Hype Cycle for IT Performance Analysis, 2020

Published: 17 July 2020 **ID:** G00448200

Analyst(s): Pankaj Prasad, Padraig Byrne

IT performance can no longer be a reactive approach as digital technology initiatives start showing up on boards of directors' radars. This Hype Cycle helps infrastructure and operations leaders manage, plan and deliver to the requirements of their businesses.

Table of Contents

List of Tables

List of Figures

Analysis

What You Need to Know

Performance analysis covers the spectrum of IT monitoring and analysis for interpreting health, performance and behavior of IT infrastructure, network and applications. End users, who include customers, but are increasingly broadening to include internal users (employees), are at the center of IT performance goals. Capturing their experience is a major focus area of the performance analysis discipline.

Many enterprises are redrafting IT monitoring strategies due to the COVID-19 pandemic. The migration to remote work environments, accelerated migration to cloud and cost pressures are key drivers for management.

An increasing focus on business value has translated in infrastructure and operations (I&O) leaders discussing contextualized information, which is a clear shift from mere visibility to action-oriented data drive insights. This trend requires heavy use of analytics, flexible dashboards and insightful reports.

Use of cloud-native architectures in production environments has also resulted in the integration of DevOps and site reliability engineering (SRE) practices to leverage the fault tolerance and agility offered by such architectures. Performance analysis technologies must now meet the data and visualization needs of DevOps and SRE teams, in addition to those of the traditional I&O team.

This research will help I&O leaders determine the relative maturity of the tools, technologies and frameworks in the market and set implementation expectations accordingly.

(For more information about how peer I&O leaders view the technologies aligned with this Hype Cycle, please see “2020-2022 Emerging Technology Roadmap for Large Enterprises.”)

The Hype Cycle

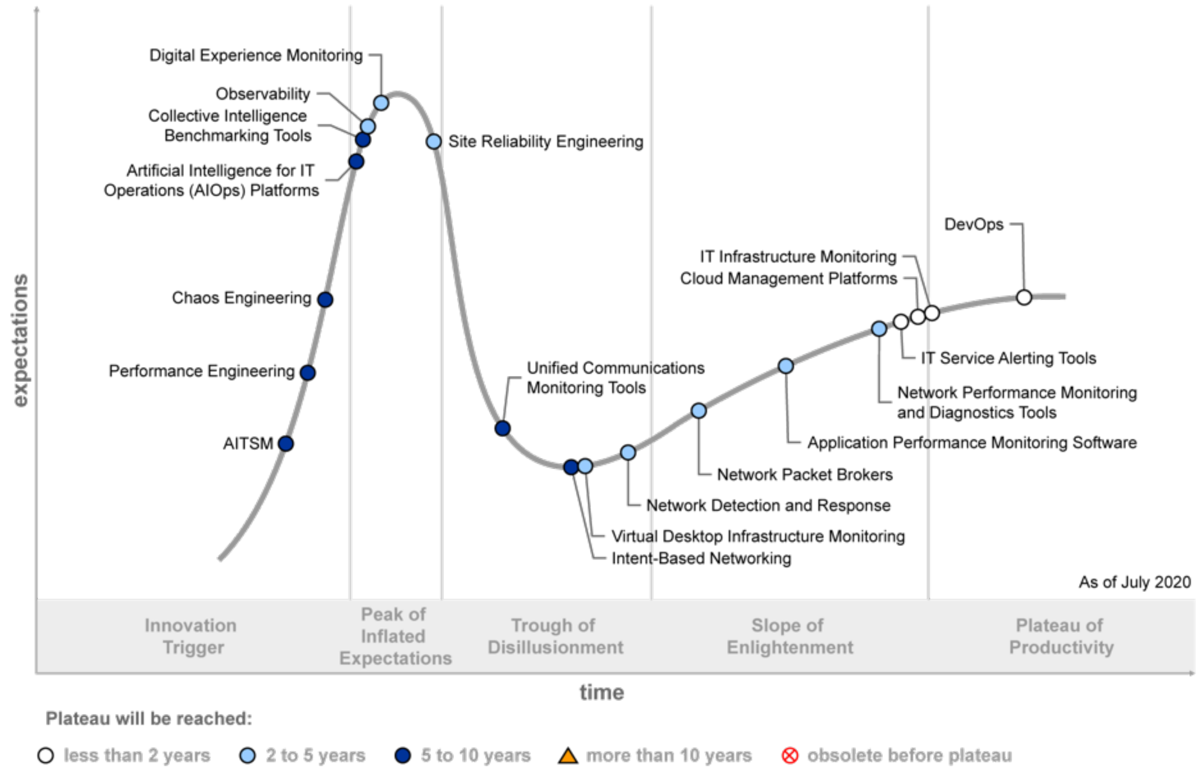
This research is one of four key Hype Cycles for I&O leaders focused on IT operations. The others are the “Hype Cycle for I&O Automation, 2020,” “Hype Cycle for ITSM, 2020” and “Hype Cycle for DevOps, 2020.”

This Hype Cycle delivers advice on IT performance analysis practices, tools and technologies, along with their visibility and market adoption.

Except for unified communications as a service (UCaaS), IT performance analysis technologies are on the maturity curve, and innovative practices are being driven through the adoption of AI-based technologies and SRE practices. Organizations can adopt any of these technologies or frameworks; however, the most interest in tools poised to change IT delivery through disruptive approaches will come from Type A organizations. Type B (i.e., “middle of the road” technology adopters) and Type C organizations, which take a more conservative approach to technology adoption, need to assess technologies at the Innovation Trigger phase and consider early adoption.

Every year, we introduce new profiles to reflect market changes. Performance engineering, chaos engineering, SRE and AITSM are existing technologies new to the Hype Cycle for IT Performance Analysis. The shared responsibilities of I&O and SRE teams include monitoring, self-healing, incident and problem management.

Figure 1. Hype Cycle for IT Performance Analysis, 2020



The Priority Matrix

The Priority Matrix maps a technology's time to maturity on an easy-to-read grid format. It answers two critical considerations:

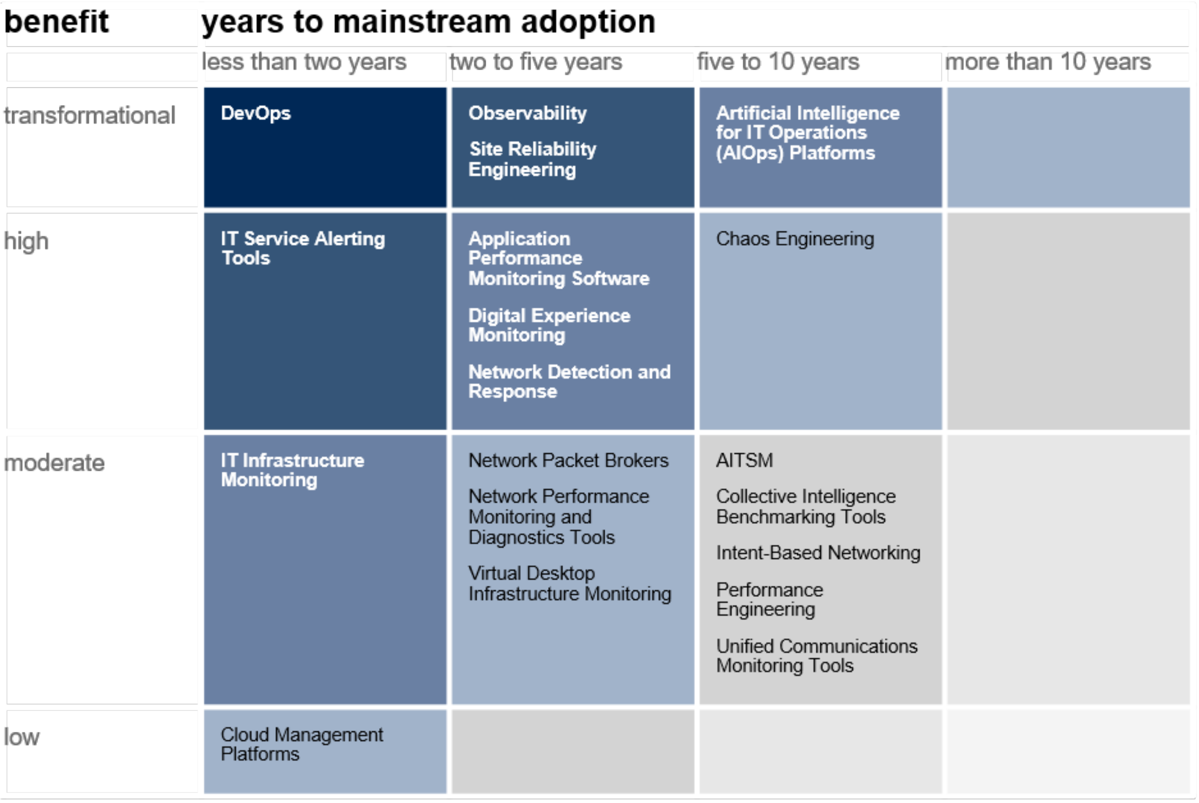
- The value an organization will receive from a technology
- When the technology will be mature enough to provide this value

For most profiles listed, the truly transformative impact is realized only by interlocking technology adoption with people and process frameworks that are aligned with clear business objectives.

For example, on this Hype Cycle, artificial intelligence for IT operations (AIOps), DevOps, observability and SRE are the technologies identified as transformational for most IT organizations. Gartner sees organizations succeed with AIOps deployments when they define a progressive roadmap that aligns with various IT operations domains, including DevOps and, more recently, SRE. Interestingly, enterprises leveraging observability use AIOps-based technologies to curate, contextualize and visualize the ingested data.

Figure 2 illustrates innovation profiles of domain-centric monitoring technologies are at the mature mainstream phase of adoption. This signifies a level of commoditization in technology in which the value proposition is well-understood. Almost all vendors covering domain-centric technologies are leveraging AIOps related technologies, which are still emerging. More-mature IT organizations will successfully adopt performance analysis and derive efficiency, reliability and predictability faster than indicated in this matrix. Conversely, cultural resistance, unrealistic expectations, and a lack of collaboration and process discipline will lengthen the time to adoption.

Figure 2. Priority Matrix for IT Performance Analysis, 2020



benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational	**DevOps**	**Observability** **Site Reliability Engineering**	**Artificial Intelligence for IT Operations (AIOps) Platforms**	
high	**IT Service Alerting Tools**	**Application Performance Monitoring Software** **Digital Experience Monitoring** **Network Detection and Response**	Chaos Engineering	
moderate	**IT Infrastructure Monitoring**	Network Packet Brokers Network Performance Monitoring and Diagnostics Tools Virtual Desktop Infrastructure Monitoring	AITSM Collective Intelligence Benchmarking Tools Intent-Based Networking Performance Engineering Unified Communications Monitoring Tools	
low	Cloud Management Platforms			

As of July 2020

Off the Hype Cycle

IT event correlation and analysis (ECA) tools, capacity planning and management, and wireless network monitoring profiles are not included in the Hype Cycle for IT Performance Analysis this year. ECA has moved off the Plateau of Productivity. AIOps tools are now replacing both ECA and capacity planning and management capabilities, the latter aligning with scalable and elastic architectures. Some of the capabilities of wireless monitoring tools are subsumed by network performance monitoring and diagnostics (NPMD) tools. Gartner has renamed the network traffic analysis (NTA) technology to network detection and response (NDR), to accurately reflect the functionality of these solutions.

