2021

# GARTNER GUIDE

## TECNOLOGIE, TENDENZE E RACCOMANDAZIONI PER L'ADOZIONE DI SOLUZIONI DI MONITORAGGIO IT CON APPROCCIO PIU' INTEGRATO.

L'IT moderno rappresenta una sfida per gli strumenti legacy del passato progettati per operare in infrastrutturestatiche. Le attuali tendenze sfidano il paradigma della "disponibilità dell'infrastruttura", spostando l'attenzione sul servizio e sulla percezione dello stesso da parte degli utenti finali.

In questa direzione criteri di integrazione e flessibilità risultano elementi determinanti nella scelta del giusto strumento di monitoraggio.

SentiNet®

# Market Guide for IT Infrastructure Monitoring Tools

Published 9 September 2021 - ID G00749361 - 24 min read

By Pankaj Prasad, Josh Chessman, Mrudula Bangera, Gregg Siegfried

---

IT infrastructure monitoring tools provide I&O leaders with data that speeds diagnosis and troubleshooting for on-premises and cloud-based systems. Use this Market Guide to identify vendors that meet your organization's specific monitoring needs.

## Overview

### Key Findings

- The blurring of lines between monitoring silos is continuing apace with vendors in spaces such as application performance monitoring (APM) and network performance monitoring (NPM) continuing to enter the IT infrastructure monitoring (ITIM) market with a focus on "full-stack monitoring."
- ITIM vendors are increasingly focusing beyond data collection and presentation, offering analytics functionality as a way to distinguish themselves, resulting in continued challenges in differentiating products.
- I&O leaders are increasingly demanding visibility across not only cloud or on-premises environments, but also hybrid infrastructures (multicloud, on-premises, etc.).
- Visibility into emerging architectures (for example, containers and microservices) and Internet of Things (IoT) devices is becoming increasingly important for organizations.
- Business leaders, DevOps and site reliability engineering (SRE) teams use data from ITIM tools along with cloud-native monitoring to derive context that improves visibility and helps achieve optimization targets.

### Recommendations

I&O leaders focused on infrastructure, operations and cloud management must:

- Select monitoring tools to meet business needs by identifying the must-have metrics the ITIM tool can provide and addressing visibility gaps through different tooling categories like APM and NPM.
- Contextualize data that ITIM tools collect from highly modular IT architectures by using artificial intelligence for IT operations (AIOps) to manage other sources, such as observability metrics from cloud-native monitoring tools.
- Improve mean time to repair (MTTR) by deploying monitoring tools that have capabilities in hybrid, multicloud and cloud-native monitoring, as well as intelligent incident management, and that use process automation to handle automated remediation.
- Improve data exchange by favoring ITIM tools that offer more complete integration and interoperability with broader IT operations management (ITOM) tools like IT service management (ITSM), AIOps and automation.
- Reduce tool management overhead by shortlisting vendors that offer modern user interfaces, support cloud-native architectures and address DevOps monitoring needs.
- Enhance the decision making of non-IT teams by providing dashboards customized with insights relevant to different personas like CIOs, application developers and business leaders.

## Strategic Planning Assumption

By 2025, usage of open-source extensions to AIOps and CSP tools will result in a 50% less investment in ITIM tools as compared to 2021.

## Market Definition

This document was revised on 12 October 2021. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

ITIM tools capture the health and resource utilization of IT infrastructure components no matter where they reside (for example, in a data center, at the edge, infrastructure as a service [IaaS] or platform as a service [PaaS] in the cloud). This enables I&O leaders to monitor and collate the availability and resource utilization metrics of physical and virtual entities, including servers, containers, network devices, 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 (see Figure 1).

