Hype Cycle for ITSM, 2025

17 June 2025 - ID G00827046 - 112 min read

By: Chris Laske, Siddharth Shetty, Chris Matchett

Initiatives:I&O Operations Management; Evolve Service Management and Cloud Operations; I&O Organizational Strategy

> The drive to streamline service management practices or even eliminate human-in-the-loop interactions at the service desk is taking center stage. In order to avoid missteps, use this information to cut through the hype and determine which innovations to build into a service management strategy.

Analysis

What You Need to Know

This year's Hype Cycle reflects the rapidly changing IT service management landscape. Security orchestration automation and response (SOAR) became obsolete before plateau and software asset management (SAM) has now reached the plateau, while continuous delivery, service integration and management (SIAM), and ITSM platforms were aged off after reaching the plateau last year.

The 2025 Hype Cycle for ITSM also provides critical insights into the practices and technologies on the forefront of IT service management. Innovations that are new on this year's Hype Cycle include agent-native I&O, natural language case extraction, and AI-powered IT agent advisory. Innovations such as autonomous endpoint management and observability have been added, reflecting significant client interest in accelerating incident response and problem resolution through critical adjacent capabilities.

To provide more in-depth analysis of AI capabilities in ITSM, a new Hype Cycle with this specific focus is being published in 2025.

The Hype Cycle

The 2025 Hype Cycle for ITSM has significant updates:

- Numerous innovations associated with AI that highlight the advancements in generative AI and agentic AI have been added in recognition of the hype and prominence of these technologies in the marketplace.

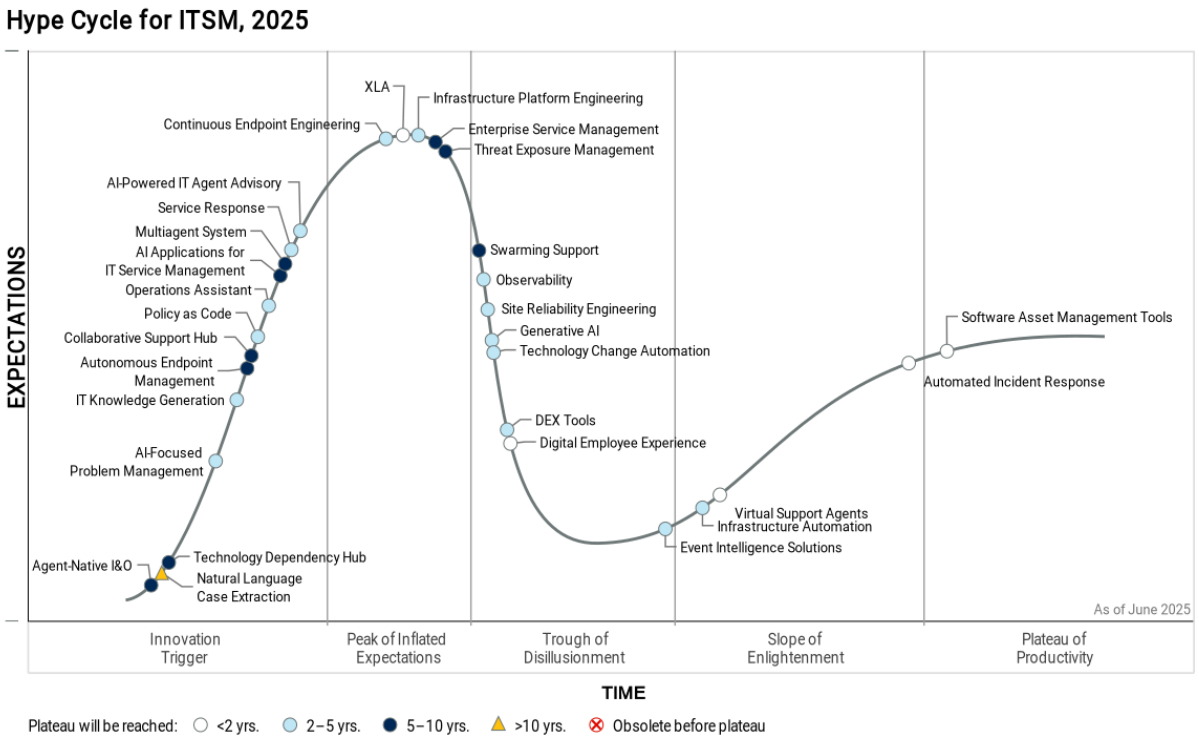
- Digital workplace remains a critical adjacent practice area for service managers, since stability of endpoints can lead to significantly fewer service desk contacts. Autonomous endpoint management has been added this year, joining DEX tools, digital employee experience and continuous endpoint engineering, which were all resident last year.
- Given the importance of real-time views of systems and services, technology dependency hubs have been added as tools that discover, identify and normalize data about an organization's infrastructure estate.
- Reduced hype on topics in the service management space has precipitated the early departure of several innovations, including work hubs, multiexperience and digital platform conductor tools.

Automation continues to generate hype in I&O and service management. Infrastructure automation, policy as code, automated incident response, and technology change automation (TCA) all remain, with infrastructure automation and TCA advancing to the Slope of Enlightenment and Trough of Disillusionment respectively.

Monitoring and observability continue to be top of mind for many service managers as they look to proactively reduce the number and impact of incidents. Observability has been added this year to emphasize the importance of understanding system behavior and associated anomalies. Event intelligence is nearing the Slope of Enlightenment as more data is generated and demands for reliability are increasing. Service response is moving up the Innovation Trigger as service managers strive for highly available and performant services by combining observability and incident management practices.

The removal of ITSM platforms from this year's ITSM Hype Cycle reinforces the understanding that the ITSM platform market is mature and the core requirements commoditized. Meanwhile, AI applications for IT service management, added last year (along with a new Magic Quadrant in 2024 and an upcoming Hype Cycle), are rapidly advancing up the Innovation Trigger. Both natural language case extraction and AI-powered IT agent advisory make their debut as capabilities in the AI applications in ITSM space.

Figure 1: Hype Cycle for ITSM, 2025



The Priority Matrix

Immediate considerations:

- Digital employee experience is a critical point of focus as I&O leaders look to reduce digital friction, drive self-healing automations and optimize IT support for internal customers.
- Given the drive toward self-service in support, I&O leaders should pursue virtual support agents to improve service desk efficiency.
- The current VUCA (volatile, uncertain, complex and ambiguous) environment is an overarching concern having a significant impact on investment decisions and driving much research. Leveraging technologies such as software asset management (SAM) tools can reduce uncertainty and limit overspending in software licensing, as well as kickstart application rationalization to identify duplicative capabilities and lessen complexity.

Short-term considerations:

- IT knowledge discovery investments will grow as generative AI capabilities mature and service managers push to automate the manual process of creating knowledge articles.
- Observability and service response can play a vital role in the overall strategy by identifying and correcting anomalies in the production environment before they impact business operations.
- Continuous endpoint engineering will become increasingly important as I&O leaders work to keep pace with rapid technological change while enhancing digital employee experience.

Long-term considerations:

- Enterprise service management is gaining traction as organizations experience increasing cost pressures and recognize the benefits of consolidating workflows and tasks beyond IT.
- Agentic AI has rapidly captured mind share with the promise of planning and executing autonomous actions. Agent-native I&O is an archetype designed to exploit agentic AI to act toward organizational goals, while multiagent systems can work toward a common goal that goes beyond the ability of individual agents.

