Hype Cycle for Midsize Enterprises, 2023

Published 17 July 2023 - ID G00795570 - 142 min read

By Analyst(s): Mike Cisek, Albert Gauthier

Initiatives: Midsize Enterprise Technology Leadership

Effective investments in technology are among the most substantive ways to augment the limited capabilities of resource-constrained midsize enterprises. This Hype Cycle helps MSE technology leaders identify and strategically apply technology solutions to execute against business and IT priorities.

Analysis

What You Need to Know

This Hype Cycle highlights technologies with wide-ranging impact and benefits to midsize enterprises (MSEs). Two categories of technologies are featured:

- The right half of the Hype Cycle includes technologies acknowledged as mature by the market, representing investments of lower risk and proven value within MSE environments. Leading MSEs leverage solutions in this category to improve operational execution and efficiency.
- The left half of the Hype Cycle highlights technologies that may be “overhyped” at the moment but still represent potential opportunities for first-mover advantage based on the size scale and attributes of MSEs.

MSE technology leaders must keep a close watch on the development of technologies that impact their industry verticals and individual organizations, as depicted in the Priority Matrix table, and make investments based on technical feasibility, affordability and appetite for risk. Specific investment decisions should be informed by examining other relevant Hype Cycles and discussions with Gartner analysts who specialize in those areas.

The Hype Cycle

The economic, cultural and operational characteristics of MSEs strongly influence technology and business decision-making. According to MSE respondents to the 2023 Gartner CIO and Technology Executive Survey, [1] the top five technology areas where the largest amount of new or additional funding, most of which are cloud based, will be allocated are:

1. Cyber/information security (69%)
2. Business intelligence/data analytics (58%)
3. Application modernization (42%)
4. Cloud platforms (42%)
5. Integration technologies/APIs/API architecture (40%)

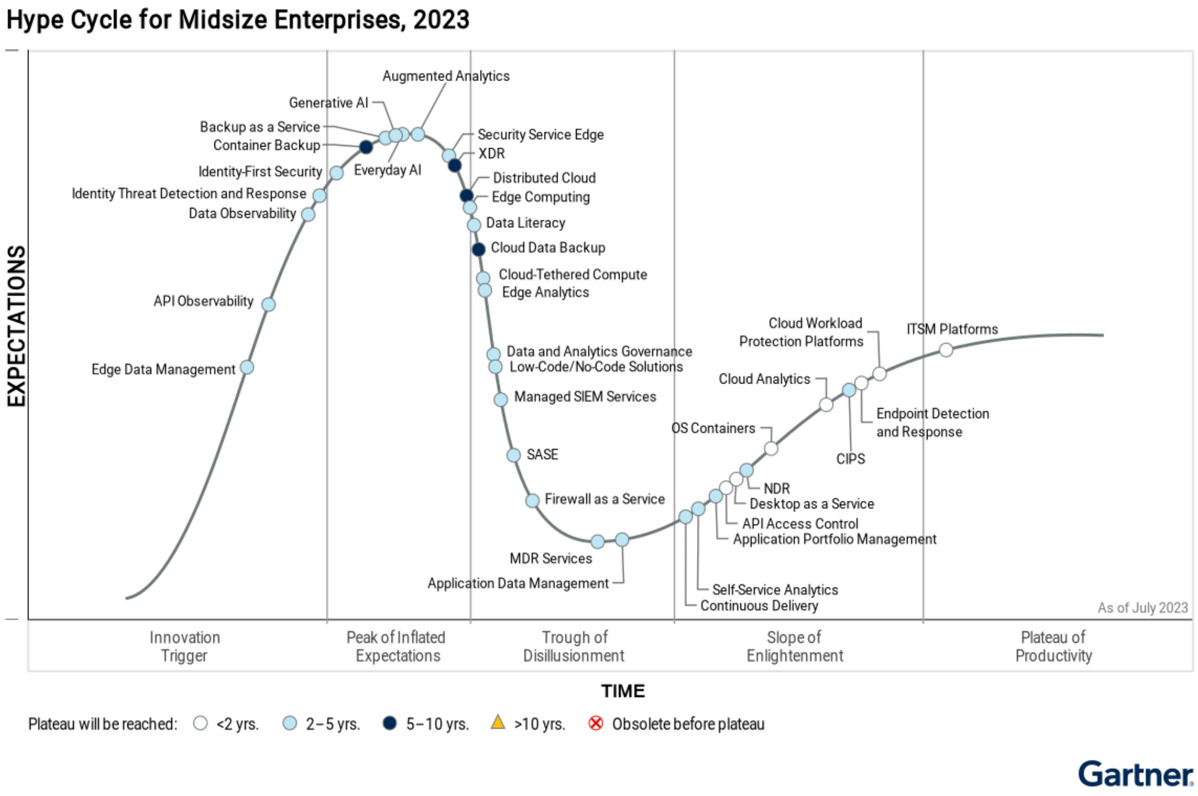
This Hype Cycle highlights technologies that encapsulate these investment categories, via innovation profiles, and aggregates them into the resulting three strategic technology trends:

- **Security and risk management** — Align security strategies to workforce and outsourcing plans to design a comprehensive cybersecurity program that addresses objectives for risk management, governance and operational requirements in a practical, cost-effective manner.
- **Data-driven insights and tools —** Empower data-driven insights and decision making through the use of integrations, analytics, generative and traditional AI focused on high impact business use cases and a collection of high-quality data.
- **Distributed hybrid infrastructure —** Enable hybrid and remote work and allow for the extension of public cloud services to locations outside of the primary public cloud regions, providing services and workloads the ability to securely and efficiently traverse on-premises, cloud-native and edge environments.

This Hype Cycle is intended to help MSE technology leaders develop a compelling vision and sound strategies aligned and rightsized to their operating environment and IT and business priorities. Effective execution at scale is dependent on their IT organizations' ability to maximize capacity for change and increase opportunities to introduce technology to innovate, address operational deficiencies and expand influence within the business. MSE technology leaders must rationalize and optimize technology portfolios while experimenting with emerging technologies to effectively:

- Develop technology thought leadership by diffusing hype and inspiring the business, showcasing the technology-enabling opportunities available to improve business outcomes.
- Determine where investments in alternative approaches and/or technology can displace legacy solutions or transform and improve long-standing processes.

Figure 1. Hype Cycle for Midsize Enterprises, 2023

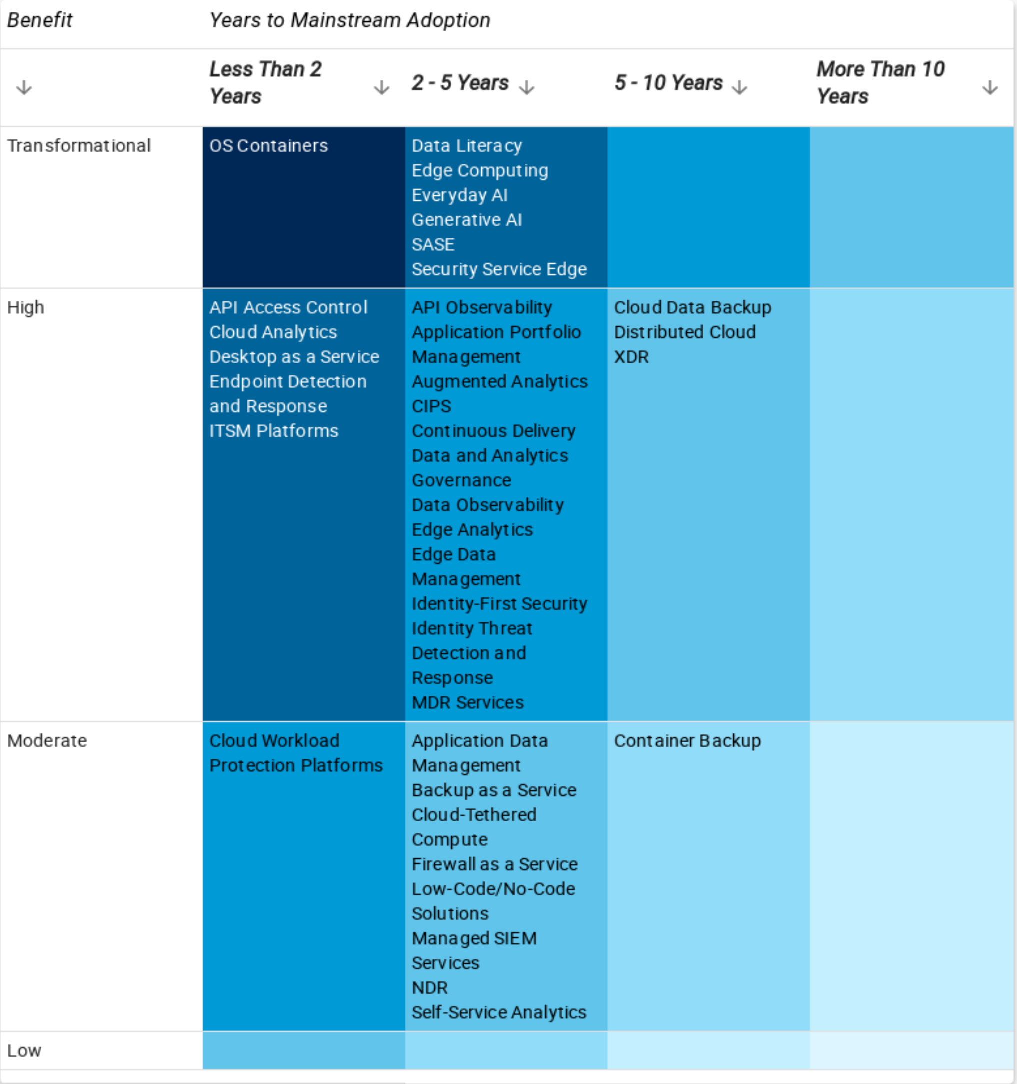


The Priority Matrix

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

Table 1: Priority Matrix for Midsize Enterprises, 2023

(Enlarged table in Appendix)



Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	OS Containers	Data Literacy Edge Computing Everyday AI Generative AI SASE Security Service Edge		
High	API Access Control Cloud Analytics Desktop as a Service Endpoint Detection and Response ITSM Platforms	API Observability Application Portfolio Management Augmented Analytics CIPS Continuous Delivery Data and Analytics Governance Data Observability Edge Analytics Edge Data Management Identity-First Security Identity Threat Detection and Response MDR Services	Cloud Data Backup Distributed Cloud XDR	
Moderate	Cloud Workload Protection Platforms	Application Data Management Backup as a Service Cloud-Tethered Compute Firewall as a Service Low-Code/No-Code Solutions Managed SIEM Services NDR Self-Service Analytics	Container Backup	
Low				

Source: Gartner (July 2023)

On the Rise

Edge Data Management

Analysis By: Aaron Rosenbaum

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Edge data management comprises the capabilities and practices required to capture, organize, store, integrate and govern data outside of traditional data center and public cloud environments. An increasing number of digital business use cases, including those based on IoT solutions, will leverage data in edge environments. This expansion creates tremendous opportunities to optimize resources and drive real-time decisions and actions, but also brings complexity and governance challenges.

Why This Is Important

Valuable data is increasingly generated and used outside of traditional data centers and cloud environments. This data often has a shorter useful life span, requiring value to be captured near the place and time of its origin. This is the role of edge-computing environments deployed closer to assets in the physical world. Edge data management will both impact and enable IT leaders and their teams, requiring new capabilities and skills while also opening up new opportunities to deliver value.

Business Impact

Edge data management creates value in various ways:

- By distributing data management to the edge, data-centric solutions better support demand for local and real-time data.
- More solutions, such as for IoT use cases, must operate in disconnected (or intermittently connected and low-bandwidth) scenarios.
- It enables smarter physical assets and collections of assets, including remote management or autonomous behavior, via edge data.

- It addresses inconsistencies, protection, sovereignty and other governance issues arising from siloed edge environments.

Drivers

- **Extreme speed:** By placing data, data management capabilities and analytics workloads at optimal points ranging all the way out to endpoint devices, enterprises can enable more real-time use cases. In addition, the flexibility to move data management workloads up and down the continuum from centralized data centers or the cloud to edge devices will enable greater optimization of resources.

- **Data gravity:** Bandwidth costs and scenarios with limited or intermittent connectivity demand the ability to organize and process data closer to the edge.

- **Expanded scale and reach:** By using distributed computing resources, and spreading the load across the ecosystem, enterprises can broadly scale their capabilities and extend their impact into more areas of the business. These areas include use cases and outcomes traditionally managed only via operational technology (OT) teams, such as those managing equipment in industrial settings. Dedicated hardware for edge processing of data will continue to amplify these benefits.

- **Resiliency:** Pushing data management capabilities toward edge environments can also bring benefits in the form of greater fault tolerance and autonomous behavior. If edge environments do not require centralized resources, then issues with connectivity to, or unplanned downtime of, those centralized resources don't disrupt processes that rely on local edge capabilities.

Obstacles

- **Management of distributed data architectures:** Data management has been largely based on principles of centralization — bringing data to central data stores (e.g., data warehouses), and then processing that data to create value. Edge environments break that model via distributed data architectures, raising complex choices about where to locate and aggregate data on the continuum of cloud/data center to edge. Determining the right balance of latency and consistency is one such choice.

- **Governance and security:** With the distribution and complexity of edge environments, data governance and security become challenging. Organizations should extend their governance practices and policies to address edge-resident data storage and processing capabilities, including disposal of ephemeral or nonvalue event data.

- **Organizational and skills considerations:** Many modern applications are being developed and deployed by OT teams lacking data management skills and oversight, or by IT teams lacking edge computing skills and experience.

User Recommendations

- Identify use cases where data management capabilities in edge environments can enable differentiated products and services by collaborating with OT and IT personnel working in edge locations.
- Expand the skill sets of IT and OT teams to include edge platforms and the technologies required to manage data and data-intensive workloads on them.
- Augment existing data management infrastructure to support edge deployment by partnering with product teams that are implementing IoT platforms and similar distributed computing architectures.
- Place a greater emphasis on end-to-end system design. Understanding the dependencies between all components of distributed data pipelines, analytics workloads and AI models will be crucial to success.
- Ensure safety and control by extending existing governance capabilities to edge data environments.

Sample Vendors

Couchbase; FairCom; IBM; Macrometa; Microsoft; MongoDB; ObjectBox; Xencia

Gartner Recommended Reading

Get Ready for Data Management at the Edge: Key Considerations and Actions

Building an Edge Computing Strategy

Forecast: Internet of Things, Endpoints and Communications, Worldwide, 2022-2032, 1Q23 Update

Forecast Analysis: Edge Hardware Infrastructure, Worldwide

API Observability

Analysis By: Dave Micko

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

APIs continue to become more important as software architecture patterns and critical integration tools, so API providers require increasing visibility into how their APIs operate and change. Observation based on telemetry emitted from logs, performance statistics and external monitoring is aggregated and normalized via OpenTelemetry (OTel) standards to provide running snapshots of API performance and reliability.

Why This Is Important

Monitoring business-critical APIs is integral to business operations. From detecting changes to monitoring running states, observability captures data from each phase. API observability has moved from simple log analysis to sophisticated dashboards aggregating telemetry across many APIs, as well as integration with code repositories and integrated development environments (IDEs). Developers and API platform and platform engineering teams are affected by API observability systems and practices.

Business Impact

API observability has grown into dashboards aggregating telemetry into action-oriented analysis. API observability can affect everything from reducing mean time to recover (MTTR) to understanding API dependencies across suites of applications (also known as "APIOps"). As platform engineering teams build observability into software development processes, customer aligned teams use observability to address pain points before they become complaints, including detecting changes to APIs.

Drivers

- API observability is key for API-first technical architectures.
- API observability can range from simple log analysis to sophisticated dashboards, from monitoring and alerting to automated analysis of important events, such as an API version change.
- As APIs proliferate, most are fronting complex microservices architectures or serverless functions. Understanding the dependencies among these systems is critical to all phases of system design, from implementation to incident management.
- OTel standards continue to evolve to aggregate views of APIs across traces, metrics and logs. OTel is an open-source framework for building observability into APIs. Many monitoring and observability vendors consume APIs that are built on OTel standards.
- Continued migration to cloud-based infrastructure is driving the need to track and manage APIs and the services that implement them, regardless of their infrastructures; however, many services rely on infrastructure events and logs for monitoring and alerting. Aggregated observability includes combining metrics from on-premises, hybrid and cloud-hosted APIs into a single, observable platform.
- APIs across large enterprises can be variably documented, developed and deployed creating challenges in discoverability and usability. Software engineers must untangle complex ecosystems with emergent behaviors. A single breaking change to an API can have effects across the ecosystem. API observability enables developers to understand ecosystem behaviors at a higher level of abstraction, supporting quicker value delivery.
- The need for higher quality and resiliency is driving the adoption of API observability practices. API observability enables engineers to understand how their APIs and services are performing locally, and how they will perform as part of the ecosystem. This allows bugs, performance issues and user experience (UX) problems to be caught early in the development life cycle.

Obstacles

- Although the techniques and practices of API observability can range from simple monitoring to sophisticated event analysis, describing the importance of observability can be challenging. Securing funding for API observability can be difficult, because a great deal of the data may be trivial and only occasionally operationally critical.

- The value of API observability improves as its scope increases from API design and development to testing and monitoring in production. Developing a platform to meet these needs can be complex and time-consuming.

- Standards that support API observability, such as OTel, are still developing, and it can be easy to make technology and standards adoption decisions that lock an organization into a particular vendor or technology ecosystem.

User Recommendations

- Explore API observability solutions that align with their overall observability strategies. Once a pattern is in place — such as monitoring as part of incident management — expand other observability practices to adjacent organizations or divisions.

- Make API observability the responsibility of a team with an adequate number of engineers working on the implementation of API observability platforms. Make the practice of API observability easy to adopt by value-stream-aligned teams by embedding it in a platform, run by a platform engineering team.

- The cost of observability platforms and approaches, whether “home-brewed” or purchased as a service, can vary greatly. Observability collects a large amount of information, which must be transported, stored and analyzed quickly under mission-critical pressure. Weigh the costs associated with these benefits carefully.

