issues relative to surveillance. Increased use of video or other surveillance technology that occurs in real-time incident command centers will encounter public resistance wherever such resistance is politically permissible.

User Recommendations

Growth of the real-time incident management, increasingly enabled by as-a-service offerings is critical to satisfy mission needs and resource utilization efficiency. CIOs supporting public safety agencies should:

- Begin interagency collaboration by itemizing information assets and owners, determining the information value and the willingness to share.
- Estimate costs by conducting market analysis for integration products and services, and developing staffing profiles for the incident management center.
- Address possible citizen privacy concerns by engaging in outreach efforts to explain use, benefits and protections for surveillance capabilities.

Sample Vendors

Fusus; Hexagon; Mutualink; Rave Mobile Safety; Verizon

Chaos Engineering

Analysis By: Jim Scheibmeir, Dennis Smith

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Chaos engineering is the use of experimental and potentially destructive failure testing or fault injection testing to uncover vulnerabilities and weaknesses within a complex system. It is systematically planned, documented, executed and analyzed as an attack plan to test components and whole systems both before and after implementation. Chaos engineering is often utilized by site reliability engineering teams to proactively prove and improve resilience during fault conditions.

Why This Is Important

Many organization's stake success on test plans that overemphasize software functionality and underemphasize the importance of validating the system's reliability. Chaos engineering (CE) moves the focus of testing a system from the "happy path" — instead, testing how the system can gracefully degrade or even continue to be useful while under various levels of impact. CE can also help identify where product documentation is less than sufficient or understanding of a system is lacking or siloed.

Business Impact

With chaos engineering, we minimize time to recovery and change failure rate, while maximizing uptime and availability. Addressing these elements helps improve customer experience, customer satisfaction, customer retention and new customer acquisition.

Drivers

- Gartner's 2020 Achieving Business Agility with Automation, Continuous Quality and DevOps Survey found that 18% of respondents were currently using or planning to use chaos engineering to improve software quality.
- Complexity in systems and increasing customer expectations are the two largest drivers of this practice and the associated tools. As systems become more rich in features, they also become more complex in their composition, and more critical to business success.
- Overall, chaos engineering helps organizations create more reliable systems and prove that systems are reliable.

Obstacles

- The first obstacle to chaos engineering is perception. Within many organizations, the predominant view is that the practice is random, done first in production, and due to these leads to more risk than less.
- Another obstacle to chaos engineering is organizational culture and attitude toward quality and testing. When quality and testing are only viewed as overhead, then there will be a focus on feature development over application reliability.
- Another common obstacle is simply gaining the time and budget to invest in learning the practice and associated technologies. Organizations must reach minimum levels of expertise where value is then returned.

User Recommendations

- Utilize a test-first approach by practicing chaos engineering in preproduction environments. Then move findings into production environments.
- Incorporate chaos engineering into your system development or testing process.
- Build-out incident response protocols and procedures, as well as monitoring, alerting, and observability capabilities in tandem with advancement of the chaos engineering practice.
- Utilize scenario-based tests — known as “game days” — to evaluate and learn about how individual IT systems would respond to certain types of outages or events.
- Investigate opportunities to use chaos engineering in production to facilitate learning and improvement at scale as the practice matures. However, be warned that Gartner believes that there are still very few organizations purposely using chaos engineering in their production environments.
- Formalize the practice by adopting a platform or tool to track the activities and create metrics to build feedback for continuous improvements.

Sample Vendors

Alibaba Cloud; Amazon Web Services; ChaosIQ; Gremlin; steadybit; Verica

Gartner Recommended Reading

Improve Software Quality by Building Digital Immunity

Innovation Insight for Chaos Engineering

How to Safely Begin Chaos Engineering to Improve Reliability

DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value

Immutable Data Vault

Analysis By: Michael Hoeck, Jerry Rozeman

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Immutable data vault is an isolated secure backup storage solution designed to be complementary to the existing primary and disaster recovery backup infrastructure. Isolated from production in an air gap architecture, it mitigates impacts from malware, ransomware or insider malicious attacks. Immutable data vaults are often a combination of multiple vendor technologies and services, and can be a critical element of an isolated recovery environment.

Why This Is Important

Against the backdrop of cyberattacks increasing in numbers and sophistication, organizations are expanding their efforts to prepare for the need to recover from an attack. With the latest round of attacks targeting backup systems, backup solutions are advancing their ability to prevent backup data from being compromised. Immutable data vaults provide additional levels of protection and security of backup data to increase the opportunity of its availability for recovery after an attack.

Business Impact

Immutable data vaults safeguard backup copies by:

- Creating a tertiary copy of backup data, separate from production and disaster recovery copies
- Isolating in physically separate and secure environment
- Restricting administration to physical console access to remove remote access
- Using immutable storage to protect copies
- Implementing Air Gap to separate vault from production environment

Drivers

- Increasing threats and sophistication of ransomware attacks and the potential risk associated with rogue administrators
- Ransomware as service offerings are being sold, increasing the threat of new attackers and variants of malware
- Work-from-home demands have significantly increased the risk of attacks via unsecured or poorly secured endpoints
- Report of attacks taking over console operations of backup solutions to expire and delete backup data
- Greater attention to alternative backup strategies to protect, detect and recover from ransomware
- Financial services organizations, led by industry-led initiatives such as Sheltered Harbor, have been rapidly adopting immutable data vaults and focus on building out cyber resilience capabilities
- Industries such as the government, education and healthcare have had a higher rate of reported ransomware incidents

Obstacles

- Implementing an additional solution to store backup data amounts to additional cost that may not be budgeted
- Immutable data vaults not only require additional backup storage, but are recommended to be physically separated within a data center requiring added infrastructure, such as a new cage or area with limited access and air gapped from the production network
- Complexity of the backup environment is increased with the addition of a new isolated copy of data, additional technologies like advanced networking and data scanning, and requirement of new procedures, runbooks and potentially limited staff to operate

User Recommendations

- Conduct a thorough cost-benefit and risk assessment to align expectations and acceptable risks to the current backup and recovery solution capabilities.
- Plan for when, not if, an attack will occur in the cost-benefit analysis to gain management buy in to phase in costs.
- Work with immutable data vaults, which are storage environments or products intended to supplement existing backup infrastructure. These are physically secure environments with physical access controls, a limited access list and two-person authentication capabilities.
- Deploy immutable data vaults in close proximity to production or disaster recovery systems to optimize recovery speed.
- Incorporate other requirements to scan, cleanse and repair backup data into the environment to prevent the reinfection of other systems during the recovery and restoration process.
- Be mindful that the data stored within an immutable data vault may also contain the agent or infectious code, as well as infected or encrypted data.

Sample Vendors

Dell EMC; Owl Cyber Defense; Unisys

Gartner Recommended Reading

Magic Quadrant for Data Center Backup and Recovery Solutions

Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

How to Prepare for Ransomware Attacks

At the Peak

Site Reliability Engineering

Analysis By: George Spafford, Daniel Betts

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Site reliability engineering (SRE) is a collection of systems and software engineering principles used to design and operate scalable resilient systems. Site reliability engineers work with the customer or product owner to understand operational requirements and define service-level objectives (SLOs). Site reliability engineers work with product or platform teams to design and continuously improve systems that meet defined SLOs.

Why This Is Important

SRE emphasizes the engineering disciplines that lead to resilience; but individual organizations implement SRE in widely varying ways. SRE teams can serve as an operations function, and nearly all such teams have a strong emphasis on blameless root cause analysis. This is to decrease the probability and/or impact of future events and to enable organizational learning, continual improvement and reductions in unplanned work.

Business Impact

The SRE approach to DevOps is intended for products and platforms that need to deliver customer value at speed at scale while managing risk. The two primary use cases are to improve reliability of existing products or platforms as well as to create new products or platforms that warrant the investment in reliability.

Drivers

- SRE is intended to help manage the risks of rapid change, through the use of SLOs, “error budgets,” monitoring, automated rollback of changes and organizational learning.

- SRE teams are often involved in code review, looking for problems that commonly lead to operational issues (for instance, an application that does not do log cleanup and therefore may run out of storage).