Table 1: Priority Matrix for ITSM, 2025

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 to 5 Years ↓	5 to 10 Years ↓	More Than 10 Years ↓
Transformational	Digital Employee Experience	Generative AI Infrastructure Platform Engineering Observability Service Response Site Reliability Engineering	Agent-Native I&O Threat Exposure Management	
High	Automated Incident Response XLA	AI-Powered IT Agent Advisory DEX Tools Infrastructure Automation Policy as Code Technology Change Automation	AI Applications for IT Service Management Autonomous Endpoint Management Enterprise Service Management Multiagent System Technology Dependency Hub	Natural Language Case Extraction
Moderate	Software Asset Management Tools Virtual Support Agents	AI-Focused Problem Management Continuous Endpoint Engineering Event Intelligence Solutions IT Knowledge Generation	Collaborative Support Hub Swarming Support	
Low		Operations Assistant		

Source: Gartner (June 2025)

Off the Hype Cycle

- ITSM platforms, SIAM and continuous delivery have been removed since they have reached mainstream status.
- IT/OT/ET alignment, GitOps, multiexperience, work hubs and digital platform conductor tools were removed given reduced hype in the service management space.
- SOAR was removed due to obsolescence before plateau.
- Operational AI systems were rebranded as AI engineering.

On the Rise

Agent-Native I&O

Analysis By: Roger Williams

Benefit Rating: Transformational

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Agent-native infrastructure and operations (agent-native I&O) is an archetype for organizing infrastructure and IT operations. It is designed to exploit agentic AI in making autonomous and semiautonomous decisions to act toward organizational goals. Humans and machines work together to understand the current and future needs of key stakeholders and adapt systems and practices to meet those needs.

Why This Is Important

Agentic AI is poised to be the biggest disruptor of I&O since the introduction of the cloud and smartphones. Agent-native I&O provides the environments required for AI agents and multiagent systems to fulfill their potential. This includes seamless delivery of infrastructure offerings that minimize waste when responding to demand spikes and observability of current and expected states of those infrastructure offerings to secure and improve system performance.

Business Impact

Agent-native I&O enables AI agents to create competitive advantages through cost leadership, differentiated capabilities and sharper focus on high-value customer segments. AI agents can self-serve infrastructure for experimental offerings within human-defined limits. People and AI agents can use simulated environments to explore disruptive possibilities. AI agents administer systems and practices to create the resilience and adaptiveness required to meet business needs now and in the future.

Drivers

- I&O leaders are interested in AI agents to address chronic challenges with complexity, talent shortages and expensive cost structures, yet are unclear on what they need to do to best obtain those results.

- Agent-native I&O provides a compelling vision for how I&O can play a critical role in business success, which addresses perennial I&O concerns about being viewed as a strategic value contributor.
- Agentic AI poses a dilemma for I&O leaders regarding how much of their effort should be devoted to preparing for agentic AI versus addressing current needs. Agent-native I&O addresses this dilemma by providing a comprehensive vision that builds future readiness for agentic AI adoption while addressing current challenges.
- Agentic AI needs trustworthy data about the hybrid infrastructure estate and the IT operating model to make accurate, timely decisions with minimal costs and risks. The intelligent simulation element of agent-native I&O addresses this by giving AI agents needed feedback on actions in complex environments to support them at the speed required for effective experimentation.
- I&O staff are at risk of not developing hybrid infrastructure expertise as AI agents take on easier tasks, which agent-native I&O accommodates through its use of intelligent simulation.

Obstacles

- **Inadequate governance of I&O:** AI agents need explicit guidance about goals, boundaries and rules that are often not documented. I&O leaders must provide clarity about the mission and the constraints AI agents must adhere to in order to fulfill it.
- **Staff readiness for AI agents:** Agent-native I&O requires people to have the motivation, expertise and time to understand how best to work with AI agents. Staff need I&O leader support and sponsorship to develop vital skills for working with AI agents and to have confidence that they will still be treated as valuable members of the organization.
- **Lack of agentic AI standardization:** Differences in vendors' agentic AI offerings will require trade-offs in how AI agents are matched to work needing to be done. I&O leaders must ensure infrastructure and operational practices are compatible with the disparate capabilities of various AI agents being used for work activities.

User Recommendations

- Create a vision for how agentic AI would change I&O by identifying where I&O is constrained due to limited resources for decision making and taking action, and imagining what would be different if these constraints were broken by agentic AI.

- Assess I&O's ability to take advantage of agentic AI with the current IT operating model by using Gartner's IT Score for Infrastructure and Operations to understand and close the most significant gaps.
- Ensure compatibility with agentic AI by requiring new infrastructure investments to be based on intelligent infrastructure and platforms that AI agents can then use to perform tasks and to augment their capabilities.
- Address quality gaps in technology asset data required for effective agentic AI use by strengthening ITAM, service management, observability and digital employee experience practices.

Gartner Recommended Reading

Top Strategic Technology Trends for 2025: Agentic AI

Emerging Tech Impact Radar: Intelligent Simulation

What Good Modern Infrastructure Looks Like

Natural Language Case Extraction

Analysis By: Chris Matchett

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Embryonic

Definition:

Natural language case extraction is the process of using natural language technologies and large language models (LLMs) to automatically recognize incidents and requests from organic conversations and create associated tickets in a case management system (e.g., an ITSM platform or a CRM customer engagement center).

Why This Is Important

Natural language case extraction (NLCE) is an essential capability for a functional collaborative support hub. It scans collaboration channels and support forums for conversations, data, knowledge and metrics for support activities that have not gone through a case management system (such as an ITSM platform or a CRM platform) and pulls them into the platform. NLCE agentically automates the slow, labor-intensive work previously done by IT service desk agents, who would trawl for incidents to manually add into the ITSM platform.

Business Impact

NLCE provides these benefits:

- Improves knowledge generation and maintenance by finding undocumented solutions used in peer support.
- Provides advance warning of service issues that employees are discussing.
- Automatically creates incident tickets without requiring a service desk contact.
- Provides visibility of support effort and impact outside of formal contact centers.
- Enables reporting of time spent by IT and business experts on the collaborative support hub and measures the impact of peer IT support.

Drivers

- NLCE is technically feasible using generative AI LLMs, which are well-suited to extracting context and data from unstructured content such as conversations.
- Vendors in AI applications for ITSM have plans for this capability within their roadmaps.
- NLCE appeals to employees and customers who prefer peer support and discussion channels.
- Organizations that implement a collaborative support hub for IT seek NLCE solutions to connect the hub to the case management system, such as their ITSM platform.

Obstacles

- Software vendors don't have functional implementations of NLCE, despite the technical feasibility, resulting in its low availability.
- Organizations must build their own AI application with integrations to their case management system(s) to be able to use this functionality today.
- Employees may resist or mistrust AI features that monitor conversations.

User Recommendations

- Add a conversational agent to communal channels as a participant to offer assistance alongside formal support channels and human moderators.
- Enable virtual support agents to mark conversations as complete once successfully resolved in order to manage the clutter of common and repeat issues that have known solutions. This allows human expert responders and community moderators to focus on the other conversations that a conversational AI agent is unable to deal with.
- Use NLCE on conversations that are instantiated by swarming, as well as on more permanent collaborative support hub channels.
- Ask your case management platform vendor about these capabilities and how to activate them. Their roadmaps are prioritized on customer demand.

Gartner Recommended Reading

Innovation Insight: Collaborative Support Hubs

Quick Answer: How to Use Virtual Support Agents With Peer IT Support

Critical Capabilities for Artificial Intelligence Applications in IT Service Management

Technology Dependency Hub

Analysis By: Ankita Hundal, Roger Williams

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

A technology dependency hub (TDH) is a solution that provides a strategic control layer that discovers, normalizes and federates infrastructure and application dependency data. By reconciling fragmented datasets and bridging CMDB gaps, TDH enables current-state visibility and insight across complex environments. This accelerates IT change, incident resolution and modernization efforts while improving operational integrity and enabling automation and/or AI-driven operations.