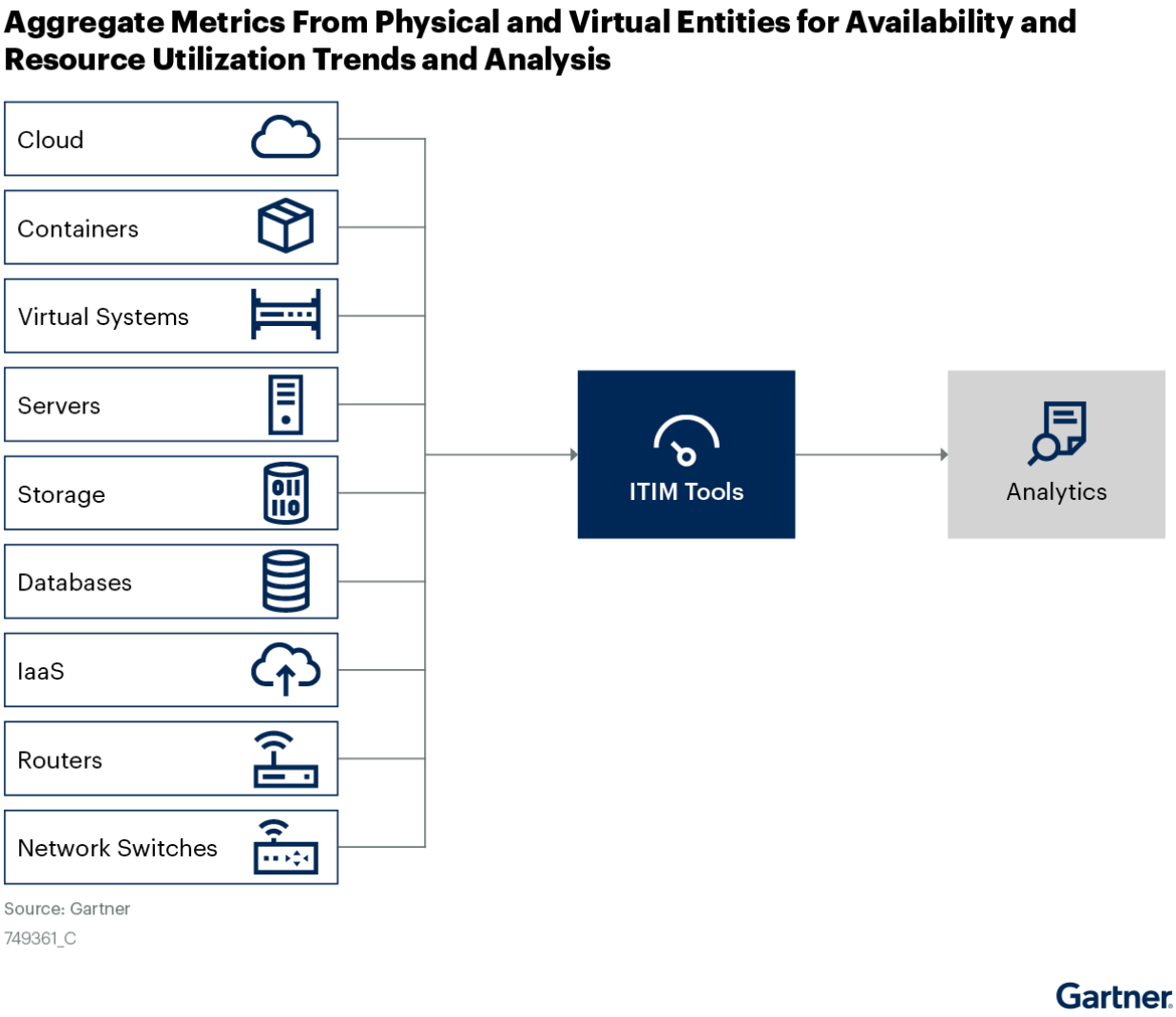


Figure 1. Aggregate Metrics From Physical and Virtual Entities for Availability and Resource Utilization Trends and Analysis

## Market Description

At a minimum, ITIM tools must indicate availability status and provide performance information at an infrastructure level and ideally should capture metrics for the attributes in Table 1.

| Attributes | Description |
|---|---|

| | |
|---|---|
| **Storage Systems** | Network-attached storage (NAS), storage area network (SAN) and SAN fabric. |
| **Servers** | Multiple operating systems — such as Windows, Linux — regardless of whether the OS instance is physical or virtualized. This will include hardware and OS-specific metrics, such as fan speed, CPU temperature, memory, CPU and disk usage. |
| **Network** | All physical and virtual elements in the network layer, including load balancers, routers and switches. |
| **Hypervisors** | Multiple hypervisors, such as Microsoft Hyper-V or Red Hat Virtualization. |
| **Database** | Multiple databases, such as Microsoft SQL, MySQL or Oracle. |
| **Containers** | Multiple container environments such as Red Hat OpenShift, Kubernetes, and Amazon Elastic Kubernetes Service (Amazon EKS). |
| **IoT Devices** | Multiple different devices across numerous areas such as IP cameras, handheld inventory devices or physical security devices. |

**Table 1: Example Attributes of an ITIM Tool**

ITIM tools also make data available to other ITOM tools used within event, availability, capacity, ITSM, automation and performance analysis processes.

As defined here, an ITIM tool is not required to perform:

- Endpoint monitoring (see Market Guide for Digital Experience Monitoring).
- Mainframe monitoring. (ITIM tools may have mainframe monitoring, but this is out of scope for Gartner's definition.)
- AIOps, which provides more advanced analytics capabilities (see Market Guide for AIOps Platforms).

## IT Infrastructure Monitoring: Adjacent Disciplines

Tools for domain-specific use cases can supplement IT infrastructure monitoring. These include:

- Application performance monitoring (see Magic Quadrant for Application Performance Monitoring and Critical Capabilities for Application Performance Monitoring).
- Network performance monitoring and diagnostics (see Market Guide for Network Performance Monitoring).
- Digital experience monitoring (DEM; see Market Guide for Digital Experience Monitoring).

In addition to the above areas, domain-agnostic AIOps platforms can act as the aggregation point, directly collecting data from monitoring tools, thus extending visualization capabilities and applying machine learning to multiple sources of data, including ITIM. (See Use AIOps for a Data-Driven Approach to Improve Insights From IT Operations Monitoring Tools.)