Sample Vendors

Akita Software; Chronosphere; Dynatrace; Moesif; New Relic Datadog; Tyk

Gartner Recommended Reading

Cool Vendors in Software Engineering: Improving Digital Resilience

Magic Quadrant for Application Performance Monitoring and Observability

Top Strategic Technology Trends for 2023: Applied Observability

Consider These Key Functional Areas for Application Performance Monitoring and Observability

How to Start and Scale Your Platform Engineering Team

Data Observability

Analysis By: Melody Chien, Ankush Jain

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Data observability is a technology that supports an organizations' ability to understand the health of an organization's data, data pipelines, data landscape, and data infrastructure by continuously monitoring, tracking, alerting and troubleshooting issues to reduce and prevent data errors or system downtime. It tells us what went wrong based on agreed upon SLAs for data quality and usage; reasons; assesses the impacts; and recommends solutions. Data observability improves reliability of data by increasing our ability to observe changes, discover unknowns and take appropriate actions.

Why This Is Important

Data observability uses data profiling, AI/ML, lineage and active metadata to provide the following benefits:

- **Monitor & Detect:** Provide a holistic view to determine how components of data pipelines are operating, evaluate whether data quality meets expectations, and detect data related issues.
- **Alert & Troubleshoot:** Send right alerts to the right people at the right time and perform root cause analysis.
- **Resolve & Prevent:** Provide recommendations to fix the issues or optimize data pipelines to meet business requirements with the goal to prevent downtime or critical data issues before affecting business.

Business Impact

- Data observability allows technical teams to gain visibility of the health of data pipelines and infrastructure. They can identify possible drifts in various areas, and minimize the time to investigate and solve issues, preventing unplanned outages or critical data errors.
- Business users will also gain visibility of data quality and associated financial impacts. This will ensure appropriate use and management of data to meet governance requirements.
- Data observability allows facilitation and improvement of the data fabric with continuous observations and evaluations of the data and analytics ecosystem.

Drivers

- Data and analytics leaders face a growing number of mixed data stacks, diversity of datasets, unexpected data drifts such as change in schema or business context, high demand for data quality and near zero tolerance of downtime. All these add to the challenges in data management. They need a holistic view of the state of data quality and data pipelines within interconnected systems.
- Data pipelines move data from point to point and deliver data to consumers. This journey can be disrupted by unexpected events such as data quality issues or a lack of infrastructure resources. The data that flows through these pipelines needs to be monitored for loss of quality, performance or efficiency. Organizations need to be able to identify points of failure before they have a chance to propagate. Data observability automatically detects important events and analyzes various signals to troubleshoot the issues, and provides actionable insights of what to do next.
- Data observability goes beyond traditional monitoring. It provides a multidimensional view of data including performance, quality, usage and financial impacts to the downstream applications. Leveraging active metadata, lineage of data and AI/ML, data observability generates real-time insight by monitoring the business context and analyzing data pattern, comparing history, and developing a semantic understanding of the data. It provides an end-to-end observability to help organizations be better equipped to handle critical events and prevent business disruptions.
- This capability is essential to the data fabric design concept and becomes an important building block to further automation in data management practices.

Obstacles

- There is no standard definition of what constitutes a data observability solution. Vendors offer a range of different capabilities often branded as data observability which is causing confusion in the market and leading to issues adopting the tools.

- The current vendor landscapes are very fragmented based on coverage areas and data environments supported. Most vendors focus on observability of the data quality and data pipelines, and are less concerned about data usages and financial impacts. The full end-to-end observations are not quite there yet from individual vendors.

- Most data observability tools only support the modern data stack. This limits their application in large enterprise environments with more complex data environments in many cases using legacy data management tools.

- Most data observability tools target the data engineer persona and are positioned as IT tools. Though business users receive important insights from data observability tools, they may find them less user-friendly.

- Organizations are embracing the concept of “observability.” But the actual adoption of the tools is not straightforward. The consideration of how they connect to the overall ecosystem and connecting this to data governance strategy is still a concern.

User Recommendations

- Identify the data elements or data pipelines which require high standards or SLA in quality, uptime, latency and performance. Pinpoint the gap of current monitoring capabilities vs. desired capabilities to support the requirements.

- Evaluate data observability tools available in the market that can enhance your observability based on priority of business requirements, primary users and interoperability with the enterprise data ecosystems.

- Pilot data observability program by building a monitoring mechanism as a starting point to increase visibility over the health of data. Invest in observability capabilities in a cloud environment first, as it's commonly supported by vendors and is faster and easier to demonstrate value.

- Include both business and IT perspectives when evaluating data observability tools by engaging with both personas early on in the evaluation process.

- Partner with business stakeholders to evaluate and demonstrate business value of data observation practices by tracking improvement of data quality, reduction in downtime and ability to meet SLAs to show tangible benefits.

Sample Vendors

Acceldata; Ataccama; Bigeye; Collibra; IBM; Kensu; Monte Carlo; Soda; Unravel

Gartner Recommended Reading

Data and Analytics Essentials: Data Observability

Quick Answer: What Is Data Observability?

The State of Data Quality Solutions: Augment, Automate and Simplify

Market Guide for DataOps Tools

Identity Threat Detection and Response

Analysis By: Mary Ruddy

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Identity threat detection and response (ITDR) is a discipline that includes tools and best practices that protect identity infrastructure itself from attacks. ITDR can block and detect threats, confirm administrator posture, respond to various types of attacks and restore normal operation as needed.

Why This Is Important

Identity is foundational for security operations (identity-first security). Only authorized end users, devices and services should have access to your systems. As identity becomes more important, threat actors are increasingly targeting the identity infrastructure itself. Organizations must focus more on protecting their IAM infrastructure. ITDR adds an additional layer of security to identity and access management (IAM) and cybersecurity deployments.

Business Impact

Securing your identity infrastructure is mission-critical for security operations. If your accounts are compromised, permissions set incorrectly or your identity infrastructure itself is compromised, attackers can take control of your systems. Protecting your identity infrastructure must be a top priority. “Business-as-usual” processes that seemed adequate before attackers began targeting identity tools directly are no longer sufficient.

Drivers

More sophisticated attackers are actively targeting the IAM infrastructure itself. For instance:

- Administrator credential misuse is now a primary vector for attacks against the identity infrastructure.
- Attackers can use administrative permissions to gain access to the organization’s global administrator account or trusted Security Assertion Markup Language (SAML) token signing certificate to forge SAML tokens for lateral movement.
- Modern attacks have shown that conventional identity hygiene is not enough. There is no such thing as perfect prevention. Multifactor authentication and entitlement management processes can be circumvented, and these tools generally lack mechanisms for detection and response if something goes wrong.

- ITDR is needed in addition to IGA, PAM, a security information and event management (SIEM) solution and an in-house security operations center (SOC) or outsourced managed detection solution. There are major detection gaps between IAM and infrastructure security controls. IAM is traditionally used as a preventive control, whereas infrastructure security is used broadly but has limited depth when detecting identity-specific threats. ITDR mechanisms are more specific and operate with lower latency than general purpose configuration management, detection and response systems.

Obstacles

- ITDR requires coordination between IAM and security teams, which some organizations find difficult to establish.
- Lack of awareness of IAM administrator hygiene, detection and response best practices means that many organizations are not adequately protecting their identity infrastructure. More is needed than just traditional AD TDR.
- IAM teams often spend too much effort protecting other group's digital assets and not enough protecting their own IAM infrastructure.
- Multiple capabilities are required to fully protect identity infrastructure, including more closely monitoring configuration changes to root IAM administrator accounts, detecting when identity tools are compromised, enabling rapid investigations and efficient remediation and the ability to quickly revert to a known good state.
- The "R" part of ITDR is still nascent. Automated responses are still relatively basic.
- Even though there are many different ITDR capabilities, specific vendors provide only some of them.

User Recommendations

- Include ITDR strategy in your formal IAM program. ITDR requires a sponsor who can identify stakeholders and spearhead this collaborative initiative.
- Prioritize securing identity infrastructure with tools to monitor identity attack techniques; protect identity and access controls; detect when attacks are occurring; and enable fast remediation.
- Use the MITRE ATT&CK framework to correlate ITDR techniques with attack scenarios to ensure that at least well-known attack vectors are addressed.
- Combine foundational IAM infrastructure hygiene, such as PAM and IGA, with ITDR. Manage security posture and configuration of user directories and token generators. This will help to achieve identity fabric immunity.
- Prevent administrator accounts from being compromised (e.g., by forcing proper termination of RDP sessions).
- Modernize IAM infrastructure using current and emerging standards (e.g., OAuth 2.0, CAEP).

Sample Vendors

Authomize; CrowdStrike; Gurucul; Microsoft; Netwrix; Oort; Proofpoint (Illusive); Semperis; SentinelOne (Attivo Networks); Silverfort

Gartner Recommended Reading

Top Trends in Cybersecurity 2022

Implement IAM Best Practices for Your Active Directory

At the Peak

Container Backup

Analysis By: Jerry Rozeman

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

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

Why This Is Important

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

Business Impact

Container backup can help:

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

Drivers

- Containerized application adoption will increase at a rapid pace during the next few years primarily driven by the rapid growth of cloud adoption, application modernization leveraging containerization and the need for application mobility. This will fuel the need to protect data in these environments.

- There is a steady increase in use of containers to run stateful applications — the 2022 CNCF Annual Survey shows that over 63% of respondents are running stateful applications in containers in production (an increase from 55% in the 2020 CNCF Annual Survey).
- DevOps processes require tight integration with backup tools that support Kubernetes and can be embedded in the continuous integration/continuous delivery (CI/CD) workflow. Container backup solutions can deliver on this need by delivering data management features that are configured with declarative and immutable artifacts.
- Recovery strategies designed for physical infrastructure and virtual machines (virtualization) don't work well with containers and Kubernetes.

Obstacles

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

User Recommendations

- Determine the need for container backup based on application criticality as not every containerized app requires backup.
- Invest in container knowledge to understand the need for backing up Kubernetes objects like namespaces, secrets, keys and configuration maps, in addition to just persistent volumes.

- Align container backup requirements with the organizational structure as, unlike traditional infrastructure, container backup operations will be performed by the platform or application engineering teams.
- Dedicate budget for protecting containers as it requires additional investments in backup solutions and infrastructure.
- Adopt a strategy for container backup just as with every other data source in your enterprise.
- Select specialized container backup solutions first while traditional backup solution capabilities mature over time.

Sample Vendors

Catalogic Software; Cohesity; Commvault; Dell Technologies; Druva; IBM; Pure Storage; Rubrik; Trilio; Veeam Software

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Innovation Insight for Backup and Recovery for Kubernetes-Based Containerized Applications

Comparing Backup and Disaster Recovery Approaches for Kubernetes

Solution Path for Cloud-Native Infrastructure With Kubernetes

Identity-First Security

Analysis By: Paul Rabinovich

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Identity-first security is an approach to security design that makes identity-based controls the foundational element of an organization's protection architecture. It marks a fundamental shift from perimeter-based controls that have become obsolete because of the decentralization of assets, users and devices. Effective identity-first security relies on context-based access policies that are continuous and consistent.

Why This Is Important

All organizations are operating in a challenging and escalating threat environment. Users and resources are no longer confined to the corporate network, and the corporate network itself cannot be trusted. Identity-first security strategies make identity a cornerstone of security. It shifts the control plane for security from the network (and the physical perimeter) to identity-based controls.

Business Impact

Identity-first security was introduced because the traditional network security model could no longer protect modern organizations. By embracing an identity-first security mindset, organizations can drastically improve their security posture and mitigate security incidents. However, this approach requires a culture shift followed by investments in new tools, processes, policies and architectures.

Drivers

- With the advent of cloud services, digital supply chains and remote access, the perimeter has become porous. A typical organization’s attack surface dramatically expanded to include assets and users outside of the corporate network.
- Hybrid and remote work are here to stay. Gartner predicts that by 2026, 75% of workers will continue to split time between home and office locations. Both company-owned and employee-owned devices may hold company data and must be protected.
- External access to organizations’ applications and data is now common. Enterprises need to collaborate with partners, vendors and suppliers, support API-based access to their information and interact with their customers through digital channels.
- Digital supply chain risks continue to rise. Some organizations share infrastructure with third parties such as managed service providers.
- Identity-first security is a key enabler of zero trust architectures (ZTAs), which depend on identity (and context) for assessing risk.
- An identity-first approach strengthens security by relying on the following core principles (the “3 Cs”): designing *consistent* identity and access management (IAM) policies for all digital assets regardless of their location, using *contextual* data when evaluating access risk, and applying adaptive controls *continuously*, both at login time and throughout user sessions.

Obstacles

- Identity-first security requires a fundamental rethinking of an organization's approach to its protection architecture. One cannot buy an enterprisewide identity-first security product and be done with it. Legacy systems are the biggest barrier to implementing identity-first security. Most software-delivered applications were written on the assumption that they would run in a closed — and benign — environment. Older IAM tools do not natively support anywhere computing, standards-based single sign-on, unmanaged devices and access by external users.

- IAM maturity at many organizations is insufficient to meet the demands of identity-first security such as handling of new types of identity (e.g., machines), new entitlements and advanced controls (e.g., adaptive access).

- Institutional inertia: One of the key principles of the zero trust model is "assume compromise — even on internal networks," but not all organizations recognize this threat or sufficiently invest in its mitigation.

User Recommendations

- Inventory all applications and services and identify where and how they rely on implicit trust. Assess risk and, for those applications and services where existing risk exceeds the organization's risk tolerance, evaluate alternative identity-first security-based architectures and tools that can support them.

- Adopt the three principles (the "3 Cs") of identity-first security. Incorporate contextual data such as risk and recognition signals into your IAM infrastructure, and establish capabilities to share and propagate them across security controls.

- Evaluate the use of device and workload identities to enable more granular access policies and support application-to-application access use cases.

- Ensure that the IAM team effectively communicates with business stakeholders, security teams, infrastructure and operations (I&O), cloud and DevOps as the newly introduced IAM controls will impact both end users and IT personnel.

Gartner Recommended Reading

Identity-First Security Maximizes Cybersecurity Effectiveness

Improve IAM Architecture by Embracing 10 Identity Fabric Principles

Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality

Quick Answer: How to Explain Zero Trust to Technology Executives

The Future of Security Architecture: Cybersecurity Mesh Architecture (CSMA)

Backup as a Service

Analysis By: Jason Donham

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

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

Why This Is Important

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

Business Impact

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

Drivers

- Data proliferation to the edge requires I&O leaders to rethink their overall backup strategy. BaaS can provide a scalable solution across the widely dispersed footprint of edge and remote office/branch office (ROBO) deployments.

- Many small to midsize organizations do not have the skill sets in-house that are required to build and operate a complex backup system.

- Enterprise organizations can utilize BaaS to augment existing backup capabilities to protect hybrid and multicloud data.

- Organizations lack the necessary levels of automation to deploy and easily manage modern backup and recovery systems for on-premises, IaaS, PaaS and SaaS application backups.

- SaaS data is rarely backed up by the SaaS application vendor on the client's behalf. This leaves clients exposed to security flaws in the vendor ecosystem that are beyond client control to identify or remediate.

- The threat of ransomware requires modernization of backup architecture which can be prohibitively expensive. BaaS eliminates the need to periodically replace or upgrade backup systems.

- Organizations want to move from a capital expenditure (capex) model to an operating expenditure (opex) model that is based purely on resource consumption.

Obstacles

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

User Recommendations

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

Sample Vendors

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

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Market Guide for Backup as a Service

Everyday AI

Analysis By: Adam Preset

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Everyday AI refers to snippets of AI services that help workers improve productivity, deliver higher-quality work and save time. Workers interact with everyday AI mostly as features of widely used personal and team productivity applications that are typically deployed across an organization horizontally. These AI services are used by employees throughout the day, and will become increasingly varied and integrated into our working lives.

Why This Is Important

Everyday AI technology aims to help employees deliver work with speed, comprehensiveness and confidence. Recent advances in generative AI promise to streamline content creation, analysis and collaboration. Machine learning and natural language processing capabilities are becoming more common and embedded in application features to enable automation and efficiency. Everyday AI supports a new way of working where intelligent software is acting as more of a collaborator than a tool.

Business Impact

Everyday AI can amplify the productivity of any worker. As digital work becomes more complex, workers are expected to master more capable yet complex applications. Everyday AI can simplify some of that complexity. Employees who wield everyday AI can focus on meaningful, high-value, creative output rather than the routine tasks that can be delegated away. Deployment of technology to meet this need is more scalable and efficient than hiring and training additional talent.

Drivers

Vendors in different technology markets seek to improve worker productivity in novel ways beyond simple application and feature enhancements. The development of everyday AI capabilities delivers these productivity benefits while also providing vendors with a marketable and monetizable set of new capabilities. Gartner expects to see continuing innovation from vendors as they expand their everyday AI features, with collaboration megavendors making the most aggressive investments and prominent announcements.

Several enterprise application markets have AI assist capability that aids workers in various ways. Following are examples of categories and functions that employ everyday AI:

- Business productivity: correcting errors, improving message clarity, coordinating meetings.
- Content creation: composing entire documents or designing presentations based on modest prompts.
- Workstream collaboration: notifications, canned responses, task execution.
- Meeting solutions: transcription, translation, highlighting and identifying action items, meeting scheduling.
- Search: aggregating, summarizing and citing information following natural language prompts.
- HR applications: streamlining access to organizational and employee information.
- Performance management: aggregating metrics data, providing coaching guidance.

Workers generally embrace everyday AI as it helps them save time while reducing drudgery and stress. Organizations will invest further in everyday AI as they see the technology is able to multiply their workers’ output and effort. Everyday AI will become increasingly sophisticated, moving from a service that, for example, can sort and summarize chats and email messages, to services that can write a report with minimal guidance. In many ways, everyday AI is the future of workforce productivity.

Obstacles

- Employees are unaware of everyday AI features. They distrust everyday AI, are concerned about privacy and may resist use due to poor early experiences with it.

