

# Hype Cycle for ITSM, 2023

Published 14 July 2023 - ID G00790912 - 117 min read

By Analyst(s): Siddharth Shetty, Chris Laske

Initiatives: [I&O Operations Management](#)

Traditional approaches to IT service management aren't suited to modern hybrid cloud environments and faster service delivery times. I&O leaders must understand the hype around new technologies, such as generative AI and process automation, and how they affect ITSM strategies and business value.

## Analysis

### What You Need to Know

Infrastructure and operations (I&O) leaders responsible for infrastructure, operations and cloud management must understand the hype around new technologies to maximize the value of their investments without exposing themselves to excessive risk. The 2023 Hype Cycle for IT Service Management (ITSM) provides guidance on the hype around newer innovations like collaborative support hubs and technology change automation. Guidance is also included on technologies related to information security that have an influence on the short-term and long-term ITSM roadmap of I&O leaders.

Much like last year, there are many technologies that are at the peak of their hype this year. However, some technologies — like infrastructure automation and multiexperience — have moved past the initial hype since their value proposition is more realistic compared to last year. AIOp platforms have also moved rapidly across the Hype Cycle compared to last year.

### The Hype Cycle

The 2023 Hype Cycle for ITSM has undergone a significant update, due to the following factors:

- Some long-standing ITSM technologies like IT service view CMDB and ITIL have reached the Plateau of Productivity and retired.
- Focus on automation has increased due to rapid increases in the pace of change and environmental complexity that I&O leaders are challenged to support.

- Interest in how AI underpins ITSM has gained momentum due to generative AI applications like ChatGPT.
- Interdependence between information security practices and IT service management has increased.

This year's ITSM Hype Cycle includes the collaborative support hub (see [Innovation Insight for Collaborative Support Hub](#)) for the first time. A collaborative support hub is a formalized system of engagement that provides support and shares best practices for both IT and non-IT employees, leveraging the collaboration capabilities of an ITSM platform.

Technology change automation has also been introduced due to the interest in process automation enabled by integrations between ITSM platforms, CI/CD tools and AIOps platforms.

The importance of information security governance has led to the inclusion of exposure management, security orchestration automation and response (SOAR), and vulnerability prioritization technology in this year's ITSM Hype Cycle. All three innovations have touchpoints to ITSM platforms and practices and hence, are tracked under the Hype Cycle for ITSM.

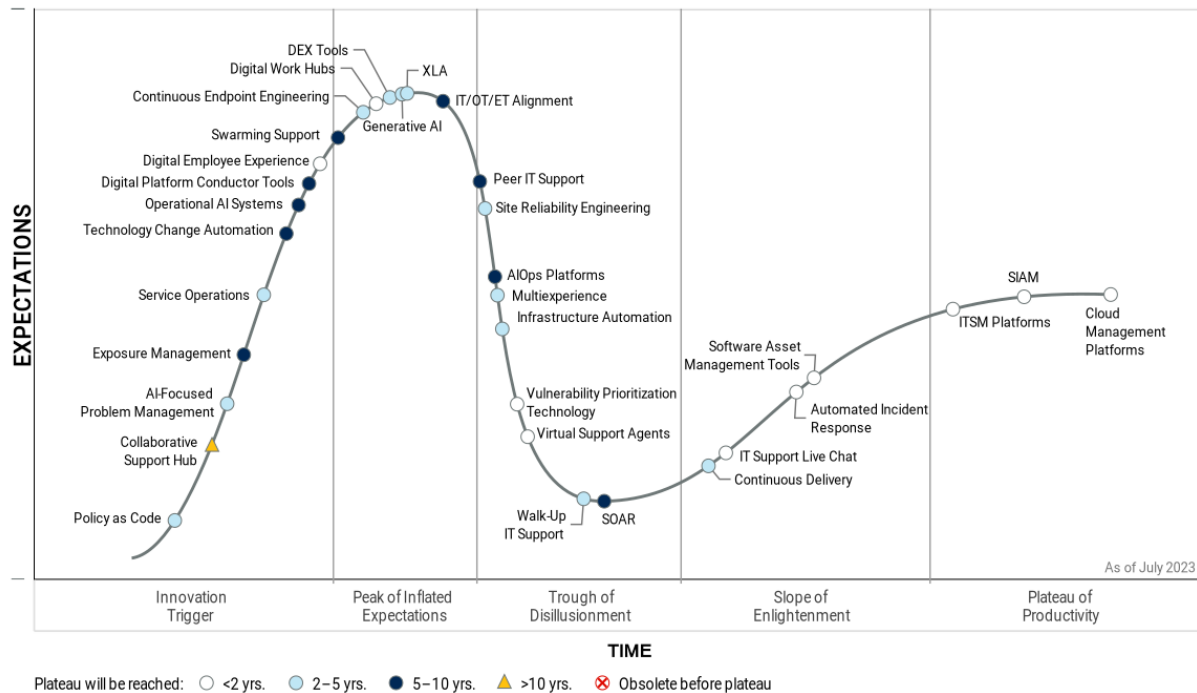
The New Work Hub Innovation Profile has been renamed Digital Work Hubs in this year's edition to reflect how the newer technology enables employees' digital skills.

Generative AI has been introduced this year due to the tremendous hype created by ChatGPT. ITSM platform vendors and buyers are exploring use cases and data integrity issues related to generative AI.

ITSM platforms and cloud management platforms have reached the end of the ITSM Hype Cycle, suggesting the markets for them have fully matured. The ITSM platforms Magic Quadrant and Critical Capabilities research has been retired for 2023, and an ITSM platforms Market Guide will instead be published by the end of 2023.

Figure 1: Hype Cycle for ITSM, 2023

## Hype Cycle for ITSM, 2023



Gartner

## The Priority Matrix

## Immediate Considerations

ITSM platforms' functionality is mature yet still widely deployed throughout organizations. I&O platforms should be selected based on the organization's practice requirements and midterm roadmap for ITSM capabilities. Service integration and management (SIAM) is also an established practice and should be considered for I&O organizations that have significant exposure to managed service providers (MSPs).

## Short-Term Considerations

Over the next two to five years, service operations adoption will become mainstream, supported by practices like site reliability engineering (SRE) and enabled by infrastructure automation, continuous delivery, policy as code and AI-focused problem management. Digital employee experience (DEX) needs to be part of short-term considerations operationalized by DEX tools and measured by experience-level agreements (XLAs).

## Long-Term Considerations

Digital platform conductor tools and exposure management will offer transformational benefits, but it will take more than five years for these capabilities to mature in the marketplace. There is a lot of interest in managing operational technology (OT) and engineering technology (ET) assets using the same tools and framework, but it will similarly take more than five years to realize their value.

**Table 1: Priority Matrix for ITSM, 2023**

(Enlarged table in Appendix)

Benefit ↓	Years to Mainstream Adoption			
	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational	Digital Employee Experience	Generative AI Service Operations Site Reliability Engineering	Digital Platform Conductor Tools Exposure Management	
High	Automated Incident Response Digital Work Hubs ITSM Platforms SIAM Vulnerability Prioritization Technology	Continuous Delivery DEX Tools Infrastructure Automation Multiexperience Policy as Code XLA	AIOps Platforms IT/OT/ET Alignment Operational AI Systems SOAR Technology Change Automation	
Moderate	IT Support Live Chat Software Asset Management Tools Virtual Support Agents	AI-Focused Problem Management Continuous Endpoint Engineering Walk-Up IT Support	Peer IT Support Swarming Support	Collaborative Support Hub
Low	Cloud Management Platforms			

Source: Gartner (July 2023)

## Off the Hype Cycle

- IT service view CMDB and IT service dependency mapping had reached peak productivity in the 2022 iteration of the ITSM Hype Cycle; neither are included in this year's ITSM Hype Cycle.
- ITIL has been dropped from this year's edition since we do not see a hype for ITIL 4, and most I&O organizations are content to adapt ITIL v3 to support their modern IT service management practices.
- IT service catalogs and IT end-user satisfaction assessments command continued interest, but both are considered foundational by most I&O leaders. Hence, their popularity should not be confused with hype, which is a key qualification for any Hype Cycle.

## On the Rise

### Policy as Code

Analysis By: Paul Delory

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

#### Definition:

Policy as code (PaC) languages express governance and compliance rules as code, so they can be enforced programmatically by automation tools. PaC languages are often domain-specific and declarative. With PaC, policies are treated as software, making them subject to version control, code review and functional testing. The most mature PaC tools can render any business logic in code. You can use them today to enforce infrastructure compliance, authorization, Kubernetes admission control, and more.

#### Why This Is Important

In the most mature automation pipelines, infrastructure and operations (I&O) engineers mostly spend time on optimization, governance and compliance. They no longer build infrastructure; that work has been automated and turned over to others. Now, the I&O function builds the guardrails around the infrastructure services that their end users consume. I&O must align with security and compliance teams. PaC brings policy enforcement into their automation pipelines, while preserving a separation of duties that mirrors a typical IT org chart.

#### Business Impact

Policy as code improves:

- **Security, compliance and automation:** PaC combined with infrastructure automation implements policies automatically, with implicit compliance guarantees.
- **Alignment of security and operations teams:** PaC allows security and compliance teams to interface directly with automation pipelines to ensure conformance.
- **Visibility and auditability:** PaC provides both documentation of policies and evidence they are being enforced.

- **Time and effort spent:** PaC means less toil for operators.

## Drivers

- **PaC tooling:** Several dedicated PaC tools are now on the market, many of them are open-source. The Open Policy Agent, a Cloud Native Computing Foundation project, has become the *de facto* standard for PaC. Indeed, even some other PaC tools now use Open Policy Agent policies alongside or instead of their own policy engines.
- **Increasing regulation:** New regulations such as GDPR have increased both the difficulty of compliance and the pressure on compliance teams. PaC allows compliance teams and auditors to document their policies in detail, and to verify that they are being enforced.
- **Security breaches:** Similarly, a spate of newsworthy security breaches at public companies — caused by infrastructure misconfigurations — has put every IT organization's security and compliance practices under increased scrutiny. No I&O team wants its security failures to be the reason for its company getting negative headlines.
- **Growth of DevOps and DevSecOps:** More and more companies are embracing DevOps and DevSecOps — which means more and more companies are encountering the hard governance problems of automation. Many teams that implement infrastructure as code quickly are finding that they need better policy enforcement, and PaC can help.
- **Cloud optimization and cost control:** Beside their benefits for security and compliance, PaC tools can also be used to enforce the build standards for infrastructure, including budgets. In the public cloud, where oversized or unnecessary infrastructure incurs direct out-of-pocket costs, programmatically enforced policies can help to control spending.

## Obstacles

- **Scarcity of downloadable content:** PaC tools will not gain real traction until they have an extensive library of community-generated content. Ideally, users would simply download the policies they need from a free, public repository, rather than having to write their own policies. Over time, as the user base expands and commercial offerings see increased adoption, PaC tools will reach a critical mass of downloadable content that supports real-world use cases.

- **Skill set:** Many I&O professionals lack the skills to operate automation and PaC tools effectively. Gartner clients routinely report that their automation and policy management are hindered primarily by people, not tools. PaC will magnify these existing skills challenges.
- **Organizational inertia:** PaC promises improved collaboration between I&O and security or compliance teams. But in some organizations, this change would be unwanted. Internal resistance of this kind will slow the rate, scope and scale of PaC initiatives.

## User Recommendations

- **Start small:** Choose a pilot use case where PaC is likely to provide real business benefits, expanding to others once PaC has proven its value.
- **Upskill staff:** PaC languages are not always intuitive. Technical staff will need practice to reach proficiency.
- **Prioritize existing templates:** Focus your PaC efforts on use cases that have ready-made implementation templates — ideally, publicly available downloadable content. For example, almost every PaC tool on the market has a canned implementation of the CIS benchmarks.
- **Break down team silos:** Use PaC to build a common workflow for automation and policy enforcement that spans I&O, security and compliance teams.
- **Integrate PaC into automation pipelines:** Use PaC to build guardrails for automation tools, so that they cannot take actions that are out of compliance.
- **Measure before and after:** Use observability tools and value stream mapping to define your starting state, then compare it to the end state. Collect real data to quantify the value of PaC.

## Sample Vendors

HashiCorp; Palo Alto Networks; Progress; Pulumi; Styra

## Gartner Recommended Reading

[Using 'Policy as Code' to Secure Application Deployments and Enforce Compliance](#)

[How to Protect Your Clouds With CSPM, CWPP, CNAPP and CASB](#)

[Innovation Insight for Continuous Compliance Automation](#)

[Innovation Insight for Cloud-Native Application Protection Platforms](#)

[Magic Quadrant for DevOps Platforms](#)

## **Collaborative Support Hub**

**Analysis By:** Chris Matchett

**Benefit Rating:** Moderate

**Market Penetration:** Less than 1% of target audience

**Maturity:** Embryonic

### **Definition:**

A collaborative support hub is a formalized system of engagement that provides support and sharing of best practices for both IT and non-IT employees, built around a central collaboration solution that is integrated with an IT service management (ITSM) platform. It enables business consumers to obtain guidance from a community of IT service desk experts, technical experts, product teams, business process experts, or peers and colleagues.

### **Why This Is Important**

Collaborative support hubs are appearing where a traditional IT service desk “Levels 1, 2 and 3” tier format struggles to address modern trends such as peer support, swarming and product management. The formal system of engagement evolves peer IT support forums and will complement the IT service desk through ITSM platform integration.

### **Business Impact**

Collaborative support hubs provide these benefits:

- Formalize and expand support channels to improve engagement for employees who choose not to contact the IT service desk.
- Improves IT visibility and ability to support activities that do not flow through the IT service desk.



- Expedite incident resolution using swarming, when expertise resides in both IT and business expert teams.
- Foster peer support, which encourages non-IT employees to develop and share skills and best practices.

## Drivers

- Interest in alternative support models surged with the shift to remote work and the need to ease the IT service desk workload.
- A third or more of digital workers outside of the IT department access digital channels where they can ask IT support questions and/or turn to IT subject matter experts for help on nonroutine tasks.
- Seventy-seven percent of digital workers have an IT specialist within their business unit. Business-led IT is becoming the norm as IT organizations reposition themselves to support improved business outcomes.
- Many organizations have deployed collaborative work management on tools such as Microsoft Teams, Cisco Webex Teams or Slack, enabling employees to communicate through broader and more diverse channels.
- Some ITSM platform vendors have added collaborative hub capabilities to their product roadmaps.
- Eighty-five percent of infrastructure and operations (I&O) leaders, surveyed in 2021, said their organizations had partially adopted a collaborative swarming model alongside traditional tiered support for incident resolution where the service desk was engaged.
- A third or more of digital workers outside of the IT department access digital channels to ask IT support questions and/or turn to IT subject matter experts for help on nonroutine tasks, according to the 2022 Gartner Digital Worker Survey.