On the Rise

AITSM

Analysis By: Chris Matchett

Definition: AITSM is the optimization of ITSM practices to enable the application of context, assistance, actions and interfaces of AI, automation and analytics on ITSM tools to improve the overall effectiveness, efficiency and error reduction for I&O staff. AITSM is not an acronym.

Position and Adoption Speed Justification: I&O leaders are seeking new opportunities to automate and provide more proactive management of their environments.

Many ITSM tools currently demonstrate capability mostly in the context domain of AITSM, but rarely in the assistance and action domains. Progress is being made, but many ITSM product roadmaps have been focused on delivering chatbot and virtual support agents (VSAs). Some advanced ITSM tools are developing and have delivered analytics capabilities to improve knowledge management and drive more effective VSA capabilities.

In addition to developments within ITSM tool suites, several vendors offer stand-alone products to work with incumbent ITSM tools. Some are branded as AITSM, but are generally focused on one or two areas, such as knowledge management tools or VSAs. Sometimes, the main AI-like component is just a natural language processing (NLP) engine that assists pattern matching knowledge and trends to speech (usually typed), but is not an adaptive system in any meaningful way beyond that.

The position of AITSM on this Hype Cycle represents AITSM in the full implementation of all four stages, not just context.

User Advice: AI solutions and adaptive systems require data and optimized practices to learn, predict and react to. Automation tools automate these reactions. Unoptimized processes can be automated, but with problematic outcomes.

Optimize ITSM practices for AITSM by identifying pockets of work that are standardized and repeatable enough to be eliminated or automated. Humans can carry out high-value cases to an extended degree (such as turning an error message diagnosis “break/fix” call into a business consumer training opportunity). This business productivity team approach will be made possible without increasing staff numbers if the lower-value interactions are dealt with by automated processes or — even better — eliminated through problem management and therefore will never need to be managed again.

Business Impact: AITSM is important for intermediate and advanced I&O maturity use cases to automate and support complex environments. Leveraging AITSM can offer benefits typically associated with automation and will be of particular interest to I&O leaders needing to optimize costs of service and support. Stage 1 AITSM capabilities (context) are unlikely to require capital investments, as these capabilities tend to be present in current ITSM tools. More advanced cases will require upgrades or procurement, so we expect to see this more often in organizations that are more focused on improving maturity than just cost cutting.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Aisera; Axios Systems; BMC; Espressive; Moveworks; ServiceNow; Symphony SummitAI

Recommended Reading:

"2019 Strategic Roadmap for IT Service Management"

"Critical Capabilities for IT Service Management Tools"

"3 Simple Ways IT Service Desks Should Handle Incidents and Requests"

Performance Engineering

Analysis By: Joachim Herschmann

Definition: Performance engineering is a systematic approach for continuous application performance improvement that involves practices, techniques and activities during each DevOps phase to achieve the performance quality goals of the business. It focuses on the architecture, design and implementation choices that will affect application performance and encompasses the practices that help mitigate performance risks before progressing to subsequent phases.

Position and Adoption Speed Justification: DevOps practices include continuous integration and continuous deployment, yet testing practices remain immature and mostly focused on functional testing. The ability to consistently deliver products that satisfy end-user expectations of overall user experience, quality of service (QoS), availability and performance has become crucial for digital businesses. Performance engineering promotes a holistic and proactive approach with performance requirements driving the design, development and delivery of products as part of a continuous quality strategy.

Although performance engineering continues to gain interest and grow, challenges remain. Although its individual elements have been known for many years, performance engineering as a holistic discipline has not yet been widely adopted. Organizational silos, traditional top-down management structures and lack of experience with continuous quality can impede adoption rates. As a result, the speed of adoption will vary between verticals and organizations.

User Advice: Application leaders must create awareness for raised end-user expectations for application quality, specifically nonfunctional characteristics such as performance efficiency. ISO/IEC 25010 — the international standard for software quality — provides a template for understanding quality characteristics and includes performance efficiency as one of the top-level nonfunctional domains. It includes overall user experience, QoS, availability and performance.

Application leaders can take this as an example to drive a more holistic view of quality that will help reduce technical debt, mitigate application performance risks and satisfy the quality expectations of the users/business. They should ensure that performance is an overarching requirement for development by engaging the key stakeholders from business, the users and IT right from the start. They should foster a culture that makes performance an explicit requirement by enhancing functional requirements with performance-related criteria, and stating precise and measurable performance targets that DevOps teams can write tests against.

By supporting their teams to adopt performance engineering practices, application leaders will help improve application performance and the behavior of production systems. This will also aid better understanding of end-user experience, which is crucial for developing applications that are fit for purpose. Together, performance engineering practices constitute a closed-loop system, providing continuous information about critical performance indicators as part of a DevOps toolchain. Operations teams, particularly cloud operations, can define and provide performance metrics based on business requirements, not just technology key performance indicators (KPIs).

Business Impact: Performance is one of the most critical nonfunctional characteristics of applications. Functional defects can typically be fixed relatively quickly and with comparatively little effort. Design flaws that impact performance are much harder to fix because they affect a larger number of features in different parts of the application. Such architectural or structural defects are typically some of the main contributors to technical debt.

Performance engineering includes both “shift left” and “shift right” testing practices and will provide additional value through tighter integration in DevOps toolchains. The adoption of a performance engineering strategy significantly improves an organization’s ability to consistently deliver solutions that delight customers by exceeding their performance expectations. It provides the framework for application performance excellence that drives value and supports the realization of business outcomes for customers.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: AppDynamics; BlazeMeter; Dynatrace; Eggplant; IBM; Micro Focus; Neotys; New Relic; Parasoft; SmartBear

Recommended Reading:

“Adopt a Performance Engineering Approach for DevOps”

“Innovation Insight for Continuous Quality”

“Take a ‘Shift Left’ Approach to Testing to Accelerate and Improve Application Development”

“DevOps Success Requires Shift-Right Testing in Production”

“Maverick* Research: Software Testing and the Illusion of Exterminating Bugs”

Chaos Engineering

Analysis By: Jim Scheibmeir; Dennis Smith

Definition: Chaos engineering is the use of experimental and potentially destructive failure or fault injection testing to uncover vulnerabilities and weaknesses within a complex system. It is systematically planned, documented, executed and analyzed as an attack plan to test components and whole systems both pre- and postimplementation. Chaos engineering is often used by SRE teams to proactively prove resilience during fault conditions, and to eliminate those potential sources of system downtime.

Position and Adoption Speed Justification: Chaos engineering has emerged from the practices first pioneered by Netflix (such as Chaos Monkey, Chaos Kong and the Simian Army) and Google (via their DiRT exercises). Early efforts at chaos engineering took simple actions (such as unexpectedly killing a virtual machine). The practice is moving beyond innovative early adopters and being utilized in leading enterprises in the financial services and online retail industry. While there continues to be substantial interest in the wider IT community, chaos engineering will eventually find its way to more enterprises over the next few years as many mature their digital initiatives.

As companies attempt to build scalable, highly available systems, they must demonstrate resilience in the face of not only worst-case scenarios (such as unexpected load and component outages), but also “corner case” and cascade events that start from minor issues. The practice is moving beyond innovative early adopters and becoming integrated into leading enterprises in the financial services and online retail industry. There continues to be substantial interest in the wider IT community, and it will find its way to more enterprises over the next few years as many commence their digital initiatives.

User Advice: We recommend the following:

- Utilize a test-first approach by practicing chaos engineering in preproduction environments and move findings into production environments.
- Incorporate as a part of your system development and/or testing process.
- Build-out incident response protocols and procedures, as well as monitoring, alerting, and observability capabilities in part with advancement of any chaos engineering practice.
- Use scenario-based tests, known as “Game Days,” to evaluate and learn about how individual IT systems would respond to certain types of outages or events.
- As your practices mature, investigate opportunities to use chaos engineering in production to facilitate learning and improvement at scale, although we believe that there are still very few organizations purposely using it in their production environments.
- Although not a security technique, chaos engineering does sometimes discover security issues.
- By adopting and then extending chaos engineering with autoremediation and continuous validation in the live operational environment, a “digital immune system” may be developed within an application or system.

Business Impact: With chaos engineering, we minimize time to recovery and change failure rate, in addition to uptime and availability — all of which help improve customer experience, customer satisfaction, customer retention and new customer acquisition.

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Sample Vendors: Alibaba Cloud; Bloomberg; ChaosIQ; Gremlin; Microsoft; Netflix; OpenEBS; Verica; VMware

Recommended Reading:

"Innovation Insight for Chaos Engineering"

"How to Safely Begin Chaos Engineering to Improve Reliability"

"DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value"

"Not Just Microservices: Choose the Right Service Granularity for Your Applications"

"Market Guide for Service Orchestration and Automation Platforms"

"Maverick* Research: Software Testing and the Illusion of Exterminating Bugs"

At the Peak

Artificial Intelligence for IT Operations (AIOps) Platforms

Analysis By: Charley Rich; Pankaj Prasad

Definition: AIOps platforms combine big data and machine learning through support of all primary IT operations functions through the scalable ingestion and analysis of the ever-increasing volume, variety and velocity of data generated by IT operations. The platform enables the concurrent use of multiple data sources, data collection methods, and analytical and presentation technologies.

Position and Adoption Speed Justification: Increased demand for AIOps platform capabilities is fueled by the growing need to intelligently drive the acceleration and automation of IT operations functions through analysis of both historical and real-time data. This is happening as roles and responsibilities converge (with DevOps and SRE as a leading examples) in the pursuit of greater agility as well as the ever increasing momentum behind digital transformation. The desire to intelligently drive automation requires continuous insights derived from machine learning algorithms based on data generated by IT operations management (ITOM) disciplines, such as application performance monitoring (APM), infrastructure monitoring (ITIM), NPMD, digital experience monitoring (DEM) and IT service management (ITSM). AIOps platform adoption — in particular, machine-generated data including logs, metrics and traces, as well as human-processed data such as incidents dependencies and changes — continues to rise in support of ensuring high-quality digital experience.

Interest and investment will continue to rise due to:

- Rapid growth in data volumes generated by the IT systems, networks and applications
- Increasing data variety — velocity at which data is generated and changing
- Challenges in maintaining observability and improving engagement due to the adoption of cloud-native and ephemeral architectures
- The need to intelligently and adaptively drive the automation of recurring tasks and predict change success and service-level agreement (SLA) failure

AIOps capabilities have evolved across multiple dimensions:

- The domain-agnostic AIOps platforms with vendors offering a general-purpose AIOps platform.
- Domain-centric AIOps vendors, that have the key components, but with a restricted set of use cases focused on one domain (for example, network, endpoint systems, APM or ITSM).
- Do it yourself (DIY), where end users can mix and match the components, essentially assemble tools for data ingest, a big data platform, machine learning (ML) and a visualization layer from multiple providers or open-source projects.

ML uses multiple analytical approaches, while remediation requires significant maturity. Gartner still sees event correlation as the predominant practical use case, while aspirational goals like real-time business insights requires end-users to invest in resources like time, effort and skills. Remediation is still being handled via rule-based approaches although vendors are beginning to deliver ways to systemize and recall the problem resolution process for later reuse.