## IT Infrastructure Monitoring: Embracing DevOps and SRE

Increased adoption of cloud-native architectures, both in preproduction and production, requires a holistic monitoring strategy. Enterprises adopting cloud-native architectures adopt DevOps and site reliability engineering practices to leverage the fault-tolerant attributes and the agility offered by such architectures. This requires ITIM to expand in line with the attributes of cloud-native architectures and the visualization needs of DevOps and SRE teams (see Assessing Site Reliability Engineering (SRE) Principles for Building a Reliability-Focused Culture).

# Market Direction

Enterprises are continuing to increase investment in cloud-native architectures (see Magic Quadrant for Public Cloud Infrastructure Professional and Managed Services, Worldwide), which bring with them beneficial attributes that challenge the target market for data acquisition including:

- Inherent resiliency of the architecture. Failures in different parts of an architecture have minimal impact on availability and performance of applications. I&O needs to worry about only large-scale failures.
- Instrumentation. “Pulling” data from the source is no longer an art, allowing I&O to focus on aggregating and analyzing the data sent by the source being monitored.

Due to the inherent resiliency in IT architecture, the need for real-time capturing of uptime data is no longer considered crucial (see 2021 Strategic Roadmap for IT Operations Monitoring). This is especially true for an enterprise that has adopted architectures with cloud-native characteristics. I&O can now focus primarily on performance insights.

For vendors, this translates into the task of providing deeper analysis via AIOps technologies, exploring new markets, and monitoring challenges and emerging target audiences for their products. Vendors are focusing on the following areas:

- AIOps. ITIM vendors are introducing analytics and, in some cases, AIOps capabilities, either through acquisitions, as a service through partnerships or through organic development.
- DevOps. ITIM vendors are focusing on data acquisition at higher granularity levels, thus aligning with the shift from a purely root cause analysis (RCA) approach toward insights that can help optimize existing infrastructure and applications for enhanced performance and efficiency.
- Observability. ITIM vendors are enabling adoption of new monitoring approaches and improving long-standing monitoring technologies for enhanced visibility to IT systems (see Innovation Insight for Observability).
- Business leaders. ITIM products are focused on analyzing data to add relevant context and use relationship information to provide business leaders with application- or service-centric insights into existing infrastructure and applications for enhanced performance and efficiency. This is a positive abstraction from an entity-centric view (that is, CPU, memory, storage).

The trends shown in Table 2 are affecting the market’s current overall direction.

| Trend | Effect on the ITIM Market |
|---|---|
| **Dynamic Infrastructure** | Modern IT architectures are increasingly modular, converged, abstract and dynamic, thus requiring a system-centric approach and dynamic discovery. |
| **Multicloud** | An IT environment fragmented across multiple providers, locations and ownership types necessitates capturing the entire view cutting across different IT architectures. |
| **DevOps** | As DevOps initiatives scale, the need for continuous data exchange between production and preproduction teams becomes increasingly relevant. |
| **Cloud-Native Architectures** | Enterprises are using scalable and elastic service-based IT architectures to support business processes. This means component-level failures cause minimal impact to applications so focus shifts toward performance and optimization goals. |
| **Internet of Things** | IoT provides many use cases and generates huge amounts of unstructured data. Organizations are aware of the need to capture, store and analyze this data for real-time insights. |
| **Exponential Increase in Velocity, Diversity and Volume of Data** | Digital business is redefining the role of IT, creating a deluge of data types and data itself, at increasing velocities, challenging existing data capture limitations. |
| **Containers and Microservices Architectures (MSA)** | Containers bring challenges of speed, visibility, risk of blind spots and scale not yet seen in the monitoring world. |

| | |
|---|---|
| **Customer-Centric Focus** | Measuring real-time impact to the customer is crucial; however, monitoring at an entity level (CPU, memory) doesn't provide the actionable insights provided by service maps. |
| **New Target Audience** | Application developers are interested in metrics for optimizing existing resource utilization, for example, internal container metrics versus impact of a container on the host architecture for IT operations.<br>Business leaders are keener for contextualized insights and visibility into the impact of IT on business in real time. |
| **Site Reliability Engineering** | Site reliability engineers understand applications as well as the infrastructure used to deliver it. This persona requires easy access to underlying telemetry to create custom analytics and dashboards, as well as ITIM solutions that interoperate well with other parts of the health and performance monitoring toolchain. |

Table 2: Trends Affecting the ITIM Market

High modularity of IT systems, coupled with the complexity of workflows, requires deeper and wider visibility across a variety of infrastructure elements. Combined with the need to cater to business leaders' requirements, ITIM tools now offer simplified user interfaces to enable designing of dashboards, for example, even by non-IT teams that need real-time insights to availability, health or impact. Vendors are also including analytics through organic development, acquisitions and/or partnerships to enable contextualization of IT and customer data for a business-centric view.