## Obstacles

- Remote working led to a drop in “ask a colleague for help” frequency according to our digital workplace surveys in 2020 and 2022. Many business consumers prefer to contact only traditional support channels.
- Collaborative hubs require collaboration tools to succeed. While there are many options, all have different limitations, making it difficult to standardize on one solution.
- ITSM platforms’ inability to recognize the time and effort of both IT experts and non-IT employees working on and solving issues requires management to manually log or estimate these metrics.
- Business executives may be resistant to allocating time/resources for this ad hoc or unstructured type of support.
- Roles required to support distributed models like collaborative support hubs differ from those associated with traditional tiered support, and I&O leaders struggle to find employees with experience managing and supporting communities.

## User Recommendations

- Pursue collaborative support hubs proactively as a complementary model to accommodate shifts in work arrangements and changes in worker engagement preferences.
- Continue to provide an IT service desk alongside the hub, to avoid alienating employees who prefer that option.
- Start with topic groups for products where substantial knowledge capital/subject matter expertise is known to exist in both IT and business domains.
- Gain and maintain endorsement from business managers by demonstrating the value gained through the collaborative support hub via reporting usage data, impact on the number of contacts IT receives and user feedback in a business value dashboard.
- Operate the collaborative support hub efficiently by appointing a community manager and community moderators.
- Create opportunities for broader engagement and career advancement by enlisting non-IT employees where they can demonstrate and develop their digital dexterity.

## Gartner Recommended Reading

[Innovation Insight for Collaborative Support Hub](#)

[Transform IT Support by Developing Collaborative Support Hub Roles and Competencies](#)

[What Workers Want: Top 10 Insights From the Digital Worker Experience Survey](#)

## AI-Focused Problem Management

Analysis By: Mark Cleary

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

### Definition:

The use of AI and pattern matching provides a more advanced form of proactive problem management. AI-focused problem management automatically identifies recurring incidents from both past and current incidents. This can have a significant impact on the quality of service provided by support teams because it highlights repetitive incidents that would otherwise go unnoticed.

### Why This Is Important

Many organizations are keen to exploit AI to optimize their service desk and reduce the number of incidents. The automation of problem management is an excellent example of using AI and pattern matching to detect underlying problems that would otherwise go unnoticed.

### Business Impact

Using AI to identify recurring incidents benefits the organization in the following ways:

- Reduces end-user frustration by reducing repetitive incidents.
- Reduces incident volume and cost by identifying underlying issues.
- Creates a more efficient problem management practice as the discipline becomes embedded.

- Helps understanding the health of the products and services provided by IT better.

## Drivers

Organizations are attracted to the ability to:

- Deliver better business outcomes by reducing the number and prevalence of incidents.
- Address underlying problems that would otherwise not be visible.
- Discover patterns and trends that may highlight structural software or hardware issues.
- Establish the value of problem management and accelerate problem detection and remediation.

## Obstacles

- AI-focused problem management depends on the accurate categorization of incidents and structured data.
- It requires completing the free-form text detailing the diagnosis and resolution for every incident in a comprehensive way to allow effective pattern matching.
- It needs an effective problem management practice to assist the second-line application, product and infrastructure teams in analyzing and addressing the problems identified in the output.
- Senior leadership support is necessary to ensure the output is prioritized and necessary actions are taken.
- AI-focused problem management requires a significant number of incidents to ensure that the results are accurate when processing previous incidents to identify problems.
- It requires an accurate and up-to-date configuration management database (CMDB) to ensure that each incident has an associated configuration (CI) record with sufficient attributes to aid in root cause analysis.

## User Recommendations

- Ensure that all incidents are correctly categorized on closure with the correct CI and matched to comprehensive free-form text covering the diagnosis and resolution.
- Pilot incident clustering by focusing on specific asset classes that are prone to high numbers of incidents to demonstrate its value and impact.
- Ensure that the CMDB is accurate and up-to-date for the chosen asset classes, and build out this process as the pilot expands.
- Track the number of problems raised and resolved (either with a workaround or by addressing the root cause) as a direct result of the approach. If possible, identify the rough cost savings of removing the repetitive incidents.
- Launch a problem management initiative to highlight the benefits. Make the second-line teams aware that their support will be required to address problems that are likely to result from this work.

## Sample Vendors

Aisera; BMC Software; ServiceNow

## Exposure Management

**Analysis By:** Pete Shoard, Mitchell Schneider, Jeremy D'Hoinne

**Benefit Rating:** Transformational

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

### Definition:

Exposure management (EM) encompasses a set of processes and technologies that allow enterprises to continually and consistently evaluate the visibility, and validate the accessibility and vulnerability of an enterprise's digital assets. EM is governed by an effective continuous threat exposure management (CTEM) program.

## Why This Is Important

EM reduces the challenges organizations face inventorying, prioritizing and validating threat exposure that exist due to a rapidly expanding attack surface where traditional vulnerability management isn't enough. The volume of effort required and the diversity of potential issues lead to conflicting priorities and "dashboard fatigue." SRM leaders struggle to prioritize risk reduction actions, leaving gaps where they feel they have less control, such as SaaS platforms and social media.

## Business Impact

Exposure management governs and prioritizes risk reduction for the modern enterprise and requires assessments of all systems, applications and subscriptions used.

- Likelihood of exploitation (visibility of the organizations attack surface).
- Inventory and prioritize (vulnerability, threat intel-based, digital assets).
- Validate the potential success of any attack and if security controls can assist with detecting or preventing them.
- CTEM is a program, not the outcome of a specific tool.

## Drivers

- Most commonly, organizations are siloing exposure activities such as penetration testing, threat intelligence management and vulnerability scanning. These siloed views provide little or no awareness of the complete situation regarding the effective risks the organization has.
- The volume of discovered vulnerabilities and issues that testing surfaces continues to grow with the complexity of environments, the increased volumes of applications used and the increased use of cloud services.
- Lack of scope and understanding of prioritization and risk, in line with high volumes of findings is leaving organizations with far too much to do regarding their exposure and little guidance on what to action first.
- A programmatic and repeatable approach to answer the question “how exposed are we?” is necessary for organizations. This must have the aim of allowing reprioritisation of priority as environments change in a rapidly changeable IT landscape.
- Organizations must reorient their priorities, and segregate these priorities into three distinct questions: “what does my organization look like from an attacker’s point of view?,” “what configuration has my organization set that will make it vulnerable to attack?”; “how would our defensive controls cope and how would response processes perform?”

## Obstacles

- The increased scope of CTEM programs over traditional VM introduces a number of new complexities often not previously considered or budgeted for.
- The concept of evaluating your attack surface is well-understood, continued security tool consolidation in this space, such as EASM with VA is beginning to simplify day-to-day operational processes, but formal integration of other technologies such as CAASM and CSPM technologies is still low.
- Processes to manage end-to-end awareness (from visibility of possible attack vectors to response to breaches) is virtually nonexistent in most organizations who often simply scan and test their networks for compliance reasons.
- The complex way an attack may manifest itself requires certain skill sets to understand, new markets such as BAS make it more simple to test the out-of-the-box scenarios. But to be more effective at using these technologies/services and develop custom-made simulations, new skills and understanding are required.

## User Recommendations

- Embrace broader CTEM programs as security and risk management professionals, rather than simply processing vulnerabilities with VA tools.
- Mobilize various organizational stakeholders as success is dependent on it. Automated remediation from tools is unlikely to have a significant impact.
- Focus on visibility, end users must have an awareness of where risks are, and plan to respond to threats even if the organization has no way to reduce exposure to them.
- Prepare response and reaction plans. Monitoring and responding to issues and risks identified as a critical part of managing exposure, validating that exposures exist and controls are functioning is useful, but it is essential that organizations also prepare to react.
- Be sure to include assets that your organization doesn't directly own, such as social media accounts, SaaS applications and data held by supply chain partners, in your exposure management program.

## Gartner Recommended Reading

[Innovation Insight for Attack Surface Management](#)

[Implement a Continuous Threat Exposure Management \(CTEM\) Program](#)



## Predicts 2023: Enterprises Must Expand From Threat to Exposure Management

### Top Trends in Cybersecurity 2023

#### Service Operations

Analysis By: Mark Cleary

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Emerging

#### Definition:

Service operations is the convergence of the infrastructure and application monitoring environments with the ITSM incident management practice to create a more effective and optimized mechanism for diagnosing and resolving incidents. The combination of the two environments with the context of AI can lead to a significant reduction in both the number and impact of incidents.

#### Why This Is Important

The ability to quickly diagnose and resolve incidents is critical for organizations as they develop and implement digital services. Intelligent automation can remove monitoring and service desk silos, creating the concept of service operations. This ensures that incident detection through monitoring can be better integrated with ITSM platforms, leading to incidents that can be more readily identified and resolved creating higher availability and more resilient services.

#### Business Impact

The convergence of ITSM and monitoring environments results in a more productive and seamless incident management practice. The contextual analysis of alerts resulting in anomaly detection and escalation can result in fewer incidents and improved mean time to resolve (MTTR), especially when integrated with the ITSM platform. Products and services are more available and less likely to suffer from poor performance or outages and disruption, costs are reduced, and overall productivity is improved.

## Drivers

- Business pressure for reliable and stable services drives the demand for incidents to be either eliminated before they can cause disruption or be diagnosed and resolved as quickly as possible.
- The closer integration of monitoring with the service desk creates a far more effective and seamless environment in which outages and disruption can be better and more effectively managed.
- ITSM platforms now feature observability and correlation functions to identify incidents as part of the monitoring capabilities now available.
- ITSM platforms can now enrich the events by applying the context of recent incidents and changes to the impacted configuration items (CIs) to radically improve the identification of the probable root cause.
- The rise in the use of AI allows anomalies and events from different monitoring systems to be swiftly correlated and analyzed and presented to technicians via the ITSM platform.

## Obstacles

- AI-based monitoring systems can take longer than expected to understand the context of the services, the traffic, and the environment creating delays in improving availability.
- Improved diagnostics and resolution times require time and effort to achieve due to dependencies including effective service mapping, the degree of automation and the quality of monitoring. This requires a concerted effort to achieve a holistic approach.
- Aligning data feeds, telemetry and log information from different sources creates data disparity leading to delays in identifying and correlating incidents.
- Accurate service mapping and comprehensive, up-to-date configuration management databases are necessary to support end-to-end incident processes if enhanced availability and resilience is to be achieved.
- Automated responses need to be carefully chaperoned to ensure that their decisions match the use case.
- Many monitoring and service desk teams operate in silos, making it difficult to create a seamless experience.

## User Recommendations

- Develop a strategy for service operations that focuses on effective incident management. Consider the implications on the monitoring and technical support staff (including the service desk), the range of tools available, how they will be integrated, and whether the service practices need to be amended.
- Identify the tool and process dependencies and build a roadmap to define and implement the solution.
- Develop or purchase runbooks as scripted solutions for common incident scenarios.
- Explore vendor options for solutions offering automated responses and self healing to ensure alignment and integration with your environment.
- Adopt a pragmatic approach and pilot the initiative on a critical business service to understand the capabilities and drawbacks.
- Use collaboration techniques such as communities of practice to bring the various teams together to understand the respective roles and responsibilities, and challenge them to reduce the cycle time to identify and process an incident.

## Sample Vendors

Atlassian; BigPanda; BMC; DataDog; Moogsoft; PagerDuty; ServiceNow

## Gartner Recommended Reading

[Market Guide for AIOps Platforms](#)

## Technology Change Automation

Analysis By: Chris Laske

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

**Definition:**

Technology change automation streamlines change management practices by automating change ticket creation, risk assessment, conflict checking and approvals. Integrations between IT service management (ITSM) platforms, continuous integration/continuous deployment (CI/CD) tools, and AIOps platforms enable rapid delivery and incident correlation while ensuring change visibility and minimizing business disruption.

**Why This Is Important**

Demand for rapid deployments and intolerance for extended outages caused by changes are rendering manual change approval, execution and follow-up insufficient. Infrastructure and operations (I&O) teams are leveraging technology change automation to auto-generate change records, streamline approval processes, and enable better visibility to changes, resulting in improved change cadence and quality while minimizing business disruption.

**Business Impact**

Technology change automation delivers value by:

- Integrating ITSM platforms with CI/CD pipelines tools to streamline change record creation.
- Automating conflict checks to avoid change collisions and target approved change windows.
- Automating risk assessment to streamline and ensure proper classification.
- Automating change approval workflows to reduce delays due to overly burdensome administration.
- Ingesting change record data into AIOps platforms to rapidly correlate incidents with production changes.

## Drivers

- Digital business demand and the adoption of agile development methodologies are driving the need for more rapid deployments.
- Manual change practices are labor intensive and strain internal resources.
- Additional conflicts and collisions are encountered as a result of higher volumes of changes.
- Organizations that have abandoned change management practices encounter numerous business disruptions.
- Poor visibility to production changes leads to delays in service restoration during major incident events.

## Obstacles

- Development teams that have abandoned change management practices fail to see the value of investing time and energy to automate change management.
- The lack of foundational change management practices, such as guidelines for standard changes, will make it difficult to establish automated approval workflows.
- Organizations that maintain multiple release and deployment technologies may be challenged to integrate each with the ITSM platform for change management.
- Organizations that have not tracked business value metrics associated with change management (e.g., value enablement, cost of business disruption associated with failed changes) may find it difficult to justify the effort required to enable change automation. Few ITSM platforms have advanced features to support end-to-end technology change automation today.

## User Recommendations

- Begin tracking and reporting business-value metrics associated with change management (e.g., rapid business value enablement/delivery, cost of business disruption due to failed changes).
- Apply consistent guidelines for change management practices including requirements for standard changes. Define review criteria to leverage for converting policy to code.
- Build automated approval workflows for standard changes. Leverage ITSM platform change management capabilities such as conflict checking and CI/CD tool integration.
- Enable integrations between ITSM and AIOps platforms for change management data to improve correlation between incidents and changes.

## Operational AI Systems

**Analysis By:** Chirag Dekate, Soyeb Barot, Sumit Agarwal

**Benefit Rating:** High

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

### Definition:

Operational AI systems (OAISSys) enable orchestration, automation and scaling of production-ready and enterprise-grade AI, comprising ML, DNNs and Generative AI. OAISSys integrates DataOps, ModelOps, MLOps and deployment services to deliver enterprise-grade governance, including reusability, reproducibility, release management, lineage, risk and compliance management, and security. It also unifies development, delivery (hybrid, multicloud, IoT) and operational (streaming, batch) contexts.

### Why This Is Important

OAISSys can help enterprises:

- Standardize, govern and automate AI engineering and deployment technologies, and accelerate productization of AI.

- Eliminate system integration friction and impedance mismatch across DataOps, ModelOps, MLOps, deployment and governance platforms.
- Scale AI initiatives by enabling orchestration across hybrid, multicloud, edge AI or IoT.
- Enable discoverable, composable and reusable AI artifacts (data catalogs, feature stores, model stores) across the enterprise context.

## **Business Impact**

OAISys deliver production AI systems that:

- Systemize analytics and AI engineering technologies, including ModelOps and MLOps platforms.
- Integrate existing data, analytics and DSML platforms.
- Utilize reusability components including feature and model stores, monitoring, experiment management, model performance and lineage tracking.
- Homogenize governance including compliance, risk, security, and cost across deployment (hybrid, multicloud, IoT) and operational (streaming, batch) contexts.