User Advice: I&O leaders must build a strategic AIOps platform investment plan that is tied to driving measurable business outcomes though analysis of performance, digital experience and delivery automation while utilizing stagewise implementation of AIOps capabilities:

- Begin with practical goals, such as reducing operational noise through event correlation and anomaly detection, and later moving on to root-cause analysis.
- Start proactively detecting the signals that indicate emerging problems before users are impacted.
- Use NLP to democratize the automation of reoccurring workflows, making it easier to initiate them without deep specialist skills.
- Apply the pattern-matching capabilities of AIOps to the DevOps build-deploy process in order to detect potential impacts to production prior to deployment.

The AIOps strategy must account for the following:

- Balancing ease of implementation/use with interchangeability of platform capabilities

- ITOM tool portfolio rationalization
- Key technology gap investment

Before embarking on an AIOps journey, I&O leaders must determine whether using a domain-centric AIOps solution such as a monitoring tool that leverages machine learning is sufficient or whether a separate AIOps solution is necessary for their use cases. The domain-centric solution will likely have a shorter time to value, but its scope will be narrow, and impact will be less. Domain-agnostic solutions may address a broad scope, and while their time to value will necessarily be longer their impact can be greater. If a domain-centric solution is already deployed for its primary purpose, evaluate its capabilities for AIOps in relation to the data sources that must be analyzed before considering a domain-agnostic solution.

Business Impact: By enabling I&O teams to enhance and transform major operational functions with a real, automated insight generation capability, organizations across all verticals stand to realize:

- Agility and productivity gains — via active combined analysis of both IT and business data, yielding new insights on user interaction, business activity and supporting IT system behavior.
- Service improvement and cost reduction — via a significant reduction in time and effort required to identify the root cause of availability and performance issues. Behavior-prediction-informed forecasting can support resource optimization efforts.
- Risk mitigation — via active analysis of monitoring, configuration and service desk data identifying anomalies from both operations and security perspectives.
- Competitive differentiation/disruption — via superior responsiveness to market and end-user demand based on machine-based analysis of shifts, beyond those that are immediately obvious to human interpretation.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: Aisera; Appnomic; BigPanda; BMC; Digitate; Moogsoft; ScienceLogic; ServiceNow; Splunk; StackState

Recommended Reading:

“Market Guide for AIOps Platforms”

“Avoid the Unexpected Consequences of IT Change Management With AIOps and CMDB”

“Assess Approaches to AIOps for a Comprehensive Solution”

“Deliver Cross-Domain Analysis and Visibility With AIOps and Digital Experience Monitoring”

“Augment Decision Making in DevOps Using AI Techniques”

Collective Intelligence Benchmarking Tools

Analysis By: Federico De Silva

Definition: Collective intelligence benchmarking (CIB) enables comparison of the relative performance of a given service, application and or IT infrastructure against an aggregated and anonymized performance observed based on data collected from a broad set of end users. This approach is typically adopted by SaaS-based IT monitoring tool providers with access to data from multiple customers and seeking explicit permission to leverage the datasets, which may include geographic, vertical industry and other segmentation.

Position and Adoption Speed Justification: Interest for CIB data is primarily among retailers, financial services, insurance, transportation, and technology and media organizations. Organizations are increasingly reliant on cloud- and SaaS-based service delivery providers, and the limitations in visibility to cloud-based environments create a need for performance benchmarking. Unified communications (UC) monitoring represents one of the strongest use cases for CIB, largely due to the prolific uptake of UC among general enterprises, coupled with a potentially large internal user base of delay-intolerant, high-profile services. Furthermore, end users' high expectations of speed and reliability in services, as compared with what they experience from large cloud providers, put pressure on the monitoring teams to provide the same levels of service.

Virtual desktop infrastructure (VDI) monitoring remains the most embryonic scenario for CIB, although it's an obvious use case for internally generated CIB (within the same organization, as opposed to across multiple clients), given the high adoption of such technologies in educational, healthcare and government organizations. The increase in remote work is adding weight to the use of CIB data, as there is wide disparity in system performance with a nearly virtually distributed workforce.

User Advice: Although CIB within monitoring is still emerging, these new tools (or components of tools) are the first steps toward providing a more consistent and standardized means of comparison for commercial applications, given that custom applications are different, thus making comparison much more difficult. The primary users of CIB are infrastructure and operations teams, but line-of-business users such as digital workplace and endpoint monitoring will benefit from comparing their applications or services to standard or expected performance. When evaluating such tools, organizations should confirm that the tool will allow for a sufficient number of datasets to be used, providing a critical mass to create meaningful segmentation for analysis. An insufficient number of datasets could result in disproportionate outliers causing misleading comparisons and incorrect interpretations.

CIB provides general visibility of overall internet connectivity to SaaS-based applications, content delivery networks (CDNs) or cloud providers. However, it is not meant to replace specific APM or other monitoring tools, which these or additional tools can deliver only with an endpoint agent.

Keep in mind vendors' CIB capabilities in specific areas of specialization (for example, the VDI and UC monitoring markets). The tools for each space are not interchangeable, given their distinct core competencies.

Determine whether this functionality is a "nice to have" or if it addresses a visibility gap for a currently exposed technology stack. It is also possible that CIB may be incorporated as a core feature by broader monitoring vendors, particularly DEM providers that offer SaaS monitoring through a variety of techniques, including endpoint, network/internet and browser monitoring. Regulations such as the General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA) may act as an inhibitor until risks are better understood and/or deemed nonissues. If the requirement is less imperative, consider holding off on any tooling procurement until the market is more mature, or ask your current monitoring provider to demonstrate regulatory-compliant CIB capabilities within its offerings.

Business Impact: CIB looks to address new challenges that the IT operations staff is facing in light of:

- Mobile device proliferation
- The explosion of Internet of Things (IoT) data sources
- The increasingly distributed methods by which one can access applications and services beyond the control of enterprise IT where it does not have access to infrastructure or application code

In such an environment, traditional monitoring tools struggle to correlate the myriad datasets from every client interaction and experience using a "bottom up" approach. CIB offers an alternative perspective whereby organizations can baseline their environment based on objective benchmarks to determine optimum or "normal" performance and business impact, such as transactions per unit of time, failures and errors, conversion rates, etc. CIB can then be used to detect deviations or suboptimal service delivery based on cross-company sharing and comparison of IT operations KPIs and infrastructure metrics. Because benchmarking, by its very nature, deals with aggregated datasets that abstract the underlying details, this is a less exhaustive approach than traditional monitoring, and is less applicable for conducting root cause analysis (RCA) and remediation.

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Sample Vendors: Aternity; Catchpoint; Indeni; Lakeside Software; Liquidware; Logz.io; Nexthink; Nyansa; ThousandEyes; Unify Square

Recommended Reading:

"Innovation Insight for Collective Intelligence Benchmarking"

"Market Guide for Digital Experience Monitoring"

"Use DEM to Understand and Enhance Your Employees' Work-From-Home Experience"

Observability

Analysis By: Padraig Byrne; Gregg Siegfried

Definition: Observability is the characteristic of software and systems that allows them to be “seen” and allows questions about their behavior to be answered.

Tools that leverage and facilitate software observability are designed to allow an observer to collect and explore the external and internal state data using automated and exploratory techniques that iteratively reduce the universe of potential explanations for errant behavior. The insights provided by observability are useful to groups within and outside of IT, such as DevOps teams.

Position and Adoption Speed Justification: Modern applications and distributed systems, their inherent complexity, and the rise of new practices and methodologies such as DevOps has left many organizations frustrated with legacy monitoring tools and techniques that are unable to do more than collect and display external signals. The multitude of potential degradations and failure modes renders this “black box” monitoring only partially effective.

In this context, observability, has entered the IT monitoring lexicon. It is not a synonym for adequate, or different, monitoring. Rather, it suggests a holistic, data-centric, debugging philosophy that includes an exploratory capability with the intention to identify “unknown unknowns.” The observations, or the data that software observability tools collect and interrogate, may be static, such as counters or log messages, or dynamic, such as traces. Industry publications often characterize three pillars of observability: metrics, logs and traces — which while functional is limiting. More importantly, these observations must be “white box,” or reflect the internal characteristics of the system.

Traditional monitoring systems capture and examine (possibly adaptive) signals in relative isolation, with alerts tied to threshold or rate-of-change violations. Observability tools enable a skilled observer — a software developer or site reliability engineer — to more effectively explain unexpected system behavior, provided that enough instrumentation is available. Integrating software observability with AIOps to automate subsequent determinations is a potential future development, but such AIOps-based observability systems do not yet exist.

Observability is an evolution of longstanding technologies and methods, and monitoring vendors are starting to include observability ideas inside their products while new companies are building around the idea. Therefore, the time to Plateau of Productivity will be quicker than normal innovation profiles.

User Advice: Users who are starting on a DevOps journey should evaluate software observability tools to integrate into their continuous integration/continuous deployment (CI/CD) pipeline, feedback loops and retrospectives.

Enterprises with existing monitoring tools should ensure that they will sufficiently cover any modern applications and platforms on their roadmaps, leveraging existing observability tool functionality where possible.

Practitioners building and deploying software products should ensure that their systems are designed to emit enough static and dynamic instrumentation data to allow questions to be answered that support problem resolution, even when the specific problems have not been anticipated.

Long-tail latency is a critical signal. Tie service level objectives to desired business outcomes, using specific metrics and leverage observability tools to understand variations.

Business Impact: Observability tools have the potential to reduce both the number of service outages and their impact and severity. Their use by organizations can improve the quality of software because previously invisible (unknown) defects and anomalies are identified and corrected. APM suites are able to deliver a subset of observability functionality through their ability to produce observations from systems that may not have been designed with sufficient internal instrumentation.

At first glance, observability tools, with their emphasis on data exploration and analytics, may seem in conflict with AIOps and the intelligent inference approach to system operation. In fact, the same machine data management techniques included in many AIOps platforms and tools are used by observability tools to accelerate the investigation process in the same way they are in business intelligence tools — to augment a skilled professional's ability to gain meaningful insights from large volumes of heterogenous data.

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Sample Vendors: AppDynamics; Dynatrace; Honeycomb; Instana; LightStep; New Relic; Splunk; Splunk (SignalFx); VMware (Wavefront)

Recommended Reading:

"Magic Quadrant for Application Performance Monitoring"

"Critical Capabilities for Application Performance Monitoring"

"Monitoring Modern Services and Infrastructure"

"Solution Comparison for Application Performance Monitoring Solutions"

Digital Experience Monitoring

Analysis By: Federico De Silva; Charley Rich

Definition: DEM technologies monitor the availability, performance and quality of experience an end user or digital agent receives as they interact with an application and the supporting infrastructure. Users can be external consumers of a service, internal employees accessing corporate tools or a combination of both. DEM technologies seek to observe and model the behavior of users as a continuous flow of interactions in the form of “user journeys.”