- Some routine work processes may not be suitable for everyday AI. Enterprises may need to create foundational governance policies and practice guidance to enable the use of everyday AI. New everyday AI tools backed by generative AI demand more cloud computing resources, so sustainability and environmental impact may limit comfort with the technology.

- The benefits of successful use may be hard to capture or attribute to everyday AI capabilities. Everyday AI may require an explicit request for service, rather than being integrated into how people work where contextual disclosure can be applied.

- Vendors may overrepresent the capabilities of everyday AI. They may create and charge for product models where varying levels of everyday AI features are available at different tiers, which can make broad adoption confusing or expensive.

User Recommendations

- Ensure that employees are aware of everyday AI capabilities in the tools they use. Find out why employees may be hesitant to use everyday AI features and methodically address objections, particularly around privacy.

- Maintain a running inventory of everyday AI features and create an everyday AI digital side hustle. Retain healthy skepticism when vendors claim to have advanced everyday AI capabilities.

- Track new everyday AI usage patterns to inform enablement strategies. Make everyday AI a top software evaluation criterion.

- Be increasingly bold in the approach to everyday AI; look for applications where the use of everyday AI can have an increasingly larger impact, such as in common activities such as creating written and visual content, data analysis and improving meetings.

Sample Vendors

AmplifAI; Beautiful.ai; Calendly; Google; Grammarly; Microsoft

Gartner Recommended Reading

Predicts 2022: Digital Workplace Is Foundational for Employee Experience

Quick Answer: How Can Everyday AI Improve Worker Digital Dexterity?

Quick Answer: How Will AI in Microsoft 365 Copilot Impact the Workplace?

Generative AI

Analysis By: Svetlana Sicular, Brian Burke

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Generative AI technologies can generate new derived versions of content, strategies, designs and methods by learning from large repositories of original source content. Generative AI has profound business impacts, including on content discovery, creation, authenticity and regulations; automation of human work; and customer and employee experiences.

Why This Is Important

Generative AI exploration is accelerating, thanks to the popularity of Stable Diffusion, Midjourney, ChatGPT and large language models. End-user organizations in most industries aggressively experiment with generative AI. Technology vendors form generative AI groups to prioritize delivery of generative-AI-enabled applications and tools. Numerous startups have emerged in 2023 to innovate with generative AI, and we expect this to grow. Some governments are evaluating the impacts of generative AI and preparing to introduce regulations.

Business Impact

Most technology products and services will incorporate generative AI capabilities in the next 12 months, introducing conversational ways of creating and communicating with technologies, leading to their democratization. Generative AI will progress rapidly in industry verticals, scientific discovery and technology commercialization. Sadly, it will also become a security and societal threat when used for nefarious purposes. Responsible AI, trust and security will be necessary for safe exploitation of generative AI.

Drivers

- The hype around generative AI is accelerating. Currently, ChatGPT is the most hyped technology. It relies on generative foundation models, also called “transformers.”

- New foundation models and their new versions, sizes and capabilities are rapidly coming to market. Transformers keep making an impact on language, images, molecular design and computer code generation. They can combine concepts, attributes and styles, creating original images, video and art from a text description or translating audio to different voices and languages.

- Generative adversarial networks, variational autoencoders, autoregressive models and zero-/one-/few-shot learning have been rapidly improving generative modeling while reducing the need for training data.

- Machine learning (ML) and natural language processing platforms are adding generative AI capabilities for reusability of generative models, making them accessible to AI teams.

- Industry applications of generative AI are growing. In healthcare, generative AI creates medical images that depict disease development. In consumer goods, it generates catalogs. In e-commerce, it helps customers “try on” makeup and outfits. In manufacturing, quality inspection uses synthetic data. In semiconductors, generative AI accelerates chip design. Life sciences companies apply generative AI to speed up drug development. Generative AI helps innovate product development through digital twins. It helps create new materials targeting specific properties to optimize catalysts, agrochemicals, fragrances and flavors.

- Generative AI reaches creative work in marketing, design, music, architecture and content. Content creation and improvement in text, images, video and sound enable personalized copywriting, noise cancellation and visual effects in videoconferencing.

- Synthetic data draws enterprises’ attention by helping to augment scarce data, mitigate bias or preserve data privacy. It boosts the accuracy of brain tumor surgery.

- Generative AI will disrupt software coding. Combined with development automation techniques, it can automate up to 30% of the programmers’ work.

Obstacles

- Democratization of generative AI uncovers new ethical and societal concerns. Government regulations may hinder generative AI research. Governments are currently soliciting input on AI safety measures.
- Hallucinations, factual errors, bias, a black-box nature and inexperience with a full AI life cycle preclude the use of generative AI for critical use cases.
- Reproducing generative AI results and finding references for information produced by general-purpose LLMs will be challenging in the near term.
- Low awareness of generative AI among security professionals causes incidents that could undermine generative AI adoption.
- Some vendors will use generative AI terminology to sell subpar “generative AI” solutions.
- Generative AI can be used for many nefarious purposes. Full and accurate detection of generated content, such as deepfakes, will remain challenging or impossible.
- The compute resources for training large, general-purpose foundation models are heavy and not affordable to most enterprises.
- Sustainability concerns about high energy consumption for training generative models are rising.

User Recommendations

- Identify initial use cases where you can improve your solutions with generative AI by relying on purchased capabilities or partnering with specialists. Consult vendor roadmaps to avoid developing similar solutions in-house.
- Pilot ML-powered coding assistants, with an eye toward fast rollouts, to maximize developer productivity.
- Use synthetic data to accelerate the development cycle and lessen regulatory concerns.
- Quantify the advantages and limitations of generative AI. Supply generative AI guidelines, as it requires skills, funds and caution. Weigh technical capabilities with ethical factors. Beware of subpar offerings that exploit the current hype.
- Mitigate generative AI risks by working with legal, security and fraud experts. Technical, institutional and political interventions will be necessary to fight AI's adversarial impacts. Start with data security guidelines.
- Optimize the cost and efficiency of AI solutions by employing composite AI approaches to combine generative AI with other AI techniques.

Sample Vendors

Adobe; Amazon; Anthropic; Google; Grammarly; Hugging Face; Huma.AI; Microsoft; OpenAI; Schrödinger

Gartner Recommended Reading

Innovation Insight for Generative AI

Emerging Tech Roundup: ChatGPT Hype Fuels Urgency for Advancing Conversational AI and Generative AI

Emerging Tech: Venture Capital Growth Insights for Generative AI

Emerging Tech: Generative AI Needs Focus on Accuracy and Veracity to Ensure Widespread B2B Adoption

ChatGPT Research Highlights

Augmented Analytics

Analysis By: David Pidsley, Anirudh Ganeshan

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Augmented analytics uses AI to automate analytics workflows in platforms, contextualizing user interfaces with automated insights, generative storytelling explanations and collaborative exploration. Driven by ML and generative AI, it enables natural language queries and personalized analytics catalogs. It democratizes advanced analytics with augmented data ingestion, preparation, analytics content and DSML model development. It also curbs human biases and accelerates insights for diverse users.

Why This Is Important

Many activities associated with data, including preparation, pattern identification, transformation, model development and insight sharing, remain highly manual. This friction limits the user adoption and business impact of analytics. Enhancing these capabilities with generative AI democratizes analytics and reduces barriers to entry by allowing users to perform complex analytics tasks with low/no code.

Business Impact

Augmented analytics is transforming how users interact with analytics content. Features like conversational interfaces are making analytics more accessible, explainable and expedient. Generative AI is changing how people interact with augmented analytics, enabling access to deeper insights from data. Once confined to experts only, insights from advanced analytics are now in the hands of business analysts, decision makers and operational workers across the enterprise. These augmented consumers are driving new sources of business value.

Drivers

- Organizations increasingly want to analyze more complex datasets combining diverse data from both internal and external sources. With an increasing number of variables to explore in such harmonized data, it is practically impossible for users to explore every pattern combination. It is even more difficult for users to determine whether their findings are the most relevant, significant and actionable. Expanding the use of augmented analytics will reduce the time users spend on exploring data, while giving them more time to act on the most relevant insights.

- Generative AI has accelerated market interest in dynamic data stories and other combinations of augmented analytics features that automate insights. Generative AI combines augmented analytics with natural language query, natural language generation, and anomaly detection to dynamically generate data stories for users in their contexts. This type of multiexperience UI will reduce the use of predefined dashboards for monitoring and analysis, and increase the use of augmented analytics.

- Vendor technology innovation is pushing augmented analytics forward. With the explosion of generative AI, augmented analytics is receiving heightened attention. ABI platforms are now integrating large language models like GPT-4, allowing users to generate, debug and convert code, create data stories, and aid in data preparation. This integration has also enabled newer users to emerge, fueling analytics adoption. In a next wave of generative analytics experiences, users may see the entire workflow become AI-driven.

- Most organizations leverage multiple ABI platforms, causing exponential proliferation of analytics content. Coupled with a lack of governance, this proliferation often leads to inconsistencies in metrics and insights, duplication of reports and dashboards, and an overall decline of trust in data. Hence, analytics catalogs, powered by augmented analytics capabilities with generative AI, are becoming key in allowing users to find and recommend analytics content.

- By integrating with digital workplace applications (e.g., Microsoft Teams and Slack), augmented analytics features allow users to share and collaborate on insights.

Obstacles

- **Lack of trust in autogenerated models and insights:** Organizations must ensure that the augmented approach is transparent and auditable for accuracy and bias. They must establish a process to review and certify analyses created. These guardrails are especially important with generative AI being included within ABI platforms.

- **Training and rapidly evolving skills needs:** Obtaining desired skill sets and data literacy standards is a never-ending challenge, and leaders need broad and diverse training for multiple personas.

- **Ecosystem requirements:** It will be critical to build an ecosystem that includes not only tools, but also data assets, people and processes to support the use of augmented analytics.

- **Cultural barriers:** Analytics developers writing analytics-as-code and business analysts accustomed to visual self-service analytics may regard augmented analytics as a “nice to have” feature. However, they neither utilize nor rely on it in their analytics content production workflows.

User Recommendations

- Identify the personas and use cases that will benefit most from augmented analytics capabilities.

- Ensure that users can get value from new augmented analytics features by providing targeted and context-specific training. Invest in data literacy to ensure responsible adoption.

- Focus on explainability as a key feature to build trust in autogenerated models. Create learning opportunities for those who wish to know more about the theory and inner workings of augmented analytics solutions.

- Assess the augmented analytics capabilities and roadmaps of ABI platforms, data science platforms, data preparation platforms and startups as they mature. Look into the upfront setup and data preparation required, the range of data types and algorithms supported, the integration with existing tools, the explainability of the models, and the accuracy of the findings.

- Provide incentives for citizen data scientists to collaborate with, and be coached by, specialist data scientists who still need to validate models, findings and applications.

Sample Vendors

AnswerRocket; iGenius; Microsoft; Oracle; Pyramid Analytics; Qlik; Sisense; Tableau; Tellius; ThoughtSpot

Gartner Recommended Reading

Market Guide for Augmented Analytics

Magic Quadrant for Analytics and Business Intelligence Platforms

Critical Capabilities for Analytics and Business Intelligence Platforms

Is Your Business Intelligence Enabling Intelligent Business?

Top Trends in Data and Analytics, 2023

Security Service Edge

Analysis By: Charlie Winckless, John Watts

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Security service edge (SSE) secures access to the web, cloud services and private applications. Capabilities include adaptive access control, data security, visibility and control. Further capabilities include an advanced threat defense and acceptable use control enforced by network-based and API-based integrations. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

Why This Is Important

SSE improves organizational flexibility to secure the usage of web and cloud services, and remote work. SSE offerings are the convergence of security functions (at least, secure web gateways [SWGs], cloud access security brokers [CASBs] and zero trust network access [ZTNA]) to reduce complexity and improve user experience. They are delivered from the cloud. When organizations are pursuing a secure access service edge (SASE) architecture, SSE is paired with software-defined WAN (SD-WAN) to simplify networking and security operations.

Business Impact

Hybrid work is continuing to drive the adoption of public cloud services, especially of SaaS applications. Both hybrid work and the adoption of public cloud services remain business enablers for most Gartner clients. SSE allows the organization to support anytime-anywhere workers by using a cloud-centric approach to enforce a security policy when accessing the web, cloud services and private applications. Simultaneously, SSE reduces the administrative complexity of running multiple products.

Drivers

- Organizations need to secure user, application and enterprise data that is distributed, decentralized and requires secure remote access.

- For many enterprises, a significant amount of critical data is now hosted in SaaS. Therefore, there is a need to perform data loss prevention (DLP) on data that is located in, going to, and leaving these SaaS platforms.

- SSE enables flexible and primarily cloud-based security for users and devices without being tied to on-premises network infrastructure and connectivity. The same security outcome is delivered to users regardless of their location or connectivity.

- Administrators can have enhanced visibility on user traffic and a single configuration and monitoring location for this traffic.

- SSE allows organizations to implement a posture based on identity and context at the edge.

- By consolidating vendors, organizations reduce complexity, costs and the number of vendors used to enforce security policy. Using a single SSE platform rather than multiple point offerings, they can both reduce complexity and reduce gaps in security coverage.

- Sensitive data inspection and malware inspection can be done in parallel across all channels of access. SSE allows doing both inspections in parallel, leading to a better performance and more consistent configuration than doing them separately.

- An adaptive access can take into account more input signals and be more consistently enforced, regardless of the application location or type.

- Organizations look for deeper security capabilities when building a SASE architecture compared to vendors that may have a minimal set of security features as part of their SD-WAN offering.

- Tight integrations that exist between discrete SD-WAN and SSE vendors allow interoperability without requiring a single-vendor approach.

Obstacles

- As the market is being formed by the convergence of capabilities, vendors may be strong in certain capabilities and weak in others. Vendors may also lack overall tight integration between SSE capabilities or with SD-WAN vendors.
- Not all vendors provide sufficiently sensitive data identification and protection to manage business risks.
- Some vendors have focused less on SaaS security and integrations. However, businesses increasingly need this visibility and protection.
- Being cloud-centric, SSE typically doesn't address every need supported by on-premises controls such as internal firewalling.
- Organizations are concerned about uptime or availability of services that they depend on for their business. This is compounded by weak SLAs from some vendors.
- Not all vendors provide all features locally in all geographies, resulting in performance or availability issues.
- Switching costs from incumbent vendors or timing of contract expirations prohibit near-term consolidation.
- Migrating from a VPN will increase costs.

User Recommendations

- Exploit the converged market, consolidate vendors, and cut complexity and costs as contracts renew for SWGs, CASBs and VPNs by replacing them with a ZTNA approach.
- Approach SSE consolidation identifying which elements you may already have in place (for example, existing cloud-based CASB or SWG). Develop a shortlist of vendors based on your use cases regarding secure end-user requirements, the cloud services you use, and the data you need to protect.
- Inventory your equipment and contracts to implement a multiyear phaseout of on-premises perimeter and branch security hardware in favor of the cloud-based delivery of SSE.
- Global enterprises should validate that remote offices have acceptable performance and features with selected vendors. Vendor point of presence (POP) locations and service support are key.
- Actively engage with initiatives for branch office transformation, SD-WAN and Multiprotocol Label Switching (MPLS) offload to integrate cloud-based SSE into the scope of project planning.

Sample Vendors

Broadcom; Cisco; Cloudflare; Forcepoint; iboss; Lookout; Netskope; Palo Alto Networks; SkyHigh Security; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Magic Quadrant for Security Service Edge

Critical Capabilities for Security Service Edge

Adopt Security Service Edge (SSE) to Replace Stand-Alone SWG, CASB and ZTNA Products

XDR

Analysis By: Eric Ahlm, Thomas Lintemuth, Franz Hinner

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Extended detection and response (XDR) delivers unified security incident detection and automated response capabilities. XDRs integrate threat intelligence and telemetry data from multiple sources, with security analytics to provide contextualization and correlation of security alerts. XDR must include native sensors. XDR can be delivered on-premises or as a SaaS offering, and is typically deployed by organizations with smaller security teams.

Why This Is Important

XDR offers a less complex approach for threat detection and response by using a systematic, rather than an integration, approach to building a detection stack. XDR vendors can include a variety of security controls, usually natively integrated by the vendor via APIs. The vendor provides prebuilt playbooks that enable collaboration in their stack, and coherence in the detection of common threats.

Business Impact

The simplicity of XDR to detect common threats reduces the need for internal skill sets and could reduce the staff needed to operate a more complex solution, such as security information and event management (SIEM). XDR can also help reduce the time and complexity associated with security operations tasks through a single centralized investigation and response system.

Drivers

- XDR platforms appeal to organizations with modest maturity needs due to the detection logic, mostly vendor-provided, that generally requires less customization and maintenance.

- XDRs appeal to organizations looking for improved visibility across the security stack, as well as those looking to lower the administration requirements of more complex incident response (IR) solutions.

- Midsize organizations that struggle to correlate and respond to alerts generated from disparate security controls appreciate the productivity gain from centralized XDR interfaces.

- Staff with the required skills to maintain and operate an extensible detection stack are hard to recruit and retrain.

- Purchasing a systemic detection stack in the form of XDR can simplify product selection and acquisition.

Obstacles

- Single-vendor systemic XDR solutions may take years to replace in the case of effectiveness or efficiency issues.

- XDR's lack of extensibility for custom detections and other use cases could cause some clients to need both an XDR and a classic SIEM solution to meet multiple needs.

- Expanding an XDR detection stack's capabilities through the addition or replacement of security controls may be limited by the vendor.

- An XDR product alone does not always meet all needs for long-term log storage for use cases other than incident response, such as compliance, application monitoring and performance monitoring. XDR may also be a poor choice for a forensically sound system of record for things such as access data.

User Recommendations

- Work with security operations stakeholders to determine if the XDR strategy is right for your organization.
- Base decision criteria on staffing and productivity levels, level of IT federation, risk tolerance, and security budget, as well as consolidation aims and the presence of existing XDR component tools.
- Develop an internal architecture and purchasing policy that is in line with your XDR strategy, one that explains when and why exceptions might be permissible.
- Plan security purchases and technology retirements in relation to a long-term XDR architecture strategy.
- Favor security products that provide APIs for information sharing, and that allow automated actions to be sent from an XDR solution.