- They also ensure that the application comes with appropriate monitoring and resilience mechanisms, and that the application meets SRE-approved standards or guidelines set to achieve negotiated SLOs.
- SRE practices are being adopted by organizations that need to deliver digital business products reliably. These practices require a culture that supports learning and improvement, highly skilled automation practices (and usually DevOps), and usage of infrastructure-as-code capabilities (which usually requires a cloud platform).
- SRE also uses automation to reduce manual processes, and leverages resilient system engineering principles and an agile development process that employs continuous integration/continuous deployment (CI/CD).

Obstacles

- Among the biggest roadblocks toward getting started with SRE is the conceptual foundation necessary to obtain buy-in from both management and agile or DevOps teams. SRE is a significant investment, and organizations need to organize implementation based on the mission and on the adequate budget.
- Implementing SRE without an experienced site reliability engineer requires considerable learning and improvement in order to be effective. By nature, SRE embraces risk, and this conceptual mindset is difficult for many traditional employees to completely understand.
- SRE calls for blameless analysis of understanding how teams can learn from a problem, rather than assigning blame. This means understanding what made the problem happen and how to mitigate, and publishing the results.

User Recommendations

- Engage an executive sponsor to support the initiative.
- Demonstrate sufficient value to improve credibility and support; have an acceptable level of risk.
- Build an initial SRE team with a collaborative engineering mindset and a desire to learn and improve, and automate tasks to reduce repetitive manual work.
- Define clear SLOs and service-level indicators (SLIs) to be monitored and reported against.

- Instill collaborative working between site reliability engineers and developers to help them learn how to design and build their product to meet SLOs.
- Drive an iterative approach to start and evolve SRE practices.

Sample Vendors

BigPanda; Blameless; Datadog; New Relic; OpsRamp; PagerDuty; Splunk

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

COVID-19 Health Risk Mitigation

Analysis By: Sam Grinter, Donna Medeiros

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

COVID-19 risk mitigation is made up of an array of functions designed to reduce the health risks COVID-19 poses. Functionality typically includes health screening, contact tracing, office booking, test data management and vaccine tracking. Additional functions such as corporate communications and a knowledge base may also be delivered.

Why This Is Important

Employers in many countries must comply with “duty of care” requirements to ensure a safe working environment. With more than 150 million confirmed COVID-19 cases and more than 3 million deaths at the time of this writing, the pandemic is the challenge of our time. Despite the development of multiple vaccines and improved therapies, it is likely we will be living with it for the foreseeable future due to differing vaccine rollout timelines and potential virus variants.

Business Impact

- COVID-19 risk mitigation aims to deliver a safer working environment for employees, their families, customers, partners and the wider community.
- COVID-19 risk mitigation can deliver the option for those working from home to safely return to the office.
- COVID-19 risk mitigation may be a compliance requirement (depending on country/state regulations), but also provides employees with the comfort and reassurance that their employer is acting with proper caution and responsibility.

Drivers

- There is a desire for employees currently working from home due to COVID-19 to have the option to return safely to the office at least part of the time. In Gartner's 2021 Digital Worker Experience Survey, employees were asked: "If you could make the schedule yourself, what proportion of time would you like to spend working?" Forty percent indicated they prefer to work from a combination of locations; 17% prefer to mostly work from the corporate office; 14% prefer to only work in the corporate office; 14% prefer to mostly work from home; 10% prefer to only work from home; and 5% prefer to only/mostly work from other locations (n = 9,725).

- COVID-19 risk mitigation technology enables employees to return safely to the office. It is anticipated that this option to return safely to the office will offer more flexible working options to employees and may also foster improved work quality and organizational culture.

- For those employees not able to work remotely, processes must be developed and maintained to ensure there is no unnecessary risk of infection while at work. Even when COVID-19 infections subside, as we have seen repeatedly, the infection rate can rise again very quickly. Furthermore, as the virus mutates, the nature of the risk changes. As such, the provision of COVID-19 risk mitigation technology for frontline and key workers not able to work from home must be continually monitored and adjusted when necessary to ensure safe working conditions for these employees.

- A longer-term driver for investment in such technology is the potential for future global pandemics and other health-related crises, which some epidemiologists have suggested is likely, as well as part of a flexible hybrid working strategy and for business continuity.

Obstacles

- A “set it and forget it” mindset will impair the ability for employers to adapt processes as the risks COVID-19 poses change. Many processes initially developed were self-built, with many organizations using spreadsheets or even paper. Such approaches may put employers at risk when it comes to data privacy regulations, and the tools in use do not deliver the agility needed as conditions change.

- Some employers and employees have not taken the matter as seriously as others, perhaps due to low local infection rates, low priority in investing in tools perceived as short term or other reasons. Such employers and employees are at severe risk.

- COVID-19 risk mitigation may not be universal to all types of workers and across multiple territories. Some workers have regular public contact, while others can perform their duties from home.

- Some countries will have higher/lower infection rates than others. This creates a complex, changing environment to develop and maintain an effective response.

User Recommendations

- Evaluate the current processes and tools in place to mitigate the health risks COVID-19 poses to ensure they are fit for purpose.

- Adapt processes and tools to ensure employees are safeguarded and that an appropriate response to the health risks is maintained as COVID-19 mutates and as infection rates rise and fall.

- Vet any manual processes initially deployed as a response to COVID-19 (Microsoft Excel, for example) for the utility as an effective/appropriate response to the pandemic, and the extent to which such processes are compliant with data privacy regulations. Replace any manually developed process with something off the shelf if the utility of the manual process is low and/or the compliance risk is moderate to high.

Sample Vendors

dev-id; Herta; Juvare; Qualtrics; Ramco Systems; Recovery Amped; ReturnSafe; SaferMe; Salesforce; ServiceNow

Gartner Recommended Reading

Plan for the Aftermath of COVID-19 for Your HCM Technology Portfolio

Peer Benchmarking on Health and Safety for a Postvaccine Return to the Workplace

The Business Continuity Management Software Ecosystem

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

5 Board-Level Issues About COVID-19 That Executives Must Discuss With Directors

Tool: COVID-19 Long-Term Scenario Planning Workshop

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

Sliding into the Trough

Social Distancing Technologies

Analysis By: Leif-Olof Wallin, Nick Jones

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Social distancing technologies help to encourage individuals to maintain a safe distance from each other. Some of these technologies and solutions also provide contact tracing capabilities if an individual is discovered to be infected. Contact tracing can be implemented in many ways, including via an app on a smartphone, as a feature of a location tracking system, via a dedicated wearable device or using observational tools such as Wi-Fi or video analytics.

Why This Is Important

Social distancing technologies provide a tactical solution to help organizations and individuals deal with the COVID-19 pandemic and implement a duty of care for employees. They can help organizations whose business requires workers to be present in spaces such as offices and factories when home working is impractical. Social distancing can help reduce the likelihood of infections spreading in the workplace, and the technologies provide contact tracing to manage risks if infections do occur.

Business Impact

Social distancing is one part of a multidimensional strategy that includes behavioral guidelines, new working practices, COVID-19 testing, attestation, workplace sterilization and controlling visitor numbers. It is valuable when the organization cannot operate without on-premises staff or where there are regulations or a legal duty of care to minimize the risks employees face. Most systems are based on modifications of existing technologies, so we expect maturity within two years.

Drivers

- Some organizations, such as factories, warehouses, construction sites and process plants, cannot operate without on-site employees.

- Minimizing infection risk is good business practice, beneficial for employee relationships and, in some cases, a legal requirement.
- The organization wants to provide tangible evidence to employees (and sometimes visitors) that the organization is concerned for their welfare.
- Without technological support, effective contact tracing is very difficult to implement.
- Some systems can support other valuable anti-COVID-19 goals, such as encouraging regular hand washing.
- Social distancing systems that track an individual's location can provide data for workplace and process restructuring to further reduce risk.

Obstacles

- Most technologies have significant flaws related to distance measurement and will generate false positives and negatives.
- Some users will feel social distancing is an invasion of privacy because it involves location and behavior tracking.
- The cost can be significant, in some cases, hundreds of dollars per employee accompanied by monthly service charges. Many solutions are seen as "throwaway" and will be discarded when COVID-19 is under control. So organizations may be reluctant to invest.
- Social distancing cannot prevent infection, only reduce the risk of infection.
- In general, social-distancing tools are more effective for use by employees than visitors.
- Smartphone-based systems have significant technical limitations unless used in conjunction with other technologies such as beacons.

User Recommendations

Organizations that need to manage risk as staff return to work after the pandemic should consider social distancing technologies because:

- Despite their limitations, any form of risk reduction is better than none.