Position and Adoption Speed Justification: Digital experience monitoring continues to evolve from a reliance on independent tools and technologies, which traditionally focused on metrics of single applications, toward a more holistic approach that measures the effectiveness of the interactions users have in relation to business outcomes such as retention, risk and revenue. DEM solutions are evolving from focusing purely on availability and performance toward helping organizations optimize and improve digital business outcomes by addressing three key topics:

- What they monitor: Availability, performance, security and quality of the application, and all of the components that may impact the end-user experience
- Who they monitor: External customers and partners who drive revenue for the organization, internal employees (particularly in a rapidly changing workplace), and digital agents as key actors in distributed application ecosystems
- Why they monitor — To enable the proactive monitoring of business outcomes and to connect technology with business KPIs

Although DEM is a critical component of a comprehensive IT monitoring strategy, it can be implemented and connected in parallel to other IT monitoring technologies. End-user customers can leverage the maturing capabilities of the components of DEM:

- Synthetic transaction monitoring
- Real user monitoring, including session replay
- Endpoint monitoring

Integrating the technologies can help to create a more comprehensive analysis of the customer experience and, ultimately, of the impact on the organization or business. This becomes critically important as more applications and workloads move to the cloud and IT organizations lose control of the components of the applications and services.

DEM plays a similar but complementary role to web and digital experience platforms. Web analytics and other IT monitoring technologies (e.g., APM, ITIM, NPMD and AIOPs) are part of the broader monitoring strategy. Organizations are able to have a more complete view of how users — internal, external, partners and more — are affected and impacted by the performance of their applications, and to troubleshoot accordingly. DEM is increasingly being integrated earlier in the software development life cycle as part of testing (via synthetic transaction monitoring, real user monitoring [RUM], etc.) within DevOps environments.

Improving and ensuring employee productivity is another important objective of DEM. And though there is considerable uncertainty surrounding COVID-19’s impact on the future of work, Gartner expects the “new normal” to require significant changes to I&O’s monitoring strategy for employees (see “Use DEM to Understand and Enhance Your Employees’ Work-From-Home Experience”). In this respect, DEM can be achieved through endpoint monitoring with the deployment of a local agent installed on a device (whether physical or virtual). Endpoint monitoring solutions also help monitor commercial off-the-shelf (COTS) and VDI platforms, such as SAP and Citrix environments.

User Advice: Organizations should deploy DEM technologies to create holistic views of a user's digital experience. To do so, organizations should use a combination of data sources:

- Endpoints: Agent-based instrumentation to understand the performance of applications from the perspective of the end user on a mobile device or PC.
- Real user monitoring: JavaScript that is injected into web applications to collect data such as response time, latency and errors or alternatively via plug-ins when HTML is not accessible in the case of SaaS applications. Session recording and replay shows what the user experienced during an application session, which the IT monitoring teams can correlate with other application performance metrics for RCA.
- Networks/internet: Analysis of packet and flow data to understand the impact of the network's performance on user experience. This includes monitoring voice over IP (VoIP) network traffic.
- Synthetic transaction monitoring (STM): Synthetic transaction execution records to simulate user interactions with applications leveraging RUM data to create most natural conditions.

Organizations should also complement the above data sources with social media analytics, NPS scores, ITSM data to correlate user-derived tickets to system performance and user experience, as well as the analysis of API performance as applications interact with each other.

Business Impact: Organizations that implement DEM tools can not only benefit from better application performance and improved user experience, but also ultimately improve business outcomes in support of digital transformation. This will require IT organizations to consider nonhuman agents in their analysis of interactions among customers, suppliers, partners and observers; they may exhibit different behaviors and operate on different time scales. With an expanded remote workforce, organizations will need to tie DEM to employee productivity and digital workplace initiatives to achieve the rapidly changing business objectives as a result of COVID-19 (see "Getting Value From Employee Productivity Monitoring Technologies for Remote and Office-Based Workers").

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Apica; Aternity; Catchpoint; GSX; ITRS Group; Lakeside Software; Nexthink; Quantum Metric; Rigor; ThousandEyes

Recommended Reading:

"Magic Quadrant for Application Performance Monitoring"

"Market Guide for Network Performance Monitoring and Diagnostics"

“Market Guide for Digital Experience Monitoring”

“Broaden Application Performance Monitoring to Support Digital Business Transformation”

Site Reliability Engineering

Analysis By: George Spafford; Daniel Betts

Definition: Site reliability engineering (SRE) is a collection of systems and software engineering principles used to design and operate scalable resilient systems. Site reliability engineers work with the customer or product owner to understand operational requirements and define service-level objectives (SLOs). The site reliability engineer then collaborates with IT stakeholders to design and continuously improve systems that will meet the SLOs. For products or platforms that meet SRE guidelines, the engineer may choose to provide operational support.

Position and Adoption Speed Justification: SRE is a discipline originally created by Google, and was described in the 2016 book, “Site Reliability Engineering: How Google Runs Production Systems.” Adoption interest continues to grow both by digital-native organizations as well as traditional enterprises. SRE emphasizes the engineering disciplines that lead to resilience, but individual organizations implement SRE in widely varying ways. SRE is a complementary practice for organizations seeking to scale their DevOps activities.

SRE is intended to help manage the risks of rapid change, through the use of service-level objectives (SLOs), “error budgets,” monitoring, automated rollback of changes and organizational learning. SRE teams are often involved in code review, looking for problems that commonly lead to operational issues (for instance, an application that does not do log cleanup and therefore may run out of storage). They also ensure that the application comes with appropriate monitoring and resilience mechanisms, and that the application meets SRE approved standards or guidelines set to achieve negotiated SLOs. SRE teams can serve as an operations function and nearly all such teams have a strong emphasis on blameless root-cause analysis. This is to decrease the probability and/or impact of future events and enable organizational learning, continual improvement and reductions in unplanned work.

SRE practices are being adopted by organizations that need to deliver digital business products reliably. These practices require a culture that supports learning and improvement, highly skilled automation practices (and usually DevOps), usage of infrastructure as code capabilities (which usually requires a cloud platform). SRE also uses automation to reduce manual processes, leverages resilient system engineering principles, and an agile development process that employs CI/CD.

User Advice: Organizations can benefit from SRE principles even if they are not sufficiently mature, agility-focused, or large enough to adopt SRE as a primary operations model. The SRE principles for risk management, release engineering, handling service-level objectives, monitoring, automation, and self-healing can be applied to a broader range of products and platforms. SRE also represents a useful means to scale DevOps initiatives.

An SRE initiative should have an executive sponsor. The first opportunity to begin with should have the following characteristics:

- The target application must change rapidly yet maintain high availability in order to maximize business value. Stakeholders should be politically friendly.
- The pilot must demonstrate sufficient value to improve credibility and support, yet also have an acceptable level of risk, allowing the stakeholders to learn.
- The initial SRE team must have a collaborative engineering mindset, strive to continuously learn and improve, and desire to automate tasks to reduce repetitious manual work, which is known as "toil." It is often easiest to move DevOps-skilled employees from different parts of the organization, due to the relative difficulty of hiring engineers with SRE experience. A site reliability engineer is typically a software engineer with an excellent understanding of operations, or, less frequently, an infrastructure and operations engineer with strong programming skills.
- There must be clear SLOs that can be continuously monitored and reported against.
- The SRE collaborates with developers to help them learn how to design and build their product to meet the defined SLOs — the SRE is not doing the actual development work or inspecting quality in.
- The application development team must collaborate with the SRE team to meet SLOs. Developers are responsible for a resilient architecture and reliable code. SREs should not spend more than 50% of their time on ad hoc operational activities. Any excess should go to the developers for support.

An iterative approach must be used to start and evolve SRE practices. The teams involved must share experiences and lessons learned.

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

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Recommended Reading: "DevOps Teams Must Use Site Reliability Engineering to Maximize Customer Value"

"SRE and DevOps: End-to-End Accountability"

"Agile and DevOps Primer for 2020"

"Innovation Insight for Chaos Engineering"

“Maverick* Research: Software Testing and the Illusion of Exterminating Bugs”

Sliding Into the Trough

Unified Communications Monitoring Tools

Analysis By: Lisa Pierce

Definition: UC monitoring tools collect and analyze information on voice, video and messaging sessions from vendor-supplied data sources, including call detail records (CDRs), quality metrics, end-user data from devices/clients and other sources. Some tools use standard APIs, and extract data from UC and VoIP vendor databases and repositories. Advanced tools have the ability to collect session and packet data, decode voice and video codecs, and employ synthetic call testing.

Position and Adoption Speed Justification: UC monitoring breadth of tooling capabilities are not as extensive as they are when compared to mainstream NPMD and APM tools. The transient nature of VoIP/UC infrastructure and platforms challenges tool vendors to maintain support for the latest underlying technology, especially as the market is making a marked shift from premises-based UC to cloud UCaaS.

Some NPMD vendors focus on broader network monitoring use cases and are not VoIP/UC specialists, yet they provide UC-oriented components to augment their holistic monitoring products. Depending on client need, these may not drill down on session-level performance to the extent needed. Conversely, niche VoIP-/UC-dedicated vendor tools solely focus on deeper VoIP/UC insight, and on specific UC vendors. Depending on the vendor, they may only look at specific application-level performance, rendering them unable to support other applications, or discern root cause absent NPMD tools. Clients seeking a blend of these tools should look at emerging digital experience monitoring (DEM) capabilities.

As clients increasingly adopt UCaaS, UC monitoring tools have evolved as well. Some of these tools are cloud-first/cloud-only — they do not look at system-/premises-based UC performance. Others are outgrowths of monitoring tools that assessed the performance of UC systems. Finally, some UCaaS providers also offer performance monitoring tools for their services.

User Advice: As VoIP/UC solutions shift more to UCaaS solutions, users should ensure that they still require dedicated UCM, because UCaaS offers often include monitoring functionality, with some of it being quite advanced. In addition, UCM vendors support the collection and analysis of API data provided by the UCaaS vendor. As part of this support, users should note that the monitoring data through APIs from specific UCaaS providers may not provide suitable enough visibility to diagnose and troubleshoot performance issues. In such cases, users can look to synthetic testing and packet-based NPMD solutions as ways to increase visibility.

Clients should seek solutions that combine the ability to monitor and diagnose problems in real time through collecting and analyzing real time data, with synthetic agents to gain performance insights into VoIP/UC infrastructures. .

Network conditions are continually changing, so collecting and analyzing packet and network health data provide a more accurate indicator of real VoIP/UC session quality. These more complex solutions come at a significantly higher cost to purchase and operate. More-granular tools include packet acquisition, analysis and storage. Although in-depth tools are focused on monitoring VoIP/UC components, they may also be applied to other NPMD use cases. Explore these cases to ensure that such investments are maximized.

Finally, support for monitoring video and/or media streaming continues to lag behind, compared with support for voice among most UCM tooling vendors. If browser-based VoIP (WebRTC) and video (VP9), desktop video, or media stream monitoring are requirements, then ensure that the chosen vendor can support the proprietary codecs and protocols being employed.

Business Impact: Enterprises are migrating VoIP/UC services to the network team, and the shift is altering the focus of and demand for VoIP/UC monitoring and management needs. Regardless of whether a VoIP/UC environment is self-managed or maintained via a third party, VoIP-/UC-specific monitoring tools are a fundamental prerequisite for the success of any VoIP/UC project. This success involves managing the performance of VoIP/UC systems in order to recognize the cost savings over legacy voice systems and improve employee engagement and collaboration. However, as the shift to network teams commences, often complex UCM tools can present usage challenges for those network operations personnel who don't have a deep enough understanding of the VoIP/UC environments they are meant to monitor. Adequate training is highly recommended.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: AppNeta; Cisco; Empirix; Nectar; PathSolutions; ThousandEyes; Unify Square; voipfuture; Vyopta

Recommended Reading:

"Market Guide for UCaaS Monitoring"

"Market Guide for Network Performance Monitoring and Diagnostics"

"Market Guide for Digital Experience Monitoring"

"Reduce the Visibility Gap for Microsoft Skype for Business With the Right Monitoring Strategy"

Intent-Based Networking

Analysis By: Andrew Lerner

Definition: An IBN system (IBNS) is a closed-loop system to help design, provision, and operate a network, based on business policies. An IBN system is typically packaged as software, and a full IBNS includes four key subcomponents that provide the following functionality:

- Can translate a higher-level business policy to a network configuration.
- Can automate network activities across network components.
- Has awareness of network state/health.
- Provides continuous assurance and enables dynamic optimization.