Leveraging analytics helps vendors correlate and contextualize data across various sources. This helps manage workflow complexity. Coupled with big data practices, analytics enables ITIM to tackle the data volume and velocity (containers and microservices), as well as data variety (from the IoT).

Monitoring a DevOps environment requires a platform approach, which is distinct from the needs of a production environment (see Don't Fail Fast in Production; Embed Monitoring Earlier in Your DevOps Cycle).

Although the demand for preproduction environment monitoring of IT infrastructure is quite low, DevOps monitoring is evolving, and some vendors have differential licensing with a lower-cost offering for the preproduction environment.

## Market Analysis

The modular nature of IT infrastructure makes it difficult to derive detailed and useful performance insights based solely on IT resource consumption. This, combined with IT operations teams' realization that ITIM tools purely capture resource utilization metrics, means that ITIM tools alone are not sufficient to get a view of overall performance. Digital business embraces customer centricity, making performance an important metric to track. Enterprises deploy digital experience monitoring and digital employee experience (DEX) tools for performance insights from the user's perspective, particularly for infrastructure and applications that are external (for example, SaaS applications). However, these tools frequently leave a gap in providing in-depth visibility to the enterprise.

ITIM tools enable sending alerts to appropriate roles and providing persona-driven visualization to support the display and analysis of collected data. Effectively, ITIM tools help I&O leaders mitigate operational risk and optimize monitoring costs by:

- Providing a descriptive capability through increased visibility of IT infrastructure.
- Enabling a diagnostic capability through improved accuracy of anomaly detection and alerting.
- Improving efficiency through ease of troubleshooting and diagnosis.
- Enhancing reliability by way of reduced outages, thereby improving infrastructure availability.
- Facilitating data exchange through integration with AIOps tools for centralized visibility and better analysis (see Adopt a Data-Driven Approach to Consolidating Infrastructure Monitoring Tools).
- Tracking IT resource utilization for optimization efforts.
- Aggregating datasets from multiple monitored entities for supporting root cause analysis.

I&O leaders should evaluate ITIM tools during any major technology refresh, including data center modernization initiatives, and when existing monitoring tool contracts are due for renewal. Increasingly, business leaders are influencing adoption of these tools (directly and indirectly) by asking for reports and dashboards that showcase IT's impact on business. I&O leaders seeking to mature their IT operations should evaluate ITIM tools for driving collaboration across teams, as well as for a unified dashboard across various domains.

## ITIM Vendor Landscape Dynamics

A number of new vendors are entering the ITIM market by leveraging open-source technologies, ease of API availability for data exchange, and mature open-source collectors and agents. Vendors from different markets like APM, NPMD, AIOps and even ITSM are now providing ITIM capabilities. A majority of new entrants are focused on small and midsize businesses (SMBs), but some of these vendors also cater to enterprise customers. In some cases, vendors have revamped their existing offerings to target new segments and personas. The product offerings of some of the newer vendors compete well with established vendors, not only on cost but also in terms of capabilities.

From a buyer's perspective, Gartner has encountered some enterprises assessing "good enough" tools, which in some cases include free versions of open-source monitoring software. This trend is not driven due to cost considerations and has been observed from before the pandemic. One of the major drivers here is the deployment of cloud-native architectures. They are resilient and fault-tolerant, which minimizes the impact due to outage of an individual IT entity, thus allowing sufficient time to rectify the outage.

Gartner is observing a convergence across multiple monitoring market segments:

- ITIM tools incorporating flow-based monitoring that provides an overlap with NPM tools. In some cases, ITIM tools also provide NPM capabilities (e.g., LogicMonitor, Nagios, Paessler).
- ITIM tools incorporating either partial or full APM capabilities (for example, Elastic, Splunk Observability).
- APM vendors offering ITIM capabilities (for example, Cisco AppDynamics, Dynatrace, New Relic).
- Domain-agnostic AIOps vendors starting to capture raw data and offering ITIM-related capabilities (for example, Elastic, Moogsoft, Splunk).
- Log monitoring solutions offering ITIM capabilities (for example, Sumo Logic, Logz.io).

## Functional Overlap and Potential Market Segment Convergence

### Data Versus Information

Gartner is observing a clear shift toward information and insights and away from a focus on data collection in the monitoring landscape. This is driven in part by increasing interest among business leaders regarding IT's impact (real time and potential). By focusing on the results of the impact of incidents, organizations are able to more closely associate infrastructure utilization and performance to business outcomes (for example, due to bandwidth utilization, 85% of users are unable to work). A focus on information helps drive decisions due to its qualitative nature. For example, here the I&O team would be able to convey which group of users and/or applications are using bandwidth and any bandwidth contention that exists for other applications. For information and insights, context must be derived from multiple other sources as well.