- Industrial, construction and blue-collar workers who may not carry smartphones in their normal work environment may benefit from dedicated proximity-warning devices or equipment such as smart hard hats that have been modified to track proximity.
- Staff in office-based environments may benefit from app-based solutions.
- Most organizations will use social distancing technologies in conjunction with processes such as reducing the number of employees in offices and establishing behavior and visual guidelines.
- Some app-based solutions may be superseded or augmented by national social distancing app initiatives or apps from megavendors such as Google and Apple.

Sample Vendors

AiRISTA Flow; Cloudleaf; Estimote; Kontakt.io; Radiant RFID; Zebra Technologies

Gartner Recommended Reading

Manage Social Distancing and Contact Tracing With Location-Aware Technologies and Devices

Market Guide for Social Distancing Technology

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

IT Vendor Risk Management

Analysis By: Joanne Spencer

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

IT vendor risk management (VRM) is the process of ensuring risk, associated with vendors and service providers, is effectively managed. The discipline of VRM addresses the mitigation and remediation of these risks to avoid business disruption and financial and regulatory impacts. VRM technology supports various activities as part of a broader VRM framework for identifying, assessing, analyzing, remediating and monitoring vendor threats and risks.

Why This Is Important

Increased reliance on vendors exposes enterprises to greater risk of business disruption and damage to their brand and reputation. Lack of visibility into the third and fourth parties (e.g., subcontractors), major security breaches, rapid adoption of cloud models, and increasing regulatory requirements heighten the need for IT VRM technology solutions.

Business Impact

IT VRM solutions provide organizations a consistent and formal approach to managing vendor risk, while helping them comply with regulations and make vendor management decisions. Organizations can also track and monitor vendor performance as IT VRM solutions are broadening to include tracking of performance and relationship issues. IT VRM solutions, when combined with content and data feeds, ensure effective vendor risk management as everything is stored in one place.

Drivers

- IT VRM is a critical element of enterprise and IT risk management. Regulatory guidance and newer privacy and data breach notification regulations in many industries have made it an essential requirement.
- IT VRM can be a catalyst for improved vendor performance, by identifying vendor-related risks early and mitigating them through effective controls and process improvements.
- IT VRM solutions automate part or all of the assessment, analysis and control validation process, provide remediation and mitigation guidance, and facilitate monitoring of risks associated with vendors and other third parties that access, support or control information assets.
- As independent stand-alone solutions arise and the ease of implementation improves, we anticipate the adoption of these solutions will continue to increase, primarily in response to increased risk, data privacy and cybersecurity regulations.
- In a postpandemic world, organizations are realizing the need to proactively manage vendor risks.

Obstacles

- Resource constraints (both personnel and budget) are hindering organizations' ability to provide ongoing monitoring and tracking of vendors.
- Lack of mature VRM programs, expertise and processes.
- Growth and adoption of security and risk rating services (BitSight, Black Kite, SecurityScorecard, RiskRecon, etc.), and vendor risk assessment data in a shared model (CyberGRX, OneTrust, Prevalent, Venminder) as alternatives to a full IT VRM solution.

User Recommendations

- Select IT VRM solutions that provide a common system of record for all parties involved in managing vendor risk.
- Ensure processes and methodologies used for IT VRM are supported by the VRM solution. Increasingly, solutions are integrating with risk and security rating services, risk exchanges and content providers to assist with ongoing vendor risk monitoring.

- Develop a roadmap to improve IT VRM maturity and align your solution decisions with your current and planned maturity levels.
- Ensure that all relevant stakeholders are engaged in VRM workflows, including risk management, IT security, procurement, vendor management, legal and business continuity management.
- Ensure vendors perform their contracted risk obligations, including risk reporting, security incident notifications and business continuity plans.
- Prioritize risk weightings on criticality of solutions and technology, and sensitivity of data or intellectual property (IP) that a vendor may access or control.

Sample Vendors

Aravo; LogicManager; OneTrust; Prevalent; ProcessUnity; Venminder

Gartner Recommended Reading

Critical Capabilities for IT Vendor Risk Management Tools

Magic Quadrant for IT Vendor Risk Management Tools

Supply Chain Risk Management

Analysis By: Kamala Raman

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Supply chain risk management (SCRM) aims to make businesses resilient to supply chain risks across the physical and digital ecosystem. A comprehensive approach to SCRM focuses on the ability to identify and mitigate risks across the extended network footprint. It is strengthened by technology used for risk identification and monitoring, holistic risk impact analysis and coordinated operational mitigation/response.

Why This Is Important

While the risks of supply and operational disruptions have become front and center in global networks during the COVID-19 pandemic, supply chain risks could be commercial, financial, regulatory, reputational, environmental or digital in nature. Organizations have found that existing risk frameworks have largely not been effective in managing pandemic response and at the same time, the importance of balancing risk against other competing network objectives has shot up.

Business Impact

Businesses are finding that the cost of managing each risk event reactively can get prohibitively expensive in the near term and reduce the ability to grow in the long term. A holistic framework to tackling predictable risks, as well as unpredictable events, is essential to build a risk management program that combines business continuity management at the operational level with a resilience program at the organizational level.

Drivers

- Conventional risk mitigation has been focused on mitigating operations disruptions once they happen or utilizing inventory or capacity buffers to avoid disruptions, but these are expensive to maintain. This reactive approach to risk management is not enough in a world where risks that are harder to predict are here to stay. Intensifying geopolitical competition is threatening unfettered global trade.

- Data breaches and cyberattacks that severely disrupt operations or impact products are growing. Climate change, extreme weather events and the threat of resource constraints must be managed.

- As outsourcing expands, the adoption of tools to monitor multiple tiers of suppliers for quality, performance or social responsibility risks is growing. Users may need to invest in technologies and data-sharing platforms to support SCRM, combining multiple analytics approaches or solutions as needed. Examples include network design tools to design for resilience, and supply chain visibility tools for live incident monitoring and intelligent response.

Obstacles

- Investments in buffer capacity or inventory are not easy to maintain. At best, such investments can be sustained for select products or locations. At worst, the scope is too complex, and when it competes with operational efficiency, it tends to be deprioritized.
- Having visibility to the extended supply network is a herculean task. With global, complex networks where the subtier partner ecosystem might be continuously shifting, identifying weak points beyond direct suppliers is expensive in time and resources.
- Identifying and prioritizing risks is complicated in global issues with high uncertainty, such as climate change or trade policies, or when the view is clouded by normal human tendencies, such as availability bias.
- Digitalization of ecosystems and the availability of data on subtier suppliers or level of impact from risk events in far-flung regions of the world are an impediment.
- Organizations must dedicate funds and resources for ongoing risk management, along with governance.

User Recommendations

- Identify product design stage gates, key suppliers, and transportation hubs to track interdependencies, bottlenecks and potential failure points.
- Identify and prioritize most impactful risks by impact, likelihood of occurrence, level of control and value at risk.
- Identify where individual risk events cannot be predicted, establish measurement criteria, such as time to survive and time to recover, and set thresholds for notification.
- Create strategies focused on risk reduction, avoidance, transfer or acceptance. Simulation and scenario planning can aid risk mitigation. Escalation plans for vendors can aid risk transfer. Business continuity plans refine risk response strategies, while inventory can help cover recovery time during disruptions.
- Regularly review and test business continuity plans. Resilience needs speedy execution of remedial actions once a risk event has been detected.
- Perform a continuous improvement assessment of risk responses that updates the SCRM framework.

Gartner Recommended Reading

Supply Chain Executive Report: Future of Supply Chain — Crisis Shapes the Profession

Assess Supplier Business Continuity Plans for Risk Mitigation and Operational Resilience

Stress-Testing Direct Material Supply Chains: A Resilience Trend for 2021

Climbing the Slope

Automated Incident Response

Analysis By: Venkat Rayapudi

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Automated incident response (AIR) solutions automate incident response processes by enabling centralized alert or incident routing. Using a policy or rule-based engine, on-call scheduler, or streamlined collaboration, this can improve operational efficiencies with action-oriented insights.

Why This Is Important

Operations centers traditionally follow manual incident response processes and escalate to Level 2 and Level 3/Level 4. The major challenges with this traditional incident response approach are the manual processes, and the lack of collaboration between teams to conduct triage and extend incident management that is unable to cater to DevOps needs to deliver application features at high velocity. The AIR solution solves this by automating most of the incident response steps.