## Drivers

- Enable business stakeholders to leverage AI as a service that is customized to their enterprise context.
- IT leaders need to deliver, manage and govern AI models within enterprise applications deployed across multiple contexts and jurisdictions (hybrid, multicloud, edge AI and IoT).
- Traditional siloed approaches of data management and AI engineering create integration challenges across the data ingest, processing, model engineering and deployment.
- OASys enables enterprises to standardize and automate development, management, deployment, maintenance and governance technologies to deliver comprehensive, flexible and composed end-to-end AI systems.
- It helps align and automate the data, AI model deployment and governance pipelines.
- Operationalization and automation platforms are a core part of how early enterprise AI pioneers scale productization of AI by leveraging existing data, analytics and governance frameworks.
- Standardizing data pipelines, including DataOps toolchains, creating reusability components such as data catalogs and ETL registries, monitoring, security, access control and lineage tracking.
- The enterprise OASys enables unification of two core contexts: deployment context across hybrid, multicloud, edge AI and IoT, and operational context across batch and streaming processing modes that commonly occur as enterprises train and deploy production models.



## Obstacles

- Enterprises with low data and AI maturity levels will find OAI Sys intimidating to build, deliver and support.
- OAI Sys requires integration of full-featured solutions with select tools that address portfolio gaps with minimal overlap. These include capability gaps around feature stores, model stores, governance capabilities and more.
- OAI Sys requires a high degree of cloud maturity, or the ability to integrate data and model pipelines across deployment contexts. The potential complexity and costs may be a deterrent for organizations just starting their AI initiatives.
- Enterprises seeking to deliver OAI Sys often seek “unicorn” experts and service providers to productize AI. Fully featured vendor solutions that enable OAI Sys are hard to come by, and enterprises often have to build and support these environments on their own.

## User Recommendations

- Focus AI engineering activities to deliver business context customized operational AI systems.
- Rationalize data and analytic environment and leverage current (simplified subset of) investments in data management, DSML, ModelOps and MLOps tools to build OAI Sys.
- Leverage cloud service provider environments as foundational environments to build OAI Sys along with rationalizing your data, analytics and AI portfolios as you migrate to the cloud.
- Avoid building patchwork OAI Sys that integrate piecemeal functionality from scratch (and add another layer of tool sprawl). Utilize point solutions sparingly and surgically to plug feature/capability gaps in fully featured DataOps, MLOps and ModelOps tools.
- Actively leverage your existing data management, DSML, MLOps and ModelOps platforms as building blocks, rather than starting from scratch.

## Sample Vendors

Amazon Web Services; Dataiku; DataRobot; Domino Data Lab; Google; HPE Ezmeral Software; IBM; Iguazio; Microsoft; ModelOp

## Gartner Recommended Reading

[2023 Planning Guide for Analytics and Artificial Intelligence](#)

[Emerging Tech Impact Radar: Data and Analytics](#)

[Quick Answer: How Should CXOs Structure AI Operating Models?](#)

## Digital Employee Experience

Analysis By: Lane Severson, Tori Paulman

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Emerging

### Definition:

Digital employee experience (DEX) is a discipline that focuses on how technology affects the overall employee experience (EX). With work becoming increasingly dependent on digital technologies, organizations must embrace experience-focused methods, such as personas, journey mapping, measurement and listening, to deliver an experience that boosts digital dexterity and personal growth, builds team unity, and helps employees achieve organizational goals.

### Why This Is Important

Employees spend more of their time working digitally than ever before; the digital experience affects the overall employee experience. Digital experiences make up most employee experiences, but 66% of employees experience moderate to high digital friction when using technology. On an average, employees must use 11 applications to do their work, with 36% using 11 to 25, and 5% using more than 26.

## Business Impact

A holistic, coordinated approach to DEX across IT and with non-IT partners can minimize digital friction and maximize workforce digital dexterity and well-being. IT teams delivering great DEX improve their organization's talent retention, team effectiveness and process efficiencies, and adopt new ways of working. DEX significantly impacts a workers's intent to stay, with 82%, who believe they work with modern technology and engaged IT staff, intending to stay and/or grow within their organizations, compared to only 58% who do not.

## Drivers

- Companies look for every advantage to attract and retain talent. Organizations must go beyond providing modern technology and services to deliver digital experiences that meet a diverse set of employees where they are in their digital workplace maturity and alignment with digital workplace ambitions.
- As foundational digital workplace technology is standardized across organizations, IT leaders are looking to provide differentiation by the way they facilitate the customization of tools to roles and processes in the organization.
- Persona, journey mapping, user experience (UX) design and design thinking are being used to ensure technology investments have a positive impact on both DEX and EX.
- Business leaders are increasingly looking for guidance on how technology can help address key strategic concerns around employee productivity, engagement experience, well-being and skills development, as well as organizational alignment.
- IT leaders are increasingly investing in DEX tools that collect and combine qualitative measurement (employee feedback) with quantitative measurement (performance, stability and use) of technology, and leverage automation and employee engagement to improve DEX.

## Obstacles

- Building a business case for DEX is difficult. Common measures are subjective and benefits can't be directly attributed to DEX initiatives.
- Cost to acquire, implement and integrate technologies to improve DEX.
- DEX requires shifting from activity- and service-based to new experience- and value-based measures of success.
- The human-centric nature of DEX may not be appreciated by technology-centric IT leadership and staff.
- Low-maturity organizations may not be ready for DEX, because their focus remains on basic IT operations concepts (for example, IT service management [ITSM], endpoint management and technical debt reduction).
- Clients often cite lack of IT leader and staff skills to pivot focus toward experience development. Most organizations still do not see this as a part of their remit.
- Because DEX and EX are directly linked, if IT and HR (who owns EX) are not collaborating, success in improving either will be impaired.
- Organizations facing staffing reductions may not have the resources to invest in DEX leadership, staffing or technology.

## User Recommendations

- Make the digital workplace the central point of coordination for all DEX activities.
- Align key partners in EX, HR and facilities, along with business leaders, by expanding the employee value proposition (EVP) to include DEX.
- Focus DEX initiatives by creating employee personas and prioritizing high-impact roles first. These may include revenue generating roles, customer service or product development.
- Identify key moments in an employee journey such as “the first day at work” or “return to the office” to improve, as opposed to attempting to change, the entire onboarding process.
- Combine personas and journey mapping to catalyze identification and reduction of digital friction points.
- Combine objective data from DEX, or other monitoring and management tools, with subjective data from employee listening and voice of the employee programs to guide DEX initiatives.

## Gartner Recommended Reading

[Deliver Peak Digital Employee Experience Excellence in 4 Steps](#)

[Tool: Digital Employee Experience Journey Maps](#)

[Innovation Insight for the Digital Employee Experience](#)

## Digital Platform Conductor Tools

Analysis By: Roger Williams, Dennis Smith

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

**Definition:**

Digital platform conductor (DPC) tools coordinate the various infrastructure tools used to plan, implement, operate and monitor underpinning technology and services for applications and digital products. They enable digital business, regardless of the environments used or who owns them. DPC tools provide a unified view of underpinning technologies and their connection to applications. This augments strategic decision making and improves the value obtained from technology investments.

**Why This Is Important**

Traditional, cloud and hybrid infrastructure management tools do not inherently provide an integrated view of infrastructure across all environments. Moreover, as infrastructure and operations (I&O) leaders struggle to manage their portfolio of investments to enable composable business, optimize costs and reduce risks, they need help with filling the gaps in visibility, assurance and coordination. DPC tools promise to help close these capability gaps and are improving in their ability to do so.

**Business Impact**

DPC tools deliver the following benefits not inherent in more focused infrastructure management toolsets:

- Visualizing digital platform performance across all life cycle stages — planning, implementing, operating and monitoring.
- Enabling continual optimal performance and placement of workloads in all environments — on-premises, in the cloud or at the edge.
- Ensuring tangible business value from improvement efforts across all technology architectures — compute, storage, middleware and network layers.

## Drivers

- Difficulty in maintaining a coherent view of all technology infrastructure resources and their dependencies that are aligned with changes to services, applications and components, as well as the configuration of their promised performance levels.
- Lack of transparency into spending on hybrid digital infrastructure and how resource capacity aligns with actual application workload demand.
- Need to guide where workloads are processed (data center, public cloud, colocation facility, etc.) based on requirements, including capacity, cost and dependency dynamics.
- Challenges with estimating the value, efficiency, quality and compliance delivered by hybrid digital infrastructure based on aggregated data from performance analysis tools and other hybrid digital infrastructure management (HDIM) toolset data feeds.
- Desire for a single point of entry and reporting for digital platform resource requests, and routing them to appropriate HDIM tooling for fulfillment.
- Desire to reduce the level of skills and effort required within initiatives to improve operations and digital employee experiences.
- Gaps, duplication and conflicts in data to support application workload migration and business continuity goals, as well as protection of data from accidental deletion or malicious activities.
- Inability to confirm compliance of application workloads and digital platforms to identity requirements and security baselines as part of the organization's cybersecurity mesh approach.
- Poor credibility of business cases for digital platform improvements, including: assessing business impact; measuring gaps between current and desired performance; providing oversight of improvement efforts; and validating benefits delivered.

## Obstacles

- Lack of interoperability: Tool sprawl and difficulties in integration inhibit DPC tool adoption. The technology landscape is littered with failed approaches that were intended to support data sharing between vendors.
- Lack of data credibility: The desire for a complete, accurate view of all technology as a precondition for decision making has been around for decades, yet is no closer to being realized. Customers that demand perfect data before they act, and vendors that require complete and accurate data for their tools to function properly, will continue to co-create expectations that will not be met.
- Lack of budget: DPC tools may be viewed as “overhead” that does not have a compelling business case. No one likes paying for something that does not appear to address specific pain points felt today.
- Lack of vendor commitment: Many vendors will be tempted to “DPC wash” their existing offerings and claim that these capabilities are already addressed or can be added for very little cost.

## User Recommendations

- Build a DPC tooling strategy that supports digital business ambitions by defining the management elements, environments and technology layers required to meet the organization’s infrastructure needs now and in the future.
- Address measurement and coordination gaps by working with key stakeholders to identify infrastructure value and risk and cost objectives, and by making targeted investments in integration, dependency mapping and continuous improvement capabilities.
- Plan for DPC tooling investments by determining which DPC capability aspects are needed in the short, medium and long term. Compare these capabilities to current and future vendor offerings for infrastructure management tooling that can provide initial DPC tool functionality.
- Ensure that DPC tooling investments can deliver sustained value by requiring that DPC tool marketers show how the tool will address current organizational pain points and how it will adapt to future needs as organizational requirements evolve.



## Sample Vendors

Cloudsoft; Flexera; HCLTech; IBM (Turbonomic); Oomnitza; OpsRamp; ReadyWorks; Snow Software; Virtana

## Gartner Recommended Reading

[Market Guide for Digital Platform Conductor Tools](#)

[3 Steps to Improve the Reliability of Large, Complex and Distributed IT Systems by Leveraging SRE Principles](#)

## At the Peak

### Swarming Support

Analysis By: Chris Matchett

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

#### Definition:

Swarming support is a triage technique that bypasses the hierarchical, traditional-tiered support structure by using collaboration capabilities to engage directly with individuals from different support teams to diagnose and resolve an incident. A swarm is an ad hoc, agile arrangement formed by those with specific skills and time to collaborate. It is an alternative to assigning tickets to functional support queues.

#### Why This Is Important

Swarming is used by agile and application teams for collaboratively working on new features and user stories. IT service desks use swarming techniques to enable direct engagement with support technicians via collaboration channels to address higher-priority incidents in real time. Major incident managers and problem managers use similar outreach techniques to form tiger teams and temporary support teams for certain high-profile issues. Swarming is a key aspect of collaborative support hubs.

#### Business Impact

Swarming support can produce positive business impacts, such as:

- Real-time incident resolution is enabled by direct access to support resources with the skills and availability to work on an incident.
- It brings expertise together from experts outside of IT.
- Increased productivity as higher-priority incidents are resolved more quickly.
- Knowledge articles are more easily created, as the agent is part of the dialogue.
- Improved efficiency as fewer tickets are sequentially passed between teams.

## Drivers

- Swarming occurs organically in peer IT support.
- Swarming is also used to respond to high-priority incidents when major incident managers form “tiger team” response teams.
- Use of swarming in agile teams to complete features and user stories is demonstrating its potential to other stakeholders, driving interest in support circles.
- Increasing availability of swarming capabilities within IT service management (ITSM) platforms is prompting interest and driving experimentation and uptake.
- Faster incident resolution reduces the overhead of support.
- The adoption of site reliability engineering is also driving adoption with a focus on collaboration and breaking silos.

## Obstacles

- Swarming support is perceived as only suitable for higher-priority incidents and unable to scale to support all types of incidents.
- Scaling swarm responses for swarms of more than a few participants requires investment into tools or platforms that include collaboration capabilities.
- Swarming doesn’t guarantee that the right expertise is brought to bear. If experts are already busy, swarms may go unanswered, resulting in inconsistent support experiences.
- An open and collaborative approach across the support environment is required to make swarming work.
- Swarming may be counter-culture in some organizations where technology-specific support is leveraged.
- Inappropriate swarming requests can be intrusive and time-intensive, and can distract experts from other important work.

## User Recommendations

- Catalog the skills and capabilities of participating IT staff, including knowledge and abilities that are not related to their formal job role.

- Provide clear prioritization guidance to swarming participants, and allocate time in their routines to contribute without disrupting other work and initiatives.
- Pilot swarming with a selected set of applications and associated tickets to establish the viability and to surface improvement opportunities.
- Use the pilot to agree with constraints as well as the type of incidents in scope.
- Measure the value of swarming in the improved mean time to resolve.
- Reward participation in swarming outreaches, as these may fall outside of the scope of standard reporting.
- Establish a collaborative support hub to facilitate and formalize a structure for swarming activities.

## Sample Vendors

BMC Software; FireHydrant; Grafana Labs; Ivanti; PagerDuty; ServiceNow; Transposit; xMatters

## Gartner Recommended Reading

[How to Integrate ITSM Teams With Product Teams](#)

[Quick Answer: How Can I Reduce the Impact of Major Incidents?](#)

[Innovation Insight for Collaborative Support Hub](#)

[Transform IT Support by Developing Collaborative Support Hub Roles and Competencies](#)

## Continuous Endpoint Engineering

Analysis By: Sunil Kumar, Dan Wilson

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Early mainstream

**Definition:**

Continuous endpoint engineering (CEE) is an agile approach for the digital workplace that helps organizations keep pace with accelerated technology updates. The cycle begins when a vendor signals an upcoming change or as IT initiatives change. Additional phases include determining applicability, pilot testing, engaging stakeholders, deployment/enabling and measuring impact.

**Why This Is Important**

Increased dependence on technology and accelerated rate of change are overwhelming IT, undermining system stability and degrading the digital employee experience (DEX). CEE speeds up the process and execution of changes by replacing traditional operating models that were designed for multiyear operating systems and application update life cycles. It reduces the frequency of poorly communicated feature releases, the difficulty of upgrades and the lack of vendor support when issues arise.