Position and Adoption Speed Justification: IBNS is being hyped by networking vendors because of the promise to improve network availability and agility simultaneously, enabling digital business transformation. However, as of early 2020 real-world enterprise adoption of full IBNSs is nascent. We estimate fewer than 100 full deployments that meet all phases of the definition. The detailed description of the subcomponents of IBNS includes:

- **Translation and validation:** System can take a higher-level business policy (what) as input from end users and convert it to the required network configuration (how).
- **Automation:** System can configure appropriate network changes (how) across existing network infrastructure.
- **State awareness:** System ingests real-time network status for systems under its control.
- **Assurance and dynamic optimization:** System continuously validates that business intent is being met; can take corrective actions when it is not.

Each of the four subcapabilities of intent can be deployed independently. There is much heavier adoption of certain individual components, including automation. These components delivered individually add value, but are not full intent when they aren’t delivered together as part of a closed loop.

In the past 18 months, the terminology around intent (including intent-based, intent-driven and IBN) has largely been taken over by vendor marketers, as there is rampant overmarketing of intent by networking vendors. Things such as automation, abstraction and programmability are described as intent. Unfortunately, many products are marketed by vendors as intent that falls short of the full capabilities of intent.

We anticipate that the number of full closed-loop IBNS commercial enterprise deployments to remain below 200 through 2020, and increase moderately by the end of 2021. We expect adoption to be pragmatic — associated with new build-outs and/or network refresh initiatives. Through 2020, early rollouts are likely to be in larger-scale environments for well-defined and specific use cases, such as spine/leaf data center networks. We expect that data center networking vendors will increasingly incorporate assurance, validation and dynamic remediation into their networking suites, getting closer to a full IBN.

We recommend and anticipate that adoption will be phased, with the different IBNS subcomponents enabled gradually over months and years. Technologically, IBNS requires the ability to abstract and model network behavior, which has proved difficult historically, particularly in multivendor environments. Furthermore, IBNS represents a substantial cultural shift in how networks are designed and operated, which will create barriers to adoption in many risk-averse enterprises.

User Advice:

- Deploy IBNS pragmatically in phases, because each of the four individual subcomponents adds value. For example, organizations can deploy an IBNS in "notify mode," whereby a skilled engineer must approve a proposed automated change suggested by the IBNS.
- Mandate support for open, RESTful APIs when purchasing new networking infrastructures to support integration within an IBNS moving forward.
- Choose an IBNS that supports multivendor network infrastructures and extends into public cloud environments to support a broader range of use cases and avoid vendor lock-in.
- Tune-out vendor marketing regarding products that are listed as intent.

Business Impact: Gartner sees the biggest benefits from IBNS as improving network agility and availability, and supporting unified intent and policy across multiple infrastructures. When the technology matures, a full IBNS implementation can reduce the time to deliver network infrastructure services to business leaders by 50% to 90%, while simultaneously reducing the number and duration of outages by at least 50%. Although agility and availability are the high-level benefits, IBNS provides several other specific benefits, including:

- **Reduced operating expenditure (opex) —** Reduce opex associated with managing networks and free up senior-level network resources to focus on more important strategic tasks.
- **Performance optimization —** Intent-based algorithms provide better traffic engineering versus traditional approaches, such as routing protocols. This can improve application performance.
- **Reduction in dedicated tooling costs —** Intent tools may circumvent the costs of other related network infrastructure tooling, because automation and orchestration are embedded in IBNS.
- **Better documentation —** IBNS provides real-time self-documentation, which also includes the rationale (intent) behind design/configuration decisions.
- **Improved compliance —** IBNSs simplify auditing, due to the algorithmic correctness of configurations, direct mapping to business intent and ongoing, dynamic, real-time validation.

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Sample Vendors: Apstra; Cisco; Forward Networks; Gluware; Huawei; Intentionet; Juniper Networks; NetYCE; VMware

Recommended Reading:

"Innovation Insight: Intent-Based Networking Systems"

"Cool Vendors in Enterprise Networking"

Virtual Desktop Infrastructure Monitoring

Analysis By: Pankaj Prasad; Padraig Byrne

Definition: Virtual desktop infrastructure monitoring (VDIM) tools provide end-user-focused, end-to-end monitoring of centralized desktop delivery (VDI) platforms. A majority of these tools also monitor stand-alone desktops and laptops. VDI platforms enable applications to execute on the server side, but render on the client side. Currently, VDIM tools tend to specialize in one or two of the following areas: visibility of underlying infrastructure components, visibility of the VDI platform and/or perception from the end-user perspective.

Position and Adoption Speed Justification: VDI is considered a relatively mature technology, but has a low penetration of less than 20% within enterprises. DaaS, which is relatively new, also has a low penetration similar to VDI. Uptake of VDIM is in an early phase in tandem with the low penetration of VDI and DaaS.

VDI is an opaque technology to the current generation of third-party APM or NPMD technologies. The challenge is not finding solutions for monitoring specific aspects of VDI platforms, but rather finding a common set of tools that can monitor all aspects of VDI, as well as other application and network environments. IT buyers have been dissatisfied with the lack of VDI support in APM and NPMD tools. The failure to deliver and manage VDI using tools that support a broader set of APM or NPMD technologies leaves a gap between providing a holistic picture of application and network performance and end-user impact. Dedicated VDIM tools have met this requirement to an extent, driving their adoption on an incremental level. However, they lack the level of user interface workflow and navigation sophistication of their APM/NPMD counterparts.

Gartner has seen scenarios where VDIM tools are deployed for stand-alone systems. Some larger enterprises are emphasizing employee experience and engagement as a priority over device health. Vendors have started to focus on the real-time perception from an end-user perspective. These tools are also deployed for DEM.

Much of the monitoring hype for VDIM has been relevant to VDI, which has a much larger installed base. End users have been largely dissatisfied with VDIM due to its singular focus on endpoint technology. While this aided in visibility and troubleshooting, the shift in enterprises toward employee engagement and the need for better visibility into user experience will positively impact this space. Also a positive impact will be the increasing shift to DaaS and potential monitoring solutions by cloud providers like AWS and Microsoft.

User Advice: Given the narrow scope of dedicated VDIM tools, it is important to weigh the value gained by such a focused solution against broader-scoped tools that may not provide the same level of granularity and depth, but may cover greater monitoring use cases. Also consider whether expansion of the VDI environment is likely. If so, examine forward planning, historical reporting and trending capabilities alongside diagnostic features.

Avoid investing in an overengineered solution when sufficiently consumable detail can be made available to the relevant staff for a more competitive cost point. Understanding the use-case scenarios for all the relevant users of the tool is key in ascertaining the precise balance between low-level insight and higher-level workflow automation, alerting and reporting requirements.

An end-to-end view does not mean all monitoring technologies ought to be deployed. If DEM is the main goal for deploying VDIM tools, evaluate whether the objective is visibility interactions with enterprise applications, in which case APM tools are a good alternative. If the objective is to assess user experience in the form of latency or quality from the network perspective, consider NPMD tools. SaaS-based applications need better assessment of monitoring tools since VDIM will have limited visibility, especially if synthetic monitoring is not the main goal. In this case, APM and/or NPMD tools will be a better fit.

Business Impact: VDI makes heavy use of the network and proves difficult to gain insight into, because of its opaque nature. If application response time is affected, end users are apt to complain loudly and quickly. Issues can range from network latency, slow connection, server-side resource overload, application issues or a single user locking out an application for others. IT operations teams, therefore, require a specific monitoring toolset and strategy for proactive and effective management of such a specific technology.

VDI adoption is more common in healthcare and certain public-sector organizations; therefore, these vertical industries are likely to find the tools particularly relevant. Other areas of applicability include structured-task workers in call centers and kiosks, on trading floors and with secure remote access.

Remote working due to COVID-19 has caused enterprises to assess tools for understanding and enhancing employee experience. VDIM is one tooling category considered along with NPMD and APM based on the organization's evolving monitoring strategy.

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

Sample Vendors: CloudPhysics; ControlUp; eG Innovations; Goliath Technologies; Lakeside Software; Liquidware; Login VSI; Nexthink; Riverbed (Aternity)

Recommended Reading:

"Market Guide for Digital Experience Monitoring"

"Use DEM to Understand and Enhance Your Employees' Work-From-Home Experience"

"Employ Multifaceted Monitoring Approaches for VDI and DaaS"

Network Detection and Response

Analysis By: Lawrence Orans; Jeremy D'Hoinne

Definition: NDR technology uses a combination of ML, rule-based detection and advanced analytics to detect suspicious activities on enterprise networks. NDR tools analyze raw traffic and/or flow records (for example, NetFlow) to build models that reflect normal network behavior. When the NDR tools detect abnormal traffic patterns, they raise alerts. NDR solutions monitor north-south and east-west traffic. These tools also provide workflow capabilities to enable security teams to respond to incidents.

Position and Adoption Speed Justification: NDR has begun to pull out of the Trough of Disillusionment as adoption of the tools continues to grow. One challenge that enterprises face with NDR is the growth in encrypted traffic, as Gartner estimates that HTTPS browsing routinely exceeds 80% of total internet traffic. Vendors offer a wide range of support for analysis of encrypted traffic. A handful of vendors are positioned in the line of traffic and natively support the termination, decryption and analysis of SSL/TLS traffic. However, the majority of NDR solutions are implemented out-of-band, and their analysis of encrypted traffic is limited to techniques that do not inspect the payload, such as JA3 fingerprinting, or similar methods. A few vendors offer more advanced analysis for detecting suspicious encrypted traffic by monitoring the lengths and arrival times of messages within traffic flows and other data transmission patterns (this technique is helpful, but not as valuable as plain text analysis).

False positives are generally not a major problem with NDR technology, but they are an unavoidable issue with any machine learning-based detection tools and have somewhat slowed adoption of these solutions. Many users of NDR solutions report that they have had to tune these tools to avoid registering false positives, particularly from traffic generated by vulnerability scanners. The NDR solutions had indicated “reconnaissance port scanning” and “anomalous lateral movement” due to traffic from the scanners.

Response functionality has begun to mature in these tools. Some vendors emphasize an automated response capability (for example, commands are sent to a firewall to drop packets), and many vendors integrate with SOAR and other automation tools. Other vendors emphasize manual response by emphasizing threat hunting tools.

User Advice: Enterprises that are considering NDR tools should ensure success by giving their security teams the training they need to gain maximum value from these solutions. Additionally, enterprises should ensure they have qualified personnel to triage the alerts and other signals from the NDR. Because these tools highlight anomalies, gaining maximum value from NDR tools requires a strong understanding of the overall traffic patterns and specific protocol patterns in your enterprise network.