Business Impact

AIR solutions deliver value through:

- Improved incident communication and visibility across the organization.
- An extended incident management practice that meets DevOps requirements.
- Analytics insights that improve operational efficiency.

Drivers

- **Automation of incident response processes**: Level 1 support resources often spend a lot of time identifying and contacting the domain experts, because operations teams use different methods of managing the on-call roster. The preferred contact information is often inaccurate, leading to increased mean time to acknowledge (MTTA) and high incident response times.

- **Incident communication and visibility challenges:** With geographically distributed teams, remote workforce, complex on-call schedules and notification channel preferences, incident triage teams often have difficulty engaging responders quickly. Incident communication may lack a single source of incident data. Data is often dispersed on call notes or email or even lost.

- **DevOps and SRE requirements:** Traditional incident management models cannot meet the needs of agile cultures because of manual tasks in the incident response workflow. When organizations do not support or recognize DevOps requirements around incident management, they are unlikely to adopt the guidance and governance model laid out by IT service management (ITSM) teams. This can lead to detrimental effects on infrastructure and operation's (I&O's) ability to underpin its offerings with an effective, consistent ITSM practice.

- **Lack of analytics:** It's impractical to measure aggregated time spent by Level 1 support to identify and contact the domain expert during major incidents. It is also impractical to attempt to measure how much time, on average, the support teams spent triaging incidents per week or why some support teams spend more time triaging with manual steps than others. Lack of actionable analytics creates cascading problems for I&O organizations, because it often leads to decisions that put I&O organizations under high stress. This leads to finger-pointing or the "blame game."

Obstacles

- **Overlapping capabilities:** Although AIR solutions offer differentiating features, they also overlap with ITSM and event management systems. This makes the value proposition harder for the organizations.

- **Service definitions:** Service definition configurations that connect the alerts or incidents to the responder teams are often challenging to configure. This is because it involves interpreting an application problem based on the information available in the notification and identifying the domain expert team that needs to investigate the problem. Service definitions are also a complex part of AIR onboarding.

- **Portability between solutions:** Migrating from one AIR vendor to another is a reset process, with no defined migration path. The integrations, team and service definitions, responder preferences, and role-based access controls must be reconfigured without sophisticated import/export mechanisms when migrated to a new solution.

User Recommendations

I&O leader and technical professionals responsible for IT operations and cloud management that are focused on an incident management practice should:

- Invest in a centralized on-call management system and AIR workflows with wide integrations that create a holistic incident response management solution.
- Integrate monitoring solutions and service desk systems with bidirectional synchronization to incident response systems, which keeps the incident status synchronized across systems.
- Leverage automation to extend incident response capabilities that can integrate with DevOps toolchain monitoring.
- Improve incident communication and collaboration by integrating incident workflow processes with ChatOps tools, such as Slack or Microsoft Teams.

Sample Vendors

Everbridge; OpsGenie; PagerDuty; ServiceNow; Splunk

Gartner Recommended Reading

Automate Incident Response to Enhance Incident Management

ZTNA

Analysis By: John Watts, Lawrence Orans, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Zero trust network access (ZTNA) creates an identity- and context-based logical access boundary around applications. Applications are hidden from discovery and access is restricted via a trust broker to a set of named entities. The broker verifies identity, context and policy adherence of specified participants and devices before allowing access, and prohibits lateral movement in the network. This removes public visibility of applications and significantly reduces the attack surface area.

Why This Is Important

ZTNA is a key technology for enabling user-to-application segmentation through a trust broker, to enforce a security policy that allows organizations to hide private applications and services and enforces a least-privilege access model for applications. It is a synthesis of concepts in the Cloud Security Alliance's Software-Defined Perimeter (SDP) guide, Google's BeyondCorp vision and O'Reilly's Zero Trust Networks book.

Business Impact

ZTNA yields immediate benefits by shielding services from attackers. In contrast to basic VPN products, ZTNA removes full network access and improves user experience, flexibility and adaptability. It enables more granular user-to-application segmentation through simplified policy management. Cloud-based ZTNA offerings improve scalability and ease of adoption. Early products on the market focused on web applications, but have expanded to work with a wider range of applications and protocols.

Drivers

- The need to support digital business transformation scenarios ill-suited to legacy access approaches, such as access to applications, services and data located outside the enterprise.
- Need for flexibility to quickly expand capacity as the sudden shift to remote work in 2020, with the onset of the COVID-19 pandemic, strained legacy on-premises VPN infrastructure.
- The rise of zero trust initiatives within organizations, which resulted in the need for more precise access and session control in on-premises and cloud applications.
- A desire for vendor consolidation, to remove point solutions and adopt more products from vendors with SASE frameworks, resulting in ZTNA additions to existing SWG or CASB services.
- A need to connect third parties such as suppliers, vendors and contractors to applications securely without exposing the network over VPN, or to connect the application to the internet for access.
- Mergers and acquisitions enabled by the ability to extend application access to acquired companies preclosure without needing to deploy endpoints or connect networks directly between the two companies.

Obstacles

- Cost: ZTNA is typically licensed per named user on a per user per year basis and may cost more than traditional VPNs.
- Limited support: Not all products support all applications. For example, some only support web, RDP and SSH protocols.
- Agent or agentless ZTNA: Some providers only offer one way to consume ZTNA. This limits applicable use cases.
- Weak identity management: Organizations with no federated identity support in the cloud find limitations with use cases as many providers rely on third-party identity providers for user authentication.
- Lack of on-premises trust brokers: Cloud-based trust brokers work well for remote access, but may not be preferred to extend the same policies on-premises. While providers exist that have both cloud and on-premises trust brokers, they are far and few between.
- Limited knowledge of acceptable application access rights for users: Organizations must map the correct application accesses upfront to get full benefit of ZTNA.

User Recommendations

- Open applications and services without requiring the use of a VPN or DMZ.
- Normalize the user experience for application access both on and off the corporate network.
- Implement application-specific access for employees and IT contractors as an alternative to VPN-based access.
- Extend access to systems prior to a merger, without having to configure site-to-site VPN and firewall rules.
- Allow access on personal devices by reducing full bring your own device (BYOD) management requirements and enabling more secure direct application access.
- Cloak systems from hostile networks, such as collaboration systems exposed to the internet.
- Permit users in potentially dangerous areas of the world to interact with applications and data to reduce or eliminate risk.
- Secure access to enclaves of Internet of Things (IoT) devices if the device can support a lightweight SDP agent or a virtual-appliance-based connector on the IoT network segment for connection.

Sample Vendors

Akamai; Appgate; Cato Networks; Ivanti; Netskope; Perimeter 81; Proofpoint; SAIFE; Zscaler

Gartner Recommended Reading

Market Guide for Zero Trust Network Access

Solving the Challenges of Modern Remote Access

Quick Answer: Cost Effectively Scaling Secure Access While Preparing for a Remote Workforce

Quick Answer: How to Securely Enable Access for Unmanaged Devices

2021 Strategic Roadmap for SASE Convergence

Crisis/Emergency Management Solutions

Analysis By: Roberta Witty, David Gregory

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Through a unified management console, crisis/emergency management (C/EM) solutions provide consistent monitoring, orchestration and management of a crisis through all its phases while maintaining compliance with government, regulatory and industry emergency management standards. C/EM solutions are used to manage data, resources, expenditures, communications and tasks before, during and after a crisis, and analyze the changing crisis conditions to enable situational awareness.

Why This Is Important

C/EM solutions help organizations implement a standardized, best-practice model (including organizationwide managerial controls) to contain and minimize a crisis/incident. This helps protect organizations' reputation in the eyes of all stakeholders — employees, customers, citizens, partners, suppliers, auditors, regulators, etc. They also reduce staff training time and ensure better integration with the broader internal and external community involved in recovering from a disaster.

Business Impact

A crisis is a situation that threatens, or is perceived to threaten, organizational resources and operations, resulting in threat to life/safety, disruption to business services, damage to reputation and brand, etc. Organizations must prepare for large and small crises (which can quickly escalate to a larger event) by developing a crisis management program to contain and minimize their impacts. A C/EM solution instantiates a command-and-control structure for all types of crises.

Drivers

- Due to COVID-19, organizations are realizing the value in using C/EM solutions for crisis management as well as preevent risk monitoring. We expect that crisis management capabilities will become part of day-to-day operations solutions so that risks can be anticipated early, and action to mitigate or respond can be better executed to protect reputation in the eyes of all stakeholders.