## Modern IT Architecture and Expanding Consumer Base

Cloud-native architectures with elasticity and resilience at their core translate into the ability of IT resources to absorb demand spikes (see Market Trends: The Rise of Cloud-Native Technology Ecosystems [Container Perspective]). This has an impact on the ITIM market due to three forces:

- Resilience. Performance occupies a primary role from a dashboarding and reporting perspective, while uptime becomes a secondary goal. Availability of IT resources in real time is no longer considered as crucial as in a legacy IT architecture because the resilient nature of design ensures some other component spins up to provide continued performance.
- API-driven infrastructure. Data can be acquired via push or pull modes. Cloud-native architectures can be instrumented to share data, for example through APIs (see 2020 Strategic Roadmap for Compute Infrastructure). In a way, these systems stream metrics to monitoring servers. Traditional monitoring tools lose their advantage where a high percentage of systems are instrumented in this

way. This feature, combined with resilience (see IT Resilience — 7 Tips for Improving Reliability, Tolerability and Disaster Recovery), means AIOps tools can now be leveraged into areas previously dominated exclusively by ITIM tools, to the exclusion of ITIM tools.

- Elasticity. Thresholds do not necessarily have a hard ceiling that cannot be breached. This gives rise to a shift from capacity management toward the concept of workload optimization in which I&O teams seek to most efficiently map resources to expected performance. Analytics and orchestration play a role here, where periodic demand is mapped through pattern recognition, and virtual machine (VM) orchestrators affect actions for rebalancing IT resources dynamically with zero downtime.

The tools, tool capabilities and consumers for such architectures expand beyond traditional monitoring capabilities.

ITIM tools are now required to provide visibility into containers, container orchestration and microservices, including the dynamic connections between them.

Visibility into dependencies, behavior and impact on the external IT environment hosting such architectures is deemed crucial for the cloud-native architectures by DevOps, SRE and I&O teams. Relationships extending to pods, clusters, hosts, and applications and service visibility are other aspects expected from the monitoring of cloud-native architectures.

This requires a combination of capabilities such as the ability to ingest data at high granularity, tagging of datasets, tracing and analytics. Many ITIM vendors offer data acquisition at high granularity, but few ITIM vendors span the entire spectrum of tracing, tagging and analytics. These capabilities typically fall in the domains of application, IT infrastructure and analytics for contextual insights (see Figure 2).