Why This Is Important

Modern CMDBs with continuous discovery improve data freshness but still lack federation, validation and cross-domain reconciliation. TDHs address this by bridging tool and team silos, enabling real-time dependency intelligence that supports automation, transformation and operational resilience.

Business Impact

TDHs complement modern CMDBs by federating, validating and operationalizing dependency data in real time. They reduce change failures, speed up incident resolution, and support modernization, compliance and automation. TDHs make dependency data a business-aligned asset.

Drivers

- Large enterprises now operate dozens of overlapping discovery tools, resulting in conflicting views of the same infrastructure. This leads to wasted effort, missed dependencies and broken change workflows.
- Cloud-first mandates are exposing the inability of traditional CMDBs to reflect ephemeral infrastructure and service-mesh-based architectures.
- Platform engineering and DevOps teams increasingly demand “dependency-as-a-service” capabilities to support developer self-service, safe release automation and golden path reliability.
- AIOps and intelligent automation platforms are underperforming due to poor dependency hygiene, often defaulting to inaccurate or outdated CI data.
- Regulatory scrutiny around operational resilience (e.g., DORA and NIS2) is pressuring financial and critical infrastructure providers to adopt live dependency mapping as audit and compliance tools.
- Organizations planning data center exits or multicloud migrations cannot effectively derisk or sequence workloads without verified service interdependencies.
- Failed change initiatives and prolonged incident resolution times have drawn executive attention to blind spots in the current service mapping efforts.
- Growing pressure to retire technical debt and rationalize legacy portfolios requires transparency into how legacy systems are entangled with critical services.

Obstacles

- A lack of ownership and unclear accountability models for dependency data results in poor data hygiene and unmaintained relationship maps.
- Many organizations struggle to rationalize the value of TDHs due to fatigue from failed CMDB and SDM efforts, reinforcing executive skepticism.
- Integration complexity across siloed tooling ecosystems (e.g., observability, ITAM and cloud platforms) delays time to value.
- Misalignment between ITSM and DevOps teams hinders cross-domain implementation and governance.
- Limited vendor maturity and inconsistent terminology (e.g., few vendors explicitly position TDH) make it difficult for buyers to articulate requirements.
- The risk of “tool sprawl” increases if TDH initiatives are not aligned with enterprise architecture or if they are deployed as tactical projects rather than strategic platforms.
- Incomplete automation and a lack of clean data from existing discovery sources reduce the quality of dependency outputs and may reinforce distrust in mapping outputs.

User Recommendations

- Define a clear enterprise mandate for TDH, positioning it as a strategic control layer for automation, modernization and risk mitigation — not a tool project.
- Establish a federated data governance model across the architecture, SRE, security and service management teams to ensure the quality, ownership and ongoing curation of dependency data.
- Start with targeted pilots, such as high-change applications and cloud migration zones, to demonstrate value and build confidence in dependency accuracy and impact analysis.
- Integrate TDH into strategic workflows — such as change control, transformation planning, release pipelines and compliance reporting — to embed its utility across the life cycle.
- Align TDH investments with platform engineering and DevOps priorities, enabling self-service environments that rely on dependency-aware automation and infrastructure orchestration.

Sample Vendors

BMC; Dynatrace; Faddom; Freshworks (Device42); ServiceNow

Gartner Recommended Reading

Drive CMDB Transformation Through Continuous Discovery and Service Mapping

Solution Criteria for AIOps Platforms

Innovation Insight: Data Observability Enables Proactive Data Quality

Innovation Insight: AI Applications in IT Operations Management Advance AIOps Beyond Platforms

AI-Focused Problem Management

Analysis By: Mark Cleary

Benefit Rating: Moderate

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

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

Why This Is Important

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

Business Impact

Here are some of the ways that using AI to identify recurring incidents benefits the organization:

- Prevents 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.
- Improves the understanding of the health of the products and services provided by IT.
- Provides a better understanding of the health of the environment

Drivers

Organizations are attracted to AI-focused problem management because of its ability to:

- Deliver better business outcomes by reducing the number and prevalence of incidents.
- Address underlying problems that would not be visible otherwise.
- Improve the desk's credibility by removing recurring incidents.

- Discover patterns and trends that may highlight structural software or hardware issues.
- Establish the value of problem management and accelerate problem detection and remediation.
- Reduce end-user frustration at continually occurring incidents.

Obstacles

AI-focused problem management:

- Depends on categorizing incidents and structured data accurately.
- Requires completing the free-form text that details the diagnosis and resolution for every incident in a comprehensive way to allow AI to pattern match effectively.
- Needs an effective problem management practice to help the second-line application, product and infrastructure teams analyze and address the problems identified in the output.
- Needs senior leadership support to ensure the output is prioritized and necessary actions are taken.
- Requires a significant volume of incidents to be input to improve the accuracy of the results.
- Requires an accurate and up-to-date configuration management database (CMDB) to ensure that each incident has an associated configuration item (CI) record with sufficient attributes to help root cause analysis.

User Recommendations

- Ensure that all incidents are categorized correctly 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 the value and impact of AI-focused problem management.
- 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; Atlassian; BMC Software; ServiceNow

IT Knowledge Generation

Analysis By: Rich Doheny

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

IT knowledge generation creates knowledge articles with generative AI (GenAI) by recognizing attempted and successful solutions from sources, including organic conversations, documents and historical cases. These articles can then be leveraged in a management system (e.g., IT service management [ITSM] platform or conversational AI tool) for both IT and end-user consumption.

Why This Is Important

Infrastructure and operations (I&O) leaders want to automate the manual process of populating and maintaining a knowledge base. While some ITSM platforms migrate verbatim data from cases and provide style templates, most development and ongoing maintenance of the knowledge assets rely on time-intensive human effort. Therefore, many organizations struggle to deliver an effective and sustainable knowledge management (KM) practice. By leveraging GenAI techniques, I&O leaders can automate the creation and maintenance of knowledge assets.

Business Impact

An effective KM system improves support quality and self-service. I&O leaders looking to scale their knowledge management practice target GenAI for knowledge creation to:

- Accelerate the authoring and publication process.
- Identify IT knowledge gaps.
- Increase the number of knowledge assets to address a wider breadth of issues.
- Deliver knowledge-article content and format standards.
- Reduce IT support overhead and faster time-to-value of the KM program.
- Shift-left to reduce human-assisted interactions.

Drivers

- I&O leaders have been looking to automate the knowledge creation process for years, and the proliferation of GenAI is now making that possible.
- Given its current manual nature, I&O leaders are challenged to keep IT staff engaged to actively build and maintain knowledge articles.
- I&O leaders want more responsive KM practices to effectively support the proliferation of technology caused by digital business initiatives.
- Product teams have led to more distributed and federated support models. Automated knowledge generation can reduce the risk of knowledge silos by simplifying the process of knowledge authoring.
- Both AI applications in ITSM and conversational AI tools are increasingly providing support for knowledge generation.
- Deep research techniques offer the promise of drafting articles sourced from multiple sources with full attribution, without the reliance on extensive case documentation.