Proper positioning of the NDR sensors is critically important. Network security professionals should carefully plan sensor deployment so that the sensors can analyze the most relevant network traffic. Scalability of the sensors is also important. Some vendors offer sensors that support up to 100 Gbps of line rate capture, whereas other vendors’ sensors can only scale up to 10 Gbps.

Business Impact: NDR solutions are valuable tools that assist network security professionals in the detection of compromised endpoints and targeted attacks. These tools have limited native blocking ability, or none at all (because most are implemented outside of the line of traffic), but they offer manual and/or automatic functionality for responding to alerts. Many NDR solutions can also be implemented to detect suspicious activity in IaaS environments.

As more enterprises adopt a "direct to net" approach from branch offices (for example, implementing a local internet breakout and sending web traffic directly from the branch office to the internet), NDR solutions positioned in a data center will not see that traffic. However, most organizations that implement the "direct to net" approach still retain their MPLS connections to their private or public cloud data centers, so NDR tools will remain valuable for that traffic.

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Sample Vendors: Awake Security; Cisco; Darktrace; ExtraHop; Fidelis Cybersecurity; FireEye; Gigamon; Lastline; Plixer; Vectra

Recommended Reading:

"Market Guide for Network Traffic Analysis"

"Infrastructure Security Primer for 2020"

"Applying Network-Centric Approaches for Threat Detection and Response"

Climbing the Slope

Network Packet Brokers

Analysis By: Josh Chessman

Definition: Network packet broker (NPB) appliances (both physical and virtual) facilitate the distribution of network packet traffic gathered from switched port analyzer (SPAN) ports or network taps between network elements. NPBs also allow manipulation of the traffic for more efficient use by NPMD tools and security-related monitoring solutions, including NTA tools.

Position and Adoption Speed Justification: The need for tools that require packet data has stabilized for NPMD use cases, but continues an upward trajectory for security use cases with continued interest in NTA tools. NPBs help solve the problem of providing data from limited source feeds to multiple destination tools in two primary ways. First NPBs can efficiently replicate source feeds to multiple destinations. Second, NPBs can be used to massage data before feeding it selectively to downstream security and performance monitoring tools. NPBs act as the mediator to ensure the necessary tools receive the specific data they need in the format they need it.

NPB solutions are offered by a relatively small number of vendors focused on this market. However, new network architectures, with the combination of programmable switching hardware and a centralized controller can deliver many of the same capabilities through software (often at a greatly reduced cost than traditional NPBs). This infrastructure-based approach sees NPB functionality as a service embedded in the infrastructure itself. Enterprise networking vendors (e.g., Arista and Cisco) offer NPB capabilities as an optional software feature on some of their latest data center switches.

The virtualization within data centers and the migration of workloads to the cloud have presented challenges to the traditional hardware based, on-premises NPB deployment. As a result, several NPB vendors have introduced virtualized solutions for both on-premises and cloud-based deployment, leveraging virtual taps to collect, analyze, manipulate, and forward packet and related data. Additionally, the rise of encryption within the data center has seen the increasing use of certain NPB vendor's technology for real-time decryption.

As a result of these changes and a maturing of the core NPB functionality NPBs have jumped forward toward the plateau.

User Advice: Pay close attention to the life spans of these technologies and how they fit into your plans for network growth. Your upgrade path is critical for making the best investment decisions. Payment tends to be biased toward capital expenditures, with large upfront sums paid for the appliances and a subsequent maintenance payment charged on a yearly basis. Hardware warranty contracts last multiple years, which when combined with significant capital expenditures can result in vendor lock-in. Given the general similarities among the NPB vendors in features, buyers can take advantage of competitive bids to attain the deepest discount.

Ensure whichever NPB supplier you opt for not only has the capacity to support both current requirements and those that may evolve over the short and medium time frames. Can the NPB vendor provide:

- De-encapsulation of tunneled traffic (such as Virtual Extensible LAN — VXLAN or Generic Network Virtualization Encapsulation — GENEVE).
- Application layer decoding to support more advanced traffic filter and forwarding.
- Appropriate deployment models, such as out-of-band, in-band, or a combination of both.

Many NPB vendors have begun expanding beyond the traditional capabilities of NPBs by moving into additional, corollary areas such as NPMD and NTA functions running on the packet broker hardware itself. When evaluating NPBs organizations should look at these additional offerings and see if and how they fit in their overall monitoring and security plans.

Finally, when evaluating the need for cloud-based NPB functionality ensure you are not forcing an on-premises approach to your cloud solutions. Collecting and analyzing packets in the cloud may have some functionality however in many circumstances it is unnecessary or redundant with other visibility solutions.

Business Impact: Gartner typically sees NPBs deployed in large enterprises, particularly financial and insurance institutions, government organizations and cloud service providers (CSPs). NPBs help these organizations meet monitoring, management, and reporting requirements considering increasing complexity of hybrid data center and cloud environments and the need to send relevant network traffic to downstream analytics tools (for example for forensic and security analysis). With its ability to provide for the aggregation and disaggregation of traffic after network upgrades, NPBs can often provide an effective way to avoid costly upgrades of existing NPMD and NTA hardware.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: APCON; Arista; cPacket; CGS Tower Networks; Cubro; Garland Technology; Gigamon; Ixia; Niagara Networks

Recommended Reading:

“Market Guide for Network Packet Brokers”

“NetOps 2.0: Embrace Network Automation and Analytics to Win in the Era of ContinuousNext”

“Market Guide for Network Performance Monitoring and Diagnostics”

Application Performance Monitoring Software

Analysis By: Charley Rich; Federico De Silva

Definition: APM software is composed of:

- Front-end monitoring to observe and analyze the performance and behavior of end-user interactions with applications.
- Application discovery, tracing and diagnostics (ADTD), used to discover and detect the relationships between web/application servers, microservices and infrastructure using bytecode instrumentation and/or distributed tracing.
- Analytics uses domain-centric artificial intelligence for IT operations (AIOps) to detect patterns, anomalies and causality.

Position and Adoption Speed Justification: Gartner continues to see increasing growth in the market size (over 15.3% growth rate on revenue of $4.3B, see “Market Share: All Software Markets, Worldwide, 2019”) driven by the continued acceleration of the digitalization of business processes and the realization that greater observability is needed to monitor the applications that are essential to digital business transformation.

APM vendors have expanded with integrated monitoring and analysis of infrastructure, including network, servers, databases, logs, containers, orchestration, service mesh, microservices, cloud services, the relation of performance metrics with business KPIs and business processes.

Increased emphasis on customer experience is stimulating the need for greater insight into the customer journey as users interact with digitalized business processes. This need goes beyond traditional front-end monitoring, as part of APM measuring latency and encompasses a broader set of capabilities including measuring end-user sentiment, as well as accomplishment of business objectives such as orders, claims and trades (see “Market Guide for Digital Experience Monitoring”).

APM is playing a critical role in providing rapid feedback to developers about the impact of the most recent production deployments. They display performance analysis within the context of a release with some solutions providing bidirectional deployment tool integration and the sharing of tags between IT ops and DevOps.

APM vendors’ adoption of open standards continues to expand. A number of APM vendors have become active in the group defining a future standard for distributed tracing, collection of metrics and logs, OpenTelemetry. (See “Magic Quadrant for Application Performance Monitoring.”) This approach is developer-intensive but, with automation it may replace or expand the standard model of application monitoring, the agent. The proprietary nature of APM agents are also evolving, pushing more of the APM value proposition into the analytics realm, reducing vendor “stickiness.” The mainstream adoption of OpenTelemetry could disrupt vendors that are slow to adopt these new technologies and could impact the rate of adoption of microservices. This is part of an ongoing trend toward self-reporting infrastructure.

APM solutions are increasingly adding ML, a technology used in AIOps solutions, into their products. ML is being used to reduce the noise operators deal with, predicting and detecting anomalies and determining causality.

User Advice: As organizations continue to embrace digital transformation, their need for agility in order to deliver on these transformation initiatives increases. Therefore, APM solutions must support that need for agility, aid in its acceleration and effectiveness, and avoid being perceived as just another performance monitoring tool.

Choose vendors that assist in relating application performance to business objectives and serve not only IT operations, but also DevOps, application owners and lines of business (LOBs), providing value throughout the life cycle of an application. Select a vendor that provides actionable answers and not just endless drill-downs to more data.

Choose APM vendors based on their abilities to support, the following:

- The mapping and monitoring of customer and business journeys
- Bidirectional integration with the DevOps tool chain
- New emerging standards in instrumentation such as OpenTelemetry
- Cloud-native monitoring with an API-first approach

Bidirectional integration with ITSM tools to bridge the gap between APM and ITSM tools (see “Avoid the Unexpected Consequences of IT Change Management With AIOps and CMDB”).

Business Impact: APM is critical for isolating problems, shortening MTTR, improving service availability and customer experience. Advanced capabilities can be used to better understand business processes by mapping instrumentation data to a business process, broadening APM’s value in performance monitoring to delivering insights into business operations. improving business relevance, communicating insight to business personas and in resolving the most important problems first. As a result, APM continues to be of use to a growing set of stakeholders including IT Ops, development/DevOps, CloudOps and application owners or LOB (see “Critical Capabilities for Application Performance Monitoring”).

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Aternity; Broadcom (CA Technologies); Cisco (AppDynamics); Datadog; Dynatrace; IBM; Instana; New Relic; SolarWinds; Splunk

Recommended Reading:

“Magic Quadrant for Application Performance Monitoring”

“Critical Capabilities for Application Performance Monitoring”

“Market Guide for Digital Experience Monitoring”

“Broaden Application Performance Monitoring to Support Digital Business Transformation”

“Advance Your Application Performance Monitoring Strategy to Support Microservices”

“2019 Strategic Roadmap for IT Operations Monitoring”

“I&O Leaders Must Use Monitoring Metrics to Optimize Customer Experience”

Network Performance Monitoring and Diagnostics Tools

Analysis By: Josh Chessman

Definition: NPMD tools provide trend analysis, and real-time alerting via performance monitoring of network infrastructure and traffic. The tools collect performance data over time and include features such as traffic analysis, service-level reporting, automated base-lining, threshold evaluation, historical reporting, and diagnostics. These tools leverage packet-based, flow-based and device-polling data collection to enhance problem diagnosis, and remediation.

Position and Adoption Speed Justification: The main use cases include network usage reporting, capacity planning, quality of service tracking, end-user experience monitoring, and preventing network degradations from becoming outages. Some NPMD tools continue to diversify into other areas covering technologies such as cloud, UC/VoIP, VDI and alternative monitoring silos, such as infrastructure monitoring and SecOps.

NPMD tool adoption falls into two categories. Some buyers invest broadly in packet-, flow- and infrastructure focused solutions, often from several vendors, but have issues with the cost and complexity of their packet monitoring solutions and with tool sprawl. Others focus on infrastructure based network monitoring and report frustration with doing RCA. Both groups struggle with gaining an overarching view into their environment and the desire for the single-pane-of-glass for comprehensive monitoring.

Innovation in this mature industry has continued with increased investment in AIOps/ML functionality and cloud-centric monitoring. Although in the early days, vendors have begun to look at ways to use AIOps/ML's algorithms to improve RCA workflows, make sense of the vast amounts of data captured, and improve event correlation. Investments in cloud-centric monitoring have centered around public cloud metrics via API, synthetic testing and virtual deployment options that facilitate the changing data flow patterns caused by migration to the cloud. Several vendors continue to make efforts to target the cybersecurity market based on growing interest in NTA tools from security operations teams.