Sample Vendors

CrowdStrike; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Stellar Cyber; Trend Micro; Trellix

Gartner Recommended Reading

Market Guide for Security Orchestration, Automation and Response Solutions

Distributed Cloud

Analysis By: David Smith, Daryl Plummer, Milind Govekar, David Cearley

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

Distributed cloud refers to the distribution of cloud services to different physical locations, while operation, governance, updates and evolution of the services are the responsibility of the originating cloud provider. Distributed cloud computing is a style of cloud computing where the location of cloud services is a critical component of the model.

Why This Is Important

Distributed cloud enables organizations to use consistent cloud-based services wherever needed, while the cloud service provider retains the responsibility of managing the technology, implementation and evolution of the capabilities. It gives organizations the flexibility to support use cases that will benefit from cloud services, regardless of their dependence on specific locations. Organizations can use distributed cloud to reimagine use cases where cloud computing is not currently feasible.

Business Impact

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

Drivers

- Historically, location has not been relevant to cloud computing definitions. In fact, the variations on cloud (e.g., public, private, hybrid) exist because location can vary.

- Distributed cloud supports both tethered and untethered operations of cloud services from the cloud provider, “distributed” out to specific and varied physical locations. This enables an important characteristic of distributed cloud operation — low-latency compute where the compute operations for the cloud services are closer to those that need the capabilities. This can deliver major improvements in performance and reduce the risk of global network-related outages.

- Data sovereignty and other regulatory issues may require services be delivered from locations beyond the data centers of the public cloud service provider.

- Perceived and real security and privacy concerns with off-premises applications and infrastructure drive some consumers to prefer on-premises solutions.

- Latency needs of IoT/edge applications require services to be located close to the edge.

- Distributed cloud is still a single-cloud provider, and the managed cloud assets are still part of the cloud provider’s portfolio.

- Disconnected operations can be supported with distributed services that can operate independently.

Obstacles

- Customers can't abandon existing technologies in favor of complete and immediate migration to the public cloud, due to sunk costs, latency requirements, regulatory requirements, and the need for integration.
- Different approaches to distributed cloud have different value propositions (e.g., portability, software, appliance). Customers need to maintain visibility back to original goals.
- Distributed services are a relatively small subset of the centralized services, will take time to expand, and will likely never reach 100% parity with public cloud.
- Distributed cloud in your data center will have limits to scale and elasticity, which do not exist with the centralized public cloud. More advanced approaches like distributed cloud embedded in networking or telecom equipment — or delivered as metro area services — are very immature.

User Recommendations

- Overcome the fear of a single franchise controlling the public cloud and on-premises cloud estates, and consider targeted use of distributed cloud.
- Identify scenarios where distributed cloud use-case requirements can be met by evolution of a hybrid cloud model and where the requirements are substantially different. Prefer distributed cloud over building a hybrid cloud. Use the distributed cloud model to prepare for the next generation of cloud computing by targeting location-dependent use cases.
- View vendor claims of the scope of services available and their functional parity with public cloud services skeptically, and demand specific details and data to back up the claims.
- Temper concern about vendor revenue recognition and reporting. As with many capabilities that are thought of as more feature than product, revenue recognition and reporting by vendors are only one indicator of success.

Sample Vendors

Amazon Web Services (AWS); Google; IBM; Microsoft; Oracle

Gartner Recommended Reading

The Cloud Strategy Cookbook, 2023

Comparing On-Premises Public Cloud Appliances: AWS Outposts, Microsoft Azure Stack Hub and Google Distributed Cloud Edge

Distributed Cloud: Does the Hype Live Up to Reality?

Edge Computing

Analysis By: Bob Gill, Philip Dawson

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

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

Why This Is Important

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

Business Impact

Edge computing improves efficiency, cost control, and security and resilience through processing closer to where the data is generated or acted upon, fostering business opportunities and growth (e.g., customer experience and new real-time business interactions). Earliest implementations succeeded in enterprises that rely on operational technology (OT) systems and data outside core IT, such as the retail and industrial sectors.

Drivers

- Growth of hyperscale cloud adoption has exposed the limits of extreme centralization. Latency, bandwidth requirements, the need for autonomy and data sovereignty or location requirements may be optimized by placing workloads and data closer to the edge, rather than centralizing in a hyperscale data center.

- Data growth from interactive applications and systems at the edge often cannot be economically funneled into the cloud.

- Applications supporting customer engagement and analysis favor local processing for speed and autonomy.

- IoT is evolving from simply reporting device status to using edge-located intelligence to act upon such status, bringing the benefits of automation and the creation of immediately responsive closed loop systems.

- Edge computing's inherent decoupling of application front ends and back ends provides a perfect means of fostering innovation and enhanced ways to do business. For example, using technologies such as machine learning and industrial sensors to perform new tasks at locations where business and operational events take place, or at the point of interaction with a retail customer, can drive significant business value.

Obstacles

- The diversity of devices, software controls and application types all amplify complexity issues.
- Widespread edge topology and explicit application and networking architectures for edge computing are not yet common outside vertical applications, such as retail and manufacturing.
- Edge success in industrial IoT applications and enhancing customer experience in retail are well-understood, but many enterprises still have difficulty understanding the benefits, use cases and ROI of edge computing.
- A lack of broadly accepted standards slows development and deployment time, creating lock-in concern for many enterprise users.
- Edge physical infrastructure is mature, but distributed application management and orchestration challenges are still beyond most vendor-supplied component management offerings. The tasks of securing, maintaining and updating the physical infrastructure, software and data require improvement before management and orchestration can mature.

User Recommendations

IT leaders responsible for cloud and edge infrastructure should:

- Create and follow an enterprise edge strategy by focusing first on business benefit and holistic systems, not simply focusing on technical solutions or products.
- Position edge computing as an ongoing, enterprisewide journey toward distributed computing, not simply individual isolated projects.
- Establish a modular, extensible edge architecture through the use of emerging edge frameworks and design sets.
- Accelerate time to benefit and derisk technical decisions through the use of vertically aligned systems integrators and independent software vendors that can implement and manage the full orchestration stack from top to bottom.
- Evaluate “edge-as-a-service” deployment options, which deliver business-outcome-based solutions that adhere to specific SLAs while shifting deployment, complexity and obsolescence risk to the provider.

Gartner Recommended Reading

Market Guide for Edge Computing

5 Top Practices of Successful Edge Computing Implementers

Sliding into the Trough

Data Literacy

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

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Data literacy is the ability to read, write and communicate data in context, with an understanding of the data sources and constructs, analytical methods and techniques applied. Data-literate individuals have the ability to identify, understand, interpret and act upon data within business context and influence the resulting business value or outcomes.

Why This Is Important

Data and analytics (D&A) are pervasive in all aspects of businesses, communities and our personal lives. Thus, data literacy is foundational to the digital economy and society. It helps stakeholders:

- Draw a directlink between D&A and desired outcomes
- Unlock knowledge workers' business acumen
- Explain how to identify, access, integrate and manage datasets
- Draw insights relevant to specific use cases
- Describe advanced analytics techniques and enable AI
- Reduce risk through improved decision making

Business Impact

To become data-driven and equipped to use data and analytics to their competitive advantage, enterprises require explicit and lasting organizational change. Chief data and analytics officers (CDAOs) need to promote and orchestrate “leadership moments” where they act as role models, exemplifying new cultural traits at critical points. To be successful, they will need to guide the workforce by addressing both data literacy and data-driven culture.

Drivers

- The continued growth in digital transformation is amplifying a focus on D&A best practices. Employee data literacy is becoming increasingly recognized as an important factor in an organization’s overall digital dexterity.

- The role of the D&A function has evolved. It is now at the core of an organization’s business model and digital platforms, and with everyone being an information worker, the footprint of business use of data and analytics is broader than ever before.

- Effective D&A strategies require an increased focus on change management. Higher-performing CDAOs prioritize their emphasis, energy and effort on change management requirements, including data literacy.

- Defining what data-driven behaviors are expected — using a “from/to/because” approach — is central to employee development plans. It ensures that creators, consumers and intermediaries have the necessary D&A skills, knowledge and competencies.

- Data literacy is not a one-off project. CDAOs need to take immediate action to create and sustain data literacy through assessment of maturity, awareness, and education. Quick wins build momentum, but lasting and meaningful change takes time because it requires people to learn new skills and behave in new ways. (For example, there is a hunger for this type of skills development within Gen Z, especially in order to future-proof their careers.)

Obstacles

- Lack of common data literacy models/frameworks/standards and terminology.

- Varying interpretations of the term “data literacy” in terms of training, curriculum and understanding, ranging from enhanced data visualization skills to fostering business curiosity about data.

- Failure to measure contribution of data to business outcomes.

- A sporadic and inconsistent approach to training and certification.
- Not recognizing that data use is a behavioral change or change management initiative.
- Lack of talent and poor data literacy within the current workforce.
- Lack of initiatives to address cultural and data literacy challenges within strategies and programs.
- Overall adoption will still take years, due to the complexity of upskilling entire workforces.
- Data literacy is treated as a checkbox activity, especially when delegated to more junior (and unempowered) resources.
- Lack of a designated leader accountable for the development and execution of the program, roadmap and communication plan.

User Recommendations

- Make the business case for data literacy by identifying stakeholder outcomes and linking these to underlying learning needs.
- Designate a leader who will be accountable for developing and executing the roadmap.
- Foster data literacy during D&A requirements gathering by bringing data and business experts together around the problem to be solved.
- Call out examples of “good” and “bad” data literacy to promote desired behaviors.
- Nurture data literacy by rewarding stakeholders who recognize this as a factor for success and sharing their stories.
- Partner with HR and business leaders to incorporate data literacy learning outcomes into job descriptions, career paths and employee value proposition.
- Use data literacy assessments to evaluate current skill levels and desire to participate.
- Go beyond vendor product training to focus on people’s role- and industry-related D&A skills. Improve learning effectiveness by using a mix of training delivery methods (classroom, online, community, on the job).

Sample Vendors

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

Gartner Recommended Reading

How CDAOs Must Lead Data Literacy and Data-Driven Culture

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

Drive Business Outcomes by Measuring the Value of Data Literacy

Tackle Data Literacy Head-On to Avoid Data and Analytics Program Failure

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

Cloud Data Backup

Analysis By: Jerry Rozeman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Cloud data backup tools back up and restore production data generated in the cloud. Data can be created by SaaS tools (e.g., Microsoft 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

Public cloud providers typically offer infrastructure resilience and availability to protect their systems from server, site or region failures, and generally provide shared responsibility for the data. When data is lost due to user or administrator error, configuration and patching changes, development issues, software corruption, or malicious attacks, user organizations are responsible, rather than the cloud provider. Cloud data backup tools address these deficiencies.

Business Impact

Adopting cloud data backup tools will deliver:

- Confidence in routine data backup of critical computing and application data
- The ability to comply with data protection policies
- Improved availability of data to recover after infrastructure failure, user or administrator errors, software corruption, or malicious attacks

Drivers

- As more production workloads migrate to the cloud (in the form of SaaS, PaaS or IaaS), it has become critical to protect the data generated natively in the cloud.
- Cloud providers focus on infrastructure high availability and disaster recovery (DR), 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 365 is widely adopted, the need for better protection is growing rapidly, which is especially driven by Microsoft's inconsistent and incomplete use of recycle bins, the requirement for retention policies, and lack of intuitive recovery processes.
- Backup of Salesforce data is the second-most-addressed workload by vendors in this space.
- Native backup of IaaS and PaaS data usually resorts to cloud-based snapshots and scripting, which may lack application consistency, restore options, data mobility, storage efficiency and policy-based automation, and do not provide a secure, independent external copy of the data.
- Interest in providing backup for Azure AD, Azure DevOps and GitHub is rising.

Obstacles

- Deploying data protection for cloud-based workloads is often an afterthought, because it is not part of the original business case for cloud-based workload deployment or migration.
- In-depth review of each cloud vendor's SLAs is another obstacle that customers have to overcome, because it limits them in their speed of cloud adoption.
- The outcome of the SLA review might block the cloud service adoption because the SLA might not meet company requirements.
- Besides Microsoft 365 and Salesforce, most SaaS-based applications do not support third-party, external backup solutions that limit customers in protecting these workloads.
- Adopting cloud data backup tools will require significant investments in software, services and/or infrastructure, knowledge and processes.
- Establishing partnerships by IT with apps, DevOps and other teams to structure data protection can be a challenge.

User Recommendations

- Ensure that an enterprise-class data backup and recovery strategy is part of every cloud deployment or migration, which aligns with organizational compliance requirements.
- Evaluate and thoroughly understand cloud-native backup and recovery capabilities, and compare them with your company protection policies before migrating applications to SaaS, PaaS or IaaS data infrastructure solutions.
- Ensure that contracts with cloud providers clearly specify the capabilities and costs associated with the backup solution, including exit fees, and understand the limitations of such solutions.
- Factor in the cost of cloud backup application, in addition to the cost of hosting the production application in 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; HYCU; Keepit; OwnBackup; Rubrik; Veeam; Veritas

Gartner Recommended Reading

Magic Quadrant for Enterprise Backup and Recovery Software Solutions

Critical Capabilities for Enterprise Backup and Recovery Software Solutions

Market Guide for Backup as a Service

Innovation Insight: Backup for SaaS Applications

Quick Answer: Should I Back Up Microsoft 365?

Cloud-Tethered Compute

Analysis By: Tony Harvey, David Wright

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

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

Why This Is Important

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

Business Impact

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

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

Drivers

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

Obstacles

- There is a risk of insufficient agility. Current three year agreements and fixed hardware investments are at odds with the dynamic and changing nature of the edge infrastructure markets.
- There are limitations on service availability, causing a misalignment with customer expectations. What services customers actually want and what the various providers are able to deliver have, to date, not matched up fully.
- There are differences in deployment models between IT-based solutions that deploy into data centers and cloud-tethered solutions that are being deployed into environments more traditionally associated with operational technologies.
- In many cases, supporting vendor expertise and maintenance of field solutions is new and untested.

User Recommendations

- Identify scenarios in which the tethered compute model provides clear business value versus a more-traditional IT solution.
- Ensure that field maintenance operations and SLAs are well-documented and understood.
- Use pilot programs to evaluate vendor capabilities and any necessary updates to I&O procedures, processes and skill sets.
- Organize a joint team that includes infrastructure and operations (I&O), operational technology (OT), vendor management and finance to evaluate all proposed cloud-tethered compute solutions.
- Assess the economics and requirements against a range of vendor solutions and consumption models. Each vendor will have very different capabilities.
- Ensure that contract terms and SLAs meet the requirements of the finance and IT teams, and that end-of-term options (or lack thereof) are fully understood.
- Clarify and document where the boundaries exist between the responsibilities of the supplier and those of the IT team. Elements such as data backup and application security are likely to be the end user's responsibility.

Sample Vendors

Avassa; EDJX; Hivecell; Microsoft; Pratexo; Spectro Cloud; Sunlight

Gartner Recommended Reading

Distributed Cloud: Does the Hype Live Up to Reality?

Comparing On-Premises Public Cloud Appliances: AWS Outposts, Microsoft Azure Stack Hub and Google Distributed Cloud Edge

Market Guide For Edge Computing

Emerging Tech Impact Radar: Cloud Computing

Emerging Tech Impact Radar: Edge Computing

Edge Analytics

Analysis By: Peter Krensky

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Analytics is the discipline that applies logic (e.g., “rules”) and mathematics (“algorithms”) to data to provide insights that drive organization strategy and decision making. “Edge” analytics means that the analytics are executed in distributed devices, servers or gateways located outside of data centers and public cloud infrastructure closer to where the data and decisions of interest are created and executed.

Why This Is Important

Gartner client inquiries about the impact of edge on data and analytics continue to increase. With a growing relevance, by 2025, more than 50% of enterprise-managed data will be created and processed outside the data center or cloud. Demand for real-time decision making closer to where the data of interest is created and stored is one of many drivers for edge analytics.

Business Impact

The origins of edge analytics offerings were primarily in the support of decentralized deployments for device-isolated insights. However, connectivity advances, demands for cross-device analytics and innovations surrounding IoT have dramatically increased the scale and complexity of edge analytics use cases. Real-time event analytics and decision making, autonomous behavior of assets, and fault-tolerant applications hold tremendous potential value for enterprises in many industries.

Drivers

- Advantages of edge analytics include faster response times, reduced network bottlenecks, data filtering, reliability, increased access to data and reduced communications costs.

- Data sovereignty and governance issues related to sensitive/regulated data can constrain D&A teams from adopting centralized/cloud-based environments — moving data outside its originating geography can violate sovereignty regulations. By locating analytics in edge environments, the data remains in the originating locations, increasing the likelihood of compliance.

- The increase of distributed cloud and hyperconverged solutions from public cloud providers, including Amazon Web Services (AWS Outposts), Microsoft (Azure Stack Hub) and Google Cloud (Anthos), are further decentralizing previously cloud-restricted workloads. This perimeter expansion of the cloud brings compute and storage closer to the edge — creating new possibilities for edge-centric analytic workloads.

- 5G networks continue to grow in relevancy and, combined with mobile edge computing, will increase edge analytics use cases — particularly for latency-sensitive deployments.

- More analytics solutions, such as those supporting IoT use cases, need to operate in disconnected (or intermittently connected) scenarios. By bringing more powerful analytics capabilities to edge environments, these solutions need not rely on centralized data centers or cloud resources. As demand grows for “smarter” physical assets in many industries, supporting autonomous behavior will be a common requirement.

Obstacles

- Some of the disadvantages of edge analytics include increased complexity, lack of cross-device analytics, overhead of device maintenance and technical currency demands.
- Architectural design and development best practices for traditional or cloud-resident analytics typically assume or prioritize data/analytics centrality and do not carry over directly for edge analytics use cases.
- Vendor choices include two extremes in terms of provider scale — with early and unknown startups competing head-to-head with global megavendors. This drives a mix of platform/protocol standards and complicates going concern considerations for prospective buyers.
- Edge analytics can increase the complexity of enterprise standards and governance (data privacy, security, etc.), which has the potential to delay overall value realization objectives.