**Business Impact**

CEE enables IT leaders to streamline operations and shift focus from technology management to generating business value. Specific impacts include:

- Less complex technology, as customization is deemphasized.
- Reduced IT overhead as more automation is used.
- Improved collaboration and productivity from increased technology adoption.
- Reduced staff disruptions from standardizing change procedures.
- An improved DEX from a more proactive and human-centric IT.

## Drivers

- Organizations' adoption of SaaS and "as-a-service" operating systems continues to increase, rendering traditional operating models obsolete.
- Technology vendors have accelerated development and release cadence to remain competitive and continuously provide increased value, challenging IT organizations to keep pace.
- Vendors have established an update cadence to simplify support and ensure more consistency across customer environments, limiting IT's control over the timing and configurability of features and updates.
- Vendors are reducing support life cycles — OS support has dropped from up to a decade to less than three years, incentivizing CEE adoption.
- The continued threat of cyberattacks is driving accelerated patch deployment and tighter alignment with vendor life cycles to reduce vulnerabilities.
- An increased amount of regulatory requirements demand transparency and compliance.
- IT leaders continue to value speed and agility, accelerating the shift to agile approaches.
- Organizations have adopted a growing number of new applications to enable the digital workplace, amplifying the challenge of keeping them updated.
- Depending on extensive testing and monolithic rollout processes have failed to uncover sufficient issues to warrant the effort required to complete them. And IT leaders are looking for more efficient ways to scale and accelerate work.
- A small number of innovative vendors now have novel offerings that provide automated user-less acceptance ("smoke") testing of applications.

## Obstacles

- Overly complex environments with too many disparate tools that lack integration.
- Highly customized environments that require extensive testing of every update prior to deployment.
- Fragile environments with a significant amount of technical debt, including legacy operating systems or applications that depend on unsupported browsers, runtime environments or plug-ins.
- Traditional siloed organizations are inflexible, sluggish and lack collaboration.
- Staff who lack automation skills and experience with agile methodologies and operate under a legacy mindset that focuses on control and customization.
- IT leaders understand the need for agile operations but don't know how to make that transition.

## User Recommendations

Hype is slowly progressing but remains pre-Peak of Inflated Expectations. Market penetration and maturity have stayed the same. IT leaders are looking to increase the adoption of CEE. However, most still struggle to implement it without wholesale organizational changes. IT leaders should:

- Keep pace with technology life cycles by implementing the complete CEE cycle.
- Avoid common barriers by reviewing policies and procedures and eliminating dependence on legacy technologies and methodologies.
- Avoid methodology mismatches by adopting CEE as a complement to other agile approaches that are less compatible with the digital workplace.
- Align CEE-related organizational changes to updated operating models, agile methodologies and shift toward product management.
- Reinforce behaviors that establish stronger partnerships by defining the new engagement model with colleagues, stakeholders and technology vendors.
- Reduce the requirement for resource-intensive UAT by automating testing with new technologies.

## Gartner Recommended Reading

[How to Implement Continuous Endpoint Engineering: An Agile Approach for the Digital Workplace](#)

### DEX Tools

**Analysis By:** Dan Wilson, Autumn Stanish, Stuart Downes, Tom Cipolla

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Early mainstream

### Definition:

Digital employee experience (DEX) tools help IT leaders measure and continuously improve the performance and employee sentiment toward company-provided technology. Near-real-time processing of aggregated data from endpoints, applications, employee sentiment and organizational context surfaces actionable insights and drives self-healing automation, optimized support and employee engagement. Insights and self-healing can also enhance IT support.

### Why This Is Important

Accelerated digital workplace investment has highlighted gaps in objective measurement and continuous improvement of DEX. Client interest in DEX has steadily increased since the start of 2021. Primary use cases focus on tactical and technology issues however mature digital workplaces are expanding to include more strategic use cases. Their cross-functional DEX strategy directly targets reduced IT overhead and improved DEX as a way to retain and attract top talent.

### Business Impact

DEX tools shift focus from technology management to more business value-added work. Specific impacts include:

- Fewer IT issues that disrupt and impede employee productivity.
- Reduced IT overhead through automation.
- Improved endpoint configuration and patch compliance.



- Better balance of objective and subjective success measures, including technology adoption, performance and employee sentiment.
- IT becoming more proactive and human-centric.
- Increased ability to retain talent.

## Drivers

- DEX is a major influencer of the overall employee experience.
- Organizations are increasingly dependent on technology to perform their work.
- Employees are suffering in silence by living with or working around issues rather than reporting issues to IT.
- IT leaders seek broader measurement and management capabilities as internally focused activity KPIs have proven incomplete.
- IT administrators are looking for better visibility into how hybrid workers' devices are performing.
- Employee sentiment toward technology cannot be measured effectively with periodic or transactional surveys alone. Feedback must also include how employees feel about and engage with specific devices or apps, and how technology changes impact their work.
- Service desk and other IT support analysts require faster access to device configuration and performance data to offset an increase in support interaction volumes and wait times.
- Increasing threat of cyberattacks demands faster identification and remediation of configuration issues and missing patches.
- Increased focus on sustainable IT is promoting consumption- and performance-based device life cycles in place of refreshing devices on a schedule.
- AI and machine learning have significantly increased the value and capability of SaaS-based DEX tools.

## Obstacles

- Legacy culture that does not trust the tool's insights or sees automation as a threat.
- SaaS- or cloud-averse organizations will be limited to less capable on-premises offerings.
- Low-maturity IT support or end-user computing (EUC) organizations may not be ready for DEX tools.
- An "ignorance is bliss" mindset fearing that a sudden unveiling of the massive volume issues will make IT leadership look bad.
- The cost to acquire, implement and integrate new tools.
- Insufficient staffing levels or skills required to operate a DEX tool.
- Failure to adjust IT staff rewards and recognition to promote new behaviors and DEX tool adoption.
- The need to account for legislative, regulatory, industry or labor union limits on data collection and use.
- The lack of maturity and feature parity among representative and similar tools including common APIs for integration.
- Smaller organizations have limited options given that many DEX tools target larger enterprises.

## User Recommendations

In its third year on the Hype Cycle, DEX tools have reached the Peak of Inflated Expectations. Market penetration and maturity have also advanced. Organizations that have not invested in DEX tools should:

- Build a broader team by collaborating with business and IT peers to define IT and non-IT use cases.
- Ensure the business case focuses on objective and measurable impacts by minimizing reliance on vendor-provided ROI templates.
- Choose a DEX tool that best fits your needs and budget by using the [Market Guide for DEX Tools](#).

- Assign dedicated ownership and allocate dedicated resources to deploy and drive DEX tool adoption and ROI. Resources can be reallocated from IT support roles as proactive automation reduces support volumes.
- Incentivize new behaviors by adapting IT performance measures to focus more on outcomes than activities.
- Avoid diminishing returns by adding features and use cases as the team and DEX tool matures.

## Sample Vendors

1E; ControlUp Technologies; HP Inc.; Ivanti; Lakeside Software; Nanoheal; Nexthink; Riverbed Technology; Tanium; VMware

## Gartner Recommended Reading

[How to Successfully Deploy a DEX Tool](#)

[Market Guide for DEX Tools](#)

[Employee Enablement Is Key to Digital Workplace Services Leaders' Survival](#)

## Digital Work Hubs

Analysis By: Joe Mariano, Gavin Tay

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

### Definition:

Digital work hubs are an assembly of ever changing team productivity and collaboration applications created for employees with diverse needs. It can be augmented with services for development, automation, artificial intelligence (AI) and analytics.

## Why This Is Important

Foundational work hub services (e.g., Microsoft 365, Google Workspace, etc.) have peaked in usage. However, gaps in these services continue demand for purpose-built work hub services (visual collaboration, collaborative work management, workstream collaboration, meeting services and content services platforms, etc.). In many cases these services are not deployed enterprisewide. Instead they are implemented at the domain or situational level to meet line of business strategic needs.

## Business Impact

The impact of effective work hub usage starts with productivity, but ends with opportunities to reduce cycle time and improve business results arising from more effective collaboration. This coordination via the hub can be especially helpful to citizen developers and business technologists working in fusion teams leveraging work hubs to meet organizational goals.

## Drivers

- Foundational work hub services, such as Google Workspace and Microsoft 365, have become the focal point of work hub application portfolios. However, IT leaders, business technologists and fusion teams are beginning to realize that they can't do everything for domain and situational needs. The impact on domain and situational work hub services means updating digital workplace charter to better align with strategic line of business needs.
- Executive leadership wants to exploit the value of work hub services long term, not just for the ROI, but to drive and enable employees' digital skills to help build digital side hustles and develop employees into business technologists.
- 2022 Gartner's Digital Worker Survey found participants on average use 11 different applications to get work done and more than 70% of the digital workers use between 6-25 applications at work. Also almost half of respondents struggled to find the information or data needed to do their job. IT leaders will need to better assess employees' needs and take greater care in creating digital employees and experience that streamline the use of multiple work hubs.

## Obstacles

- IT leaders think that a foundational work hub services will meet all their collaborative needs. In fact, best-of-breed services will be needed to meet the contextualized use cases of groups such as frontline workers, marketing and sales.
- The rate of additional functions added to work hub services has accelerated to the point that IT resource and business employees cannot keep up, which is limiting the overall value of tools.

## User Recommendations

- Assume that a single work hub vendor will not meet all your needs. In order to meet your digital employee experiences (DEX) goals it will take a combination of both foundational and domain or situational services.
- IT leaders must take on more of a collaborative role, working with business functions to understand the employee needs, especially with business technologists who can help drive new use cases and popularize digital workplace technology rather than IT working with one another.
- Use Gartner's ACME framework to govern usage efforts by focusing on domain and situational needs.
- Assess the technical fitness of your work hub applications to determine fit for purpose. If applications with similar functionality can be merged, better resource allocation can be reached. Deem the work hub to be a source of continuous innovation in a form that is relatively easy to adopt. Tie augmentation services (e.g., everyday AI, cross-tool integration and citizen development tools) to further growth in the value of the services.

## Sample Vendors

Alibaba; Google Workspace; Microsoft 365; Monday.com; Salesforce; Slack; Zoho

## Gartner Recommended Reading

[Video: Use Gartner's ACME Framework to Rationalize Your Digital Workplace Application Portfolio](#)

[Tool: Digital Employee Experience Journey Maps](#)

[Innovation Insight for Collaborative Workflow Automation](#)

## Generative AI

Analysis By: Svetlana Sicular, Brian Burke

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

### Definition:

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

### Why This Is Important

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

### Business Impact

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

## Drivers

- The hype around generative AI is accelerating. Currently, ChatGPT is the most hyped technology. It relies on generative foundation models, also called “transformers.”
- New foundation models and their new versions, sizes and capabilities are rapidly coming to market. Transformers keep making an impact on language, images, molecular design and computer code generation. They can combine concepts, attributes and styles, creating original images, video and art from a text description or translating audio to different voices and languages.
- Generative adversarial networks, variational autoencoders, autoregressive models and zero-/one-/few-shot learning have been rapidly improving generative modeling while reducing the need for training data.
- Machine learning (ML) and natural language processing platforms are adding generative AI capabilities for reusability of generative models, making them accessible to AI teams.
- Industry applications of generative AI are growing. In healthcare, generative AI creates medical images that depict disease development. In consumer goods, it generates catalogs. In e-commerce, it helps customers “try on” makeup and outfits. In manufacturing, quality inspection uses synthetic data. In semiconductors, generative AI accelerates chip design. Life sciences companies apply generative AI to speed up drug development. Generative AI helps innovate product development through digital twins. It helps create new materials targeting specific properties to optimize catalysts, agrochemicals, fragrances and flavors.
- Generative AI reaches creative work in marketing, design, music, architecture and content. Content creation and improvement in text, images, video and sound enable personalized copywriting, noise cancellation and visual effects in videoconferencing.
- Synthetic data draws enterprises’ attention by helping to augment scarce data, mitigate bias or preserve data privacy. It boosts the accuracy of brain tumor surgery.
- Generative AI will disrupt software coding. Combined with development automation techniques, it can automate up to 30% of the programmers’ work.

## Obstacles

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



## User Recommendations

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

## Sample Vendors

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

## Gartner Recommended Reading

[Innovation Insight for Generative AI](#)

[Emerging Tech Roundup: ChatGPT Hype Fuels Urgency for Advancing Conversational AI and Generative AI](#)

[Emerging Tech: Venture Capital Growth Insights for Generative AI](#)

[Emerging Tech: Generative AI Needs Focus on Accuracy and Veracity to Ensure Widespread B2B Adoption](#)

[ChatGPT Research Highlights](#)

## XLA

**Analysis By:** DD Mishra, David Groombridge, Karl Rosander

**Benefit Rating:** High

**Market Penetration:** 5% to 20% of target audience

**Maturity:** Adolescent

### **Definition:**

Experience-level agreements (XLAs) aim to drive better employee experience by leveraging a combination of digital experience monitoring (DEM), sentiment analysis and traditional service-level metrics to monitor the timeliness and effectiveness of supporting processes, while focusing on employee productivity and engagement.

### **Why This Is Important**

Modern workplace technologies are often delivered by multiple parties, which requires coordination. XLAs allow organizations to measure digital employee experiences in the workplace to improve end-to-end digital experience, thus eliminating digital friction and boosting workforce productivity.

### **Business Impact**

Traditional service desk and field services have proved to be of low value for a digitally dexterous workforce that expects organizations to provide a workplace that is engaging and adapts to modern work-from-anywhere user needs. Having XLAs that enable improvement in a modern digital workplace for employees is critical to attracting and retaining talent, especially in a world of hybrid work. Traditional SLA measures revolve around IT outcomes and have limited success in delivering and measuring business value, while XLAs are much more connected to business outcomes.

## Drivers

- Traditional IT-centric performance measures fail to capture the end-user experience properly, as they rely on specific data points that are a small component of overall user experience. Outcome-centric experience measures are required to fix this challenge.
- Digital experience (DEX) tools can measure each touchpoint in the overall user journey, which enables the implementation of XLAs and drives the motivation for capturing them. They should also incorporate some measure of user feedback such as traditional user experience surveys.
- The need for business-outcome-based performance measures also drives the adoption of XLAs. XLAs enable the impact of IT systems and services to be mapped directly to business KPIs, allowing the creation of outsourced service deals that contract for defined business outcomes. XLAs deliver more executive-level metrics.
- Outsourcing initiatives must demonstrate business value. Providers often drive this change within organizations. The ability to measure these elements needs to be prebuilt by service providers. The decision of which specific metrics to use should be made through co-creation with a provider. The aim is to bridge the gap between the intended business performance improvements and the services that will be delivered and measured through the XLA metrics.
- The key purpose of an XLA is to create a composite of metrics that are measured and combined together to create an IT or a business outcome resulting in an improved experience. The underlying metrics should measure individual factors that make up the user experience, such as network performance at the end-user device, endpoint performance, performance of the applications that are relevant to the specific intended experience objectives, time to access needed applications, and — critically — user sentiment.
- The impact of modern technology is driving XLAs as it is becoming much easier to monitor sentiment scores and draw conclusions using analytics.