Obstacles

- IT support teams often lack ticket documentation standards which will reduce the value of knowledge generation.
- Automating the production of knowledge can also increase the risk of knowledge bloat through low-value or redundant knowledge due to poor management controls on newly generated knowledge.
- Large language models (LLMs) risk misinterpreting the data fed into them, causing hallucinations (i.e., making up facts).
- There are data privacy, data ownership and security concerns about LLM data usage.
- Solutions offering this capability are often bundled with other GenAI features that are priced at a premium, requiring a broader strategy to drive the ROI.
- Few knowledge generation solutions integrate into and drive automation for the publishing pipeline and life cycle management for knowledge, as most only focus on creating the knowledge asset text.

User Recommendations

- Expedite the ROI by selecting an AI-enabled knowledge generation solution that is integrated into the publishing life cycle and knowledge base (e.g., the ITSM platform, AI application for ITSM or conversational AI tool) and provides domain-trained LLMs.
- Have a human review and validate any AI-generated content, even previously published information that is only being updated.
- Investigate how GenAI can flag related knowledge and automate the maintenance of existing knowledge to keep knowledge assets current.
- Avoid dissolving the existing KM practice; instead, evolve it to account for system-generated knowledge.
- Encourage knowledge managers to work closely with the AI platform teams.

Gartner Recommended Reading

How Generative AI Impacts Knowledge Management

Use-Case Prism: Artificial Intelligence for IT Service Desk

Autonomous Endpoint Management

Analysis By: Tom Cipolla

Benefit Rating: High

Market Penetration: Less than 1% of target audience

Maturity: Emerging

Definition:

Autonomous endpoint management (AEM) is a next-generation approach that is enabled by new functionality within advanced endpoint management tools. AEM leverages configuration, compliance, risk, performance and experience data to intelligently perform common endpoint and digital employee experience (DEX) management tasks. The first foundational use case for AEM is autonomous patching that accelerates patch deployment and compliance and reduces IT overhead and degradation of DEX.

Why This Is Important

End-user services and digital workplace leaders are simultaneously pressured to increase the velocity of patching and maintain DEX. AEM is accelerating endpoint patching and promises to streamline and automate configuration management, while protecting DEX and reducing IT overhead.

Business Impact

End-user services leaders can further automate endpoint and DEX management tasks and reallocate efforts toward business-value-added work. Specific impacts include:

- Reduced IT overhead through the automatic resolution of issues that impede employee productivity.
- Enforced endpoint configuration standards based on vendor, industry or self-defined baselines.
- Reduced cyber risk by automating patch and configuration management.
- Automated software and configuration deployment based on policy and persona.

Drivers

- IT staff is overwhelmed with the growing number of endpoint devices, operating systems and applications.
- Largely driven by increased AI and ML capabilities, technology vendors have accelerated development and release cadence, and IT cannot keep pace.
- Increased cyberattacks demand faster patch deployment, better device configuration compliance and closer alignment with vendor life cycles to reduce vulnerabilities.
- Adoption of DEX practices and tools continues to grow rapidly as many accelerate their focus from a technology-centric to an employee-centric experience.
- Cloud-based endpoint management and DEX tools are demonstrating how AI- or ML-powered intelligence can quickly process a significant amount of data, provide actionable insights and recommendations, and execute automations.
- Developing and maintaining automation for common administrative tasks and applying standard policies and configurations is time-consuming and requires integration across multiple tools.
- End-user services leaders struggle with utilizing and consolidating data from other endpoint management tools and agents.
- AEM directly supports the end-user services leader’s goal of speed and agility.
- AEM use cases are promising in addressing the management of applications and replacing human execution of routine IT processes.

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.
- Low- to midmaturity organizations lack the competencies, tools and roles to ensure that more basic processes and concepts are already deployed.
- Device operating system limitations or controls may prohibit experience and automation capabilities.
- AEM is not possible on-premises, so cloud-averse organizations will not be supported.
- Organizations that lack experience with agile methodologies and automation skills operate with a legacy mindset prioritizing control and customization.
- AEM tools are unlikely to address niche use cases due to insufficient data to train ML and AI models to perform the automated activities.

User Recommendations

- Avoid vendor lock-in by ensuring strategic endpoint and DEX management vendors have a roadmap that directly provides or includes necessary partnerships to enable AEM.
- Reduce location dependence by migrating experience and endpoint management, security and identity solutions to the cloud.
- Prepare your organization by assessing current and future skills requirements, updating existing and defining new roles, and implementing strategies for upskilling and professional development.
- Eliminate inertia by promoting a human-centric and enablement mindset, while adopting modern management principles and agile methods.

Gartner Recommended Reading

Innovation Insight: Autonomous Endpoint Management

Magic Quadrant for Digital Employee Experience Management Tools

Critical Capabilities for Digital Employee Experience Management Tools

How to Successfully Deploy a DEX Tool

Market Guide for Endpoint Management Tools

Collaborative Support Hub

Analysis By: Julian Edwards, Chris Matchett

Benefit Rating: Moderate

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

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

- Formalizes and expands 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
- Accelerates resolution by swarming expertise from IT and business expert teams like agile and fusion teams
- Fosters 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 and hybrid work arrangements, and an evergreen need to ease the IT service desk workload.
- Many organizations have deployed collaborative work management on tools such as Microsoft Teams, Cisco Webex or Slack, enabling employees to communicate through broader and more diverse channels.
- In 2022, only 31% of workers sought IT for best practices on using technology, and a mere 15% collaborated with IT to solve business problems. By 2024, these figures rose dramatically; 43% of workers sought IT for best practices and 25% collaborated with IT on business solutions (see Top End-User Services Insights From the 2024 Digital Worker Survey).
- Many ITSM platform vendors have added collaborative hub capabilities to their product roadmaps.
- In the 2024 Gartner I&O Signature Role Survey, 54% of infrastructure and operations (I&O) leaders identified innovation, collaboration and strategic decision making as the top nontechnical skill priorities in I&O.

Obstacles

- Remote working led to a drop in “ask a colleague for help” frequency.
- Many business consumers prefer to contact IT only through traditional support channels.
- Collaborative hubs require integrating collaboration tools to succeed. While there are many options, all have different limitations, including integration capabilities, making it difficult to standardize on one solution.
- The inability of ITSM platforms 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. Additionally, I&O leaders struggle to find employees with both the desire and experience to manage and support 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 live interactions.
- Start with topic groups for products where substantial knowledge capital exists in both IT and business domains.
- Operate the hub efficiently with a community manager and moderators.
- Integrate with digital workplace tools to provide a unified experience for users seeking support.

Gartner Recommended Reading

Drive ITSM Growth by Enabling Collaborative Support

Innovation Insight: Collaborative Support Hubs

How to Operate and Manage a Collaborative Support Hub

Essential Roles and Competencies for a Collaborative Support Hub

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 PaC today to enforce infrastructure compliance, authorization, Kubernetes admission control and more.

Why This Is Important

Platform engineers use PaC to build optimization, governance and compliance controls into automation pipelines. Infrastructure and security teams have used it for years to build guardrails around infrastructure and data while preserving a separation of duties that mirrors a typical IT organization chart. With the rise of generative AI (GenAI), PaC is poised to become a way to control AI agent behavior and enforce standards programmatically, which current GenAI tools often struggle to do.

Business Impact

- **Security, compliance and automation:** PaC, combined with automation, enforces policies with implicit compliance guarantees.
- **Alignment of security and operations teams:** PaC allows security and compliance teams to interface directly with automation pipelines.
- **Visibility and auditability:** PaC documents policies. PaC tool logs can be audited to prove policies are being enforced.
- **Time and effort spent:** PaC means less toil for operators because it forestalls configuration drift and out-of-spec elements.