User Recommendations

Analytics leaders should consider edge analytics across the following five imperatives:

- Provide analytic insights for individual devices, assets or a larger distributed site even in the midst of disconnection from cloud or data center infrastructure and resources (e.g., driverless cars).
- Provide data sovereignty. Many regulations or data privacy laws require data be kept in the location of origin or the organization deems the transfer of data to introduce too many security vulnerabilities.
- Adapt to scenarios where network connectivity does not have the ability to support desired latency or stability requirements.
- Address scenarios where cross-device interdependencies serving as part of a larger system require edge-resident analytics.
- Redesign analytic strategies where it costs too much to upload the full volume of generated data and where there is no benefit to moving device-level data to a central location for aggregated analysis.

Sample Vendors

Amazon Web Services; Arundo; CloudPlugs; FogHorn; Microsoft; PTC; Samsara; TIBCO Software

Gartner Recommended Reading

Market Guide for Edge Computing

Innovation Insight for Edge AI

The Edge of the Edge Overview

Emerging Technologies Impact Radar: Edge AI

Data and Analytics Governance

Analysis By: Saul Judah, Andrew White

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

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

Why This Is Important

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

Business Impact

Data and analytics leaders should anticipate the following impacts:

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

Drivers

- Higher levels of risk appetite and growth expectations in organizations are based on digital as an implicit part of growth strategies. This requires data and analytics governance capabilities that enable flexibility, scale and resiliency. Data and analytics governance is hence recognized by CDAOs as among the top three critical enablers for successful data and analytics initiatives.
- Investment in data and analytics is widespread across enterprises, with business functions spending as much as central IT teams on these initiatives, causing proliferation of information silos. The need for effective governance capabilities has therefore become an increasing concern for data and analytics leaders as a framework for enabling the connected enterprise, while also addressing the local information needs of business functions.
- Organizations with higher information maturity increasingly recognize that taking a data and analytics governance approach — rather than one focusing on individual information asset types (e.g., data governance) — yields better business results. Elsewhere, we have seen organizations recognize the urgent need to establish governance "to get the ball rolling," even if it is for only data governance or analytics governance. This significant increase in effort and hype relating to data and analytics governance is being seen in all industries, geographies, organization types and maturity levels.
- Hype and interest are also growing in many areas related to data and analytics governance. These areas include AI model governance, analytics governance in data warehouses and data lakes, trust-based governance, IoT data governance, and ethics as a discrete governance policy type.

Obstacles

- Data and analytics governance is complex, organizationally challenging and politically sensitive. It is often difficult to get executive-level consensus for data and analytics governance programs, and as a result, they are led by IT, with a view to "bringing in the business later." Because these initiatives are not business-outcome-based, they typically result in failure.

- Despite the diversity and complexity of business scenarios, most organizations continue to take a one-size-fits-all, command-and-control approach to their data and analytics governance. Furthermore, most organizations have a poor understanding of executive leader accountability and decision rights for information. Establishing an effective governance for data and analytics is therefore difficult to achieve. As organizations' expectations of what can realistically be achieved through data and analytics governance decline, we see its position on the Hype Cycle descend into the Trough of Disillusionment.

User Recommendations

- Identify critical business outcomes that need good data and analytics to be successful. Focus your governance work there to maximize your investment, developing a business case if needed.

- Engage key business stakeholders and the CDAO in sponsoring and driving the initiative to enable information culture change.

- Focus on the least amount of data with the maximum business impact, while managing your risk to embed data and analytics governance in the full business context.

- Clearly define the scope of work related to data and analytics governance: policy evaluation and setting, policy interpretation and enforcement, and policy execution. The first two must be led by the business; the latter can be enabled by IT.

- Examine how data standards and metadata management can be used to implement data and analytics governance in the enterprise. Though business leaders may not fully understand their importance, an industrial governance capability needs enterprise-scale data and analytics capabilities.

Gartner Recommended Reading

7 Must-Have Foundations to Build a Modern Data and Analytics Governance Program

2022 Strategic Roadmap for Data and Analytics Governance

Quick Answer: How Can I Apply Composable Design Principles to Data and Analytics Governance Organization Capabilities?

Next Best Actions to Improve Your Data and Analytics Governance

5 Steps to Build a Business Case for Data and Analytics Governance That Even Humans Will Understand

Low-Code/No-Code Solutions

Analysis By: Laurie Shotton

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Low-code/no-code solutions are application platforms that support rapid application development, deployment, execution and management using declarative, high-level programming abstractions such as model-driven and metadata-based programming languages, and one-step deployments. Low-code/no-code solutions provide and support user interfaces, business processes and data services.

Why This Is Important

Life and P&C insurers look to low-code/no-code solutions for the promise of fast development of solutions and flexibility in process definition across business lines and value chain processes, with minimal IT involvement. They are seen as a way to harmonize and alleviate legacy systems and spreadsheet processes providing a mechanism to develop applications with modern user experiences while retaining their legacy systems.

Business Impact

Low-code/no-code solutions are applicable across the value chain at life and P&C insurance companies.

- They can be used to create common processes across disparate legacy systems or enable easy-to-create solutions for portals.

- They provide a more robust option for manual processes developed in Microsoft Excel and other less-sophisticated approaches.

- They enable business technologists with business user interfaces, offering them the freedom to create and maintain business applications.

Drivers

- Interest in low-code/no-code solutions remains high with the 2022 Gartner Financial Services Technology Survey revealing that 56% of insurance respondents have already deployed or are in short-term planning/experimenting with low-code/no-code solutions.

- Solutions that promote efficiency and enable rapid change with minimal code cutting have been gaining traction for a while, in particular, robotic process automation (RPA). Low-code/no-code solutions represent an extension of this promise.

- Low code is seen as an approach to tackle application modernization and reduce technical debt.

- The duplicity of core and supporting systems that overlap in functional features have led to business users having to be skilled in different user interfaces to achieve the same goals. Low-code/no-code solutions offer the opportunity to harmonize and streamline process steps.

- Central IT backlogs are driving interest in solutions to solve business application needs with the promise of shorter implementation times and reduced reliance on IT.

- Low-code/no-code solutions offer the opportunity to build standardized persona-driven processes on top of legacy systems that lack that capability.

- Business users are requesting IT to help them launch products quicker to market as their legacy systems make launching new marketable products complex and time consuming. Insurers are turning to low-code/no-code solutions with the promise of more configurable product engines.

- With rapid deployment promises and ease of configuration statements, insurers are turning to low-code/no-code solutions to respond to the challenges of their legacy environments.

- Low-code/no-code solutions address the business need for greater resilience, while also supporting the drive for faster technology deployment and process change.
- Insurers are also looking for alternatives to the incumbent core and supporting system providers, and see low-code/no-code solutions as a way of self-developing their offerings.

Obstacles

- A proliferation of the term low-code/no-code has seen vendors across a spectrum of technologies adopt the term to describe the configuration capabilities of their solutions. This complicates vendor selection processes and requires more scrutiny of the capabilities and differentials of vendors adopting the term.
- Low-code/no-code solution hype doesn't really match the reality of the ease of adopting such solutions.
- Many solutions lack any knowledge of insurance processes and rules, requiring insurers to define and enter the rule base.
- Where insurance-focused solutions exist, they are only available for certain parts of the value chain (for example, claims data ingestion and facilitation) or are unable to support a full range of products.
- Typically, the solutions are no more configurable than traditional core and supporting systems that already contain the insurance knowledge, industry content and rule base.
- Deployments risk masking the inefficiencies of legacy technology, while diluting the business case for legacy modernization.

User Recommendations

- Avoid being led by the term low-code/no-code and look at defining the business outcomes and functional capabilities that solution needs to provide and use that assessment to evaluate a portfolio of vendors.
- Develop a checklist to ascertain the real need for low-code/no-code solutions over traditional incumbent vendors.
- Adopt an adaptive governance approach to low-code/no-code system deployments to balance control with business agility.
- Extend the responsibilities of an enterprise architect to ensure consistency in rule and process definition to create greater reusability and consistency when deploying low-code/no-code solutions.
- Reduce software shelfware by agreeing at an executive leadership or board level that all signoff for purchasing low-code/no-code solutions needs to be centralized to avoid duplicate software being acquired.

Sample Vendors

Appian; INSTANDA; Mendix Technology; OutSystems; Salesforce; Socotra; Unqork

Gartner Recommended Reading

Quick Answer: 5 Considerations for Insurance CIOs to Evaluate Low-Code Vendors

Insurance CIOs: Use This Checklist to Determine Low-Code/No-Code System Adaptability and Flexibility

Insurance CIOs: Low-Code/No-Code Solutions Require an Adaptive Governance Framework

Managed SIEM Services

Analysis By: Pete Shoard

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Definition:

Managed security information and event management (MSIEM) services provide remote management and/or monitoring of a client-owned SIEM solution. Services ensure availability and performance, and assist with the creation of a wide range of SIEM use cases, data acquisition, and reporting content.

Why This Is Important

Organizations of all sizes are making strategic investments in SIEM. Flexibility, customization and service requirements are at the center of a decision to utilize managed SIEM. The lack of available skills for deployment and maintenance means that buyers require the assistance from a managed service. The challenge that faces organizations is not the investment in technology, but the ongoing complexity, staffing and cost of supporting SIEM deployments.

Business Impact

Organizations make SIEM purchases, but often struggle to operate them effectively. Detection and response is critical to the success of any security strategy. SIEMs are becoming more accessible, as more midsecurity and midmaturity buyers are entering the market by adopting cloud-based IT. Managed SIEM provides value in overlooked areas, such as creation and tuning of detection content/reporting, maintenance, and lightweight investigation of security issues.

Drivers

- The complexity of SIEM deployments and configuration requirements means that many buyers do not have the in-house expertise to build, configure, and maintain SIEM.

- Buyers require the ability to continuously build and update the detection content and reporting within the SIEM. This requires expert knowledge of the threat landscape and other data manipulation skills, which are hard to acquire and retain.

- Different to turnkey services, such as managed detection and response (MDR) managed SIEM, provides buyers greater flexibility and customization in configuring a dedicated detection and response capability. Managed SIEM is often a follow-up pathway to MDR, which is chosen as an organization’s security maturity increases and internal skill sets grow.

- Managed SIEM provides resources to triage the large volume of alerts and threats discovered by SIEM deployments in a cost-effective manner. It also provides resources outside of normal business hours.

- Buyers may already have a services provider or systems integrator, where this partner has implemented a SIEM for threat detection and incident response on behalf of the buyer.

- Many buyers have adopted, or plan to adopt, SaaS SIEM offerings in line with other infrastructure investments, migrating from legacy on-premises deployments or existing SaaS SIEM platforms. The requirements of these migrations are complex and can benefit from assistance from experienced managed SIEM vendors.

Obstacles

- Direct requirements setting is imperative for engagement with a managed SIEM provider, as most services focus on technology implementation rather than scoping.
- The flexibility of managed SIEM engagements means several elements are customizable, including technology choice and implementation. While it is important to have a clear vision, understanding what is of value for the organization is troublesome.
- Managed SIEM providers operate on a consultative basis regarding requirements, which could increase cost if not correctly worded before engaging with the provider.
- Managed SIEM services augment security staffing and operational internal capabilities, but internal staff will still be needed to consume the raw outputs.
- Sharing operational responsibilities between an internal team and an external partner can be challenging, with segmentation of responsibility being hard to define effectively, often leading to dissatisfaction with services.

User Recommendations

- Identify details of use cases early to establish requirements for log data, threat detection and incident response, and any compliance reporting needs to ensure the project costs are well-controlled.
- Evaluate the use of SaaS SIEM to identify whether a managed SIEM provider is required. SaaS SIEM offers lower overheads for technology maintenance.
- Document the organization’s network architecture, including deployed security controls, SaaS and IaaS investments, and details of other high-priority integrations, such as identity services, before engaging with managed SIEM vendors. If they are not available, invest in a consultative engagement before purchasing a service.
- Separate requirements aligned to the management of the technology, the creation of content to run on the SIEM, and the operational tasks associated with running and maintaining the platform. Decide which components are best aligned with the support you seek from a service.

Sample Vendors

AT&T; BlueVoyant; Capgemini; NCC Group; ReliaQuest; Talion; Vodafone; Wipro

Gartner Recommended Reading

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

Market Guide for Managed SIEM Services

A Guidance Framework for Architecting and Deploying a Modern SIEM Solution

SASE

Analysis By: Neil MacDonald, Andrew Lerner

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

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

Why This Is Important

SASE is a key enabler of modern digital business transformation, including work from anywhere and the adoption of edge computing and cloud-delivered applications. It increases visibility, agility, performance, resilience and security. SASE also dramatically simplifies the delivery and operation of critical network and security services mainly via a cloud-delivered model. SASE reduces the number of vendors required for secure access to one or two explicitly partnered vendors.

Business Impact

SASE enables:

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

Drivers

- Digital business transformation including the adoption of cloud-based services by mobile workforces, edge computing and business continuity plans that must include a flexible, anywhere, anytime, secure, identity-based logical perimeter model of SASE.
- The need to flexibly support digital business transformation efforts with a zero trust security architecture while managing complexity is a significant factor for the adoption of SASE, primarily delivered as a cloud-based service.
- For IT, SASE can reduce the deployment time for new users, locations, applications and devices.
- For information security, SASE enables a single way to set policy enforcement consistently across all types of access — internet, web applications and private applications, reducing the attack surface and shortening remediation times.
- Enterprise desire to simplify network and network security deployments via the reduction of policy engines and management consoles.

Obstacles

- **Organizational silos, existing investments and skills gaps:** A full SASE implementation requires a coordinated and cohesive approach across security and networking teams, which is challenging given refresh/renewal cycles, silos and existing staff expertise.
- **Organizational bias and regulatory requirements for on-premises deployment:** Some customers have an aversion to the cloud and want to maintain control.
- **Global coverage:** SASE depends upon cloud delivery, and a vendor's cloud footprint may prevent deployments in certain geographies, such as China, Africa, South America and the Middle East.
- **SASE maturity:** SASE capabilities vary widely. Sensitive data visibility and control is often a high-priority capability, but it is difficult for many SASE vendors to address. While your preferred single vendor may lack the capabilities you require, two-vendor partnerships can be a viable approach.

User Recommendations

- Involve the security architect and network architect when evaluating offerings and roadmaps from the incumbent and emerging vendors to ensure an integrated approach.
- Leverage WAN, firewall, VPN hardware refresh cycles or software-defined WAN (SD-WAN) deployments to update network and network security architectures.
- Explore single-vendor SASE, dual-vendor SASE and managed SASE options when investing, but avoid deploying SASE with more than two vendors, regardless of vendor marketing for all core services to minimize complexity and improve performance.
- Use vendor combinations — when selecting a dual-vendor solution — that have explicit integration including turnkey automation and visibility, and ideally management and data plane integration.
- Combine branch office and remote access in a single implementation to ensure consistent policies and minimize the number of vendors required.
- Leverage branch office transformation and dedicated circuit offload projects to adopt SASE.

Sample Vendors

Cato Networks; Cisco Systems; Cloudflare; Forcepoint; Fortinet; Juniper Networks; Netskope; Palo Alto Networks; Versa Networks; Zscaler

Gartner Recommended Reading

2022 Strategic Roadmap for SASE Convergence

Market Guide for Single-Vendor SASE

The Future of Network Security Is in the Cloud

Magic Quadrant for SD-WAN

Magic Quadrant for Security Service Edge

Firewall as a Service

Analysis By: Adam Hils, Rajpreet Kaur

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

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

Why This Is Important

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

Business Impact

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

Drivers

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

Obstacles

- Network firewall hardware appliances comprise the largest security equipment market. The appliance approach has been predominant, and many organizations use appliances effectively and efficiently. Many organizations lack compelling reasons to change to a new form factor.

- Security teams find some FWaaS solutions difficult to implement and manage. New FWaaS deployments often require professional services engagements.

- Over 80% of outbound traffic in organizations uses HTTP and HTTPS. Cloud-based SSE services can protect and inspect this traffic at scale to offload existing hardware firewalls. This makes it much easier and less costly to extend investments in existing firewall hardware than to rearchitect the edge to forward all traffic to a FWaaS.

- FWaaS licensing is based on per-user per-year subscription pricing. This can be more expensive for large organizations with high user counts than hardware-based solutions that may have lower subscription costs, and that can be deployed and used beyond their capital depreciation life span.

User Recommendations

- Verify that the additional hop to FWaaS infrastructure does not create unacceptable latency for some of your sites, and look at models that limit initial investment until acceptable latency is proven. Simpler architecture and increased flexibility must materialize in faster deployment and easier maintenance.

- Determine whether your organization is ready to move its entire security workload to the cloud, or whether you need thicker local devices to address privacy concerns and perform some on-premises segmentation or virtual LAN trunking.

- Assess how FWaaS might impact your branch architecture. Current FWaaS offerings offer mostly outbound security or protect mobile workers or companies that are primarily cloud-hosted. Consider maintaining on-premises firewalls for data center use cases.

- Evaluate the strength of the cloud service in three key respects: data center locations, points of presence and SLAs.

- Determine whether the complexity of an FWaaS project will necessitate a professional services engagement for initial setup and configuration.

Sample Vendors

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

Gartner Recommended Reading

Magic Quadrant for Network Firewalls

Critical Capabilities for Network Firewalls

Select the Right Strategy for Securing Web Access

MDR Services

Analysis By: Andrew Davies

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Managed detection and response (MDR) services provide customers with remotely delivered security operations center (SOC) functions. These allow organizations to rapidly detect, analyze, investigate and actively respond through threat disruption and containment. MDR providers offer turnkey experience, using a technology stack that commonly covers endpoint, network, logs and cloud. This telemetry is analyzed in the provider's platform by experts skilled in threat hunting and incident management.