## Obstacles

- **Lack of awareness:** Many enterprises are unaware of the existence of new outsourced digital workplace services and put out prescriptive RFPs asking for value-deprived legacy service desk and field service support. This often lacks the added value of focusing on the employee experience rather than operation efficiency.
- **Resistance to change:** Some enterprises are unwilling to embrace the workplace transformation required to improve the user experience.
- **Inability to leverage flexible dynamic sourcing approaches:** Many enterprises still rely on strict linear models that revolve around traditional RFI/RFP. This prevents them from co-creation and using flexible and iterative approaches to evolve the requirements.
- **Implementation cost:** The high initial cost of implementation due to deployment of tools is one of the limiting factors for some clients who are more cost-focused than value-focused.
- **Implementation time:** The implementation of XLAs often requires a lot of preparation and due diligence along with change management, which extends the implementation time and discourages clients from taking the next steps.

## User Recommendations

- Identify and configure XLAs that measure end-to-end user experience by including more than simple timeliness and technical metrics. The key to success is to implement monitoring that focuses on the employee experience, not on what the service provider or internal IT organization is responsible for delivering.
- Select partners with a strong track record in process mapping, analytics and digital experience monitoring by prioritizing providers that have demonstrated referenceable business improvement from ongoing XLA delivery.
- Improve internal operations by identifying the leading causes of employee dissatisfaction with IT services and addressing them with a series of XLAs.
- Implement a governance mechanism which is typically an experience management office (XMO) for managing, monitoring and evolving the XLAs who will work closely with provider and/or internal organizations to identify XLAs, develop improvement plans and provide stakeholder involvement and governance to the implementation.
- Ensure that contracts are structured properly to accommodate the changes required from governance and implementation of XLAs.

## Gartner Recommended Reading

[Magic Quadrant for Outsourced Digital Workplace Services](#)

[Infographic: Digital Workplace Innovation Impact Matrix](#)

[Innovation Insight for the Digital Employee Experience](#)

[Market Guide for Digital Experience Monitoring](#)

[Infographic: The Five Essential Components of an XLA](#)

## IT/OT/ET Alignment

Analysis By: Kristian Steenstrup, Marc Halpern

**Benefit Rating:** High

**Market Penetration:** 1% to 5% of target audience

**Maturity:** Emerging

**Definition:**

IT/OT/ET alignment is the coordination of information technology (IT), operational technology (OT), and engineering technology (ET) through shared standards and governance. Each plays a complementary role to the other two technologies. While IT records transactions and business processes, OT operates and monitors industrial assets, and ET is used to define, design, simulate, analyze, visualize and validate those assets (e.g., GIS, computer-aided design and manufacturing [CAD]/CAM).

**Why This Is Important**

For asset-intensive industries, system interoperability is improved when OT, ET and IT systems and processes share infrastructure and planning. This also enhances the agility to change configurations to adapt to market demands, improve product quality and optimize productivity. As a result, organizations seek common architecture plans and standards for the technology acquired, and increasingly look for vendors that support this direction. Most companies are at least beginning this exercise.

**Business Impact**

The impact of IT/OT/ET alignment is mainly focused on four aspects:

- More efficient use of technology and support resources across IT, OT and ET investments.
- Easier sharing of data from design documents (ET) to operational systems (OT) and business administration, supporting digital threads and digital twins.
- Easier sharing of performance data from OT into the ET process for design and improvement.
- Consistent security and risk management across all technology.

## Drivers

- Cost reduction by not duplicating licensing, maintenance and support for common software components.
- Cost optimization by consolidating via cloud, virtualization or colocating servers and back-end hardware in a common data center.
- Agility by being able to start new hybrid IT/OT/ET projects quicker and reacting to changes in a consistent way.
- Risk avoidance by aligning security, patching, disaster recovery and upgrading processes.
- Benefits of using the same support and configuration tools, support contracts, and purchase processes.
- Process and information sharing between domains driving collaboration and cross-pollination of practices and approaches, leading to effective management of digital threads.
- Easier access to ET and OT data for IT analysis such as digital twins, predictive maintenance and production optimization.
- Leveraging OT performance data in product development using ET systems.
- Designing of systems via ET that better cater to OT effectiveness, and future OT system support and data acquisition.

## Obstacles

- Coordination between three domains is complex technically and politically. Different cultures and approaches of IT departments, manufacturing/operations and design/engineering need to be reconciled.
- There may be a possible temporary increase in cost on the OT or ET side initially, as technology investments are made to bring software up to the required IT standard/version and to deal with any license compliance gaps.
- The lack of common tools for software asset management (SAM) that caters for IT and OT technology makes centralized control difficult.
- The absence of short-term benefits in terms of cost avoidance make project approval more challenging.
- The entrenched separate positions and practices associated with OT and ET systems, and their criticality, safety and stability, means that realignment takes time.
- Aligning risk appetite and security requirements across three domains with different pedigrees increases the effort needed to identify and manage risk and security.

## User Recommendations

- Get agreement on a change imperative, so you have a mandate for change.
- Establish a common governance model across the three domains.
- Evaluate technology management processes to determine how much IT process is applicable to OT and ET, how the unique needs of OT and ET must be recognized and supported, and how to get them aligned and secured by design.
- Incorporate OT and ET requirements in enterprise risk management by adopting an integrated security strategy across IT, OT, ET, physical security and cyber-physical systems (CPS) for greater visibility.
- Create combined hardware platform and architecture policies to ensure compatibility between IT, OT and ET systems by formulating compatible governance for software, communications, and infrastructure.
- Use a responsible, accountable, consulted and informed (RACI) analysis to help manage this transition, and to map out organizational responsibilities for different parts of the technology environment.



## Sample Vendors

Bentley Systems; Dassault Systèmes; PTC; Siemens

## Gartner Recommended Reading

[2022 Strategic Roadmap for IT/OT Alignment](#)

[What Should I Know About OT Security?](#)

[How IT Standards Can Be Applied to OT](#)

[Survey Analysis: IT/OT Alignment and Integration](#)

[When Does a CIO Need to Be Involved in OT?](#)

## Sliding into the Trough

### Peer IT Support

Analysis By: Chris Matchett

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

#### Definition:

Peer IT support occurs when business consumers get technical support and advice from other employees at Level 0 (self-service) before (or instead of) contacting a Level 1 IT service desk. This commonly takes place unofficially via forums and collaboration tools, or in person.

#### Why This Is Important

Peer IT support is happening in many places, but it is often organic and informally defined. This is happening in both the consumer world — on commercial product support forums and social networking sites — and also in companies, where application and product teams have already set up their own forums, and collaborative support hubs.

#### Business Impact

Peer IT support can have the following impacts:

- Peer support decreases the workload of Level 1 and 2 support teams, reduces costs and enables the IT service desk to concentrate on other activities.
- Incident resolution can be expedited when the expertise resides outside the IT organization.
- Peer support encourages non-IT employees to develop digital dexterity and share best practices, which supports organizational goals around building digital skills and competencies.

#### Drivers

- The consumerization of IT is increasing digital dexterity within the business consumer community, leading to some employees choosing and supporting IT applications directly.
- The 2022 Gartner Digital Worker Survey found that younger digital workers prefer engaging with colleagues for support questions more than contacting the IT service desk.
- Infrastructure and operations (I&O) leaders' interest in peer support increased to ease the IT service desk workload.
- Employees found it easier to support each other and engage with IT support using collaborative work management (CWM) tools (see [Market Guide for Collaborative Work Management](#)).
- Some IT service management (ITSM) platform vendors are beginning to provide features that facilitate peer IT support.

## Obstacles

- I&O leaders have been slow to introduce formal channels and similar collaborative support hubs (see [Transform IT Support by Developing Collaborative Support Hub Roles and Competencies](#)).
- Older digital workers still prefer to contact IT via traditional support channels.
- Some business leaders don't want non-IT employees spending work time on IT issues.
- Hybrid work models have reduced the convenience of being able to ask a nearby peer for help.
- ITSM platform integration into tools for collaboration hubs is not yet generally available, and lack of features pushes I&O leaders to rely on the service desk for full management oversight and simplicity.

## User Recommendations

- Analyze the preferences and requirements of business consumers before offering new support channels.
- Seek out unofficial peer IT support that is already occurring in your organization. These may coincide with influencers or champions networks.

- Establish collaborative support hubs to empower peer IT support for compatible audiences.
- Solicit collaboration features from your ITSM platform vendor or use existing CWM tools to facilitate and track the interactions.
- Interface with the IT knowledge management (KM) processes to discover common issues, and update the knowledge base where needed.
- Identify and reward employees that provide peer IT support.
- Utilize gamification to promote additional participation.

## Gartner Recommended Reading

[Don't Abuse Business Users for Peer-to-Peer IT Support](#)

[Transform IT Support by Developing Collaborative Support Hub Roles and Competencies](#)

[Innovation Insight for Collaborative Support Hub](#)

[Tailor Your IT Service Desk Support Based on Business User Personas](#)

[How to Build and Manage a Digital Workplace Influencers Network](#)

## Site Reliability Engineering

Analysis By: George Spafford, Daniel Betts

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

### Definition:

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

## Why This Is Important

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

## Business Impact

The SRE approach to improving reliability and resilience 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 the reliability of existing products/platforms or to create new products or platforms that need reliability from the start.

## Drivers

- Clients are under pressure to meet customer requirements for reliability while scaling their digital services and are looking for guidance to help them.
- While Google originated what became known as SRE and continued to evolve it, practitioners are developing and sharing new practices as well. Potential practitioners looking for pragmatic guidance to improve the reliability of their systems have a rich body of knowledge they can leverage that works well with agile and DevOps.
- Organizations are adopting highly skilled automation practices (usually DevOps), and usage of infrastructure-as-code capabilities (which usually requires a cloud platform) to deliver digital business products reliably.
- The most common use case based on inquiry calls with clients is to leverage SRE concepts to improve the reliability of existing systems that are not meeting customer requirements for availability, performance or are proving difficult to scale.

## Obstacles

- Insufficient internal marketing to understand what agile, DevOps or product teams need or would value and then explaining how the value SRE can deliver will justify the costs and risks incurred. Without marketing its benefits, SRE adoption tends to be less certain or slower. The SRE concept by itself is insufficient — people must continuously believe it is worthwhile.
- Finding SRE candidates who have the right mix of development, operations and people skills is a big challenge for clients. Impacts on initial adoption and scaling efforts as well.
- Rebranding of a traditional operations team without changing to adopt SRE practices, only SRE in name.
- Clients have voiced problems with product owners who overly focus on functional requirements and not nonfunctional requirements thus slowing improvements and support of SRE within the organization.

## User Recommendations

- Leverage practices pragmatically based on need. Don't feel that you must implement SRE exactly the way Google does it, learn what works for you.
- Detect an opportunity to begin that is politically friendly, will demonstrate sufficient value and has an acceptable risk profile.
- Start small, focus, learn, improve, and demonstrate value — do not try to change everything at once.
- Work with the customer or product owner to define clear, obtainable SLOs based on their needs.
- Implement monitoring and improve observability to objectively report on actual performance relative to the SLOs.
- Product owners must be accountable for functional and non-functional requirements of their products.
- Instill collaborative working between site reliability engineers, developers and other stakeholders to help them learn how to design, build and evolve their products to meet SLOs.
- Create a community, implement effective organizational learning practices and evolve SRE practices.

## Sample Vendors

Atlassian; Blameless; Datadog; Dynatrace; New Relic; OpsRamp; PagerDuty; Splunk

## AI/ops Platforms

Analysis By: Matt Crossley, Matthew Brisse

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

## Definition:

Gartner defines AIOps platform as the application of AI/ML and data analytics at the event management level in order to augment, accelerate and automate manual efforts in the event management process and associated procedures. AIOps platforms are defined by the key characteristics of cross-domain event ingestion, topology assembly, event correlation and reduction, pattern recognition, and remediation augmentation.

## Why This Is Important

The combination of increasing application complexity, monitoring tool proliferation, and increasing volumes and varieties of telemetry has shifted complexity from gathering data to interpreting data. AIOps platforms apply machine learning (ML) and data analytics to classify and cluster cross-domain events in near real time, at scale, and in ways that can exceed human capacity. These inferences can augment human analysis, accelerate human response, or automate a process to resolve an issue.

## Business Impact

AIOps platforms deliver value through:

- **Agility and productivity:** By reducing alert fatigue through identification and correlation of related events, operators can focus on fewer, more critical events.
- **Service availability and triage cost:** By reducing the time and effort required to identify root causes and augmenting, accelerating, or automating remediation.
- **Increased value from monitoring tools:** By unifying events from siloed tools and learning actionable event patterns across domains.

## Drivers

Demand for AIOps platform capabilities is accelerating and is fueled by:

- **Increasing complexity:** Organizations use an increasingly complex mix of IT assets that rely on a highly integrated combination of on-premises assets, cloud IaaS/PaaS providers and SaaS platforms to deliver solutions.



- **Increasing monitoring expectations:** Investments and improvements in monitoring and the pursuit of observability are generating more data from more sources. Increasing demand and advances in monitoring trends, like application performance management (APM) and digital experience monitoring (DEM), present operators with extremely detailed views into their business applications and the end-user experience. Effective use of this additional data requires near-real-time analysis and rationalization of events from related assets and services.
- **Demands for reliability:** Shifts in roles and responsibilities driven by modern operating models, like DevOps and SRE, in the pursuit of greater availability and faster incident resolution. AIOps platforms enable agility by offloading some of the mechanical tasks of event triage, root cause analysis and solution identification. This both accelerates response for common issues and frees up human creative capacity for novel events and business priorities.

## Obstacles

- **Unrealistic expectations:** Hype is a major obstacle to AIOps platform adoption. Clients struggle to separate claims of AI and magical automation from achievable use cases. This impacts demonstrating value of AIOps platforms, specifically quantifiable return on investment.
- **Maturity of dependencies:** Benefits of AIOps platforms beyond event correlation requires maturity in dependencies such as automation.
- **Time to value:** AIOps platforms learn through observation, modeling normal data patterns, and associate a solution with these patterns. This can take time depending on the frequency of occurrence. Developing accurate detection models for rare events can take months.
- **Market shifts and maturity:** Monitoring vendors are moving up the stack, AIOps platform vendors are reaching into monitoring domains, and ITSM vendors use AIOps capabilities to extend their reach. Expect further convergence and market shifts to change the definition of “state of the art.”

## User Recommendations

- Establish clear, realistic use cases for an AIOps platform pilot and validate them individually, rather than all at once. This approach helps reveal pockets of potential value that might be missed when evaluating only the aggregate impact. Ultimately, this fundamental step underpins an eventual strategy, while scoping the vendor landscape, clarifying technical and process dependencies, and separating hype from reality.
- Layer the AIOps features within monitoring tools with the cross-domain analysis of an AIOps platform. This approach enables efficient data ingestion and analysis, and the surfacing of insights across domains.
- Do not require automation outcomes for all AIOps applications. There is tremendous value in accelerating and augmenting human activity. These approaches often avoid the challenge of the probabilistic uncertainty combined with automated change in production environments.