- C/EM solutions establish a command-and-control structure and process for all types of crisis events and improve organizations' ability to protect public/workforce safety and restore services as quickly as possible.
- C/EM solutions codify the roles, responsibilities and decision-making authority involved with a crisis.
- These solutions also improve the efficiency of crisis/emergency command and related emergency responses via continuous communication and progress assessments.
- C/EM solutions ensure effective management of relationships and communications with internal stakeholders, visitors, the public and external stakeholders, including communications between critical infrastructure service providers and government agencies during regional and nationwide disasters.
- C/EM solutions support administration of response, recovery and restoration phase actions for the event through task and workforce management; media communications, including national services and social media traffic; and expenses incurred during the crisis to better ensure repayment from business interruption insurance policies and government disaster management funding.
- C/EM solutions enable management of program documentation that needs to be submitted to national authorities; all crisis-related data, ensuring it is tracked for postevent analysis; and postincident reviews for regulatory reporting and overall process improvement.

Obstacles

- Finding one C/EM solution to meet all crisis use cases (e.g., pandemics, cyberattacks, IT outages, traditional natural disasters, terrorist attacks, supply chain outage and other man-made events) may not be possible. Implementing multiple solutions, on the other hand, hinders whole-of-enterprise impact analysis of a potential hazard/threat as well as enterprisewide management of the crisis event, due to different buyers within the organization (e.g., BCM, corporate security leaders, IT leaders, cybersecurity leaders, supply chain leaders).

- Integrating a C/EM solution with other resilience-related solutions, such as hazard/threat intelligence, BCMP, EH&S, EMNS, supply chain risk management, integrated risk management and IT resilience orchestration solutions, is highly complex.

- Industry-specific requirements may not be available in a solution that meets most but not all C/EM needs of the organization.

User Recommendations

- Establish an enterprisewide effort to identify all C/EM program needs so that as few C/EM solutions as possible need to be implemented.

- Assess the extent to which the functionality of purpose-built C/EM, BCMP, IT service management and IT resilience orchestration solutions best supports your organization's C/EM program requirements.

- Heavily weigh the ease-of-configuration functionality when selecting a C/EM solution so you can add your day-to-day business processes to the solution, allowing you to move toward a single solution for both crisis and day-to-day business operations use.

- Assess the C/EM solution's application and data integration methods to ensure it can meet the integration needs of your organization to support situational awareness.

- Choose a platform that adheres to public-sector emergency management protocols as well as environmental, health and safety (EH&S) public service protocols. This helps ensure timely and efficient responses that minimize damage.

Sample Vendors

4C Strategies; Esri; Everbridge; Fusion Risk Management; IntraPoint; Juvare; LiveProcess; Swan Island Networks; Tableau; Veoci

Gartner Recommended Reading

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

Market Guide for Business Continuity Management Program Solutions, 2021

Hazard/Threat Intelligence Services

Analysis By: Roberta Witty, David Gregory

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Hazard/threat intelligence services evaluate incidents (local and worldwide) that threaten the health and safety of citizens and the workforce, cause damage to critical physical and technology infrastructure, or cause a disruption to normal business operations. These predictive hazard/threat intelligence alerts for weather, public health, terrorism, civil unrest, earthquakes and other events are sent to customers in real time for early warnings and in-progress events aka situational awareness.

Why This Is Important

Due to the increased awareness since the COVID-19 outbreak, adoption is growing for this technology with organizations seeing its value for more frequent use cases, such as duty of care. Increased adoption of this technology will help mature the overall crisis/emergency management processes within organizations. Therefore, this technology has moved past the trough, with a shortened time to plateau of less than two years.

Business Impact

Organizations should use these services to mature their crisis/emergency management processes when:

- Their operations are in locations (now including remote work locations) that have a level of threat from environmental, geopolitical, weather-related or health-related incidents.

- They are expanding their travel risk management practices as the workforce travels regularly (for example, daily or weekly) to and from medium-to-high-risk locations.

Drivers

- Without accurate and timely information, knowing when an incident will turn into a crisis requiring a directed organizational response can be daunting. Also, monitoring a multitude of data sources can result in information paralysis and underreacting/overreacting to an incident. Hazard/threat intelligence services help address these challenges.

- Government and private enterprise professionals use hazard/threat intelligence services in various functions like corporate security, BCM, HR, supply chain management, etc., for: risk assessments of operating locations as part of due diligence for business decision making and personnel/operations relocation; situational awareness to gauge the disruption's impact on production operations, and traveler and expatriate duty of care; and preparedness and response management for large-scale scheduled events, such as sports events, government meetings and political conventions.

- Hazard/threat intelligence services deliver alerts and reports at the facility, neighborhood, regional, national and international levels to clients via email, SMS, phone and print. They use AI tactics to leverage thousands of information sources such as news outlets, social media, government agencies, academic, political and business sources, and technology resources.

- Situational awareness is greatly improved through services such as GIS for geolocation analysis of people, facilities, suppliers and other resources, as well as layered data visualization for risks an organization may face. Therefore, more organizations are adopting these tools, especially those with a multilocation footprint. By categorizing the severity of incidents and geocoding their resources/assets in the system, alerts can be prioritized and directed to the right people within the organization in real time for investigation and faster, coordinated responses.

Obstacles

- The largest obstacle to using hazard/threat intelligence services is not technical. Rather, it is ensuring the organization has an internal procedure to process the alerts.
- A siloed approach to managing hazard/threat intelligence can lead to over- or under-responding to an event. For example, physical operations alerts might be sent to the corporate security department, while public health alerts might be sent to HR or facilities management (for occupancy management).
- Organizations are challenged to determine a centralized point in the organization responsible for hazard/threat intelligence monitoring so that the impact of the alert is a coordinated, business-informed activity across the organization.

User Recommendations

- Evaluate solutions that integrate with EMNS and crisis/emergency management tools to gain improved situational awareness before and during an event.
- Ensure your solution provides a visualized map of the hazard/threat facing organizational facilities, suppliers and other operational assets.
- Select a solution that includes multiple sources of alerts covering multiple crisis types for your operating locations — global as well as hyperlocal. Events types can include weather, natural disasters, law enforcement, medical/public health, government directives such as lockdowns, stay-at-home orders, social distancing and return-to-the-workplace protocols, supply chain, traffic, social media, biohazards, accidents, economic crises, cultural events, geopolitical/terrorist attacks, crime, civil unrest, etc.
- Ensure solutions include GIS capability that can be customized to your operational footprint, and a mobile device app for communications and interactive situational awareness activities.

Sample Vendors

AlertMedia; CountryWatch; Crisis24; Dataminr; Everbridge; International SOS; Kinetic Global; Risk Intelligence; WeatherOptics; Willis Towers Watson

Gartner Recommended Reading

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

Market Guide for Emergency/Mass Notification Services Solutions

Market Guide for Business Continuity Management Program Solutions, 2021

BCMP Solutions

Analysis By: David Gregory, Roberta Witty

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Business continuity management program (BCMP) solutions are the primary tools used to manage BCM programs through all phases of the life cycle, from planning to crisis activation and business recovery. BCMP solutions provide capabilities for availability risk assessment, business impact analysis, business process and resource/asset dependency mapping, recovery plan management, exercise and crisis management, and BCM program management metrics and analysis.

Why This Is Important

Organizations need a consistent, repeatable and scalable process for effective BCM program development. The impact of COVID-19 has led to a realization of the value of a robust BCM strategy with executives seeking assurance that they have best practice BCM methodologies and frameworks in place. As a result of this, BCMP solution sophistication is continuously improving with most now offered as SaaS solutions which is beneficial in a real disaster where internal IT systems are not available.

Business Impact

In the 2021 Hype Cycle, we moved BCMP solutions forward from its 2020 position and shortened its time to plateau to less than 2 years. There has been increased interest from a wider variety of organizations through 2020 with more organizations looking to either begin or mature a business continuity program. This in turn has led to an upturn in the focus on the BCMP market as organizations seek solutions that could support ongoing business continuity planning development.

Drivers

- BCMP solutions will benefit every organization wanting to perform a comprehensive analysis of its preparedness level to cope with business or IT interruptions.

- Many vendors will offer a modular, “prebuilt” or “out of the box” approach to the implementation of their solution enabling smaller organizations to commence a program while controlling costs and to build their BCMP’s at their own pace.