Figure 2. Monitoring Cloud-Native Architectures

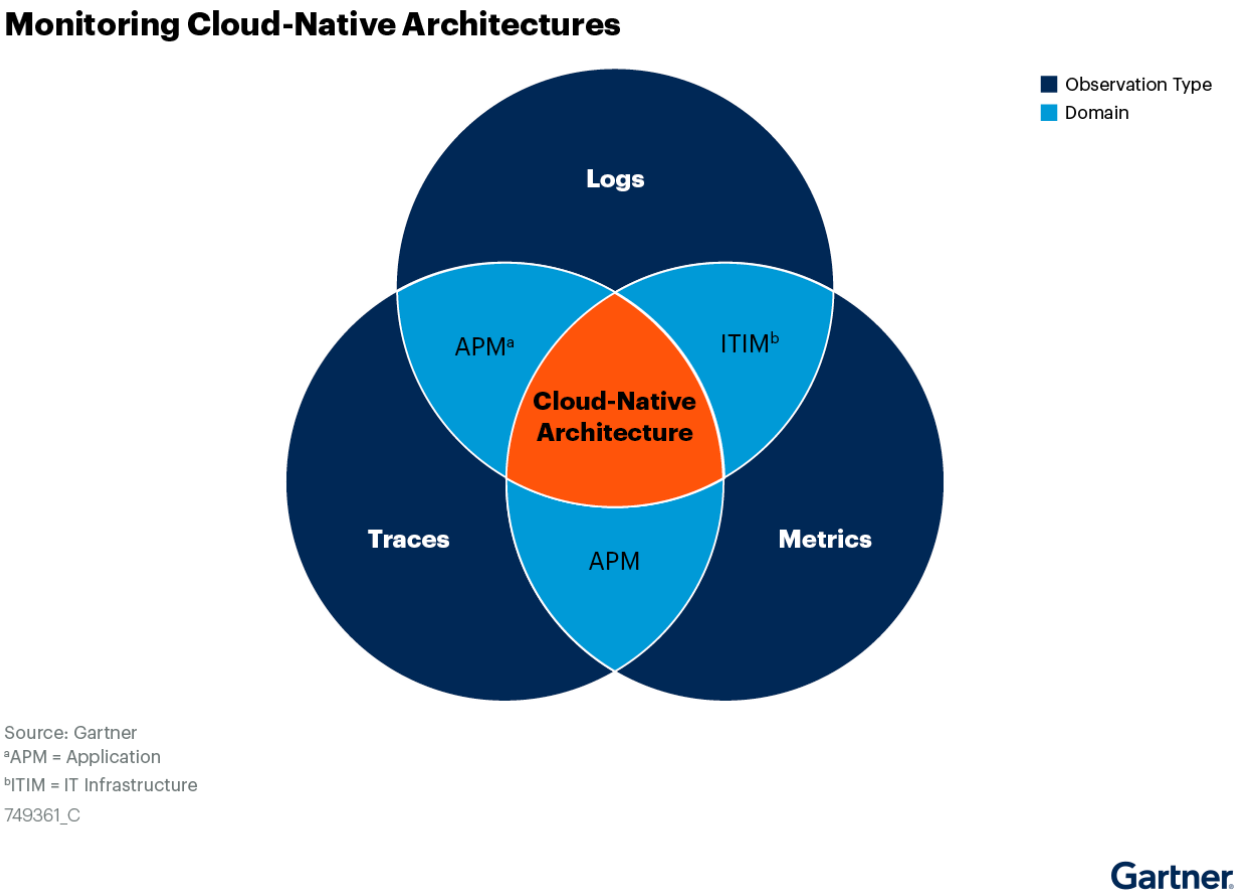


Figure 2. Monitoring Cloud-Native Architectures

By contrast, some vendors focus purely on cloud-native architecture monitoring and do not focus on broader infrastructure monitoring (for example, network, storage and database monitoring).

The final picture is one in which, instead of using both an ITIM tool (for monitoring) and an AIOps tool (for deeper analytics), a single tool will provide the combined capability of data acquisition and in-depth analytics (see Figure 3). ITIM vendors will acquire analytics capabilities through organic or inorganic means — and in some cases through partnership with AI service providers. Domain-agnostic AIOps vendors are also strengthening their data acquisition capabilities and reducing their reliance on monitoring tools for data acquisition. The approach is similar to the approaches taken by ITIM vendors: through organic or inorganic means, or through partnerships.

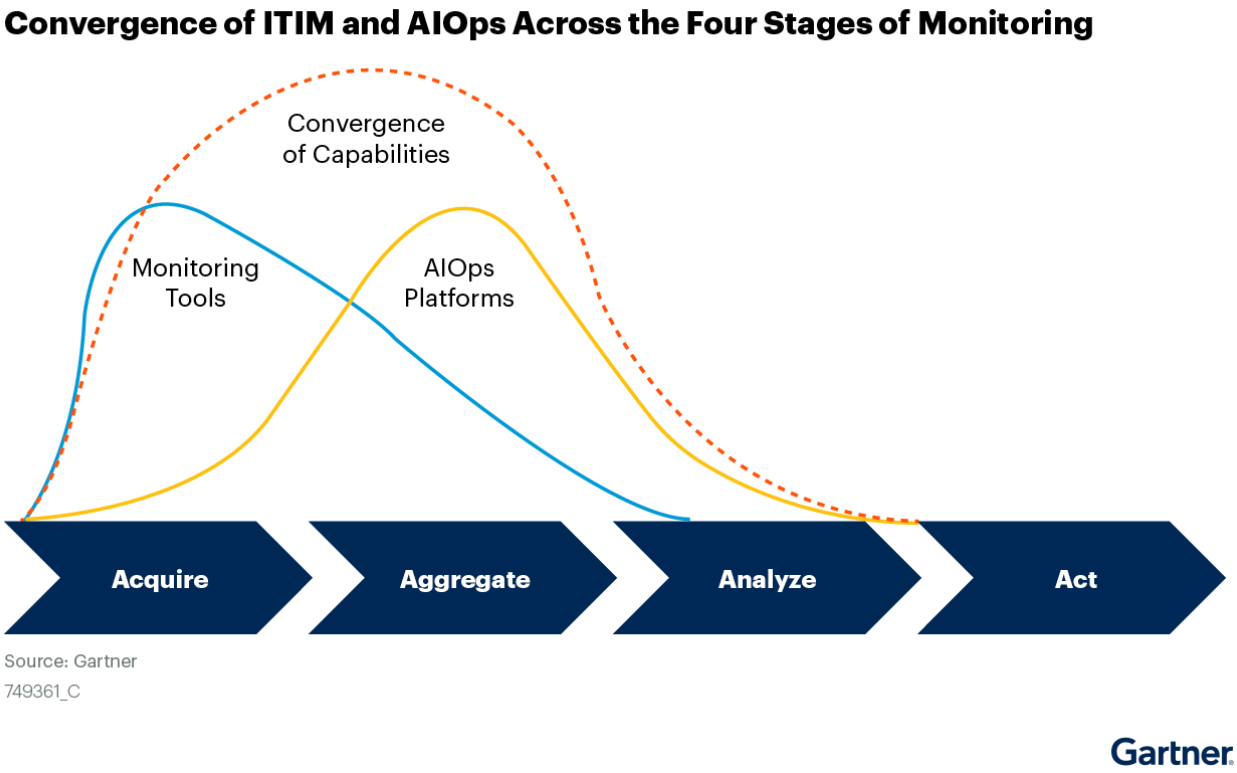


Figure 3. Convergence of ITIM and AIOps Across the Four Stages of Monitoring

## Cloud Providers Offering ITIM Monitoring

Cloud providers are offering ITIM tools or capabilities but, in a majority of cases, visibility is limited to the cloud provider's own environment. Some of the providers have agents for extending monitoring to other environments, including on-premises (example vendors include Amazon CloudWatch, Amazon Web Services [AWS], Google Cloud's Operations Suite [formerly Google Stackdriver] and Microsoft Azure Monitor). ITIM vendors are providing visibility across multiple cloud providers through a combination of the following methods:

- By establishing partnerships with multiple cloud providers to extend visibility across on-premises and cloud architectures or by leveraging APIs (example vendors include ScienceLogic and Zenoss).
- Through agents deployed on public cloud instances (example vendors include Site24x7 and OpsRamp).
- Using data from the cloud provider's monitoring tool (for example, using events from Amazon CloudWatch), often accessed via APIs.