## Sample Vendors

BigPanda; BMC Software; Digitate; IBM; Interlink; Moogsoft; OpsRamp; PagerDuty; ServiceNow; Splunk

## Gartner Recommended Reading

[Market Guide for AIOps Platforms](#)

[Deliver Value to Succeed in Implementing AIOps Platforms](#)

[Infographic: Artificial Intelligence Use-Case Prism for AIOps](#)

[Infographic: AIOps Architecture for Analyzing Operational Telemetry](#)

[How Do I Plan for Migrating My Data Center Infrastructure Into an XaaS Model?](#)

## Multiexperience

Analysis By: Tigran Egiazarov

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

**Maturity:** Adolescent

**Definition:**

Multiexperience (MX) describes interactions that take place across a variety of digital touchpoints (i.e., web, mobile apps, conversational apps, AR, VR and wearables), using a combination of interaction modalities in support of a seamless and consistent digital user journey. Modalities include text, voice, vision and gesture. Multiexperience is part of a long-term shift from the individual computers that we use today to a multidevice, multisensory and multilocation ambient computing experience.

**Why This Is Important**

Through 2030, the digital user experience (UX) will undergo a significant shift in terms of how consumers, partners, citizens and employees experience their environments. MX represents a shift in both UX perception and interaction models — creating a multisensory, multidevice, multilocation and multitouchpoint digital journey for the user.

**Business Impact**

To achieve digital business transformation, it is essential to understand and exploit multiexperience. Applying multiexperience design to digital experiences removes friction and effort for the users — both customers and employees. MX delivers positive business outcomes by serving customers and employees in ways that best suit their needs and expectations. Adopting MX enables optimization and reuse of business capabilities, implementation components and data.

## Drivers

- Organizations are shifting their delivery models from projects to products, but beyond products is the experience — the collection of feelings, emotions and memories. Web and mobile apps are already commonplace, but they are undergoing UX changes driven by new capabilities like progressive web apps, WebXR and artificial intelligence (AI) services. Conversational platforms, powered by Generative AI such as ChatGPT, allow people to interact more naturally and effortlessly with the digital world. Reinforced by hardware innovations and AI, immersive technologies such as virtual reality (VR), augmented reality (AR), mixed reality (MR) and the metaverse are changing the way people interact with and perceive the physical-digital world.
- As organizations continue to invest in customer experience (CX) and employee experience (EX), they will need to apply MX front-end architecture and technology strategies to be more agile at serving business needs and user expectations. When MX discipline is applied with great UX in support of CX and EX strategies, total experience (TX) transformation is achieved. TX requires MX to be executed with CX, EX and UX in harmony and synchronicity.
- The long-term manifestation of MX is a composable digital experience that is adaptive, seamless, collaborative, consistent, personalized and ambient. Design and architecture patterns, such as micro-front-ends, backends for frontends and superapps are important enablers.
- Greater availability of development technologies to build for multiexperience more easily, including multiexperience development platforms, digital experience platforms and cross-platform frameworks (i.e., Flutter, .NET MAUI, React Native, Vue Native).

## Obstacles

- Privacy and security concerns may dampen the enthusiasm and impact of MX adoption. Multiple devices or digital touchpoints with different levels of security capabilities will increase risk of security breaches.
- On the technical front, the fragmentation of many consumer devices and the inconsistency of interoperability standards are enormous barriers to seamless MX integration of front-end technologies. Legacy noncomposable and non-API-ready service architecture makes those barriers even higher.
- The cost and effort, required for implementing MX, often do not justify the benefits of the resulting output.
- The skills needed for MX development, such as immersive interaction design, are still lacking in most enterprise software engineering teams.
- Currently, automatic plug and play of off-the-shelf devices, applications and services is not feasible for MX. Instead, proprietary hardware and software ecosystems of MX solutions will exist in the near term.

## User Recommendations

- Identify three to five high-value pilot projects in which MX design can lead to more effortless, compelling and transformative experiences, such as e-commerce, healthcare, frontline workers and edge computing.
- Evaluate business applications, frameworks and platforms, such as field service management and digital experience platforms, for their native MX capabilities and support for custom MX development.
- Collaborate with UX design teams to create a design system that spans desired MX touchpoints and modes of interaction.
- Establish a multidisciplinary fusion (product) team including (but not limited to) IT, product managers, UX designers and business stakeholders.
- Invest in modern service architecture and technologies to ensure a seamless integration between MX applications with back-end services through APIs.
- Focus on understanding how unified digital experiences impact the business, and use evolving MX technologies to create targeted solutions for customers, partners and staff.

## Gartner Recommended Reading

[Adopt a Mesh App and Service Architecture to Power Your Digital Business](#)

[Market Guide for Multiexperience Development Platforms](#)

[2023 Strategic Roadmap for Adopting Modern Application Architectures and Technologies](#)

[How to Make the Right Technology and Architecture Choices for Front-End Development](#)

## Infrastructure Automation

Analysis By: Chris Saunderson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

### Definition:

Infrastructure automation (IA) enables DevOps and infrastructure and operations (I&O) teams to deliver automated infrastructure services across on-premises and cloud environments. This includes the life cycle of services through creation, configuration, operation and retirement. These infrastructure services are then made available through platform delivery, self-service catalogs, direct invocation and API integrations.

### Why This Is Important

IA delivers velocity, quality, efficiency and reliability, with scalable, declarative approaches for deploying and managing infrastructure. These tools integrate into delivery pipelines targeting deployment topologies that range from on-premises to the cloud, and enable infrastructure consumers to build what is needed when they need it. Once deployed, IA provides day-2 and beyond operational automation, and extends to provide policy compliance and enforcement capabilities.

### Business Impact

Implementing and maturing IA services will enable:

- **Agility** — continuous infrastructure delivery and operations

- **Productivity** — version-controlled, declarative, repeatable, efficient deployments
- **Cost improvement** — reductions in manual effort expended via increased automation
- **Risk mitigation** — compliance driven by standardized configurations
- **Collaboration** — delivering environments that product teams need with security, cost and compliance requirements baked in.

## Drivers

I&O leaders must automate delivery through tool and skills investments to mature beyond simple deployments. The target should be standardized platforms that deliver the systemic, transparent management of platform deployments. This same discipline must be applied to the operation of these deployed platforms, ensuring that efficient operations (including automated incident response) can be achieved. IA tools deliver the following key capabilities to support this maturation:

- Multicloud/hybrid cloud infrastructure delivery
- Support for immutable and programmable infrastructures
- Predictable delivery enabling automated operations
- Self-service and on-demand environment creation
- Integration into DevOps initiatives (continuous integration/delivery/deployment)
- Resource provisioning, including cost optimization capabilities
- Operational configuration management efficiencies
- Policy-based delivery and assessment/enforcement of deployments against internal and external policy requirements
- Enterprise-level framework to enable maturing of automation strategies
- Skills and practice development inside infrastructure teams, enabling agile and iterative development and sustaining of services

## Obstacles

- The combination of tools needed to deliver IA capability can increase tool count and complexity.
- Software engineering skills and practices are required to get maximum value from tool investments.
- IA vendor capability expansion overlaps and confuses the tool landscape, resulting in over-investment.
- Steep learning curves can cause developers and administrators to revert to familiar scripting methods to deliver required capabilities.

## User Recommendations

- Identify existing IA tools in use to catalog capabilities, identify use cases and document overlaps to aid decision making.
- Assess existing internal IT skills to incorporate training needs that more fully enable IA, especially for an automation architect role to coordinate standards development and implementation.
- Baseline how managed systems and tooling will be consumed (e.g., engineer, self-service catalog, API or on-demand).
- Integrate security and compliance requirements into scope for automation and delivery activities.
- Develop an IA tooling strategy that incorporates current needs and near-term roadmap evolution.

## Sample Vendors

Amazon Web Services; HashiCorp; Microsoft; Perforce; Pliant; Progress; Pulumi; RackN; Upbound; VMware

## Gartner Recommended Reading

[Market Guide for Infrastructure Automation Tools](#)

[Innovation Insight for Continuous Infrastructure Automation](#)



To Automate Your Automation, Apply Agile and DevOps Practices to Infrastructure and Operations

How to Start and Scale Your Platform Engineering Team

## Virtual Support Agents

Analysis By: Chris Matchett

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

### Definition:

Virtual support agents (VSAs) are conversational agent applications that deliver information, provide answers to common questions and perform transactions to provide IT support to business consumers in an IT service management (ITSM) scenario. They are an IT-support-specific subset of virtual assistants that use chatbot capabilities, but also take actions such as reset passwords, deploy software, escalate support requests and execute scripts to restore IT services.

### Why This Is Important

ITSM platform vendors commonly leverage simple capabilities they see as good enough to meet a chatbot requirement in a competitive bid. These tools often require considerable manual effort to manage. A submarket of third-party vendors specializing in VSAs that integrate to ITSM platforms emerged, with claims of more sophisticated AI capabilities, which compete against the ITSM vendors. Large language models (LLMs) and generative AI have dominated this topic in 2023.

### Business Impact

VSAs can displace some of the incoming call and live chat volume (with knowledge-base articles transcribed into Q&A), alongside traditional live agent intake channels. Advanced implementations enable the execution of more complex task-based actions (e.g., software request and installation). VSAs add value by reducing time to resolution, saving steps by leveraging contextual information or offering extended support hours without increasing staff. Staffing costs can also be controlled or reduced.

## Drivers

- Cost optimization drives I&O leaders to identify new efficiencies, while necessitating cuts to services using human agents.
- We saw a marked increase in the number of I&O leaders evaluating features and pricing of VSA capabilities of ITSM platforms and stand-alone products through 2022.
- Early adopters report successful rollouts of VSAs in their environment.
- ITSM platform vendors continue to invest in and roll out chatbot capabilities and partnerships in response to customer demand. Several have launched or are about to deploy LLM technologies, including GPT.

## Obstacles

- The 2022 Gartner Digital Worker Survey revealed that comparatively few employees prefer to use a VSA for their support needs, although this number is rising. (The online survey was conducted from September through November 2022 among 4,861 respondents from the U.S., China, the U.K. and India.)
- Many organizations are surprised and deterred by the level of manual scripting and integrations needed to achieve results with many of the products currently in the market.
- Add-on VSA products can be expensive, and this cost will be in addition to ITSM platforms that may already have similar — albeit lesser — features.
- Genuine VSA offerings are uncommon, as many sold as chatbots for IT support are actually general virtual assistant platforms that require further development. In many cases, the natural language processing (NLP) capabilities and AI benefits in improving outcomes are limited.
- Many vendors and marketers use key terms and concepts interchangeably, leaving buyers confused.

## User Recommendations

- Determine employee interest by observing consumer trends outside the digital workplace and through direct engagement, including surveys, focus groups and product demos with employees. Digital employee engagement and demographics will influence adoption potential.
- Invest when the long-term benefits of efficiency and additional contact channels outweigh any short-term negative impact on engagement.
- Focus on high-impact use cases (driven by high volume or business criticality) to ensure ongoing commitment toward VSAs.
- Invest in VSAs that offer multiple ways to engage with users (such as being accessible in the portal as well as within collaboration tools).
- Target the needs of specific employee segments where the capability truly matches the need. Avoid a “can do anything” approach that will fall short of expectations.
- Ask VSA vendors how they can provide LLM technologies, while mitigating the risks of “hallucination” (i.e., generated errors or nonsense) and privacy.

## Sample Vendors

Aisera; Espressive; Moveworks; ServiceNow

## Gartner Recommended Reading

[Innovation Insight for Virtual Support Agents](#)

[Leverage 4 Domains of AITSM to Evolve ITSM Tools and Practices](#)

[Critical Capabilities for Enterprise Conversational AI Platforms](#)

[Magic Quadrant for Conversational AI Platforms](#)

[Applying AI — Business Domains](#)

## Vulnerability Prioritization Technology

Analysis By: Mitchell Schneider, Craig Lawson

Benefit Rating: High

**Market Penetration:** More than 50% of target audience

**Maturity:** Mature mainstream

**Definition:**

Vulnerability prioritization technology (VPT) streamlines a range of vulnerability telemetry sources into a single location – using intelligence sources, analytics and visualizations and to efficiently provide prioritized, pragmatic recommendations on how best to perform critical remediation/mitigation activities. The approach considers the exploitability of a vulnerability, asset or business-criticality, the severity of a vulnerability and compensating controls in place.

**Why This Is Important**

VPT supports a risk-based vulnerability management (RBVM) approach. These products and services provide a consolidated view of exposures by leveraging the telemetry from sources, including vulnerability assessment (VA) tools, configuration management databases (CMDBs), endpoint detection and response (EDR), penetration testing results and application security testing (AST). VPT adds intelligence and efficiency by leveraging analytics and various threat and vulnerability intelligence sources.

**Business Impact**

VPT is a form of automation that leverages data science, advanced analytics and vulnerability intelligence to improve VA and prioritization, and rapidly identify the highest-risk exposures for remediation. Moreover, VPT provides the ability to track the VM life cycle via a centralized view. The increase of security incidents and breaches drives many organizations to adopt VPT solutions to implement an effective VM program. This has also caused VA vendors to align more to the RBVM methodology.

## Drivers

- Organizations are inundated with vulnerability findings prioritized solely by Common Vulnerability Scoring System (CVSS) scores. VPT solutions contextualize these findings with active threat information, resulting in increased actionability. For example, a vulnerability that is a low risk today might be a high-impact vulnerability tomorrow due to the dynamic changes driven by attackers, while the CVSS score would remain relatively static.
- Interest in the VPT market has accelerated within the last 12 months, according to Gartner research and client inquiries. VPT identifies more pragmatic risks to the organization and helps prioritize actions for vulnerability treatment — whether via remediation (e.g., patching) and/or compensating controls (e.g., intrusion prevention system [IPS] and web application firewalls [WAFs]) — to avoid potential compromise or beginnings of a breach.
- VPT can provide savings in terms of operational full-time employee (FTE) costs due to the automation of vulnerability prioritization, which facilitates attack surface reduction efforts, and results in improved continuity of operations. This is especially beneficial for organizations looking to retain talent by focusing them on more value-added activities.
- The need to take more proactive security actions is offered through other forms of vulnerability prioritization, such as attack path mapping. Attack path mapping is understanding if and how the attacker targets your organization, and what path they could potentially take to get in — uncovering paths to high value assets and contextualizing vulnerabilities risks.

## Obstacles

- VPT solutions require a more mature vulnerability management program to be effective. If there are broken processes in the exposure management program, the value of VPT will be limited.
- Organizations that are fixated on CVSS severity as the defining characteristic of how serious a vulnerability is will not be able to get full value from VPT approaches since that metric-driven output is rarely based on risk — as factors like threat activity, asset context and existing security controls are not considered.
- There are overlapping capabilities between VPT and cyber asset attack surface management (CAASM), leading to buyer confusion. CAASM is focused on aggregation of data and visibility, while VPT is focused on improving an organization's RBVM operational processes.
- Attack path mapping is an output of vulnerability prioritization and breach and attack simulation (BAS) to support cybersecurity validation initiatives, but is different from testing security controls. Your organization may already have this capability via another tool.