Why This Is Important

The cyberthreat landscape is in constant movement, and the complexity of attacks are escalating against organizations. Most organizations lack the resources, budget or appetite to build and run their own 24/7 SOC function, which is required to help them protect and defend against attacks that increasingly cause more impact and damage to operations. MDR services enable organizations to mature their threat detection and response coverage.

Business Impact

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

Drivers

- MDR services enable organizations to focus on business-risk-driven outcomes, as they provide the expertise to interpret and deliver against a set of requirements in a turnkey format. Ultimately, this delivers relevant and actionable business outcomes.
- The expansion of an organization's IT infrastructure and digital footprint, moving into a broader set of providers and technologies, puts pressure on organizations to maintain visibility across an ever broader set of attack surfaces. MDR providers offer high-fidelity threat detection and coverage of a wide range of data sources, technologies and SaaS platforms.
- MDR providers allow for remotely delivered response actions, enabling buyers to respond and mitigate issues faster with lower impact to their business. However, the level of autonomy granted to vendors varies according to the trust level. With the improved access to MDR service providers' portals, clients can validate the response for a scenario, and possibly execute it.
- With the variety of risk-based issues that organizations are paying attention to, MDR providers are expanding their capabilities to include exposure management and risk management. The combination of these, with a traditional detection and response capability, are helping clients with the visibility they require.
- Buyers increasingly require fast adoption of mature capabilities that would have taken a long time to build or buy, and have been prohibitively expensive to operate. MDR delivers a turnkey solution for those who have no desire to build and maintain internal capability, or require capability quickly.

Obstacles

- The high diversity of vastly different approaches to offering MDR services often causes buyers to question how strategically to engage a provider.

- Technology vendors with detection and response solutions offer closely named, but often more light-touch overlay services, such as managed endpoint detection and response (MEDR), managed security information and event management (MSIEM), and managed extended detection and response (MXDR). This ends up increasing buyers' confusion.

- Performance issues with MDR service providers and failed engagements are often due to misaligned expectations. Buyers should clearly outline what they require the services to deliver, rather than focus on the technology or data that they want monitored.

- Not assigning staff as the point of contact to the service can cause challenges. Segmentation of operational responsibilities between internal contacts and an external partner, if not defined effectively, usually leads to dissatisfaction with services.

User Recommendations

- Focus on outcomes, not technologies, for MDR buyers. Organizations underinvested in technologies such as EDR and network detection and response (NDR) should favor an approach in which a vendor provides the tools and delivers the desired outcomes, and ensures it is in the contract language.

- Assess MDR services if buyers are lacking staff and expertise to handle incident response activities once a threat has been identified, or want to add threat-hunting capabilities.

- Examine compatibility as a requirement if there are existing investments in threat detection technologies, such as EDR and SIEM.

- Buy MDR services that offer a migration path to more self-service in the future. Looking for vendors that have open communication channels with analysts and delivery teams can support that goal.

- Choose broader managed security service (MSS) capability providers if technology management, compliance monitoring and other MSSs are required — especially those that offer MDR-type services.

Sample Vendors

Arctic Wolf Networks; BlueVoyant; eSentire; Expel; Optiv Security; Pondurance; Rapid7; Red Canary; ReliaQuest; Secureworks

Gartner Recommended Reading

Market Guide for Managed Detection and Response Services

Quick Answer: Key Questions to Ask When Selecting a Managed Detection and Response (MDR) Provider

The Top 3 Technology Priorities in Midsize Enterprises

Application Data Management

Analysis By: Andrew White, Tad Travis

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Application data management (ADM) is a technology-enabled discipline where business and IT work together to ensure uniformity, accuracy, stewardship, governance, semantic consistency and accountability for data in an application or suite, such as ERP, customer data platform or custom-made app. Application data is the consistent and uniform set of identifiers and extended attributes used within an application or suite for items like customers, products or prices.

Why This Is Important

Clients continue to be shocked to find their cloud and application vendors offer modern SaaS and business applications that take scant care of governance of the data they use. The vast majority of business application implementations (including ERP, supply chain management [SCM] and even CRM) still lack holistic solutions for governance and stewardship of data. Whereas master data management (MDM) applies governance to shared data across all applications, ADM applies governance to data in a specific application.

Business Impact

ADM can offer the following benefits:

- Application data, once identified, ensures the correct governance effort is aligned to the right kind of business impact the application should have.
- Stewardship roles in the business, and in operational and analytical use cases, can be determined more effectively.
- Business goals for business applications are more likely assured with a more organized data and analytics governance approach that includes application data.
- MDM programs will help govern such application data that is shared with other applications.

Drivers

- The vast majority of "successful" go-lives of business applications, such as ERP, CRM or custom-built applications, do not include any qualification of data and analytics governance. The result, very often observed in client inquiry, is that, on average, seven months after the go-live, organizations spot the vast array of small but noticeable business issues held hostage to the lack of governed data. Business performance and process integrity fail, and business outcomes start to be negatively impacted.
- MDM was and still is misunderstood. An MDM program should have a laserlike focus on the minimal number of most widely shared attributes describing things like customer and product. Bloated MDM programs will continue to fail, leading to a greater need to split the effort up and create distinct ADM programs/requirements.
- Digital business success hinges not on the quality and governance of all data equally, but on a graduated, efficient means to classify data and apply only the needed level of governance. Such growing demand on scaling digital business will, of necessity, drive increased need to recognize and adopt ADM.

Obstacles

- Some MDM programs associated with large, global ERP, CRM and SCM implementations mistakenly centralize all the work related to governing application data. Others create a hybrid organization across business and IT, and call it all "MDM" (when it isn't). Put another way, these programs conflate MDM and ADM, making both too slow, expensive and unwieldy. As a result, neither program is a success.
- The half-life of a successful business application go-live is, anecdotally, seven months. After that, clients tell Gartner, "We have lost control of our data." This situation has become acceptable because, overall, most organizations don't fail.
- The organization's ability to change is held back, and consequently, budgets are set that even support mediocrity via poor governance practices. This is not an acceptable way to run an organization, but too few data and analytics leaders stand up and say so.
- Traditional top-down governance programs lead to the same misunderstandings and poorly scoped initiatives.

User Recommendations

Starting with a focus on business outcomes to identify what data matters most, organize, classify and govern data based on which data drives the most important business outcomes:

- Identify your application data to scope ADM. That is, identify the data that matters most to a specific set of use cases supported by one application or suite like ERP, e-commerce, product information management or customer data platform.
- Examine reusing MDM solutions to support your ADM implementation — even if in a distinct instance. The business requirements are very similar — but the value propositions are different.
- Demand from your business application provider (and those in the cloud) the necessary capability to set (that is, govern) and enforce (that is, steward) information policy pertaining to data used in the application or suite.
- Implement ADM alongside any MDM program so that they can operate at their own speeds and benefit. They do align and share metadata in support of a wider enterprise information management (EIM) program.

Sample Vendors

ChainSys; Epicor; Oracle; PiLog Group; Tealium; Utopia Global

Gartner Recommended Reading

4 Master Data Best Practices for ERP

Why CIOs in Midsize Enterprises Must Emphasize ERP Data Management

Create a Master Data Roadmap With Gartner's MDM Maturity Model

Climbing the Slope

Continuous Delivery

Analysis By: Hassan Ennaciri

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Continuous delivery (CD) is a software engineering approach that enables teams to build critical software quickly, while ensuring the software can be released reliably anytime. Through dependable, low-risk releases, CD allows continuous adaptation of the software to incorporate user feedback, market shifts and business strategy changes. This approach requires the engineering discipline to facilitate complete automation of the software delivery pipeline.

Why This Is Important

The growing success of DevOps initiatives continues to drive investments in CD capabilities. CD improves software release velocity and reliability, while simplifying compliance enforcement via automation. It is a prerequisite and the first step to continuous software deployments for organizations that aspire to push changes with zero downtime.

Business Impact

CD is a key practice for a DevOps initiative as it reduces the build-to-production cycle time. As a result, it accelerates the positive impact of new applications, functions, features and fixes by increasing velocity across the application life cycle. The positive impacts include improved business delivery and end-user satisfaction, improved business performance and agility, and risk mitigation via rapid delivery of updates.

Drivers

- Increased adoption of Agile and DevOps practices to deliver solutions.
- Pressure from digital business to improve release velocity and reliability.
- Additional compliance requirements that require automation and orchestration of release activities for better traceability and auditability.

- The need to improve delivery outcomes to deploy application builds and updates more consistently, by extending the benefits of continuous integration (CI) and automated testing to continuously build deployable software.

Obstacles

- Organizational culture and collaboration between teams with different roles and skills are major barriers to CD success. Agile practices that helped bridge the gap between business and development must be extended to deployment, environment configuration, monitoring, and support activities.
- Lack of value stream mapping of product delivery hinders visibility and quick feedback loops for continuous improvements. Teams struggle to improve and focus on value work, as they don't have insights into the critical steps in the process, the time each step takes, handoffs, and wait states.
- Manual steps and processes involved in deploying to production environments impact software flow delivery.
- Other challenges impacting the success of CD include application architecture, lack of automation in all areas of testing, environment provisioning, configuration security and compliance.

User Recommendations

- Evaluate all associated technologies when you start a CD initiative and take an iterative approach to adoption. This will require collaboration with different stakeholders from the product, development, security and operations teams.
- Establish consistency across application environments for a higher likelihood of success and implement a continuous improvement process that relies on value stream metrics.
- Evaluate and invest in associated tooling, such as application release orchestration tools, containers, and infrastructure automation tools. These tools provide some degree of environment modeling and management, which can prove invaluable for scaling CD capabilities across multiple applications.
- Explore a DevOps platform that provides fully integrated capabilities and enables continuous delivery of software.

Sample Vendors

Broadcom; CloudBees; GitLab; Harness; JFrog; Red Hat

Gartner Recommended Reading

How to Build and Evolve Your DevOps Toolchains

Market Guide for Value Stream Management Platforms

Beware the DevOps Toolchain Debt Collector

Self-Service Analytics

Analysis By: David Pidsley, Alys Woodward, Peter Krensky, Sharat Menon, Anirudh Ganeshan, Edgar Macari

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Self-service analytics (SSA) refers to technology and processes in which line-of-business professionals are enabled to autonomously prepare and visualize data, perform queries, and generate reports, with nominal IT support or involvement. SSA is often characterized by low-code/no-code tools that are increasingly augmented via AI. These tools provide increasingly sophisticated data preparation and analytics capabilities, but are simplified for ease of understanding and frictionless data access.

Why This Is Important

Self-service analytics fosters agility by enfranchising business analysts. It gives analysts direct access to data, enabling them to blend data, derive insights and collaborate on data visualizations. This approach reduces IT bottlenecks, accelerates decision making and enhances efficiency. While SSA is useful for rapid prototyping, complex scenarios may still necessitate IT support and analytics developer intervention for data integration, cataloging, pixel-perfect reporting or advanced analytics.

Business Impact

Self-service analytics is critical to scaling the benefits of data-driven decision making. Many centralized D&A functions struggle to keep up with requests for data and insights coming from decentralized teams. Emerging business technologists or citizen data scientist personas who understand the business context of the data are able to use powerful no-code/low-code data preparation and analytics platforms to quickly discover insights.

Drivers

- **Enhanced vendor offerings:** Analytics and business intelligence (ABI) platforms and vendors in adjacent markets continue to improve SSA capabilities, ensuring alignment with the abilities of less technical users, such as business analysts.

- **Evolving business-user needs:** As business users' information requirements advance, they expect SSA to extend into data management. Tasks such as adding data sources, selecting from data catalogs and integrating external data sources are anticipated capabilities for advanced business analysts (power users or citizen developers).

- **Decentralized budgets and spending patterns:** Compared with central IT teams, lines of business allocate a larger proportion of their overall IT budgets to D&A, emphasizing the need for self-service solutions that cater to their specific requirements.

- **Demand for timely insights:** Business users require prompt insights, but centralized teams may struggle to provide the necessary support. This support gap drives users to seek modern BI tools enabling SSA.

- **Decision-making empowerment:** SSA allows business users to access critical information and make data-driven decisions faster, uncovering valuable insights that might have been overlooked by centralized teams.

- **Analytics collaboration:** Organizations are increasingly seeking to provide environments where a diverse range of users can simultaneously co-produce analytics projects. This collaboration enables users to share knowledge, streamline workflows and drive collective decision making, further boosting the adoption of SSA.

- **Metrics stores and governance:** A virtualized layer that allows users to define and manage metrics as code supports governing metrics from data warehouses and servicing all downstream SSA, data science and business applications.

- **Generative AI:** ABI platforms are increasingly integrating large language models like GPT, which can be leveraged in data preparation, code generation, debugging, and creation of data stories and visualizations. Generative AI accelerates SSA, allowing newer users to enter this workflow. However, intelligent prescriptive applications lessen the need for visual SSA.

Obstacles

- **Governance challenges:** Inadequate user enablement and training often lead to overwhelming governance issues, hindering self-service tools' effectiveness.
- **Struggles between agility and control:** Organizations grapple with striking the right balance, risking either stifled innovation or jeopardized data integrity.
- **Intense data engineering collaboration:** The increased need for data engineering involvement creates collaboration requirements, potentially disrupting workflows and causing metric inconsistencies.
- **Cumbersome DataOps practices:** DataOps introduces complex processes that challenge organizations to adapt effectively, making analytics collaboration more difficult for business analysts.
- **Persistent data quality issues:** Organizations continue to battle poor data quality, risking misunderstandings and detrimental misuse of data.
- **Overhyped vendor claims:** Many exaggerated claims have yet to be fully realized in products, necessitating advancements in augmented analytics and data literacy programs.

User Recommendations

- Segment your users by their ability and inclination to become self-servicing, and deliver to the most prepared users first. Build data literacy and certification programs to ensure users are best prepared to add value from self-service without mistakenly delivering bad or siloed information. Success often compounds and drives further successes, and aids in improving D&A maturity over time.
- Evaluate analytics catalogs and SSA capabilities to allow business users to add curated or external sources to their data landscapes.
- Form communities (analytics franchises) consisting of both business analysts doing self-service and augmented consumers. Self-service should not be self-serving. Communities where sharing, collaboration, education, project overviews and success evangelism occur are critical as analytics audiences grow.

Sample Vendors

Domo; Microsoft; Oracle; Pyramid Analytics; Salesforce (Tableau); TIBCO Software

Gartner Recommended Reading

Critical Capabilities for Analytics and Business Intelligence Platforms

Toolkit: Create a RACI Matrix for Self-Service Analytics

Infographic: Self-Service Analytics and BI Adoption Roadmap

How to Balance Control and Agility in Your Self-Service Analytics

Rethink Self-Service by Establishing Analytics Franchises to Drive Adoption and Break Bottlenecks

API Access Control

Analysis By: Nathan Harris, Erik Wahlstrom

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

API access control is a critical API security capability that provides authentication and authorization for APIs to deliver required security risk mitigation for access related threats. At a minimum, this involves an OAuth 2.0 authorization server, which supports and implements consent, manages authorization through scopes and associated claims, and issues customizable JSON Web Tokens (JWTs) to web servers, mobile apps, modern web apps and services used to access APIs.

Why This Is Important

Most web traffic now happens through APIs, rather than traditional web applications (i.e., web browser traffic), and the attack surface of APIs is now larger than the user interfaces (UIs). Along with this, attacks exploiting API vulnerabilities continue to increase. Organizations looking to mitigate the effects of this broadened attack surface should add authentication and authorization controls to API process flows when deploying API security.

Business Impact

API access control capabilities are important in several scenarios:

- Developer use cases, offering libraries, out-of-the-box integrations and best-practice examples of API access controls.
- Enabling user-present (including browser-based, single-page apps and mobile apps) and machine-to-machine access to API targets.
- Workforce and customer use cases, including customer data protection/privacy and consent management.
- Architecture standardization with central access controls for APIs.

Drivers

- API access control adoption has benefited from the popularity of access management tools (with market share adoption increases of more than 35% since 2020). Access management tools providing OAuth 2.0 have made the protocol an industry standard, driven by the continued increase in API delivered versus browser delivered functionality.

- Organizations' digital transformation efforts and need to provide secure API access for customer engagement journeys (CIAM) drive improved API access control strategies.

- The application attack surface has grown with the increased use of exposed APIs. Gartner estimates that more than 90% of web-enabled applications have more surface area for attack in the form of exposed APIs, rather than the user interface (UI).

- Lack of advanced IAM capabilities of API gateways (e.g., advanced adaptive access and support for evolving identity standards) has increased demand for specialized access control for APIs, delivered by AM, externalized authorization management and other IAM and API security specialist tools.

- Beyond OAuth 2.0 authorization servers, IT leaders also need the ability to centralize authentication and authorization services for libraries, sidecars and out-of-the-box integrations with APIs and API mediators.

- Developer self-service capabilities are also increasing in demand, for managing apps and services and support for flows such as OAuth mTLS, JWT and SAML grant types; the device flow; token exchange; introspection; and revocation. Authorization servers also provide strong, agile cryptographic mechanisms for signing tokens.

- Modern applications and service patterns (e.g., service mesh and REST) are adopting JWTs as authentication and authorization mechanisms. JWTs are becoming the de facto standard to convey authorization information and claims about users and services, enabling a scalable, privacy-preserving, zero trust architecture that helps developers quickly deploy protected services.

Obstacles

- Time to market for features/functions is often seen as more important than applying rigorous API protection.
- A lack of generally accepted API access control best practices, along with a lack of developer and security staff training in IAM best practices.
- The belief that API gateways (or any single tool) are sufficient to enable and securely run API-based applications.
- Lack of tooling that enables scaling centralized policy authorizing and continuous policy life cycle management to an increasingly diverse set of API targets and mediators that enforce these policies.

User Recommendations

- Define a comprehensive API access control strategy by broadening tool selection. This requires authorization servers, externalized authorization managers, secrets managers, API mediators and other in-line proxies. This is delivered by a combination of access management, API gateways and other specialized API security and IAM tools. In other words, plan for an identity fabric architecture approach to API access control.
- Improve the security risk mitigation delivered by API security controls by implementing API access control (to control which humans and machines can access APIs), alongside API discovery and API threat protection.
- Evaluate the quality of IAM tools by examining their capabilities for token exchange, access policy management, libraries and API gateway integrations.
- Reduce the incidence of API vulnerabilities by providing IAM training for developer and security staff, highlighting API access control.
- Protect services by deploying API access control enforcement points as close as possible to the service being protected. This will help enable defense in depth and supports a zero-trust approach.