## Demand for ITIM

The following are key demand drivers for ITIM tools:

- Digital business, with its need for better insights for control and influencing positive behaviors in the end user. DEM is the primary tool of choice here, but ITIM tools become a necessity as secondary

tools of choice because of resource utilization metrics, deeper visibility across infrastructure elements and relationships between different entities.

- The IoT, which generates huge volumes of data that are of interest to many enterprises. Data from these systems is needed for two reasons: to monitor the performance of the devices themselves, and to capture data from the environment where the devices are deployed.
- Hybrid, where enterprises want a single platform for visibility to their mixed IT environment (encompassing multiple cloud and/or on-premises environments).
- AIOps platforms, which have a major intersection with ITIM at the data collection and storage layer (see Market Guide for AIOps Platforms). ITIM provides a crucial data acquisition function across diverse IT architectures to feed AIOps platforms.

### Deployment and Licensing Options

ITIM tools are available as open-source, commercial open-source and proprietary software. Deployment types vary, with some vendors providing just software (either on their own hardware or customer provided), some providing a managed cloud option, some a SaaS option, and some a combination of all three. The deployment architecture may also vary depending on the number of devices, monitoring granularity and other factors.

Licensing options include per-device or node-based licensing, network-port-based licensing, and licensing based on number of metrics monitored and number of reports generated. In some cases, tools are offered as a hardware appliance with a configuration that limits the number of devices that can be monitored. This physical-appliance-based licensing is rare, and very few vendors offer it.

## Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

### Market Introduction

ITIM vendors cater to a broad spectrum of requirements, cutting across small and midsize enterprises to large enterprises, and ranging from less than 10 entities to far more than 100,000 entities being monitored. There are a number of viable approaches to infrastructure monitoring including modular solutions, offerings with bare-bones capabilities, offerings for agile architectures and those specifically designed for smaller-scale environments.

This year, we have switched to a single table presenting a representative list of ITIM vendors (see Table 3). This is intended to be an example list of vendors covering a range of different ITIM areas (such as on-premises, cloud-native, containers and hybrid) as well as a number of different functional areas (such as granular data capture with tracing, tagging, and analytics or AIOps).

| ITIM Vendor | Headquarters | Product Name |
|---|---|---|
| Ártica | Spain | Pandora FMS |
| BMC | U.S. | TrueSight Infrastructure Management |
| Broadcom | U.S. | DX Infrastructure Manager |
| Centreon | France | Centreon |
| Datadog | U.S. | Datadog |
| Dynatrace | U.S. | Dynatrace |
| eG Innovations | U.S. | eG Enterprise |
| Elastic | U.S. | Elastic Observability |
| **Fata Informatica** | **Italy** | **SentiNet3** |
| Grafana Labs | U.S. | Grafana Cloud, Grafana Enterprise |
| Icinga | Germany | Icinga 2 |
| Infosim | Germany | StableNet |
| ITRS Group-OP5 | U.K. | OP5 Monitor |
| LogicMonitor | U.S. | LogicMonitor platform |

| | | |
|---|---|---|
| ManageEngine | U.S. | OpManager, Applications Manager, Site24x7 |
| Micro Focus | U.K. | Operations Bridge |
| Microsoft | U.S. | System Center Operations Manager (SCOM), Azure Monitor |
| Nagios Enterprises | U.S. | Nagios Core |
| Netreo | U.S. | Netreo |
| New Relic | U.S. | New Relic One |
| Opmantek | U.S. | Network Management Information System (NMIS) |
| OpsRamp | U.S. | OpsRamp |
| Opsview | U.K. | Opsview Monitor |
| Oracle | U.S. | Oracle Enterprise Manager |
| Paessler | Germany | PRTG Network Monitor |
| Progress (formerly Ipswitch) | U.S. | WhatsUp Gold |
| Prometheus | U.S. | Prometheus |
| ScienceLogic | U.S. | ScienceLogic SL1 |
| SolarWinds | U.S. | Server & Application Monitor, Network Performance Monitor |
| Splunk | U.S. | Splunk Observability Suite |
| Sysdig | U.S. | Sysdig |
| Tigera | U.S. | Calico Open Source, Calico Cloud, Calico Enterprise |
| Virtana | U.S. | Virtana Platform, VirtualWisdom |
| VMware | U.S. | vRealize Operations, Wavefront |
| Zabbix | U.S. | Zabbix |
| Zenoss | U.S. | Zenoss Service Dynamics (ZSD) |

Table 3: Representative IT Infrastructure Monitoring Tool Vendors

In addition to the above vendors, there are vendors that operate on a free or freemium model (some vendors may also be included above). Some examples include Cacti, Centreon, Nagios, OpenNMS, Prometheus with Grafana, and Zabbix.