## User Recommendations

- Implement a risk-based approach that correlates asset value and business impact to calculate a risk rating, and automate this through a VPT.
- Augment VA tools with stand-alone VPT solutions for better prioritization, or use existing VPT capabilities that assist with the effective methodology for real risk reduction. This enables vendor consolidation and places less effort on new training and tool deployment.
- Identify vendors with patching and SOAR integrations. This puts the security team in control of workflows. Evaluate if this approach is appropriate. If so, leverage remediation workflow automation and avoid using two different tools.
- Deploy VPT that takes into account the presence (and configuration) of existing security controls to enhance prioritization efforts. This capability is increasing across the market.
- Identify vendors with CAASM capabilities, or who have connectors with your CAASM to better integrate the two products to solve both visibility and improve operational processes.

## Sample Vendors

Brinqa; Cisco; Flashpoint; HivePro; Ivanti; NopSec; NorthStar; Nucleus Security; ServiceNow; Skybox Security

## Gartner Recommended Reading

[How To Implement a Risk-Based Vulnerability Management Methodology](#)

[Tracking the Right Vulnerability Management Metrics](#)

[Quick Answer: What Are the Top and Niche Use Cases for Breach and Attack Simulation Technology?](#)

[Innovation Insight for Attack Surface Management](#)

## SOAR

Analysis By: Eric Ahlm, Craig Lawson

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

### Definition:

Gartner defines security orchestration, automation and response (SOAR) as solutions that combine incident response, orchestration and automation, and threat intelligence (TI) management capabilities in a single solution. SOAR tools can be leveraged for many security operations tasks, such as documenting and implementing processes, supporting security incident management, applying machine-based assistance to human security analysts and operators, and better operationalizing the use of TI.

### Why This Is Important

SOAR tools are flexible and can be applied to various security operations centers (SOCs) and broader SecOps use cases. Current buyers tend to be end-user organizations and security services providers with a SOC function that are looking to optimize the efficiency, consistency and effectiveness of their threat monitoring, detection and incident response activities. Threat management use cases for SOAR are still emerging.

## Business Impact

SOAR solutions can help clients:

- Reduce errors in handling incidents by codifying activities.
- Scale security operations by adding efficiency in handling various tasks and activities.
- Improve SOC team morale and reduce analyst turn over by removing repetitive tasks from humans.

## Drivers

- SOAR can improve the process and execution speed of repetitive tasks that often torment SOC teams, especially tasks that consume time and require little human expertise. This frees teams to spend more time on critical tasks and activities.
- SOAR can increase alert fidelity and actionability by adding more context and data enrichment. This helps reduce noise due to the high volume of alerts that needs to be handled by the SOC team.
- Security orchestration and automation (SOA) as a capability is increasingly needed by security operations. SOAR solutions offer flexible SOA in the platform. However, SOA is also becoming more available as canned, baked-in functionality in other security technologies, such as email security solutions, to help improve both analysis and triage, and automate responses to threats.

## Obstacles

- SOAR requires both development and ongoing operational cycles to maintain, similar to other coding development practices. As such, not all activities will warrant the investment in SOAR development and maintenance.
- SOAR and automation is best applied to existing practice and activities. Clients wanting to use SOAR for building new activities in the SOC may find the time to value is much longer than expected.
- Justifying the expense of automation and a SOAR purchase remains an obstacle for clients. The value of automation is best described in the language of gains into existing areas of operations.



## User Recommendations

- Assess the availability of development skill sets internally to develop SOAR's required functionality. Security leaders should also review the time and cost this may add to the total cost of owning an SOAR toolset.
- Involve the entire security organization when scoping requirements for SOAR. Organizations must look beyond simply plugging a new technology into security information and event management (SIEM), and engage with wider security.
- Select an appropriate product based on buyer understanding and its applicable use cases, such as SOC optimization, threat monitoring and response, threat investigation and hunting, and TI management.
- Implement well-defined processes and playbooks before acquiring SOAR. Although SOAR promotes lots of benefits, not every security organization is ready for SOAR tools, and a considerable amount of time is required to develop playbooks.

## Sample Vendors

Cyware; D3 Security; Google; Palo Alto Networks; Rapid7; ServiceNow; Splunk; Swimlane; Tines; Torq

## Gartner Recommended Reading

[SOAR Will Not Make You Better at Running SIEM](#)

[Market Guide for Security Orchestration, Automation and Response Solutions](#)

## Walk-Up IT Support

Analysis By: Siddharth Shetty

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

**Definition:**

Walk-up IT support is a formal face-to-face support channel that offers a location where business consumers can interact with IT personnel. Walk-up centers provide standard support services, such as break/fix, troubleshooting and “how to” support through prescheduled appointments or ad hoc requests. Walk-up centers can also serve a broader function with services such as new-hire onboarding, technology training, education around new IT offerings, marketing and other available IT services.

**Why This Is Important**

The consumerization of IT and the shift toward mobility continue to develop expectations of IT support. Walk-up IT support offers an opportunity to improve business consumer satisfaction among users. As organizations evolve to offer greater flexibility to employees about where they can work from, IT walk-up centers are also expected to adapt to the needs of an increasingly mobile workforce.

**Business Impact**

Walk-up IT support applies to large worksites, where support can be provided in person, usually during business hours only. This is particularly helpful for mobile users as they can bring their smartphones, laptops and tablet devices for in-person troubleshooting. Walk-up centers can also improve the experience of onboarding and training for self-service. Walk-up IT support is part of the omnichannel strategy to support business users.

**Drivers**

- Increasing staff engagement and IT responsiveness by helping business users in real time. It helps users associate real people with IT, which provides a better connection to IT. Hence, this provides an improved experience to business users.
- An enhanced experience for on-site employee onboarding, showcasing (and receiving feedback on) new technologies and devices, and/or conducting in-person training and how-to's.
- Easier access to directly issue and/or troubleshoot hardware, such as mobile devices and peripherals (e.g., headsets, laptops and mice).
- Replacing informal habits of employees walking up to IT personnel desks for support by meeting this business consumer demand through more-formalized processes.

- Periodically or temporarily providing support for smaller worksites or special events (such as an annual meeting) when remote workers are being brought on-site. Temporary walk-up support centers (via a booth or pop-up table) can be set up for limited, predetermined windows or one-time use in common areas or conference rooms.
- Walk-up IT support complements the IT service desk during peak business hours.
- Walk-up IT support can play an important role for organizations that offer a hybrid work model for their employees. Employees that usually work remotely can engage with walk-up IT support when they are on-site to address issues with their equipment or workplace applications in an efficient way.

## Obstacles

- Walk-up IT support does not reduce costs or increase scalability. The cost of building out the infrastructure (including the office space, furniture and automation tools required) and staffing with the necessary skill sets often requires an initial capital investment.
- With more organizations adopting hybrid work models, there has been a slippage in the number of tech employees dedicated to IT walk-up support. Where walk-up IT support still exists, their role has evolved to supporting break-fix issues and employee onboarding on specific days of the week.

## User Recommendations

- Choose IT walk-up support only when a critical mass of employees are operating from an office campus at some point. Organizations that do not run at full capacity due to a hybrid work model (resulting in lesser employee footfall) can offer walk-up IT support on specific days of the week, instead of a full-time commitment.
- Encourage appointment-based walk-ins, where possible, to gauge demand and staff walk-up IT support accordingly.
- Identify locations, where possible, that are easily accessible and with high business consumer activity to generate increased foot traffic, such as near the cafeteria. Consider walk-up support for large office campuses only for maximum impact.
- Add vending machines to dispense fast-moving IT equipment such as mice, keyboards, webcams, headsets and so on to reduce this transactional activity at walk-up support.

- Implement smart lockers for quick drop or pickup of equipment without the need for the physical handover of the equipment.

## Gartner Recommended Reading

[5 Best Practices to Create a Successful IT Walk-Up Center](#)

## Climbing the Slope

### Continuous Delivery

Analysis By: Hassan Ennaciri

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

#### Definition:

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

#### Why This Is Important

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

#### Business Impact

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

#### Drivers

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

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

## Obstacles

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

## User Recommendations

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

## Sample Vendors

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

## Gartner Recommended Reading

[How to Build and Evolve Your DevOps Toolchains](#)

[Market Guide for Value Stream Management Platforms](#)

[Beware the DevOps Toolchain Debt Collector](#)

## IT Support Live Chat

Analysis By: Chris Matchett

Benefit Rating: Moderate

Market Penetration: More than 50% of target audience

Maturity: Early mainstream

### Definition:

IT support live chat facilitates real-time support interactions between business consumers and live service desk agents via text chat. A live chat session can take place via a mobile or browser-based web chat application or an instant messaging (IM) client. During a chat session, business consumers may share their screens or applications to help with remote troubleshooting and resolution.

### Why This Is Important

Due to increased remote work in general, employees find live chat more appealing. Multichannel strategies are needed to address the increasingly complex needs of the digital workforce. Live chat offers real-time engagement and the convenience of multitasking, while obtaining support, thereby improving business consumers' experience and perception of the IT service desk.

### Business Impact

Live chat in the IT service desk:

- Enables on-demand, real-time interaction with IT support agents, when the use of other channels may be impractical or inconvenient.

- Is more conducive to business consumers who would like to multitask while they have technical issues resolved, rather than stopping their work to interact on the phone.
- Adds value, and can reduce staffing costs in certain circumstances where parallel conversations are appropriate for both consumer and agent.

## Drivers

- Many ITSM platforms include native live chat capabilities or integrations to common third-party tools, such as Microsoft Teams and Slack.
- Increases in mobility and in the number of hybrid remote teams, due to the COVID-19 pandemic, have increased adoption of support channels, as compared to calling IT by phone or asking a deskmate for peer support. Some organizations have found the need to introduce devices such as laptops to roles previously without, so that they could work from home.
- Stronger digital dexterity among employees (business consumer behavior and experiences with chat-based customer services and help on websites, as well as adoption of collaboration tools, driving familiarity with the medium) drives demand for support for live chat.
- Increasing market penetration of enterprise conversational platforms drives further usage of live chat, so that human agents can take over conversations that virtual agents need to escalate.

## Obstacles

- Interest in IT support live chat has traditionally been based on hopes of cost containment by increasing the number of tickets that an IT service desk can handle at one time. However, live chat is largely unable to reduce the burden on the IT service desk, because the ratio of parallel conversations an agent can handle at once does not add significant efficiencies in all cases.
- This channel is only viable for employees with easy and convenient access to a PC or mobile device with chat capability.
- Some IT leaders struggle to get started with or sustain live chat as a support channel. They find it difficult to identify the personas within the workforce that would be willing or interested in using live chat.



## User Recommendations

- Add value, rather than viewing it as a cost-saving mechanism. Agent-to-chat ratios, call times and satisfaction must be monitored to ensure that value is being added and not degrading service as the ratio increases.
- Evaluate end-user requirements and culture, as well as internal skills and tooling, to ensure that this support channel is relevant.
- Complement existing channels where text-based interactions offer new opportunities for business consumers. Examples include large contact center environments, regions where language constraints make telephone support cumbersome, and organizations that already show heavy adoption of collaboration tools, such as Slack and Microsoft Teams.
- Integrate chat capabilities directly into ITSM workflows to avoid manual effort and improve administration.

## Automated Incident Response

Analysis By: Pankaj Prasad, Padraig Byrne

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Mature mainstream

### Definition:

Automated incident response (AIR) centralizes alert or incident routing through a policy or rule-based engine, on-call scheduler and streamlined collaboration. AIR solution capabilities improve operational efficiencies with action-oriented insights, shorter incident durations and automated workflows for event routing, easier collaboration, remediation and escalations.

## Why This Is Important

Manual processes for incident resolution is a challenge, especially when multiple experts need to be involved, time is of essence and the organization wants to improve efficiency. For DevOps teams, the juggling of contact lists and lack of seamless collaboration inhibit speedy delivery of application features, as well as the stability of features after the release. AIR solutions solve this by automating most of the incident response process and collaboration, and enabling iterative improvement.

## Business Impact

AIR solutions deliver value through:

- Automated incident communication to the relevant recipient and visibility across the organization.
- Quick incident resolution minimizing customer impact.
- A well-integrated incident management practice that meets DevOps requirements.
- Insights into incidents and their responses, which helps improve process and operational efficiency.
- Automated workflows that eliminate fatigue and human errors and reduce the turnaround time.

## Drivers

- **Incident communication and visibility challenges:** With geographically distributed teams, remote workforce, complex on-call schedules and notification channel preferences, incident triage teams often have difficulty engaging responders quickly. Incident communication itself may lack all the relevant inputs or rely on multiple sources of incident data.
- **Automation of incident response processes:** AIR reduces mean time to acknowledge (MTTA) by automating the process of identifying and contacting the relevant domain experts, and speeds up the resolution process.
- **DevOps and site reliability engineer (SRE) requirements:** Traditional incident management models cannot meet the needs of agile cultures because of manual tasks in the incident response workflow. AIR caters to the need for seamless collaboration across various groups enabling DevOps to underpin its offerings with an effective, consistent IT service management (ITSM) practice.
- **Transparent review and analysis:** AIR tools capture an incident's progress from identification through resolution, including the handoffs needed across various teams. This includes the time and action taken at each step of the incident, and provides vital information for postincident review (PIR) and process review for further enhancements.
- **Workflow automation:** These tools can automate workflows that are part of processes like creating incidents for actionable alerts, opening a communications channel in instant messengers for collaboration, updating on a web-portal and one-click remediation for existing runbooks.

## Obstacles

- **Overlapping capabilities:** Although AIR solutions offer differentiating features, they also overlap with ITSM and event management systems, making it difficult to articulate the value of investing in AIR.
- **Service definitions:** Service definitions that connect alerts to responder teams are often challenging to configure as it involves interpretation of a problem based on the notification to identify the domain experts that need to be engaged. Service definitions are also a complex part of AIR onboarding.
- **Portability between solutions:** Migrating from one AIR vendor to another is a reset process, with no defined migration path. The integrations, team and service definitions, responder preferences, and role-based access controls must be reconfigured without sophisticated import/export mechanisms.
- **Maturity in I&O:** Few organizations have the required I&O maturity to quantify impact due to time lost in contacting the right personnel for resolving an issue to justify investing in these tools.

## User Recommendations

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

## Sample Vendors

AlertOps; Atlassian; Derdack; Everbridge; OnPage; PagerDuty; ServiceNow; Splunk

## Software Asset Management Tools

Analysis By: Yolanda Harris

**Benefit Rating:** Moderate

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Mature mainstream

**Definition:**

Software asset management (SAM) tools help maintain compliance with software and cloud licensing agreements. They optimize software and cloud spending by identifying opportunities to reuse software, monitor software consumption and provide data to support software negotiations. SAM tools facilitate this by aggregating an organization's entitlement and consumption of data, then reconciling it to establish an effective license position (ELP) and properly govern software use.

**Why This Is Important**

SAM tools continue to attract interest from organizations across industries. They are designed to simplify the management of complex software licensing (on-premises and SaaS) by discovering, collecting, normalizing and reconciling software consumption with entitlement data to deliver and identify real-time cost and usage optimization opportunities and noncompliance risks. These benefits often extend the use of SAM tools to support security and risk use cases and to manage cloud consumption.