- BCMP solution database’s are a “gold mine” that can be used to enhance business operations and resilience outside of recovery.

- Businesses from all market sectors across differing enterprise types have shown an increasing interest in BCMP solutions because they are seeing them as an easy way to jump-start a BCM program. It delivers great benefit due to the standardization and centralization of BCM activities.

- The BCMP solution market continues to enter the Plateau of Productivity level for large and extra-large organizations, regulated enterprises, government agencies, as well as for organizations with complex business operations. However, more vendors are taking a modular approach to the implementation of a solution and are offering adaptability to increase accessibility from the SME sectors. The BCMP Market Guide, published in January 2021, confirmed a wide adoption of BCMP solutions from the following sectors: Financial Services/Banking; Insurance; Healthcare/Life Sciences; Public Sector/Government.

- We are also seeing adoption in technology solutions and manufacturing. The following geographic regions continue to be the main consumers of BCMP Solutions: North America; UK/Europe; APAC; Canada

- The UEA and South America are also starting to adopt BCMP solutions and we anticipate continued adoption during the next five years, given the increase in preparedness initiatives across all industries.

Obstacles

- Consider all use cases related to risk management, business continuity, emergency notification and crisis management to ensure it can fulfill both current and future requirements.
- Finding one solution to meet all crisis use cases, e.g., pandemics, cyberattacks, IT outages, traditional natural disasters, terrorist attacks, supply chain outage, and other man-made events may be challenging.
- Multiple solutions may need to be implemented to ensure robust enterprise wide risk/hazard threat analysis, impact analysis and management of the crisis event are in place.

User Recommendations

Consider a BCMP solution when:

- Starting a new BCM program and want to follow standard practices throughout the organization.
- Updating or automating your current BCM program and processes.
- Maturing your BCM program where greater program management analytics are required.
- Expanding your BCM program's automated footprint for more control over the execution of the BCM program life cycle.
- Integrating plans from several departments, business units, divisions and legal entities into a consistent and easily updated set of recovery plans.
- Developing future pandemic plans and procedures.

Do not overbuy; focus on:

- Ease of use for all business users.
- Ease of configuration and reporting.
- Ease of integration with other key business applications, ie. enterprise directories, HR tools, business process management tools, IT asset management (ITAM) tools and any existing BCM solutions.

- Mobile device (smartphone or tablet) support for recovery plan access and execution at the time of a business disruption.

Sample Vendors

BC in the Cloud by Infinite Blue; Castellan Solutions; Continuity Logic; Fusion Risk Management; Premier Continuum; RecoveryPlanner; RSA; SAI Global; ServiceNow

Gartner Recommended Reading

Market Guide for Emergency/Mass Notification Services

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

Market Guide for Business Continuity Management Program Solutions

Critical Capabilities for Business Continuity Management Program Solutions, Worldwide

IT Service Dependency Mapping

Analysis By: Roger Williams

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

IT service dependency mapping (SDM) tools discover, snapshot and track configuration relationships by creating blueprints to map dependencies among infrastructure components (e.g., servers, networks and storage), services and applications in physical, virtual and cloud environments. This forms an IT service view that provides crucial information for improving IT service delivery. Key differentiators are breadth of blueprints and depth of discovery across different environments.

Why This Is Important

IT SDM tools provide data that enables improved application availability and reduced service disruption for targeted systems, impacting stakeholder perceptions of IT and overall service delivery. They reduce the risk of high-profile initiatives, such as cloud migration, IT service view CMDBs, software asset management. As digital business initiatives become more critical, dependency information becomes essential for making service delivery decisions at speed without sacrificing quality.

Business Impact

IT SDM tools can provide the following benefits:

- Support day-to-day requirements to improve SACM competency
- Enable automated change impact analysis
- Provide missing relationship data critical to disaster recovery initiatives
- Supply information useful for stabilizing the IT environment, which reduces unplanned downtime for critical IT services, saves money and increases support staff efficiency

Drivers

IT SDM tools are of interest for the following reasons:

- IT teams need visibility into how components come together to provide an IT service to improve service delivery decision making.
- Vendors in the ITSM tool, stand-alone discovery tool and related technology markets, such as software asset management (SAM), security or monitoring promote these capabilities for their labor saving and service delivery benefits.
- End users often seek IT SDM capabilities as part of ITSM investments. Competitive pressures have reduced the number of ITSM tool vendors that do not offer IT SDM tooling.
- IT SDMs tools are often used by end-user organizations and service providers for projects like data center consolidations or cloud migrations.
- IT SDM for cloud infrastructure and applications has become more of a focus, as this information is crucial for hybrid digital infrastructures.

Obstacles

- IT SDM tools often fall short in the discovery of homegrown or custom applications, yet have made improvements.
- Validating dependency relationships with business capabilities or services remains labor-intensive.
- Difficulties in showing returns on IT SDM tool investment have slowed adoption of the tools beyond their primary use of discovery.
- IT SDM tools are not well-suited to cloud environments due to lack of access to cloud environments, lack of transparency into component details and high rates of change.
- IT SDM tools do not yet focus on tracking performance promises, which are the non-functional aspects such as latency, throughput, error rate, etc., required from the cloud service provider for a dependent application, product or service to function as intended. Such visibility enables more effective decision making and data management, and will become a key differentiation point for IT SDM tools.

User Recommendations

- Manage IT SDM tooling investments as part of a broader service asset and configuration management (SACM) program. These tools require effective governance of IT services to yield meaningful value and improve data accuracy.
- Limit IT SDM investment in low-maturity I&O organizations to current state visibility or specific projects like a data center migration.
- Evaluate vendor capabilities and roadmap to ensure there is a focus on emerging technology requirements, such as support for containers and edge computing.
- Ensure complementary functionality is in place to yield intended business value. For instance, although most IT SDM tools aren’t capable of action-oriented configuration functions, such as patch management, they can document what is installed and where, and can provide an audit trail of configuration changes useful for patching.
- Require IT SDM tool integration into the ITSM tool, if they are not from the same provider, to ensure timely information is available for decision making.

Sample Vendors

Atlassian; BMC; Device42; Eracent; Flexera; Resolve Systems; ScienceLogic; ServiceNow; Tanium

Gartner Recommended Reading

Break the CMDB Failure Cycle With a Service Asset and Configuration Management Program

3 Steps to Improve IT Service View CMDB Data Quality

How to Modernize the Configuration Management Database

ITSM Best Practices: A Guidance Framework for Implementing a Configuration Management Database

Emergency/Mass Notification Services

Analysis By: Roberta Witty, David Gregory

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Emergency or mass notification services (EMNS) automate the distribution and management of messages to relevant stakeholders for local and regional events and catastrophic disasters across multiple channels. Use cases include organizational crises, business-critical operations, IT outages, travel risk, and public and personal safety. EMNS is used when normal communications are not available or suitable for use, when the need to communicate is in minutes and for off-hours communications.

Why This Is Important

COVID-19 has increased EMNS adoption because organizations needed to reach all of their workforce in every location. End-user awareness and maturity have increased, with more customers testing the full functionality of EMNS.Its use cases are building access management integration, IT network location, personal safety, active intruder/shooter, personnel safety, travel risk management, workforce scheduling, pandemic management, critical IT change/outage notification and industrial accident.

Business Impact

Crisis communications' best practice is to notify people in as many ways and in as short time frame as possible. This ensures that life/safety is preserved, response and recovery teams are quickly assembled, transparency of the event is known to all stakeholders, secure communications is established, and the organization's reputation and brand can be preserved.

Drivers

- Key personnel (e.g., crisis management team members, IT personnel, physical security, and other life safety and security personnel) and large numbers of affected personnel, visitors or the public can receive critical information about the event on multiple channels in minutes. This speed allows them to rapidly respond after an event to ensure the health, wellness, life, and safety of people, and that organizational RTOs are met.

- Personnel can be tracked for life, safety and security purposes.

- Management can focus on critical decision making and exception handling.

- Human error, misinformation, rumors, emotions and distractions can be managed and corrected.

- Messages can be tailored to different audiences and languages, so that the right information is targeted and not broadcast to those who need to know.