Sample Vendors

Amazon Web Services; Authlete; Cloudentity; Curity; ForgeRock; Microsoft; Okta; Ping Identity

Gartner Recommended Reading

Magic Quadrant for Access Management

Critical Capabilities for Access Management

Architect a Modern API Access Control Strategy

API Security: What You Need to Do to Protect Your APIs

Critical Capabilities for Full Life Cycle API Management

Application Portfolio Management

Analysis By: Stefan Van Der Zijden

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

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

Why This Is Important

Application portfolio management (APM) leads to more conscious management of application assets and investments. Organizations can develop strategies and roadmaps that optimize available resources when using APM to drive agreement between business, finance and IT on how to evolve the application portfolio.

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

Business Impact

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

Drivers

- The application portfolio is an important business asset, and its health, composition and life cycle must be carefully managed.
- The need to increase the business fit, business value and agility of applications, and to reduce their cost, complexity and risk, are major drivers behind APM.
- APM helps prioritize IT investment to achieve desired business outcomes in initiatives like application rationalization, modernization and cloud migration.

Obstacles

- Organizations underestimate the value of applications as business assets, and the cost, risk and complexity they carry.
- Getting business engaged and supportive of the change in applications is difficult.
- There is a lack of ownership and stewardship of applications in both business and IT.
- The value of APM is not well-understood and it is often seen as a bookkeeping exercise.
- The responsibility of monitoring and reporting application portfolio fitness is not assigned or fragmented.
- APM loses out when competing with other initiatives since it’s often seen as an IT-driven initiative.
- APM is often seen as an ad hoc or one-off activity instead of an ongoing discipline.
- APM is typically started as a response to a major business event, or when a critical point is reached and the current state is no longer tolerable for the organization. Examples are a security breach, compliance risk, high cost or poor stability.

User Recommendations

- Undertake APM regularly to fuel continuous improvement of the application portfolio and identify ways to increase its operational advantages; this is especially applicable to peak performers.

- Undertake APM to help allocate limited resources to the most critical gaps from a business stakeholders' lens, to drive adoption of better practices across lines of business and to move toward more efficient support of business services; this is especially helpful for lagging organizations.

- Trigger adoption for other organizations via a business event or critical point — a significant event that highlights portfolio inefficiencies/issues and begins an APM initiative.

- Use value stream mapping to analyze the current state of application support and to identify business obstacles and friction points.

- Co-create application portfolio management with IT, business, and finance to strategically align investment with desired business outcomes.

Gartner Recommended Reading

Managing a Portfolio of Applications Demands More Than Application Portfolio Management

Quick Answer: Why Do You Need an Application Owner?

Using TIME for Application and Product Portfolio Triage: Data From the Field

How to Prioritize Application Inventory and Rationalization — By the Numbers

Market Guide for Application Portfolio Management Tools

Desktop as a Service

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

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

Definition:

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

Why This Is Important

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

Business Impact

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

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

Drivers

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

- DaaS enables business continuity and remote work, with no data residing on the endpoint.

- The technology securely extends services to external contractors and third parties.
- Endpoint computing models allow device-independence and bring your own PC (BYOPC) endpoints.
- On-demand desktops enable a financial model that allows scaling of cloud resources and an operating expenditure (opex) model.
- DaaS can be purchased for short periods, enabling use cases such as seasonal workers or short-term contracts.
- DaaS enables rapid access to systems during mergers, acquisitions and divestitures.
- Rich graphics use cases like engineering, games development, video editing and geographic information systems (GIS) benefit from GPU-enabled workstation-class virtual desktops and applications.
- DaaS can be delivered to users in hours. The supply of a physical device, on the other hand, can take weeks, incur shipping costs and retrieval is not always guaranteed.
- The technology eliminates the need for complex and static VDI implementations.

Obstacles

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

User Recommendations

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

Sample Vendors

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

Gartner Recommended Reading

Market Guide for Desktop as a Service

How to Choose a Desktop Delivery Model for the Digital Workplace

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

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

NDR

Analysis By: Jeremy D'Hoinne, Nat Smith, Thomas Lintemuth

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Network detection and response (NDR) products detect abnormal system behaviors by applying behavioral analytics to network traffic. They continuously analyze raw network packets or traffic metadata for both internal (east-west) and "public" (north-south) networks. NDR can be delivered as hardware and software sensor, and software or increasingly SaaS management console. Organizations rely on NDR to detect and contain postbreach activity, such as ransomware, or insider's malicious activity.

Why This Is Important

NDR focuses on detecting abnormal behaviors, with less emphasis on signature-based controls detecting known threats. NDR is effective in detecting weak signals and previously unknown behavior from traffic on networks such as lateral movement or data exfiltration. NDR solutions expand to hybrid networks, adding new detections. Automated response capabilities, provided natively or through integration remain important, but incident response workflow automation becomes an increasing area of focus.

Business Impact

NDR solutions provide visibility into network activities to spot anomalies. The machine learning algorithms that are at the core of many NDR products help to detect anomalies in traffic that are often missed by other detection techniques. The automated response capabilities help to offload some of the workload for incident responders. NDR products also help incident responders with their threat hunting by providing useful context and drill-down capabilities.

Drivers

- Detecting postbreach activity: NDR complements traditional preventative controls by detecting activities based on deviations from baseline. This allows the security team to investigate insider's activities resulting from breaches without relying on having observed a previous occurrence of the same activity.

- Low risk — high reward: Implementing NDR products is a low-risk project because the sensors are positioned out-of-band, so they don't represent a point of failure or a "speed bump" for network traffic. Enterprises that implement NDR products as a proof of concept (POC) often report high degrees of satisfaction because the tools provide much-needed visibility into network traffic and enable even small teams to spot anomalies.

- Monitoring cloud traffic: A growing number of NDR vendors offer the ability to monitor IaaS traffic and M365 by leveraging available APIs from the cloud providers. Organizations expanding their cloud presence use NDR to avoid creating gaps in their ability to monitor interactions between their systems.

Obstacles

- Enterprises with a lower maturity security operation program might struggle to justify the expense for a technology that cannot simply be evaluated by counting the number of alerts it triggers.
- The response features of the NDR products are more rarely deployed or narrowed down to specific use cases, such as ransomware, due to a risk of false positives. Many organizations postpone their implementation until they understand how to use the NDR tool better.
- NDR is expanding to support more detections in the cloud but have yet to prove they are the right tool for the use case.
- False positives are inevitable with any behavioral-based detection tool. NDR tools might require fine-tuning of the configuration to reduce the amount of false positives, especially in early days of the deployment. This explains why response capabilities are more rarely deployed initially.
- NDR increasingly competes for budget with consolidated platforms such as SIEM and extended detection and response (XDR).

User Recommendations

- Develop a strong understanding of the overall traffic patterns and specific traffic patterns in your enterprise network to gain maximum value from NDR.
- Carefully plan sensor types and deployment locations so that the most relevant network traffic can be analyzed. Proper positioning of the NDR sensors is critically important to limit the number of false positives and control the cost of the deployment.
- Tune out false positives in the implementation phase (false positives may be triggered by vulnerability scanners, shadow IT applications and other factors that may be specific to your environment).
- Plan for ongoing tuning as new detection models are deployed from the vendor.
- Select sensor capturing capacity that is sized appropriately for your network.

Sample Vendors

Cisco; Corelight; Darktrace; ExtraHop; Fortinet; IronNet; MixMode; Plixer; Trend Micro; Vectra

Gartner Recommended Reading

Market Guide for Network Detection and Response

Emerging Tech: Top Use Cases for Network Detection and Response

OS Containers

Analysis By: Thomas Bittman, Philip Dawson

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

OS containers are a shared OS virtualization technology that enables multiple applications to share an OS kernel without conflicting. A "container daemon" provides logical isolation of processes. This enables several applications to share an OS kernel while maintaining their own copies of specific OS libraries.

Why This Is Important

Containers were previously used to increase the density of lightly used workloads, for improved infrastructure management. Now containers are focused on developer requirements for agile development, rapid provisioning and real-time horizontal scaling, especially for microservices architecture applications and cloud-native computing.

Business Impact

Container technologies are part of a development architecture that helps enterprises become more agile, with applications that can change quickly, and scale rapidly to demand. In production, containers will often be used for new applications designed for agile development. However, for developer ease of use, containers will also be used as wrappers for traditional, monolithic workloads.

Drivers

- Lightweight overhead for small applications (improving capacity utilization and density)
- Portabability — containers package up the code and its dependencies making it easier to migrate workloads reliably and predictably
- Ease of use and reuse by application developers
- Alignment with microservices architecture and agile development

Obstacles

- Reliance on the OS for application isolation can create security concerns, especially in multitenant environments.
- Containers are not direct replacements for hypervisors and, unlike with hypervisors, existing applications require redesign to take full advantage of the benefits of containers.
- Container use is constrained by the immaturity and complexity of tools and operations, especially in security, monitoring, data management and networking.
- Developing the right operational model for Kubernetes deployments is difficult, and requires organizational evolution and new skills.

User Recommendations

Infrastructure and operations leaders responsible for data center infrastructure should:

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

Sample Vendors

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

Gartner Recommended Reading

Market Guide for Container Management

Prioritizing Security Controls for Enterprise Servers and End-User Endpoints

Designing and Operating DevOps Workflows to Deploy Containerized Applications With Kubernetes

Cloud Analytics

Analysis By: Julian Sun, Fay Fei, Jamie O'Brien

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud analytics delivers analytics capabilities as a service. It often comprises database, data integration and analytics tools. As cloud deployments continue, the ability to connect to both cloud-based and on-premises data sources in a hybrid model is increasingly important. Cloud-native architecture and multicloud deployments are also becoming popular in order to cater to the cloud ecosystem.

Why This Is Important

Adoption of cloud analytics is growing, with most analytics deployments originating in the cloud. The majority of respondents to the 2022 Gartner State of Data and Analytics Cloud Adoption Survey say they are using or plan to use the cloud for analytics and data science. Cloud capability among analytics and BI vendors is also expanding, with emerging capabilities coming from cloud-first. The cloud is an ideal place to build modular analytics capabilities that enable greater agility and reuse of existing investments in support of composable business.

Business Impact

A cloud-enabled, composable platform can innovate by assembling modular analytics capabilities on demand. More advanced analytics can complement key components of the analytics infrastructure in the cloud. The high computational power needed to process tasks such as ML and advanced analytics can be more easily accessed and scaled in the cloud. Business users can pilot cloud-first augmented analytics within a sandbox provisioned by the cloud. Cloud deployment offers faster time to value and more targeted analytics for specific business areas.

Drivers

- To better leverage scalability and elasticity from the cloud, many platforms have rearchitected themselves to be cloud-native.
- To bring more flexibility for organizations that are already using multicloud, vendors are adding more deployment options and management capabilities. These additions enable portability through microservices architectures that are readily supported via containerization across multiple clouds.
- Startups continue to join the analytics market with cloud-first or cloud-only solutions, which are complementary to established platforms.
- The range of capabilities is growing too. Reporting and data visualization were already commodified capabilities. Customers can now also subscribe to self-service data preparation; augmented data discovery; predictive modeling; other advanced capabilities, such as ML or streaming analytics; and even data/context broker services from several vendors.
- The growing cloud DBMS market naturally supports and expands the cloud analytics market as companies embrace the cloud for managing their data.

Obstacles

- Security is a top concern for organizations moving to the cloud. Organizations need to plan how they will integrate their growing cloud analytics deployments with additional data sources, provide access to more advanced (potentially open-source) analytics tools, and embed analytics in business processes. Such planning becomes even more challenging across multiple cloud and on-premises ecosystems.
- Organizations' adoption of the cloud is closely tied to data gravity. Data gravity refers to data's attractive force: As data accumulates and the need for customization, integration and access grows, data has greater propensity to "pull" data services, applications and other data/metadata to where it resides. Thus, smaller organizations with data originating in the cloud have higher adoption rates than larger organizations with data predominantly in on-premises legacy solutions.
- Even as cloud analytics becomes more predominant and mature, organizations with deployment and governance challenges face growth obstacles.

User Recommendations

- Establish a measured approach to move to the cloud incrementally — rather than simply “lifting and shifting” — as cloud analytics becomes a dominant option in most scenarios in the analytics space.
- Include innovative cloud analytics solutions in your portfolio, renovating on-premises components or complementing your on-premises platform, to gain competitive advantage through analytics and BI. Completely disregarding cloud analytics solutions means risk for many organizations, as most vendors don’t focus their R&D efforts on legacy products.
- Be aware of extra costs and the total cost of ownership (TCO) as you adopt new capabilities and offerings within your vendor’s cloud stack. Although cloud analytics solutions do not require significant upfront investment like on-premises solutions do, the former will likely be more expensive to license over four or more years. Also be aware of the performance downgrade in the cloud — benchmark the platform, and carefully plan the data integration approach.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Databricks; Domo; Google; Microsoft; Oracle; Qlik; Sigma Computing; ThoughtSpot

Gartner Recommended Reading

Adopt Cloud Analytics to Drive Innovation

Use Cloud to Compose Analytics, BI and Data Science Capabilities for Reusability and Resilience

Magic Quadrant for Analytics and Business Intelligence Platforms

Critical Capabilities for Analytics and Business Intelligence Platforms

CIPS

Analysis By: Sid Nag

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

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

Why This Is Important

- Customers are looking for integrated platforms to simplify development, deployment and operations.
- CIPS offerings are the most complete cloud platforms in the industry, thereby driving significant market consolidation.
- Independent software vendors (ISVs), systems integrators (SIs) and management service providers (MSPs) have embraced the leading CIPS platforms, making them the foundation for most organizations' cloud operations.
- Workloads of today are complex, and cloud providers are addressing the problems by offering CIPS platforms.

Business Impact

A well-functioning CIPS will offer enterprises a more natural, flexible and comprehensive cloud computing environment for their workloads, thereby addressing today's IT needs from an application and data perspective.

Drivers

- The appeal for CIPS is not necessarily in best-of-breed offerings, but in the unification and integration of platform capabilities across these services enabling broad support of workloads ranging from ERP to cloud-native.
- Most customers that use a CIPS from a hyperscale provider, such as Amazon Web Services or Microsoft Azure, have adopted a blend of the provider's IaaS and PaaS capabilities. Indeed, the availability of this broad portfolio of services is a key aspect of choosing a strategic cloud platform provider.
- Hyperscale CIPS providers deliver PaaS services that are well integrated with their IaaS services so that both are easily used together. As a customer, whether you are using PaaS services or IaaS services, they are built on a common substrate. The combination of these services means you are making a strategic bet on the cloud provider.

Obstacles

- Public CIPS markets have consolidated around the market leaders which results in limited options and choices for the buyer.
- IaaS-only or PaaS-only cloud providers will continue to exist, but only as secondary cloud providers compared with CIPS providers.
- This, in turn, could make it a market dominated by a handful of cloud providers, which could stifle competition and drive stand-alone cloud providers out of the market.
- The limited set of hyperscale cloud provider options may limit options or create concentration risks for customers.
- The complexity and level of investment required to offer a full, integrated portfolio of multifunctional PaaS and IaaS services have limited the vendor options in this market to a handful of hyperscalers. Some hyperscalers will form ecosystems, enabling smaller PaaS specialists to be included in this market. However, the maturity of this technology will be primarily dependent on the capabilities of the hyperscalers.

User Recommendations

- Use CIPS in cloud-native and legacy migration projects to expand your design and deployment options and reduce complexity. This may involve using capabilities from multiple cloud providers.
- Prioritize consolidating systems on a hyperscaler CIPS offering when you are operating and governing fleets of applications at enterprise scale. This improves your economies of scale, skills and resources through standardization and consistency across your company and industry.
- Treat integrated CIPS providers as long-term strategic technology providers to your organization. Work to optimize costs, limit contractual risk and maintain failover and portability options for business-critical workloads.
- Focus on those services that are multicloud and can be colocated with multiple larger suites of CIPS capabilities as not all services of the providers are of same maturity, functional completeness or quality.
- Invest to maintain an appropriate level of integration across multiple cloud providers for foundational enterprise IT services such as networking, identity and access management, and security.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Google; IBM; Microsoft; Oracle

Gartner Recommended Reading

Magic Quadrant for Cloud Infrastructure and Platform Services

Critical Capabilities for Cloud Infrastructure and Platform Services

What Buyers Want From CIPS Providers

Risk and Opportunity Index: Cloud Infrastructure and Platform Services

Extending the CIPS Business to New Markets and Opportunities

Endpoint Detection and Response

Analysis By: Franz Hinner, Satarupa Patnaik, Eric Grenier

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Endpoint detection and response (EDR) analyzes system, process, and user activity to detect security threats. It provides remedial guidance for threats that bypass prevention controls and enables endpoint threat investigations. EDR capabilities are often included in endpoint protection platforms and delivered as software agents connected to centralized cloud-based security analytics and management software.

Why This Is Important

EDR is an essential defense component for most enterprise endpoints. It requires the installation of an agent to assist in the discovery and reporting of suspicious and malicious behaviors, visualization of attack propagation, and remediation guidance. EDR can stop known malware and ransomware families, and it can also help discover and remediate more stealthy and unknown threats.

Business Impact

- All devices and servers that connect to corporate networks or handle data need EDR protection.
- New threats and covert exploits require early identification and quick reaction.
- Cyber insurers and regulators demand EDR, and some EDR solutions provide low-cost ransomware insurance.

Drivers

- The nature of threats has changed. It is no longer practical to achieve 100% prevention, and older endpoint protection platform (EPP) tools should be updated to also contain EDR functionality.

- Stealthy malware and ransomware campaigns, state-sponsored adversaries and supply chain attacks use advanced techniques to remain undetected and to bypass older security controls.