**Business Impact**

- SAM tools benefit organizations, because managing software and SaaS is a universal challenge that is becoming more difficult with larger software estates, decentralized purchasing, complex licensing and hybrid environments.
- SAM tools help IT and procurement leaders simplify software management by providing a consolidated view of an enterprise software estate. They also support decision making, and the ability to mitigate software risks, optimize software spend and improve life cycle management.

## Drivers

- Sourcing, procurement and vendor management (SPVM) leaders often invest in SAM tools to gain visibility into software inventory and usage to improve the enterprise's ability to negotiate with software vendors and proactively manage renewals.
- SAM tools help IT finance and budget owners gain insights into software expenditures for improved forecasting, cost allocation and IT financial management.
- SPVM leaders are under pressure to minimize software costs associated with complex licensing models and increasing usage, as well as to identify unbudgeted compliance fees associated with software vendor audit risks.
- Enterprise architects and IT security teams look to SAM tools to provide visibility into the entire IT estate. They also want to enrich information, such as known vulnerabilities and exposures, end of life, and end of support, which enable enterprises to mitigate risks and plan for upgrades.
- Within infrastructure and operations (I&O), SAM tools have become valuable, because they help consolidate and normalize data from various discovery and inventory sources. This cleansed data can support configuration management database (CMDB) tooling efforts and accelerate time to value for IT service delivery.
- The growing adoption of cloud computing and SaaS has increased the complexity of SAM, with expanding requirements on cloud cost management, complex licensing rules and business-led technology buying.
- The need to manage SaaS software leads to investment in tools that expand the capabilities of traditional SAM tools or replace them with SaaS management platforms (SMPs) and SaaS security tools, which partially address cloud licensing challenges.

## Obstacles

- Most sourced software fails to comply with ISO/IEC 19770-3 standards, which supply data and format structures for software publishers to provide entitlement data. This supports automated loading of software entitlements. Due to the lack of adoption, loading entitlements is a resource-intensive process often overlooked when purchasing SAM tools.
- Coupled with complex and hybrid environments, the speed of change often requires manual intervention and SAM managed services providers (MSPs) or additional data collection tools to produce an effective license position (ELP).
- Due to specific use cases and the presence of adjacent tools in their environment that conflict with SAM, organizations often struggle to identify and prove the value of SAM tools.
- Many organizations underestimate the number of direct and indirect resources with specialized skills required to properly use SAM tools for entitlement loading, inventory sources health and data quality checks, or remediation and optimization.

## User Recommendations

- Establish a clear, realistic scope by determining which three to five publishers you initially want to manage with your SAM tool. Then, prioritize by compliance risks, spend volume, business-criticality or renewal schedule. Develop a set of use cases the tool must deliver against in managing these publishers, and build on that to add publishers.
- Determine what license metrics, environments — e.g., infrastructure as a service (IaaS) and software as a service (SaaS), — OSs and virtualization technologies are involved with your in-scope publishers. This will help you select appropriate SAM tool(s) for your enterprise.
- Use out-of-the-box integrations with existing inventory sources, where available, and regularly monitor data for accuracy.
- Evaluate SAM MSPs to complement investments in a SAM tool and address tool limitations. Augment resources for tool administrations and operations, such as entitlement loading, ELP creation, and actions to address noncompliance and savings opportunities.

## Sample Vendors

Certero; Eracent; Flexera; Matrix42; ServiceNow; Snow Software; USU

## Gartner Recommended Reading

[4 Keys to Unlock SAM's Strategic Value](#)

[The Future of the Software Asset Manager Is About Governance, Not Counting Licenses](#)

[Target Software and Cloud Costs by Uniting Software Asset Management and FinOps](#)

[Magic Quadrant for Software Asset Management Managed Services](#)

[Market Guide for Software Asset Management Tools](#)

[How to Select the Right Software Asset Management Tools](#)

[Mature Your SAM Discipline by Investing in the Right SAM Tool](#)



## Entering the Plateau

### ITSM Platforms

Analysis By: Rich Doheny

**Benefit Rating:** High

**Market Penetration:** More than 50% of target audience

**Maturity:** Mature mainstream

#### Definition:

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

#### Why This Is Important

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

#### Business Impact

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

#### Drivers

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

- IT leaders are increasingly inquiring about applying service management into other areas of the business through a unified platform offering. ITSM platforms continue to expand service management workflows with out-of-the-box content to support line-of-business needs, such as HR and facilities case management.
- DevOps and DevSecOps are driving the need for more ITSM platform functions to be integrated into adjacent tooling and workflows for greater efficiencies, agility, and visibility.
- ITSM vendors are investing in new capabilities supporting more federated and agile ITSM practices, AI and artificial intelligence for IT operations (AIOps) integration, workforce and process optimization, integration with development and collaboration tools, and multichannel support.

## Obstacles

- More than 400 vendors offer ITSM products, but most are basic or intermediate tools that focus on IT service desk and ticketing functions targeted at basic service desk requirements. With core process workflows built around common frameworks, many vendors struggle to create meaningful differentiated messaging and help their customers justify the ROI.
- Despite the large number of participants, the enterprise market is dominated by a small number of vendors.
- Advanced features typically require pricey add-ons or higher tiers of licensing. This will be a challenge for customers who do not align their product roadmap with their budget planning.
- Customers who try to implement too many platform features at once, across IT and multiple lines of business, will struggle to mature their practices and often lose momentum on their investments.

## User Recommendations

- Identify current ITSM needs along with what you can pragmatically deploy over an 18-month roadmap to avoid overspending.
- Avoid costly customization by prioritizing tools that provide advanced process support and machine learning, as well as strong orchestration tools and out-of-the-box integration with other IT operations management and collaboration solutions.

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

## Sample Vendors

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

## Gartner Recommended Reading

[Magic Quadrant for IT Service Management Platforms](#)

[Critical Capabilities for IT Service Management Platforms](#)

[A Buyer's Guide to ITSM Platforms](#)

[Quick Answer: How to Successfully Implement Your ITSM Platform](#)

## SIAM

**Analysis By:** DD Mishra, Pablo Arriandiaga, Andrew Miljanovski, Karl Rosander, Biswajit Maity

**Benefit Rating:** High

**Market Penetration:** 20% to 50% of target audience

**Maturity:** Mature mainstream

### Definition:

Service integration and management (SIAM) sourcing model coordinates and integrates service delivery of multiple internal and external IT with business process service providers. SIAM can be undertaken by the client or by a third-party service provider.

## Why This Is Important

Multisourced environments are not a new reality, but managing multiple vendors is often complex. As the complexity increases, service quality can drop and the benefits of using best-of-breed providers may shrink. The SIAM role addresses these potential problems by improving provider collaboration to deliver end-to-end service outcomes to business users. It increases the opportunities to tap the benefits and strengths of single-sourced deals to a multisourced environment.

## Business Impact

Expect SIAM to bring the following business impacts:

- Service reliability, quality and excellence
- Reduced cost-to-serve and operational efficiency
- Better governance, risk, compliance and control
- Improved automation
- Increased supplier accountability
- Reduced complexity
- Improved transparency
- Improved service flexibility and velocity
- Improved user experience (UX)/customer experience (CX)/employee experience (EX)
- Improved end-to-end business and IT outcome
- Improved cycle time

## Drivers

- The complexity of managing a multisourced environment with a number of providers and the complexity created by a mix of digital services have driven the ongoing adoption of the SIAM role.
- In a complex multivendor scenario, there is a greater need to foster interprovider collaboration for better productivity.
- SIAM addresses the need to improve service delivery excellence through a series of initiatives such as standardization, optimization, governance, business agility, resulting in improved operational efficiency and business effectiveness over time.
- The growing adoption of digital, agile, DevOps and Internet of Things (IoT) services is driving the evolution of SIAM toward more business outcomes, platform delivery, and product-centric delivery approaches.

## Obstacles

- Deciding whether and where to insource or outsource the SIAM role involves a lot of internal hurdles, spanning many internal IT functions. This results in hybrid internal/external delivery model use.
- If taking a DIY approach, obstacles include the lack of budget to buy and integrate the required IT service management (ITSM) toolsets and dashboards.
- Contracts often limit the execution of SIAM function and can be an obstacle to smooth execution, as they are not often structured to accommodate the SIAM sourcing model of execution.
- The lack of supplier agreement and commitment to implement SIAM sourcing model is another obstacle.
- Misaligned toolsets, hasty implementation and operating model complexity often prevent organizations from leveraging the full SIAM benefit.
- The lack of effective operational-level agreements (OLAs) between parties often creates an impediment to SIAM implementation.

## User Recommendations

- Prepare an extensive business case, ensuring allocation of a suitable budget for building and undertaking the SIAM role.
- Foster a collaborative working environment driven by collective reward and punishment, and built on trust among all parties. Prepare the use cases and outcome requirements specific to your organization, and take an incremental approach toward SIAM.
- Ensure that OLAs, KPIs and service provider interfaces are set up between all parties. Evaluate the use of emerging offerings (e.g., for SLA/OLA auditing and solution brokering) and SIAM-focused toolsets.
- Offer a build, operate and transfer model that is often promising, especially for organizations that lack competency to build the SIAM function on their own. End customers can explore competitive co-creation for approaching the SIAM role.

## Sample Vendors

Accenture; Capgemini; Cognizant; HCLTech; Infosys; Tata Consultancy Services; Unisys; Wipro Enterprises

## Gartner Recommended Reading

[Market Guide for Service Integration and Management Services](#)

## Cloud Management Platforms

Analysis By: Dennis Smith

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Mature mainstream

**Definition:**

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

**Why This Is Important**

Enterprises and managed service providers will deploy CMPs to increase agility, reduce the cost of providing services and increase the likelihood of meeting service levels. CMPs promote cost-effective governance and accountability through self-service interfaces, automation, and adherence to standard best practices. They also play an important role in creating a unified layer of consumption and abstraction for organizations adopting a hybrid and multicloud model.

**Business Impact**

CMPs address issues related to aggregation, integration, customization and governance in the adoption of hybrid multicloud by organizations. The recent CMP market continually focuses on preventing enterprises from overspending or leaving themselves vulnerable to security issues — two key items to avoid when adopting cloud services. CMPs also address the need of managed cloud service providers for multitenant customer operations and support through a single management portal.

## Drivers

- Organizations are acknowledging the need to foster end-user self-service provisioning with embedded governance.
- Vendors are addressing the key issues enterprises face. Many vendors are looking to combine cost management and security functionality into governance tooling. A few vendors are also looking to provide infrastructure-as-code assistance by overlaying cloud management functionality to this capability.
- Many vendors have added container management to their CMP offerings. The ability to serve both application developers, and infrastructure and operations (I&O) personas is key. This requires CMPs to be linked into the application development process to enable I&O teams to enforce provisioning standards, without imposing a workflow that inhibits agility.
- Global system integrators (GSIs) and management service providers (MSPs) leverage CMPs to build a services layer in order to create multicloud managed services.

## Obstacles

- Cloud management comprises a complex and varied set of activities, and no CMP platform has been successful at addressing all customer needs.
- The CMP market has been gradually fragmenting, moving from integrated all-in-one tools to specialty tools that focus on a subset of capabilities, such as security, operations or financial management.
- Challenges vendors face include interfacing with multiple public clouds, cost transparency with workload optimization to remediate cost overruns, handling newer functions (e.g., containers and serverless deployments), and edge computing.
- Market dynamics have caused confusion among potential buyers. There have been acquisitions by CMP vendors and vendors in adjacent markets, combining CMP functionality with their existing functionality. Cloud service providers (CSPs) and MSPs have entered the market, and many long-standing vendors have introduced new products that target gaps in their previous ones.



## User Recommendations

- Identify your full vertical (infrastructure as a service [IaaS], platform as a service [PaaS] and SaaS) and horizontal (on-premises, public cloud and edge) needs.
- Choose a single-focused specialized tooling, if your requirements do not expand beyond a limited scope.
- Select between native cloud services if you value depth with a cloud provider, or CMPs if you want breadth across cloud providers and your on-premises deployment.
- Determine the utility of functionally-focused tools by defining the organization's functionality needs. Integrate cloud management or traditional management tools because no vendor has a total cloud management solution.
- Ensure staffing to operate CMP platforms by planning new roles (e.g., cloud engineers and/or operators).
- Develop skills in financial and capacity management.
- Align with GSIs and MSPs to embed your CMP in their offerings as a key component of their multicloud managed services offering.

## Sample Vendors

Arrow Electronics; CloudBolt; Kion; Morpheus Data; Snow Software; Turbot; VMware; Wipro Enterprises

## Gartner Recommended Reading

[Market Guide for Cloud Management Tooling](#)

[Market Guide for Container Management](#)

[6 Best Practices to Create a Cloud Management Services Offering in the World of Multicloud and Hybrid Cloud](#)

## Appendixes

See the previous Hype Cycle: [Hype Cycle for ITSM, 2022](#)

## Hype Cycle Phases, Benefit Ratings and Maturity Levels

**Table 2: Hype Cycle Phases**

(Enlarged table in Appendix)

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

Source: Gartner (July 2023)

Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

**Table 4: Maturity Levels**

(Enlarged table in Appendix)

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

Source: Gartner (July 2023)

**Document Revision History**[Hype Cycle for ITSM, 2022 - 13 July 2022](#)[Hype Cycle for ITSM, 2021 - 21 July 2021](#)[Hype Cycle for ITSM, 2020 - 27 July 2020](#)[Hype Cycle for ITSM, 2019 - 11 July 2019](#)[Hype Cycle for ITSM, 2018 - 18 July 2018](#)[Hype Cycle for ITSM, 2017 - 19 July 2017](#)[Hype Cycle for ITSM 2.0, 2016 - 4 August 2016](#)[Hype Cycle for ITSM 2.0, 2015 - 17 July 2015](#)**Recommended by the Authors**

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

[Understanding Gartner's Hype Cycles](#)

[Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder](#)

[Innovation Insight for Collaborative Support Hub](#)

[Transform IT Support by Developing Collaborative Support Hub Roles and Competencies](#)

[Leverage AIOps and Adapt ITSM Practices to Optimize Hybrid Cloud Support](#)

[Improve Product Reliability by Applying SRE Principles to Service Operations](#)

[Market Guide for Digital Platform Conductor Tools](#)

[Predicts 2023: Enterprises Must Expand From Threat to Exposure Management](#)

---

© 2023 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

Table 1: Priority Matrix for ITSM, 2023

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational	Digital Employee Experience	Generative AI Service Operations Site Reliability Engineering	Digital Platform Conductor Tools Exposure Management	
High	Automated Incident Response Digital Work Hubs ITSM Platforms SIAM Vulnerability Prioritization Technology	Continuous Delivery DEX Tools Infrastructure Automation Multiexperience Policy as Code XLA	AIOps Platforms IT/OT/ET Alignment Operational AI Systems SOAR Technology Change Automation	
Moderate	IT Support Live Chat Software Asset Management Tools Virtual Support Agents	AI-Focused Problem Management Continuous Endpoint Engineering Walk-Up IT Support	Peer IT Support Swarming Support	Collaborative Support Hub
Low	Cloud Management Platforms			

Source: Gartner (July 2023)



Table 2: Hype Cycle Phases

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



Phase ↓

Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

Table 4: Maturity Levels

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

Source: Gartner (July 2023)