Drivers

- **Emerging standard:** Several dedicated PaC tools are now on the market, many of them open source. The Open Policy Agent (OPA), a Cloud Native Computing Foundation project, has become the de facto standard for PaC. Even some other PaC tools now use OPA policies alongside or instead of their own policy engines.
- **Increasing regulations:** Regulations such as General Data Protection Regulation 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 verify that they are being enforced.
- **Agentic AI:** The advent of GenAI agents is transformational across almost every industry, but organizations struggle to control the behavior of AI agents. PaC can provide both effective control and meaningful testing and auditing of agents' outputs.
- **Security breaches:** 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 infrastructure and operations team wants its security failures to be the reason its company gets negative headlines.
- **Continued growth of DevOps and DevSecOps:** As more companies are embracing DevOps and DevSecOps, they are also encountering the hard governance problems of automation. Many teams that implement infrastructure as code quickly find that they need better policy enforcement, and PaC can help.
- **Cloud optimization and cost control:** Besides 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 extensive libraries of community-generated content from which users can download the policies they need rather than having to write their own. Over time, as the user base expands, PaC tools will reach a critical mass of downloadable content that supports real-world uses.
- **Skill set:** Many technical professionals lack the skills to operate automation and PaC tools effectively. As the learning curve might be steep for some, you may need to accept some flubbed policy enforcement due to lack of experience.
- **Integration challenges:** Integrating with existing tools is complex and often requires additional configuration.
- **Organizational inertia:** In some organizations, collaboration between infrastructure and operations teams and security or compliance teams is actually unwanted. This dynamic may slow the rate, scope and scale of PaC initiatives.
- **Costs:** Even if PaC tools themselves are free, you may still require training or consulting.

User Recommendations

- **Start small:** Choose a pilot use case where PaC will likely provide real business benefits, then expand to others once PaC has proven its value.
- **Upskill staff:** PaC languages are not always intuitive. Technical staff will need practice and/or training. Adopt the four-eyes principle to prevent flawed policies from impacting operations.
- **Promote reusability:** Focus your PaC efforts on use cases that have ready-made implementation templates — ideally, downloadable content. For example, almost every PaC tool on the market has a canned implementation of the customer information systems benchmarks.
- **Break down team silos:** Use PaC to build a common workflow for automation and policy enforcement that spans platform engineering, infrastructure and operations, 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

IBM (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

Operations Assistant

Analysis By: Chris Matchett, Matt Crossley

Benefit Rating: Low

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Operations assistants are conversational interfaces intended to assist infrastructure and operations (I&O) teams leverage data-driven insights to carry out their role. They provide access to AI and generative AI (GenAI) capabilities, such as case summarization, on-demand communications and other features that use natural language technologies.

Why This Is Important

While traditional virtual support agents have focused primarily on helping business consumers, there's now a demand for solutions that cater specifically to the needs of I&O workers. This demand has led to a heightened interest in operations assistant solutions, which aim to provide similar user experiences to other AI assistants but are tailored toward helping I&O workers increase their productivity.

Business Impact

Operations assistants provide these benefits:

- Optimized and improved IT support processes through insight and automation.
- Faster resolutions and improved accuracy in triage, categorization and expert identification.
- Easy access to deeper insight by analyzing processes, tickets and workflows to identify opportunities for improvement.
- Improved experience for I&O workers, leading to fewer frustrations and improved morale.

Drivers

- While business-consumer-facing virtual support agents have been a prominent focus in the past, there is now a demand for solutions that cater specifically to the needs of I&O workers.
- A high level of interest in AI assistant solutions has prompted I&O leaders to seek similar user experiences aimed at helping I&O workers boost productivity.
- Some organizations have purchased or are piloting Microsoft Copilot and hope to use the same technology within I&O.
- Increasing numbers of vendors in IT operations management (ITOM) and AI applications in IT service management (ITSM) markets have branded part of their offering as AI assistants.
- Some I&O leaders believe that conversational interfaces will become a primary method of agent interaction with IT operations and service management software.
- I&O leaders believe that AI-enabled assistant technology can help them meet the challenges of macroeconomic conditions to find cost savings through increases in productivity.

Obstacles

- General-purpose AI assistants primarily designed for meeting transcription and summarization use cases are not suited to be an operations assistant to facilitate I&O workflows.
- Operations assistants are too new to be considered as must-have. However, commercially available products that offer these are costly if only being used as an experimental nice-to-have.
- I&O users may not want a simplified conversational interface to carry out their tasks, instead preferring fully featured forms or command line UI.
- Agent advisory capabilities do not require an operations assistant; instead, more commonly show up as other user interfaces, such as the classic web form UI of ITSM platforms.
- The term “copilot” is heavily marketed, but product branding does not guarantee a feature-rich operations assistant. Instead, the capabilities may be more suited to general chatbots.
- Operations assistants rely on other underpinning AI capabilities such as agent advisory.

User Recommendations

- Treat “copilot” branding with skepticism and ask vendors to demonstrate how their operational assistant can help your I&O workers boost productivity.
- Seek operational assistants that are designed for ITOM and ITSM use cases, because general-purpose AI assistants would need extensive customization.
- Confirm that existing expert users can benefit from conversational interfaces rather than preferring traditional user and command line interfaces to interact with tools.
- Ensure that novice or new target user groups have sufficient domain knowledge to identify erroneous generative output.
- Since stand-alone operations assistant products have yet to mature, and they don’t contribute to a drop in product cost and implementation overhead, most I&O leaders should wait before committing to emergent products.

Sample Vendors

Aisera; BigPanda; Freshworks; Opentext; PagerDuty; SymphonyAI

Gartner Recommended Reading

Magic Quadrant for Artificial Intelligence Applications in IT Service Management

Critical Capabilities for Artificial Intelligence Applications in IT Service Management

AI Use-Case Assessment for IT Service Desk

AI Applications for IT Service Management

Analysis By: Chris Matchett

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

AI applications in IT service management are tools that augment and enhance IT service management (ITSM) workflows using AI. These analyze ITSM data and metadata (primarily found in ITSM platforms) to provide intelligent advice and actions on ITSM practices and workflows, such as IT service desk and support activities. This software can either be a stand-alone product, features extending an ITSM platform or an add-on to an ITSM platform.

Why This Is Important

Infrastructure and operations (I&O) leaders seek the benefits of AI to maximize the value of their ITSM but are not replacing ITSM platforms to obtain AI capabilities. Instead, they choose between incumbent platform capabilities and third-party, specialist AI solutions. This market is evolving rapidly, alongside developments in generative AI and large language models (LLMs).

Business Impact

AI applications for ITSM enable:

- Faster resolutions and improved accuracy in triage, categorization and expert identification.
- A tangible reduction in costs, such as labor savings, by handling support issues and requests automatically.
- Improved employee-facing user experience and enhanced relationship with the business consumer.
- Deeper insight into service, practice and staff performance.
- AI advisory and automation features can help avoid disruptions and provide reliable IT services.

Drivers

- The popularity of generative AI (GenAI) is prompting I&O leaders to have higher expectations of conversational AI platforms and look beyond previous-generation chatbot features in ITSM platforms.
- ITSM platforms provide a variety of AI features, but I&O leaders often purchase add-ons or integrate stand-alone products from third-party vendors when they require more extensive capabilities.
- GenAI capabilities are increasingly sought by I&O leaders to automate content generation and improve communications. Examples include summarizing information, such as knowledge base articles or case work-log updates, and generating major incident notifications.
- Most of the vendors in Gartner's Magic Quadrant for Artificial Intelligence Applications in IT Service Management provide a large language model (LLM), and a growing number of ITSM platforms provide integration to a public LLM. LLMs are a key component of this market, which demonstrates the increased awareness and penetration.
- Vendors are enthusiastically promoting agentic features in their marketing, and agentic search techniques such as "deep research" offer potential improvements for use cases such as IT knowledge generation.