- A notification activity dashboard and associated reporting can be used for event management: a documented notification audit log for real-time and postevent management; preevent activities — for example, notices to not come into the office due to the likelihood of a storm affecting the area within the next two days; real-time event activities — for example, initial messages and timely updates to events as they occur and unfold, tracking of contacts in dangerous areas, workforce mustering and scheduling; postevent management — for example, improving crisis management procedures, life/safety follow-ups to personnel, audits or legal investigations.

- During a cyberattack, you don’t want the attackers to know you are aware of their presence, so communicating via offline channels is an important crisis management tactic.
- Some EMNS vendors are expanding into more general employee communication scenarios which can broaden use cases and better rationalize investments and broader use.

Obstacles

- Not keeping contact information up to date — A regular process is required to maintain current workforce contact information synched to typical systems of record for contact information such as HR or the enterprise directory.
- Not every worker may be in a system of record — for example, part-time workers, consultants, and contractors. Having every worker in the EMNS is critical for providing duty of care support.
- With EMNS use cases expanding beyond traditional emergencies, customers are using more EMNS functionality complicating integration with more applications.
- COVID-19 has shown that organizations want a single solution for all employee communications — crisis and operational. This can lead to message fragmentation and less effective crisis communications.

User Recommendations

- Strengthen crisis communication procedures before implementing EMNS — bad processes are only exaggerated by automation.
- Document all messaging use cases by location, department,business service, channels, contact groups, role types, languages, systems of record, application integration points and privacy requirements, before selecting the EMNS solution.
- Survey the workforce's level of comfort in using a corporate-issued mobile app on their personal mobile device. You may not realize the benefit of mobile app-only functionality.
- Select an EMNS vendor that has messaging data centers locations to ensure compliance with your privacy requirements, and that the same crisis doesn't impact you and the vendor.
- Work with HR, corporate communications and IT departments to create notification groups.
- Create templates for each event type your organization may experience, as well as templates to cover the full crisis life cycle.
- Conduct quarterly tests to improve contact currentness and response rate.

Sample Vendors

AlertMedia; AlertSense; Aurea; BlackBerry; Everbridge; Kinetic Global; OnSolve; Rave Mobile Safety; Singlewire Software; xMatters

Gartner Recommended Reading

Market Guide for Emergency/Mass Notification Services SolutionsMarket Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to WorkMarket Guide for Employee Communications Applications

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

Entering the Plateau

Continuous Data Protection

Analysis By: Santhosh Rao, Jerry Rozeman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

CDP is an approach to continuously, or nearly continuously, capture and transmit changes to applications, files and/or blocks of data. Depending on solution architecture, real-time changes are journaled or replicated to a local or remote storage target. This provides options for more granular recovery point objectives and is used for operational recovery, disaster recovery and data migration use cases.

Why This Is Important

CDP changes how data is protected, decreasing backup and recovery times and providing multiple recovery points. Compared to traditional backup, where the recovery point can be a day old, CDP can support RPOs measured hours, minutes or even seconds. Through integrating live-mounting capabilities, CDP technology can also meet quite demanding Recovery Time Objectives. This combination of flexible and reduced RTO can make CDP an effective countermeasure against ransomware.

Business Impact

Backup typically operates on a daily schedule. As a result, there is significant data loss if the organization is forced to restore from conventional backup. In contrast, true CDP operates continuously, capturing changes as they happen to provide more recovery points and minimize potential data loss. Near-CDP runs with new recovery points created every few minutes. CDP systems can meet much more demanding recovery point and recovery time objectives than possible with conventional backup.

Drivers

True-CDP and near-CDP capabilities are increasingly integrated with backup software capabilities, but can still be packaged as server-based software, as network-based appliances or as part of a storage controller snapshot implementation. The delineation between frequent snapshots (one to four per hour, or less granularity) and near CDP is not crisp. Administrators often implement snapshots and CDP solutions in a near-CDP manner to strike a balance between resource utilization and improved recoverability. More recently, backup vendors have introduced CDP capabilities for VMware environments by integrating vSphere APIs. Gartner has observed that true-CDP implementations are often used for files, email and laptop data, but adoption for replication and recovery of VMs, databases and other applications is also a common use case.

Obstacles

Ensure that the bandwidth requirements of CDP are addressed before implementing the solution.

CDP deployments are often bandwidth intensive and may require upgrading the existing network infrastructure. Procuring dedicated CDP solutions alongside traditional backup solutions will increase overall total cost ownership. Additionally, in some cases, CDP solutions may impact application performance and may require resizing the production environment.

User Recommendations

- Select CDP for critical data where regular snapshots and/or backups are unable to meet RPO requirements.
- When implementing CDP solutions, understand the data change rate and ensure that the replication bandwidth requirements are addressed.
- Select backup vendors that provide integrated CDP.