User Advice: The goal of collecting and analyzing performance data is to enable NetOps teams to be more proactive. Users expect reliable wired and wireless networks with consistently high performance. Therefore, NetOps teams should invest in tools that support today's demands, accepting they may have to reinvest in the future as needs change. Future plans may include SDx investments and strategies, and the migration of workloads from the data center to the cloud. Cloud services adds strain and complexity to the network irrespective of deployment model.

Specifically, when planning for NPMD solutions users should keep the following in mind:

- Network infrastructure joined with flow-based monitoring continues to be an introductory, cheaper starting place, reporting on device health, protocol distribution and the makeup of application traffic on the network. This approach, however, lacks granularity and critical network and application performance metrics and, thus, should be pursued with caution, especially at larger organizations.
- Broad, flow-based coverage should be balanced with fine-grained packet capture abilities in critical network segments, to provide depth of visibility and meet the broadest use cases. However, investment in packet capture capabilities comes with high costs and increased complexity and may prove fruitless without adequate investment into the operation of these solutions.
- Wi-Fi network monitoring should be leveraged where appropriate to ensure wireless access meets the same performance and reliability levels as traditional wired connections.

Gartner has observed an uptick in interest in leveraging AIOps/ML against network data, going beyond what is available with simplistic baselining. Organizations should carefully consider the options, functionality provided, and evaluate success rates in real-world environments before spending budget on up and coming technologies with potentially unproven track records. While many vendors are making strides in applying AIOps/ML to a variety of types of data the most success is still seen in areas such as event correlation.

A significant increase in vendors providing SaaS-based monitoring tools will help drive costs down and the inclusion of digital experience monitoring functionality is another area of differentiation.

Business Impact: NPMD helps improve network performance, confirm service quality and justify investments. The network is critical whether it is the campus, WAN, data center, or remote access (VPN), even as hybrid IT environments increase, requiring more in-depth NPMD. Every business, regardless of history or industry, is leveraging technology to gain advantages over competition. The delivery of additional services, internally and externally, will increase strain on the network (and internet WAN connectivity) and will require increased monitoring and modelling.

Ongoing capacity utilization analysis enables allocation of network resources to higher-priority users or applications, without the need for additional capital investment. As virtualization of the network occurs, the dynamic provisioning and management of data-center-based workloads changes network monitoring requirements. Without visibility of historical performance, it's impossible to determine the effects of changes and additional investments on current SLAs, and their relative improvement. Without a baseline service-level measurement for comparison, network professionals can't measure and analyze growth trends, or be forewarned of expansion requirements.

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Sample Vendors: AppNeta; cPacket; Kentik; LiveAction; LogicMonitor; Micro Focus; Paessler; Progress; ThousandEyes; VIAVI

Recommended Reading:

"Market Guide for Network Performance Monitoring and Diagnostics"

"Market Guide for IT Infrastructure Monitoring Tools"

"Toolkit: RFP for Network Performance Monitoring and Diagnostics"

IT Service Alerting Tools

Analysis By: Pankaj Prasad; Padraig Byrne

Definition: IT service alerting (ITSA) tools automate the distribution and management of notification messages to identified recipients. These tools integrate with ITSM and monitoring tools, which are the source of the events, incidents and alerts related to IT outages. The messaging can be delivered by SMS, voice calls, pager and/or a mobile app.

Position and Adoption Speed Justification: ITSA tools have been in existence in one form or another for over a decade, but their application is increasing due to the proliferation of dedicated mobile apps. This has given rise to extended use cases — for example, basic analytics capabilities for event correlation and the ability to configure workflows. Automated remediation through prescribed actions is also a commodity feature in these tools.

Digital workplace practices and increased use of DevOps practices is driving the uptick in ITSA tooling investment. Business users want real-time insights into business impact, which is further stimulating demand for the technologies. Vendors have responded to this demand with tailored capabilities for business stakeholders outside traditional IT operations, through different licensing models for IT operators and business stakeholders. Vendors are also introducing analytics capabilities into the toolsets and the ability to design scenario-based workflows cutting across multiple tools.

Notwithstanding the above, ITSA tooling adoption remains comparatively low within IT operations due to a lack of process maturity among several existing adopters of the technology that are not extracting the full value from their investments. On the other hand, adoption for the DevOps use case has seen an uptick due to the ability to collaborate seamlessly across multiple teams and toolchains.

User Advice: For enterprises with business-critical processes that rely on an IT infrastructure, invest in closed-loop ITSA tools for urgent communications to ensure that IT operations personnel, on-call engineers and business stakeholders, no matter where they are, receive critical alerts.

Although ITOM product vendors focus on web-based displays for alert notification (consoles, administration interfaces and information portals), consider using ITSA tools for when IT professionals are not in front of their primary display screens, or acknowledgment and automated escalation procedures are time-sensitive and mandatory.

Before deploying an ITSA tool, focus first on improving the underlying event management tools monitoring tools and processes, because ITSA tools are not a cure for poor event management. IT organizations must ensure that good event management practices (such as event correlation, categorization, deduplication and root cause analysis) are in place to avoid event overload. Eliminate the noise (for example, insignificant faults) before configuring policies about how to urgently communicate the critical faults. Further, for the business and senior IT stakeholders, establish what information they want/need to see to avoid spam. Finally, modify communication methods, frequency and language to suit different stakeholders and to maintain sensitivity. In short, users must take care of technical debt and not expect these tools to compensate for lack of monitoring governance.

IT organizations that have already implemented ITSA tools should explore extended use cases such as executing predefined actions to rectify known errors remotely from mobile devices, and further refine existing processes by using the detailed annotations.

Small and midsize organizations that do not want to invest in an overengineered ECA or ITIM solution should examine the event correlation and basic analytics in ITSA tools for postprocessing of events and for notifications.

Business Impact: ITSA tools can lower the risk of critical issues being missed by IT operations teams. They increase IT operations efficiencies by enabling IT personnel to perform their other IT operations duties and still be notified of critical IT issues that require immediate attention. ITSA tools also help establish ownership and/or acknowledgment of a critical IT event, no matter where the alert recipient is located.

The use of ITSA tools can reduce the MTTR by automating the delivery of alerts to the appropriate IT operations personnel through the most-effective communications channel, in support of availability and established escalation and outage procedures.

ITSA tools can also provide seamless communications over multiple channels (mainly mobile app, instant messenger and web-portal) across multiple DevOps teams. Flexible workflows within these tools can automate processes and actions that need to be taken across multiple tool chains, thereby reducing the possibility of errors.

Business leaders benefit by having instant visibility into critical or sensitive issues pushed on the device of their choice.

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: AlertOps; Atlassian; Derdack; Everbridge; OnPage; OnSolve; PagerDuty; Splunk; xMatters

Recommended Reading:

"Market Guide for Emergency/Mass Notification Services"

"Complement IT Infrastructure Monitoring With IT Service Alerting"

Cloud Management Platforms

Analysis By: Dennis Smith

Definition: Cloud management platforms (CMPs) enable organizations to manage private, public and multicloud services and resources. Their specific functionality is a combination of provisioning and orchestration; service request management; inventory and classification; monitoring and analytics; cost management and resource optimization; cloud migration, backup and disaster recover; and identity, security and compliance. This functionality can be provided by a single product or a set of vendor offerings with some degree of integration.

Position and Adoption Speed Justification: Although the CMP market is continually changing, vendors and enterprise customers are getting a better feel about where such tooling can and cannot be used. Vendors are still being challenged with evolving customer requirements (for example, interfacing with multiple public clouds, cost transparency with workload optimization to remediate cost overruns and handling newer functions like containers and serverless deployments). At the same time, major market consolidation will continue. For example, many vendors, that initially targeted cost management, have been acquired as this functionality is becoming a part of the basic

CMP. Additionally many vendors in adjacent markets are acquiring CMP vendors and combining this functionality with asset management (software and hardware) and SaaS operational management.

CSPs and management service providers (MSPs) are also entering the market. Additionally, many long-standing vendors are introducing next-generation products, often targeting holes that their previous products had. Finally vendors in different markets (e.g., monitoring) are also entering the market. Some of the core CMP functionality is also being combined (for example, monitoring and analytics with cost management and resource optimization). The ability to serve both application developer and I&O personas is the key. This requires that CMPs be linked into the application development process without imposing a workflow that inhibits agility while also allowing infrastructure and operations (I&O) teams to enforce provisioning standards.

Organizations have an increasing need to address multicloud requirements. In some cases, they want to become internal cloud service brokers (CSBs) and manage public services that were previously acquired — often by LOBs outside the I&O organization — and have become difficult to manage operationally.

User Advice: As CMP market volatility increases, IT organizations must:

- Consider CMP vendor’s viability along with evaluating features.
- First consider native cloud services as an alternative or option versus CMPs, particularly if you favor depth with an individual cloud provider versus breadth across different cloud providers.
- Consider functionally focused tools (e.g., cloud expense management tool) if you only require a limited set of functionalities.
- Augment, swap out or integrate additional cloud management or traditional management tools for many requirements, because no vendor provides a complete cloud management solution.
- Standardize, because deriving value from your CMP will depend heavily on the degree of standardization offered by the infrastructure, software and services.
- Set realistic expectations on deployment times, as mature organizations implement CMP in a relatively short period (one to two years); however, less mature organizations may require two or more years to design effective, repeatable, and automatable standards and processes.
- Plan for new roles, such as cloud architects and CSBs, including developing skills in the financial management and capacity management areas.

Business Impact: Enterprises will deploy CMPs (increasingly as a part of a larger product suite) to increase agility, reduce the cost of providing services and increase the likelihood of meeting service levels. Costs are reduced and service levels are met because CMP deployments require adherence to standards, as well as increased governance and accountability. Desirable IT outcomes include:

- Policy enforcement (e.g., on reusable standard infrastructure components)
- Reduced lock-in to public cloud providers, although at the cost of CMP vendor lock-in that can slow innovation

- Enhanced ability to broker services from various cloud providers and to make informed business decisions on which providers to use
- Ongoing optimization of SLAs and costs
- Management of SLAs and enforcement of compliance requirements
- Health and performance monitoring of cloud applications
- Accelerated development, enabling setup/teardown of infrastructure that mimics production, resulting in lower overall infrastructure costs and higher quality (this can be in support of DevOps initiatives)

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

Sample Vendors: CloudBolt; CloudSphere; Flexera; Morpheus Data; Scalr; Snow Software; VMware

Recommended Reading:

"Magic Quadrant for Cloud Management Platforms"

"Critical Capabilities for Cloud Management Platforms"

IT Infrastructure Monitoring

Analysis By: Pankaj Prasad; Josh Chessman

Definition: ITIM tools capture the health and resource utilization of IT infrastructure components that reside across the on-premises data center and edge, as well as cloud-based IaaS and PaaS. This enables I&O leaders to monitor and collate the availability and resource utilization metrics of physical and virtual entities, including servers, containers, networks, database instances, hypervisors and storage. Notably, these tools collect data in real time and perform historical data analysis or trending of the elements they monitor.