Obstacles

- Gartner's Critical Capabilities for Artificial Intelligence for IT Service Management found that all products on the market have significant room for improvement, particularly in areas such as intelligent escalation and IT knowledge generation.
- I&O groups lack existing skills in areas such as prompt engineering to accelerate deployments using LLMs.
- I&O organizations lack sufficient foundational data to train their AI capabilities — whether consistently categorized incidents or knowledge for their virtual support agent.
- ITSM platform vendors that offer AI capabilities report that active customer adoption of these features is still low, although the use of virtual support agents is growing.
- As I&O leaders must choose between incumbent ITSM platforms and add-on products specialized in AI today, there is a significant chance that some smaller vendors may be acquired and merged into larger offerings in this market.
- AI applications in ITSM have yet to deliver on confirmed agentic capabilities beyond marketing hype.

User Recommendations

- Use the Use-Case Prism: Artificial Intelligence for IT Service Desk to determine which AI use cases will provide the most transformational value, while being sufficiently feasible to implement quickly.
- Invest in AI applications for ITSM to achieve significant enhancements across a broad range of ITSM practices.
- Consider general-purpose conversational AI solutions for commodity features like using a virtual support agent to deflect calls from the service desk.
- Verify whether the incumbent ITSM platform can already meet these needs. If an add-on or upgrade is required, then assess the licensing and implementation costs before comparing with third-party solutions.

Sample Vendors

Aisera; BMC; Espressive; Freshworks; Halo Service Solutions; Moveworks; OpenText; Serviceaide; ServiceNow; SymphonyAI

Gartner Recommended Reading

Magic Quadrant for Artificial Intelligence Applications in IT Service Management

Critical Capabilities for Artificial Intelligence Applications in IT Service Management

Infographic: Choose an AI Solution for ITSM

AI Use-Case Assessment for IT Service Desk

Multiagent System

Analysis By: Leinar Ramos, Pieter den Hamer, Anthony Mullen

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A multiagent system (MAS) is a type of AI system composed of multiple, independent (but interactive) AI agents, each capable of perceiving, making decisions, taking action and achieving goals in their physical or digital environment. Multiple agents can work toward a common goal that goes beyond the ability of individual agents, with increased adaptability and robustness.

Why This Is Important

Current AI is focused on the creation of individual agents built for specific use cases, limiting the potential business value of AI to simpler problems that can be solved by single agents. The combined application of multiple AI agents can tackle complex tasks that individual agents cannot, while creating more adaptable, scalable and robust solutions.

Business Impact

Multiagent systems can be used in:

- **Generative AI:** Orchestrating AI agents for complex tasks
- **Robotics:** Warehouse optimization, search and rescue, environment monitoring

- **Complex business workflows:** For example, customer service, marketing and sales
- **Energy and utilities:** Smart grid optimization and load balancing
- **Supply chain:** Optimizing scheduling, planning, routing and supply chain optimization
- **Transportation:** Traffic flow optimization, autonomous vehicle coordination
- **Telecom:** Network optimization and fault detection
- **Healthcare:** Using agents to model actors (individuals, households, professionals)

Drivers

- **Generative AI agents:** Large language models (LLMs) are increasingly augmented with additional capabilities, such as an internal memory and tools, to implement AI agents. An emerging set of design patterns is to assemble and combine these LLM-based AI agents into multiagent systems.
- **Multiagent frameworks:** The emergence and increased popularity of multiagent frameworks is increasing the feasibility of experimenting and deploying these systems, particularly ones based on LLM-based AI agents. These frameworks simplify the creation, orchestration and management of multiple AI Agents.
- **Limitations of single AI agents:** Current AI agents are not reliable enough to perform well in a broad scope of tasks. Given this limitation, it is often best to break down a process into different tasks and have AI agents that are more narrow and specialized for each task, which are then coordinated together by a multiagent system.
- **Increased decision-making complexity:** AI is increasingly used in real-world engineering problems containing complex systems, where large networks of interacting parts exhibit emergent behavior that cannot be easily predicted. The decentralized nature of multiagent systems makes them more resilient and adaptable to complex decision making.
- **Simulation and multiagent reinforcement learning:** Advances in the realism and performance of simulation engines, as well as the use of new multiagent reinforcement learning techniques, allow for training multiagent AI systems in simulation environments. These trained systems can then be deployed in the real world.

Obstacles

- **Training complexity:** Multiagent systems are typically harder to train and build than individual AI agents. These systems can exhibit emergent behavior that is hard to predict in advance, which increases the need for robust training and testing.
- **Monitoring and governing multiple agents:** Coordination and collaboration between agents is challenging. Careful monitoring, governance and a common grounding are required to ensure the combined multiagent system behavior achieves its intended goals.
- **Reliability:** Multiagent approaches without a form of centralized planning are typically too unreliable. Successful multiagent implementations tend to have a tighter control of the workflow between AI agents, which increases reliability but decreases the flexibility of the system.
- **Fragmented vendor landscape:** A fragmented vendor landscape inhibits customer adoption and engagement.

User Recommendations

- Use multiagent systems for complex problems that cannot be solved by single AI agents. This includes problems with changing environments where agents need to adapt and problems where a diverse set of agents can be combined to accomplish a goal.
- Shift to a multiagent approach gradually since this is an emerging area of research and the risks and benefits are not yet fully understood.
- Establish clear guardrails when implementing multiagent systems, including legal and ethical guidelines around autonomy, liability, robust security measures and data privacy protocols.
- Invest in the use of simulation technologies for AI training, as simulation is the primary environment to build and test multiagent systems.
- Educate your AI teams on multiagent systems, how they differ from single-agent AI design and on some of the available frameworks to build and manage these systems.

Sample Vendors

Alphabet; Ansys; Cosmo Tech; CrewAI; LangChain; MathWorks; Microsoft; OpenAI; The AnyLogic Company

Gartner Recommended Reading

Case Study: Multiple AI Agents' Recommendations Improve Efficiency

Innovation Insight: AI Agents

Innovation Insight: AI Simulation

Service Response

Analysis By: Mark Cleary

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Service response capability focuses on the provision of highly available and performant services by detecting and responding to potential or actual interruptions to a service or a reduction in the service quality. This is achieved through converging observability practices with incident management practices to create a dynamic and responsive end-to-end discipline that more effectively diagnoses and resolves incidents.

Why This Is Important

The ability to quickly diagnose and resolve incidents is critical for organizations in deploying digital services. Techniques including AI and automation can remove the monitoring and service desk silos, creating the concept of a unified service response and ensuring better integration of incident detection via monitoring with IT service management (ITSM) platforms. Such techniques lead to enhanced identification and quick resolution of incidents, thus creating higher availability and more resilient services.