- Remote work has accelerated the adoption of cloud-managed solutions, which now represent 80% of the installed bases and most new deployments.

- Detection of user- and machine-identity-related exploits and credential misuse is an emerging must-have feature.

- Rapid real-time response, as incidents unfold, is critical to contain a threat and stop it from spreading.

- Augmenting existing vulnerability management programs and providing a means to reduce the attack surface are increasingly needed to ensure systems are not misconfigured and have no unpatched vulnerabilities.

- The collection of logs and events from EDR agents forms the basis for retrospective threat detection and threat hunting.

- Sophisticated attacks require a new breed of EDR tools that work holistically together with other security tools as a composable security ecosystem to maximize protection and minimize exposure.

Obstacles

- Many businesses lack and underestimate the knowledge and resources to install and employ EDR tools successfully. EDR adoption requires responder training, including “range” training that mimics assaults.
- Traditional endpoint security technologies and agents don’t function with cloud-hosted workloads’ “agile” deployment pipelines. This splits agile deployed workloads from containers or serverless computing.
- Non-Microsoft-Windows systems may lack feature parity. Endpoint security solutions for these systems lack EDR detection and response capabilities.
- In hybrid and remote working models, older on-premises technologies are difficult to adopt and maintain.

User Recommendations

- Choose solutions with a single unified agent and fast remote deployment.
- Prioritize technologies with ease of use and prebuilt automated playbooks.
- Favor cloud-hosted solutions with flexible deployment options.
- Assess the organization’s ability to monitor and manage detection and response services to identify gaps and determine if a managed service is required for your organization. Ensure appropriate data retention and fulfill regulatory compliance.

Sample Vendors

Cisco; CrowdStrike; Cybereason; Fortinet; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Trellix; Trend Micro

Gartner Recommended Reading

Magic Quadrant for Endpoint Protection Platforms

Critical Capabilities for Endpoint Protection Platforms

Cloud Workload Protection Platforms

Analysis By: Charlie Winckless, Neil MacDonald

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Cloud workload protection platforms (CWPPs) protect workloads in hybrid and cloud deployments. CWPPs provide consistent visibility and control over physical machines, virtual machines, containers and serverless workloads, regardless of location. CWPP offerings protect the workload using a combination of system integrity protection, application control, behavioral monitoring, intrusion prevention and optional anti-malware protection.

Why This Is Important

As enterprises spread diverse workloads across data centers and public clouds, they need to maintain their visibility and control over these workloads during runtime. The most effective way to address the speed, scale and complexity of cloud-based workload security is to use an offering that is fit for purpose. Simply using a solution designed for on-premises data centers or end-user endpoints is a poor approach to these diverse workloads.

Business Impact

Enterprises are implementing hybrid data center architectures, with workloads spanning on-premises and public cloud IaaS providers, container-based implementations and serverless functions. These workloads are diverse, and their security requirements and threat models differ significantly from end-user systems and even traditional servers. To secure these workloads and realize the benefits of cloud-native applications, it is necessary to use security tooling designed for this environment.

Drivers

- The most effective way to address the speed, scale, complexity, and the ephemeral and elastic nature of cloud workload protection is to use a tool designed for how these workloads are deployed.

- Simply using a solution designed for on-premises data centers or end-user endpoint protection platforms (EPPs) is suboptimal. Thus, many vendors, including both startups and established EPP vendors, are now explicitly targeting the CWPP market.

- Cloud server workload protection strategies must be based on a foundation of solid operational hygiene, including proper administrative control, patching discipline and workload configuration management.

- Workloads are no longer remotely homogeneous. Tools must protect containers, virtual machines and serverless workloads, and grant the appropriate levels of visibility and security to each.
- Unlike end-user endpoints, server workloads do not commonly encounter and execute unknown arbitrary code, thus lending themselves to a default deny, zero-trust-based protection strategy that well-engineered CWPPs are built to support.
- As vendor convergence continues to be important to Gartner clients, the convergence of CWPP and cloud security posture management (CSPM) into a cloud-native application platform (CNAPP) consolidates previously siloed offerings and provides the same or greater value.

Obstacles

- Some organizations are maturing their approach to cloud protection and have not identified a need for cloud-native security toolsets, or prefer to continue with existing endpoint tools despite their lack of suitability for cloud deployments. Such organizations often still wish to extend on-premises controls and control patterns to the cloud, regardless of suitability.
- Single cloud-using organizations may wish to use CSP-native tools. This can be suboptimal due to potential future multicloud deployments, increasing options for cost and feature improvements.
- Not all vendors offer all capabilities. Some specialize in only one or two forms of workload protection.
- Not all vendors offer support for physical servers or out-of-support and older operating systems that still require protection.
- Some vendors utilize eBPF, which supports only newer versions of Linux.
- Serverless functions require new approaches that don’t require agents or privileged containers.

User Recommendations

- Don't use an end-user EPP solution to protect cloud server workloads.
- Architect for consistent visibility and control of all workloads, regardless of location, size or type, as well as in cases where runtime agents may not be used or may not make sense.
- Evaluate converged CNAPP offerings to see if their CWPP capabilities are sufficient, since information sharing is highly valuable for detection, false positive reduction and prioritization.
- Require vendors to support well-integrated deployments in leading cloud platforms, especially for managed container and serverless approaches.
- Prioritize a default deny or application control approach.
- Extend workload scanning and compliance efforts into development (DevSecOps), especially for containers and serverless functions. Prefer platforms that support container and serverless environments.
- Require CWPP offerings to expose all functionality via API.

Sample Vendors

Aqua Security; CrowdStrike; Lacework; Microsoft; Palo Alto Networks; SentinelOne; Sophos; Sysdig; Trellix; Trend Micro

Gartner Recommended Reading

Market Guide for Cloud-Native Application Protection Platforms

5 Things You Must Absolutely Get Right for Secure IaaS and PaaS

Magic Quadrant for Endpoint Protection Platforms

Entering the Plateau

ITSM Platforms

Analysis By: Rich Doheny

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

IT service management (ITSM) platforms offer workflow management that enables organizations to design, automate, manage, and deliver integrated IT services and digital experiences. Supported processes include request, incident, problem, change, knowledge and configuration management, and case management for non-IT business needs. IT leaders select these solutions to be consumed by service desks and service operations, and for business workflow administration in other IT-adjacent departments.

Why This Is Important

IT leaders require robust ITSM platforms to drive business value in the services they provide and enable digital business transformation outside of IT. These platforms help infrastructure and operations (I&O) teams to automate processes, design workflows, and support continual service improvement initiatives. They provide actionable insights that enable service operations, orchestration and process automation, and multichannel support.

Business Impact

ITSM platforms are most heavily used by IT service support and IT service delivery functions to enable the tasks and workflows for ITSM processes. They drive agility and help scale service delivery efforts through integration into adjacent IT operations management, digital experience, collaboration, and development solutions. In addition, out-of-the-box case management and low-code features extend request management into other areas of the business.

Drivers

- The ITSM platforms market is functionally mature. Features aligned with common ITSM practices and standards are commoditized.

- IT leaders are increasingly inquiring about applying service management into other areas of the business through a unified platform offering. ITSM platforms continue to expand service management workflows with out-of-the-box content to support line-of-business needs, such as HR and facilities case management.

- DevOps and DevSecOps are driving the need for more ITSM platform functions to be integrated into adjacent tooling and workflows for greater efficiencies, agility, and visibility.

- ITSM vendors are investing in new capabilities supporting more federated and agile ITSM practices, AI and artificial intelligence for IT operations (AIOps) integration, workforce and process optimization, integration with development and collaboration tools, and multichannel support.

Obstacles

- More than 400 vendors offer ITSM products, but most are basic or intermediate tools that focus on IT service desk and ticketing functions targeted at basic service desk requirements. With core process workflows built around common frameworks, many vendors struggle to create meaningful differentiated messaging and help their customers justify the ROI.

- Despite the large number of participants, the enterprise market is dominated by a small number of vendors.

- Advanced features typically require pricey add-ons or higher tiers of licensing. This will be a challenge for customers who do not align their product roadmap with their budget planning.

- Customers who try to implement too many platform features at once, across IT and multiple lines of business, will struggle to mature their practices and often lose momentum on their investments.

User Recommendations

- Identify current ITSM needs along with what you can pragmatically deploy over an 18-month roadmap to avoid overspending.

- Avoid costly customization by prioritizing tools that provide advanced process support and machine learning, as well as strong orchestration tools and out-of-the-box integration with other IT operations management and collaboration solutions.

- Select tools that support adaptive process models and integration into your DevOps toolchains, if you are pursuing DevOps and agile methodologies.
- Account for the total resource overhead associated with the product by factoring in licensing, cost and timing of implementation, ongoing maintenance, training required, and third-party products to meet base requirements.
- Involve business leaders for any non-IT case management decisions to ensure minimum functionality is met. Identify multichannel access and broader integration requirements into other line-of-business systems of record.

Sample Vendors

Atlassian; BMC Software; EasyVista; Freshworks; Ivanti; ManageEngine; ServiceNow

Gartner Recommended Reading

Magic Quadrant for IT Service Management Platforms

Critical Capabilities for IT Service Management Platforms

A Buyer’s Guide to ITSM Platforms

Quick Answer: How to Successfully Implement Your ITSM Platform

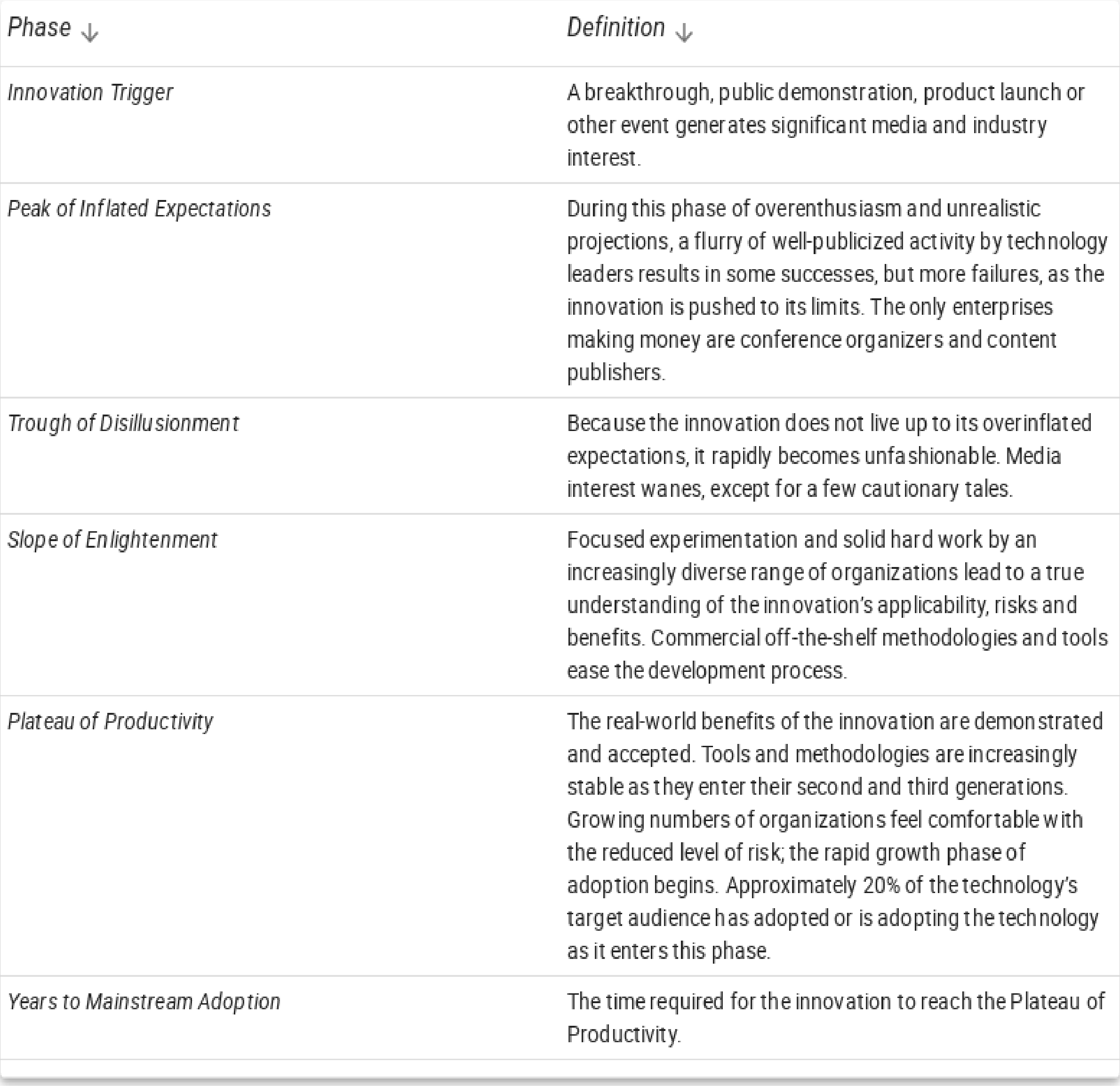
Appendixes

See the previous Hype Cycle: Hype Cycle for Midsize Enterprises, 2022.

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)



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

Source: Gartner (July 2023)

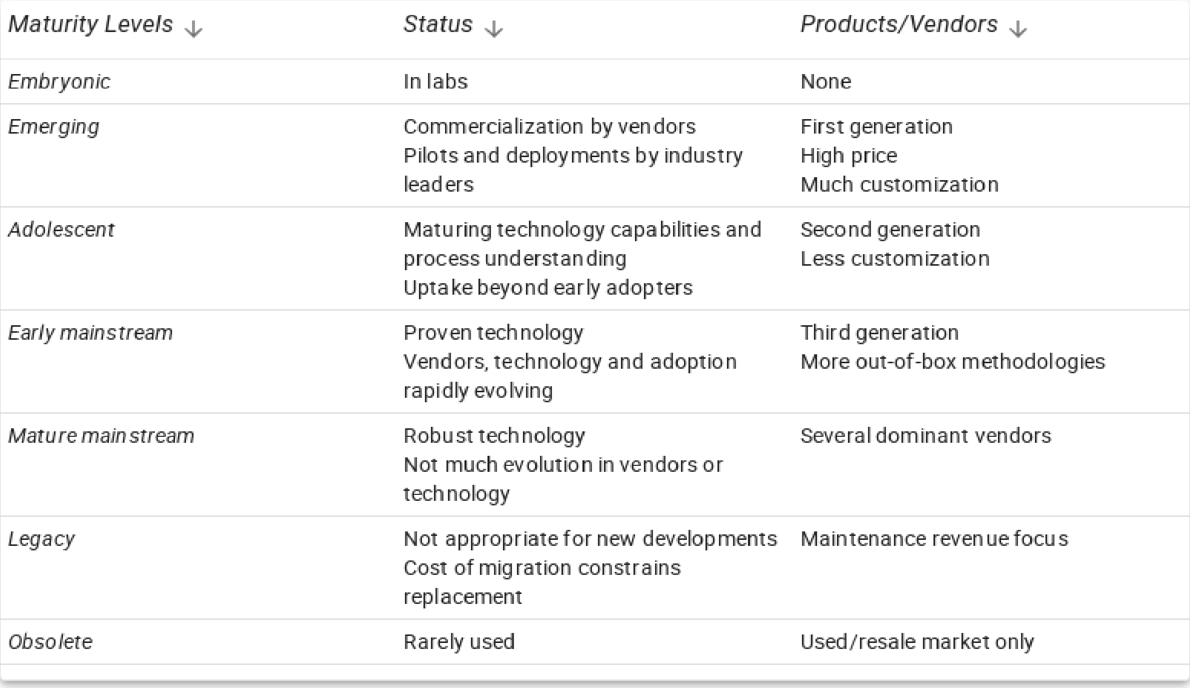
Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)



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

Source: Gartner (July 2023)

Evidence

2023 Gartner CIO and Technology Executive Survey. This survey was conducted to help CIOs and technology executives overcome digital execution gaps by empowering and enabling an ecosystem of internal and external digital technology producers. It was conducted online from 2 May through 25 June 2022 among Gartner Executive Programs members and other CIOs.

Qualified respondents are each the most senior IT leader (e.g., CIO) for their overall organization or some part of their organization (for example, a business unit or region). The total sample is 2,203 respondents, with representation from all geographies and industry sectors (public and private), including 358 from midsize enterprises.

Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.

Document Revision History

Hype Cycle for Midsize Enterprises, 2022 - 11 July 2022

Hype Cycle for Midsize Enterprises, 2021 - 19 July 2021

Hype Cycle for Midsize Enterprises, 2020 - 30 July 2020

Recommended by the Authors

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

Understanding Gartner's Hype Cycles

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

Leadership Vision for 2023: Midsize Enterprise Technology Leader

3 Dynamics That Drive Midsize Enterprises

How and When to Change Your Managed Security Service Provider

How Midsize Enterprises Can Extend Active Directory Identities to the Cloud Securely

Quick Answer: How Can Midsize Enterprises Benefit From Security Vendor Consolidation?

Midsize Guide to Securing a Hybrid Environment

Quick Answer: How to Make the Right Choice Between Hyperconverged, Traditional and Distributed Cloud Infrastructure

Table 1: Priority Matrix for Midsize Enterprises, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	OS Containers	Data Literacy Edge Computing Everyday AI Generative AI SASE Security Service Edge		

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
High	API Access Control Cloud Analytics Desktop as a Service Endpoint Detection and Response ITSM Platforms	API Observability Application Portfolio Management Augmented Analytics CIPS Continuous Delivery Data and Analytics Governance Data Observability Edge Analytics Edge Data Management Identity-First Security Identity Threat Detection and Response MDR Services	Cloud Data Backup Distributed Cloud XDR	

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Moderate	Cloud Workload Protection Platforms	Application Data Management Backup as a Service Cloud-Tethered Compute Firewall as a Service Low-Code/No-Code Solutions Managed SIEM Services NDR Self-Service Analytics	Container Backup	
Low				

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

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

Phase ↓	*Definition* ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

Table 4: Maturity Levels

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

Source: Gartner (July 2023)