Position and Adoption Speed Justification: ITIM tools have been available for decades, supporting IT infrastructure components across all primary domain groups (such as servers, networks, storage and databases). These are usually the first set of tools in which enterprises invest to monitor availability, as well as to enable the ability to troubleshoot in a reactive manner. Because of the length of time ITIM tools have existed and the functionality the tools offer, the ITIM market is rapidly approaching maturity.

ITIM tool vendors have been continuously adapting to changes in IT architecture by:

- Providing the ability to capture granular data at speed and scale

- Adding improved analytics and visualization with the goal of providing relevant information through interactive dashboards and dynamic drill down to component levels
- Improved use cases such as dynamic thresholds, topology and dependency maps, which, when combined with log parsing, allow for cause-and-effect correlation and easier and faster troubleshooting resulting in better mean time to repair
- Providing a one-stop solution incorporating application performance monitoring (APM) functionality either through acquisition, partnerships or adding functionality to existing tools

ITIM tools are a “must have” for capturing IT resource utilization, troubleshooting and root cause analysis (RCA) capabilities. Enterprises tend to leverage NPMD or APM solutions for visibility to IT performance. Increasingly, vendors across these two markets are offering ITIM capabilities as part of their toolsets. NPMD and APM products have been aggressively adding ITIM capabilities to their own offerings over the past few years and Gartner expects that process to continue going forward.

Domain-agnostic AIOps vendors have started offering ITIM capabilities. This capability now relies on the AIOps’ vendors’ ability to capture raw data through agent-based and agentless methods. Although some AIOps vendors limit visibility to cloud environments, the trend is toward providing comprehensive ITIM capabilities.

User Advice: Enterprises must make investments in ITIM for proactive monitoring of their IT landscape across on-premises and IaaS architectures. Organizations using point solutions such as separate monitoring solutions for Windows servers, UNIX servers and storage systems must consider investing in ITIM solutions. These solutions will enable cross-domain visibility across their IT landscape and to ease event overload by leveraging the inbuilt ECA engine. Although there is often functional overlap between different monitoring siloes (e.g., APM, NPMD and ITIM), each silo brings its own focus with its own workflows and use cases. Ensuring that the tools you have are correct for the job is critical to success.

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

- The scope of their footprint when collecting relevant metrics
- Ease of deployment
- Ability and ease of integration with other ITOM tools
- Ability to deal with data at speed and scale (e.g., IoT, microservices and containers)
- User interface and price
- Future roadmap and alignment with the organization’s strategy

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

Organizations may extend their visibility into the application layer by deploying APM tools for application-specific visibility, DEM tools for user experience metrics and by leveraging AIOps platforms for correlation.

Business Impact: ITIM tools monitor the health and quality of service of IT systems and components within the infrastructure. They also improve availability, and lower risk and the total cost of ownership (TCO) of managing a large and complex infrastructure environment.

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

ITIM also brings in efficiency and enhances productivity of IT operations teams by providing ECA capability. Postprocessing of events, policy-driven workflows and alert notifications help avoid event overload and workflows help avoid human error. Data from ITIM tools is being sent to AIOps platforms for leveraging pattern recognition and ML capabilities, thereby easing the ability to assess the impact of IT on customers.

Data from ITIM tools is being used by multiple personas, and is not limited to I&O groups (for example, it is used by DevOps and SRE groups in enterprises that leverage cloud-native architectures).

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Sample Vendors: Datadog; eG Innovations; ITRS Group; ManageEngine; Nagios; New Relic; OpsRamp; SolarWinds; Zabbix; Zenoss

Recommended Reading:

“Market Guide for IT Infrastructure Monitoring Tools”

“Monitoring Beyond 2020: Focus on Performance”

“2019 Strategic Roadmap for IT Operations Monitoring”

“Use AIOps for a Data-Driven Approach to Improve Insights From IT Operations Monitoring Tools”

“The Road to Intelligent Infrastructure and Beyond”

Entering the Plateau

DevOps

Analysis By: George Spafford; Joachim Herschmann

Definition: DevOps is a customer-value-driven approach to deliver solutions using agile methods, collaboration and automation. DevOps emphasizes people and culture to improve collaboration between development, operations and other stakeholders to navigate uncertainty, and accelerate the delivery of customer value. DevOps implementations use architecture and tools to improve the flow of work.

Position and Adoption Speed Justification: DevOps doesn't have a concrete set of mandates or standards, or a known framework (such as ITIL); thus, it is subject to a more liberal interpretation. In general, it is about cross-functional teams collaborating to deliver business value faster. DevOps is associated with processes, tools and organizational styles intended to optimize the flow of work across the application life cycle, from development to production. DevOps concepts have become widely adopted for initiatives with a style of work that is focused on exploration and agility, including digital business, ML, mobile apps and the IoT. Also, there is potential for use in more traditional enterprise environments; however, every implementation is unique. Good practices are emerging, the sharing of lessons learned is vibrant among practitioners. Vendors are developing and delivering supporting tools and professional services. Although some new adopters are having challenges, clients report that DevOps does deliver value.

User Advice: DevOps initiatives must be iterative, focused on business value and have executive sponsorship, with the understanding that new team(s) will have to make an often-difficult organizational philosophy shift toward the development of agile capabilities. DevOps hype remains elevated among tool and service vendors, with the term applied aggressively and claims outrunning demonstrated capabilities. Many tool vendors are adapting their portfolios and branding their offerings as DevOps-related to gain attention. Some vendors are acquiring smaller point solutions specifically developed for DevOps to boost their portfolios. Clients are recommended to clearly tie investments to business outcomes to help improve internal adoption.

IT organizations must establish key criteria that will differentiate DevOps tooling traits (strong toolchain integration, workflow, automation, etc.) from traditional management tools. Both development and operations should look to tools to replace custom scripting with improving deployment success and cycle times through more predictable configurations and seek to continually improve the flow of work via refactoring.

IT organizations should approach DevOps as a set of flexible guiding principles. Start small and focused — don't try a "big bang" approach. Select a product that is politically friendly, and offers acceptable value and risk involving development, operations and other critical stakeholders, such as information security and architecture. Stakeholders need to work together to accomplish the business objective, while learning how to organize and determining what methods and tools to use. At a minimum, seek to continually improve the flow of work from developer through to the new or changed application being in production and the customer receiving the promised value. These stakeholders must also collaborate to scale efforts.

Business Impact: DevOps is focused on delivering customer value and enables hypothesis-driven development and the aggregation of data to make decisions about future functionality. Release cadence can be varied to meet demands for organizational learning and change absorption. DevOps approaches are made possible by the adoption of continuous learning, improvement and incremental release principles adopted from agile methodologies. Smaller, more frequent updates to production can work to improve organizational learning and overall quality, including both stability and control, thus reducing risk. A successful DevOps implementation will improve the delivery of customer value. This delivery of value justifies the scaling and expansion of DevOps using an iterative approach.

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Recommended Reading:

“Adopt an Iterative Approach to Drive DevOps Success in Large Organizations”

“DevOps — Eight Simple Steps to Get It Right”

“DevOps Primer for 2019”

“Three Ways Midsize Enterprises Can Maximize Value From DevOps”

“Four Steps to Adopt Open-Source Software as Part of the DevOps Toolchain”

“DevOps Success Requires Shift-Right Testing in Production”

“Avoid Failure by Developing a Toolchain That Enables DevOps”

“Top 5 Causes of DevOps Failure and How to Avoid Them”

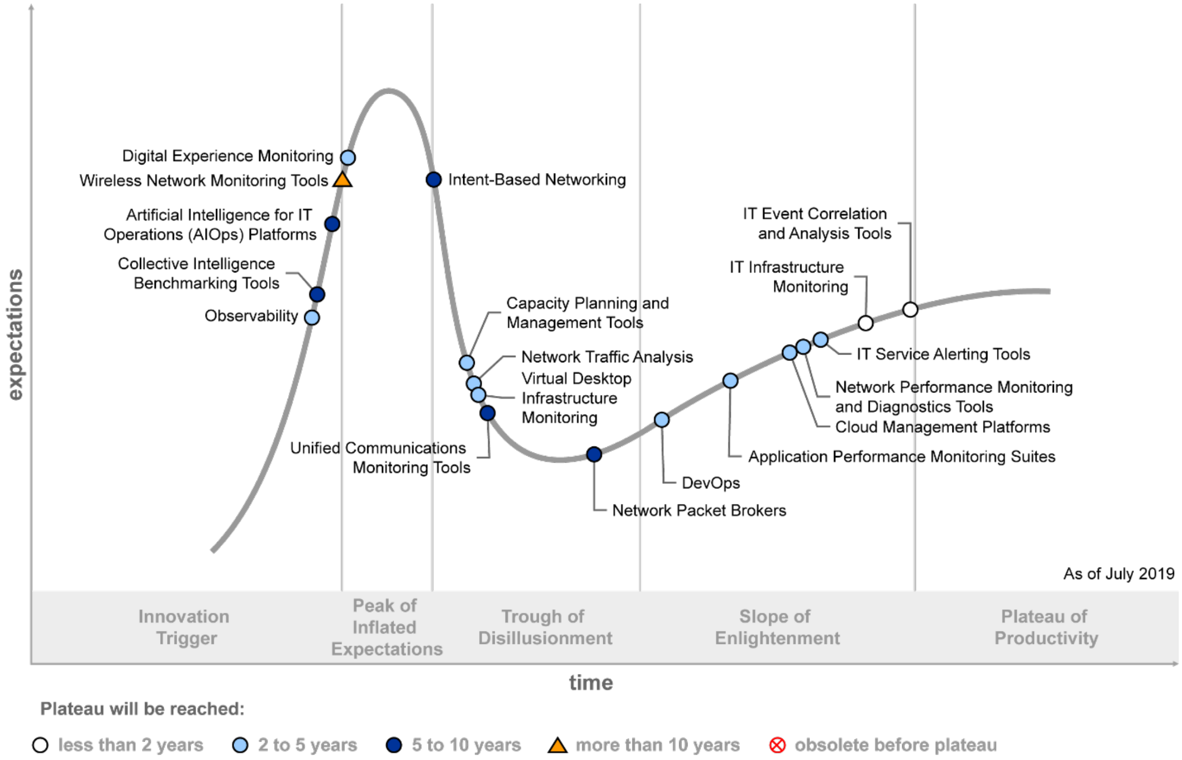
“How to Avoid Compliance and Audit Concerns When Using DevOps”

“How to Scale DevOps by Building Platform Teams”

“Top SRE Practices Needed by Teams Scaling DevOps”

Appendixes

Figure 3. Hype Cycle for IT Infrastructure Availability and Performance Management, 2019



Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 1. Hype Cycle Phases

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

Source: Gartner (July 2020)

Table 2. Benefit Ratings

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

Source: Gartner (July 2020)

Table 3. Maturity Levels

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

Source: Gartner (July 2020)

Gartner Recommended Reading

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

Understanding Gartner's Hype Cycles

Cool Vendors in Performance Analysis for Cloud-Native Architectures

2019 Strategic Roadmap for IT Operations Monitoring

Leadership Vision for 2020: Infrastructure and Operations Leader

Magic Quadrant for Application Performance Monitoring

Market Guide for AIOps Platforms

Market Guide for IT Infrastructure Monitoring Tools

Market Guide for Network Performance Monitoring and Diagnostics

Market Guide for Digital Experience Monitoring

Market Guide for UCaaS Monitoring

GARTNER HEADQUARTERS

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

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

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