Business Impact

The convergence of ITSM and observability 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 have higher availability and are 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 diagnosed and resolved as quickly as possible.
- The closer integration of observability with the service desk creates a far more effective and seamless environment for effectively managing outages and disruption.
- ITSM platforms now feature observability and correlation functions to identify incidents as part of their newly available monitoring capabilities.
- Staff can be more effectively utilized through managing as one team of specialists to manage the environment
- ITSM platforms 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 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.
- Achieving improved diagnostics and resolution times requires time and effort because of the need to better manage dependencies, including effective service mapping, the degree of automation and the monitoring quality. 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 correlating incidents.
- Accurate service mapping and comprehensive, up-to-date configuration management databases are necessary to support end-to-end incident processes to achieve enhanced availability and resilience.
- Automated responses require oversight 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 service response strategy that focuses on effective incident management. Consider the implications on the monitoring and support staff (including the service desk), the range of tools available, their integration strategy and the need to amend service practices.
- Identify the appropriate tool strategy and define the end-to-end process, including dependencies, and use this to build a roadmap to deploy and implement the solution.
- Develop runbooks to provide 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 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

BigPanda; BMC; Datadog; Moogsoft; PagerDuty; ServiceNow;

Gartner Recommended Reading

Magic Quadrant for Observability Platforms

AI-Powered IT Agent Advisory

Analysis By: Chris Matchett

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

The use of AI to analyze IT service management (ITSM) data and metadata and generate recommendations that accelerate and enhance ITSM practitioners' activities. Example features include intelligent categorization, triage, routing, escalation, swarming, risk advisory and sentiment analysis.

Why This Is Important

IT agent advisory features are a core capability of AI applications for ITSM that elevate these products from simply conversational agents such as virtual support agents. This expands capabilities to meet the needs of the ITSM practitioner (such as IT service desk or service manager) through advice and actions embedded in the UI of an ITSM platform or via an operations assistant conversational interface.

Business Impact

AI-powered IT agent advisory provides these benefits to infrastructure and operations (I&O) leaders and ITSM practice leads:

- Helps IT support tasks, enhancing cognitive connections for IT agents.
- Reduces costs associated with labor savings and faster resolutions.
- Improves accuracy in triage, classification, swarming and routing.
- Provides change-risk advisory to avoid disruptions and ensure reliability.
- Sentiment analysis improves service experiences.
- Frees up IT expert time from routine tasks.
- Optimizes processes through insights.

Drivers

- I&O leaders believe that AI can help them meet the challenges of current macroeconomic uncertainty to find cost savings through automation.
- I&O leaders recognize that AI can be used to improve the operational efficiency of I&O teams and look for agent advisory features from ITOM vendors.
- AI technologies such as GenAI and LLMs that enable AI-powered IT agent advisory features are evolving rapidly.
- Availability of IT agent advisory features in both ITSM platforms and AI applications in ITSM has increased rapidly during 2024 and 2025.

Obstacles

- Gartner's Critical Capabilities for Artificial Intelligence for IT Service Management found that all products on the market have significant room for improvement, particularly in areas such as intelligent escalation, which is part of agent advisory.
- I&O organizations often lack sufficient foundational data to train their AI capabilities — whether consistently categorized incidents or knowledge for their virtual support agent.
- AI skills such as prompt engineering are needed to maximize the benefits of agent advisory but are not yet sufficiently developed within I&O.
- Software that provides AI-powered IT agent advisory often requires an upgrade or additional software purchase that I&O leaders sometimes struggle to justify without evidence of proven ROI.

User Recommendations

- Use the Use-Case Prism: Artificial Intelligence for IT Service Desk to determine which AI use cases will provide the most transformational value while being sufficiently feasible to implement quickly.
- Invest in AI applications for ITSM to gain AI-powered IT agent advisory features. This could be paired with an operations assistant to use a conversational interface to leverage the advisory.
- Verify whether the incumbent ITSM platform can already meet these needs. If an add-on or upgrade is required, then assess the licensing and implementation costs before comparing with third-party solutions.

Sample Vendors

Aisera; Freshworks; ServiceNow; SymphonyAI

Gartner Recommended Reading

AI Use-Case Assessment for IT Service Desk

Magic Quadrant for Artificial Intelligence Applications in IT Service Management

Critical Capabilities for Artificial Intelligence Applications in IT Service Management

How to Achieve Success With AI at the Service Desk

At the Peak

Continuous Endpoint Engineering

Analysis By: Sunil Kumar

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 an 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 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" systems continues to increase, rendering traditional operating models obsolete.
- Organizations struggle with the broad scope of the Microsoft 365 offering as separate teams manage different components of Microsoft 365 without alignment and clear overall vision.
- 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.
- Organizations are investing in DEX, which offers a continuous view on the technology experience for employees allowing quick identification of potential issues.
- 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 demands 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.
- 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 acceptance testing of applications, enabling faster turnaround in onboarding new applications and updates.

Obstacles

- Overly complex environments have too many disparate tools that lack integration.
- Highly customized environments require extensive testing of every update prior to deployment.
- Fragile environments have a significant amount of technical debt, including legacy operating systems or applications that depend on unsupported browsers, runtime environments or plug-ins.
- Lower-maturity organizations have a siloed approach, which is inflexible, sluggish and lacks collaboration.
- Some staff 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 should:

- Keep pace with technology life cycles by implementing the complete CEE cycle which moves from product changes to applicability to pilot and test to stakeholder engagement to deploy/enable to measuring impact, and then the cycle starts again with product changes.
- Align CEE with the DEX strategy and DEX tools to provide user insights, faster detection of issues and streamline the CEE life cycle.
- Align CEE-related organizational changes to updated operating models including Gartner's digital workplace operating model, 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 user acceptance testing (UAT) by automating testing with new technologies.

Gartner Recommended Reading

Evolve the Digital Workplace to Improve DEX

Magic Quadrant for Digital Employee Experience Management Tools

Digital Workplace Maturity Assessment Tool

Digital Workplace and End-User Services Job Description Library

XLA

Analysis By: DD Mishra, Karl Rosander, David Groombridge

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Experience-level agreements (XLAs) aim to improve the 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 experiences.

Business Impact

The goal of XLAs is to improve end-user experience and business outcomes, which results in efficiency and talent retention. Traditional SLA measures, which are often transactional in nature, center around operational results and have limited success in measuring the entire user experience.

Drivers

- An XLA creates a composite of metrics for various KPIs that, when acted upon, results in improved experience. The underlying metrics should measure individual factors that make up the user experience, such as network performance at the end-user device, service desk experience and application experience.
- Traditional IT-centric performance measures fail to capture the end-user experience properly, as they rely on specific data points(generally when an incident occurs) that are a small component of the overall user experience. Outcome-centric experience measures are required to fix this challenge.
- Digital experience tools can measure each touchpoint in the overall user journey, which enables the XLA implementation and drives the motivation for capturing the touchpoints. These tools should also incorporate some measure of user feedback.
- The need for business outcome-based performance measures drives XLA adoption. XLAs enable the impact of IT systems and services to be mapped directly to business KPIs, which allows the business to create outsourced service deals that contract for defined business outcomes. XLAs deliver more executive-level metrics like productivity improvement, Net Promoter Score, etc.
- Outsourcing initiatives must demonstrate business value. Decisions about 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 impact of technology in capturing the experience of various signals and supporting the analysis of experience-related challenges has enabled the adoption of XLAs and made it easier.

Obstacles

- **Lack of awareness:** Many enterprises are unaware of how XLAs are contracted. This approach often misses the added value of prioritizing employee experience over operational efficiency.
- **Resistance to change:** Some enterprises are unwilling to embrace the workplace transformation required to improve the user experience. Very often vendors don't proactively mention it unless asked.
- **Inability to leverage flexible, dynamic sourcing approaches:** Many enterprises still rely on strict linear models that revolve around traditional RFIs/RFPs. This prevents them from using flexible and iterative approaches, such as co-creation, to evolve the requirements.
- **Implementation cost:** High initial implementation cost, due to tools deployment, is a limiting factor for clients that focus more on cost than value.
- **Implementation time:** Implementing XLAs often requires extra preparation and due diligence, along with change management, which can discourage clients from taking the next steps.
- **Variability in implementation**: When it comes to contracting for XLAs, no two vendors use the same framework for how to measure or how to be held accountable for outcomes. This makes it difficult for end clients to harmonize the different approaches.