Sample Vendors

Commvault; Dell; Veeam Software; Veritas; Zerto

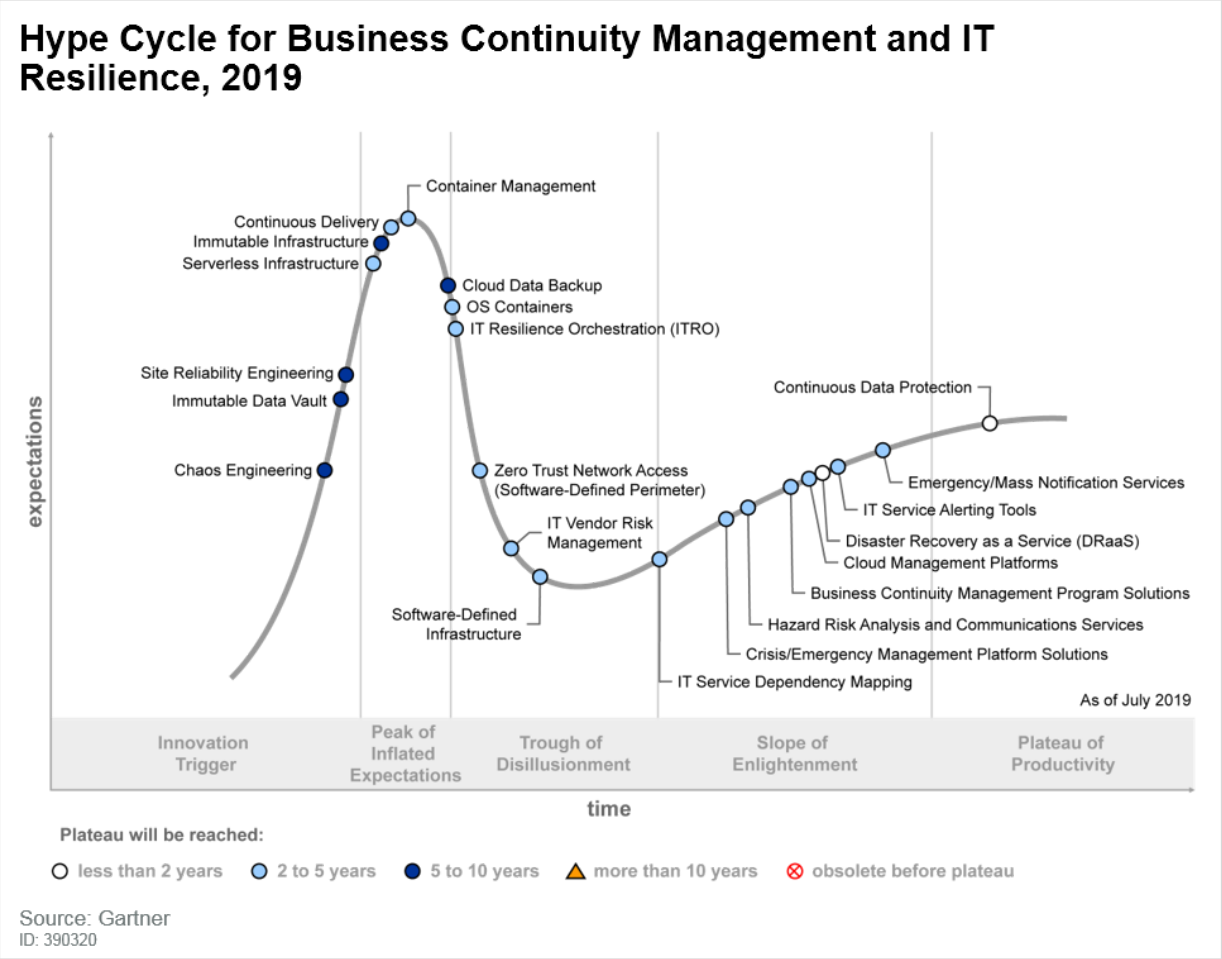
Gartner Recommended Reading

Magic Quadrant for Data Center Backup and Recovery Solutions

Critical Capabilities for Data Center Backup and Recovery Solutions

Appendixes

Figure 2. Hype Cycle for Business Continuity Management and IT Resilience, 2019

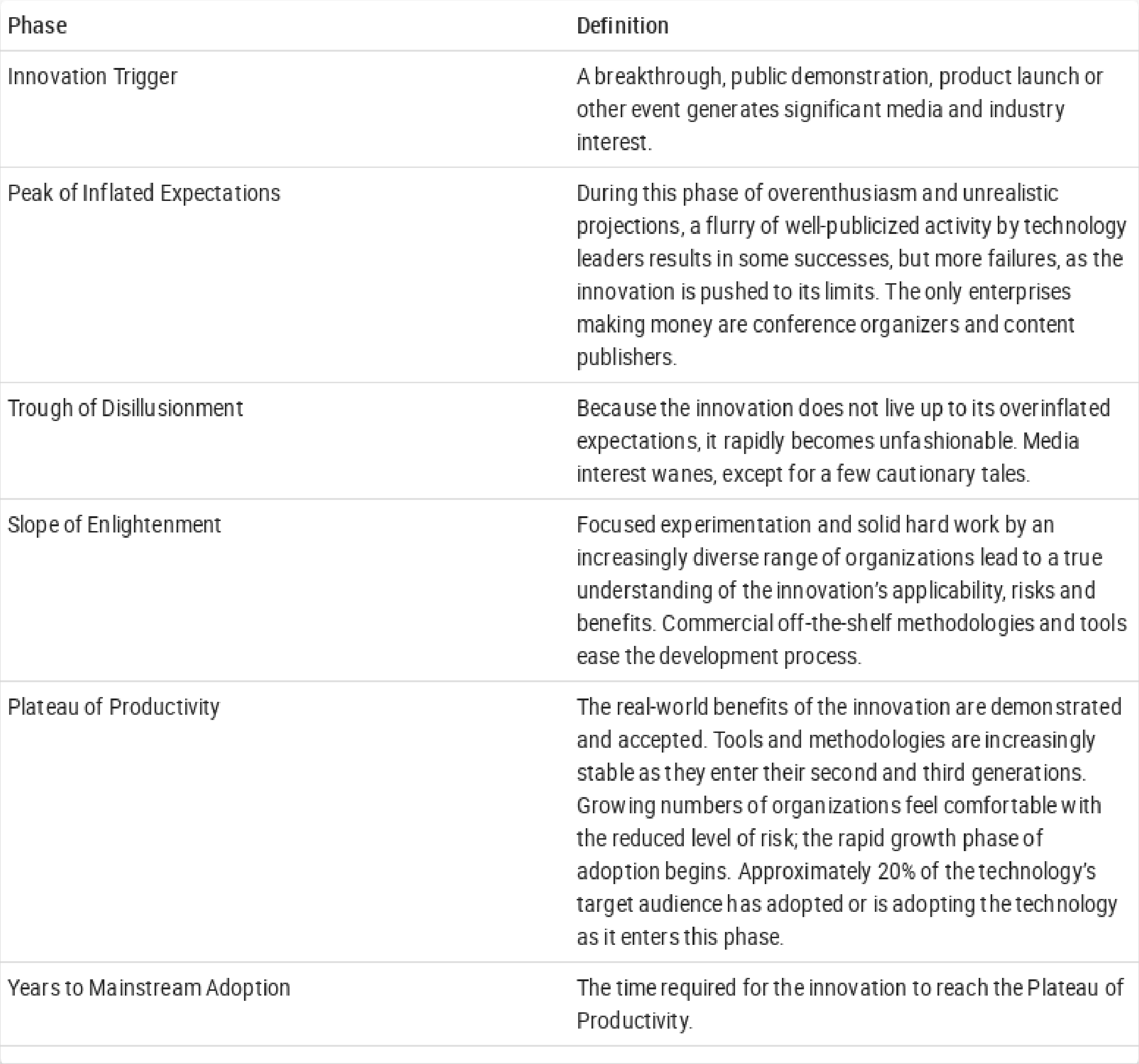


Source: Gartner (July 2019)

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)

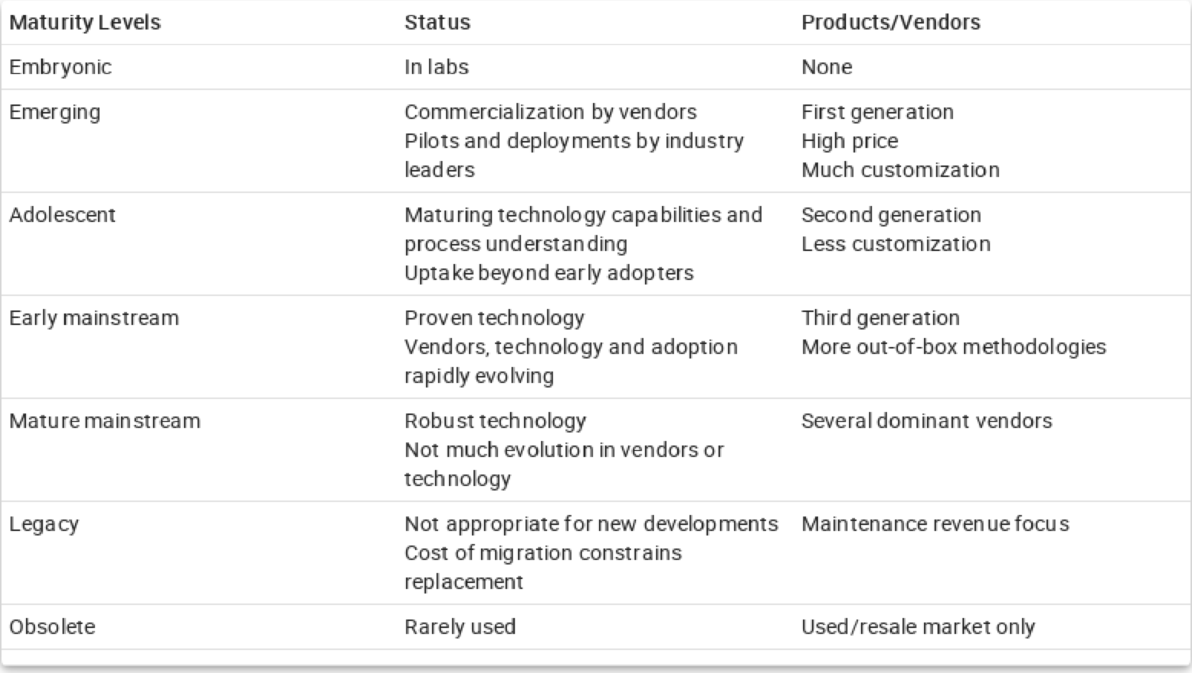
Table 3: Benefit Ratings

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 Business Continuity Management and IT Resilience, 2019 - 31 July 2019

Hype Cycle for Business Continuity Management and IT Resilience, 2017 - 2 August 2017

Hype Cycle for Business Continuity Management and IT Resilience, 2016 - 2 August 2016

Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2015 - 15 July 2015

Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2014 - 22 July 2014

Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2013 - 31 July 2013

Hype Cycle for Business Continuity Management and IT Disaster Recovery Management, 2012 - 23 July 2012

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

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

Market Guide for Emergency/Mass Notification Services Solutions

Market Guide for Crisis/Emergency Management Solutions and COVID-19 Safe Return to Work

Market Guide for Business Continuity Management Program Solutions, 2021

2020 Strategic Road Map for Business Continuity Management

Table 1: Priority Matrix for Business Continuity Management and IT Resilience, 2021

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational		Real-Time Incident Center as a Service Site Reliability Engineering		
High	BCMP Solutions COVID-19 Health Risk Mitigation Emergency/Mass Notification Services Hazard/Threat Intelligence Services IT Service Dependency Mapping Social Distancing Technologies	Automated Incident Response Continuous Data Protection Crisis/Emergency Management Solutions Immutable Data Vault	Chaos Engineering Supply Chain Risk Management	
Moderate	Disaster Recovery as a Service IT Resilience Orchestration	IT Vendor Risk Management ZTNA	Cloud Data 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.

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)