## Market Recommendations

When choosing an ITIM tool, select an offering that closely matches organizational requirements and capabilities. The following are key considerations to prioritize during the evaluation process:

- Business stakeholders. Ensure alignment with the organization's overall strategy by engaging business leaders throughout the tool selection process. For example, if business leaders are proponents of cloud solutions, vendors that have partnerships with your preferred cloud providers must be given priority. Similarly, if IoT is on the business radar, then shortlist tools that make extensive use of technologies for data ingestion, provide more than basic analytics capability or integrate well with analytics tools.
- Focus on "must have" features. Avoid overbuying by scrutinizing requirements to identify must-have versus nice-to-have functionality. Begin by identifying a lean tool with the minimal features that meet all your requirements; there is no value in implementing features your organization will never use.
- Implementation and integration. Facilitate implementation by ensuring that ITIM tools integrate with any existing ITOM tools and align with the existing skill level of the IT operations team.
- Rightsized solutions. Given feature parity, select tools that are easy to deploy, provide the closest fit to current requirements and align with the enterprise's future needs. The more complex a tool is, the more effort required for deployment and configuration. Verify whether professional services are needed for tool deployment, and whether training by the vendor for managing and configuring the tool is available.
- Analytics and automation. Enhance ITIM functionality by selecting a tool that can easily implement automation and ingest data from other monitoring tools to allow for correlation and root cause analysis.
- Predictive thresholds. Some tools use basic pattern recognition to automate the setting of thresholds. This feature will reduce the efforts needed from the IT operations team toward manually setting thresholds for identifying actionable events that have the correct priorities.

- SaaS and on-premises offerings. Note the differences between on-premises and cloud-only functionality, and do not assume that features in one will be available in the other, even if they both come from the same vendor.

Key features and considerations for achieving maximum value from ITIM tools include:

- Contextualized data. Help the operations team with cause-and-effect correlation for events under investigation (for example, by using basic log analytics to provide logs relevant to metrics or events under investigation).
- Dashboards tailored for the audience. Use the flexibility and the dynamic dashboard capability to provide a business-centric view for the business user, a service-level view for the IT operations head or CIO, and a granular view for the IT operations teams.
- Planning for analytics. Leverage event correlation capabilities and plan ahead to replace these with AIOps capabilities, as benefits from event correlation alone are limited.
- Leveraging existing ITOM tools. Improve event and incident management, as well as other IT operations processes like capacity management, through integration and data interchange, making more extensive use of ITOM tools.
- Using correct and relevant metrics. Do not get carried away capturing all the data that the tool can monitor. The usefulness will be limited by the volume of data the IT operations team has to traverse. Pare down the metrics collected so that minimal and relevant metrics are captured. Turn on the metrics that meet monitoring requirements and adjust the monitored metrics to meet requirements in an ongoing fashion.
- Flexible configurations. Ensure that the tools provide flexibility to allow for granular monitoring and ease of configuration (for example, to troubleshoot a recurring problem or performance issue).
- Data and analytics platform monitoring. Invest in tools that have the ability to monitor and report on data and analytics platforms deployed in enterprises. The business's increasing dependence on forecasts and predictions from analytics platforms means these technologies need a monitoring approach that reflects their growing importance.
- Hybrid environments. Some enterprises have IT infrastructure spread across on-premises and cloud environments and would benefit from tools that provide visibility, through a single dashboard, to a distributed IT infrastructure.
- Application monitoring. Be wary of ITIM tools that claim to monitor applications but actually capture resource utilization metrics. Although these tools may provide availability metrics for applications, they lack the end-to-end, transactional visibility of APM tools.

## Evidence

Gartner's observations are based on more than 500 end-user interactions in the past 12 months related to IT monitoring. In more than 50% of these interactions, IT leaders have reported:

- Increasing interest of business leaders in IT infrastructure performance analysis and its impact on business.
- The need for consolidation across existing monitoring solutions.
- The need for trimming down the number of monitoring tools, which in the case of larger enterprises is more than 30 in number, while some of the smaller organizations have monitoring tools ranging in number from three to 10.
- The need for putting together a monitoring strategy to align with modern IT architectures and to address data requirement needs for application developers and business leaders and for efficient IT operations.

The vendors listed in this research were chosen as a sample based on meeting one or both of the following criteria:

- Having different offerings that include proprietary, open-source, free, commercialized versions including deployment that cuts across physical and virtualized appliances, and hosted and SaaS-based options.
- Providing coverage from a geographic and vendor-size perspective.