User Recommendations

- Identify and configure XLAs that measure end-to-end user experience instead of individual metrics; for example, “speed of service,” which is a composite metric. The key to success is to implement monitoring and identify bottlenecks that focus on the employee experience, instead of just IT deliverables.
- Select partners that have demonstrated referenceable business improvement with a strong track record in process mapping, analytics and digital experience monitoring
- Improve internal operations by collaboratively identifying and addressing the leading causes of employee dissatisfaction.
- Implement an experience management office (XMO) for managing, monitoring and evolving the XLAs. The XMO should work closely with providers 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 to govern and implement XLAs, as well as reward and penalty regimes.
- Identify and select appropriate toolsets to trace the XLA data point.

Sample Vendors

Gartner Recommended Reading

Establishing XLAs When Engaging With IT Service Providers

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

Infrastructure Platform Engineering

Analysis By: Hassan Ennaciri, Paul Delory

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Emerging

Definition:

Infrastructure platform engineering (IPE) is the discipline of building infrastructure platforms as products that abstract complex IT infrastructure, making it easily consumable for users and other systems. Infrastructure platforms provide self-service tools for nonexpert users to deploy and manage infrastructure, while I&O retains governance, security and compliance. These platforms form the foundation for higher-order self-service layers such as internal developer platforms.

Why This Is Important

Organizations are pressured to innovate and deliver products faster while mitigating costs to meet customer needs. This requires adopting new operating models and modern practices to deliver scalable, reliable platforms that enable faster product delivery. IPE provides automated delivery of curated, secure, reliable and scalable infrastructure services made available via self-service or APIs, and reduces the effort and cycle time for users to request and access the products.

Business Impact

IPE simplifies complex infrastructure, delivering evolving platforms as products to meet customer needs. This agile approach empowers developers with self-service tools for on-demand access to environments, services and tools, boosting productivity and improving customer experience. It balances agility with control, enabling efficient, governed infrastructure management while accelerating digital transformation.

Drivers

- **Boosting business agility and innovation:** Demand to meet rapidly evolving customer needs and market conditions. Infrastructure platforms enable quick delivery of products and features, accelerating time to market and fostering innovation.
- **Modernizing infrastructure platform delivery:** I&O must evolve to strategic infrastructure management capabilities, providing self-service to empower their users.
- **Improving developer experience and productivity:** Abstracting infrastructure complexity reduces developer cognitive load and frustration. Self-service access to environments, services and tools streamlines workflows and maximizes developer productivity.
- **Strengthening compliance and security:** Integrating automated security and compliance controls directly into infrastructure delivery pipelines, in collaboration with security and risk teams, strengthens the organization's security posture.
- **Optimizing costs and efficiency:** Automation within infrastructure platform engineering drives scalability, reliability and security, improving operational efficiency and reducing resource costs associated with manual work and change-related downtime. Platform standardization further optimizes resource utilization and eliminates redundant tooling expenses.
- **Scaling operations effectively:** As organizations grow, managing infrastructure becomes increasingly complex. Infrastructure platforms provide a scalable solution, enabling I&O teams to support growth without a proportional increase in headcount or manual effort.

Obstacles

- **Skills gaps:** Building and maintaining infrastructure platforms demands diverse skills (automation, development, security, operations). This includes platform owners with the right mix of people and tech skills.
- **I&O organization silos:** The organizational structure of I&O teams is set up by domain specializations, making it hard to develop and deliver end-to-end services.
- **IT service management approaches:** Current approaches are process-heavy and rely on tickets and manual handoffs.
- **Initial investment:** Building an infrastructure platform requires an upfront investment in time, resources and tooling.
- **Demonstrating value:** Demonstrating the return on investment can be challenging in the early stages.
- **Tooling complexity:** The landscape of infrastructure automation tools is vast and complex. Choosing the right tools, integrating them effectively and avoiding tool sprawl can be difficult.

User Recommendations

- **Start small and evolve:** Define clear goals and objectives of the platform by understanding common user needs and delivering viable products that continuously evolve to meet those needs.
- **Build a dedicated team with the right skills:** Successful infrastructure engineering practice requires dedicated teams with diverse skills in infrastructure platforms and software engineering.
- **Identify and fill critical roles such as platform owner and platform architect:** Acquire new talent with the required technical skills, the right mindset and strong interpersonal skills. Develop existing resources by provisioning continuous learning opportunities.
- **Adopt a product mindset:** Treat platform users as customers. Talk to them and continuously get their feedback to meet their existing and future needs.
- **Measure and demonstrate value:** Track key platform effectiveness metrics (deployment frequency, cost, adoption and user satisfaction) and regularly report performance/value to stakeholders.

Gartner Recommended Reading

Adopt Platform Engineering to Improve the Developer Experience

How to Implement Cloud Platform Operations

Video: Demystifying Infrastructure Platform Engineering

How to Develop Infrastructure Platform Engineering Teams

Enterprise Service Management

Analysis By: Siddharth Shetty

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Enterprise service management is the use of service-management principles, tools and best practices to enhance service delivery and support to non-IT functions, such as HR, facilities and legal.

Why This Is Important

As a term, enterprise service management (ESM) has been in use for several years. However, only in the past couple of years has it been picked up by IT leaders as a means of streamlining operations, optimizing costs and providing a consistent user experience (UX). ESM promises to address inconsistencies in UX and user fatigue related to using different enterprise applications when consuming services from enterprise support functions such as IT, HR, facilities and legal.

Business Impact

The traditional approach to service delivery across enterprise IT, HR, facilities, legal and other functions relied on separate tools, separate portals, separate help desks, inconsistent UX and varied automation levels. ESM helps reduce application sprawl and harmonize UX when consuming enterprise services through cooperation among support functions and by leveraging integrated workflows and service delivery capabilities, such as case management, self-service and knowledge management.

Drivers

- Most prominent ITSM vendors are upselling ESM as part of their marketing strategies to extend workflow and self-service capabilities to other support functions.
- IT leaders are being called on by the head of IT and lines of business (LOBs) to lead ESM projects that consolidate best practices around end-user support and service orchestration to deliver enterprise services beyond IT.
- Reducing application sprawl will help address challenges with inconsistent UX, user fatigue and talent required to support the tools used for enterprise support.
- Opportunities to automate manual workloads across enterprise support groups reduce service delivery time and free up time for support teams.
- Traditionally, each support function had a different number of channels to support the end users. ESM offers multichannel support to provide business users with choices that align with demographic and hybrid workplace complexities.
- Employees face a disjointed experience when receiving services that rely on multiple disparate delivery groups — for example, onboarding and offboarding, due to lack of coordination between the support groups.
- ESM fosters collaboration across enterprise functions. Processes like employee onboarding, service reporting and service-level management are driven with better coordination and consensus among enterprise functions.

Obstacles

- ESM programs are usually focussed on ESM platform selection. Business outcomes and program roadmap are usually ignored in the pursuit of ESM tools/platforms, resulting in limited business value from the ESM program.
- Vendor definitions of ESM are aligned with their respective market offerings. This means that there is a general lack of standards and defined scope around the ESM market definition and its capabilities.
- Clients often underestimate the organizational change management and collaboration efforts required to implement an ESM program. This can undermine the success of the ESM program and affect stakeholder confidence.
- Few ESM vendors offer ESM as a product. Most offer ESM as a capability across their product portfolio. This means investments across multiple products, which will increase the total cost of ownership of the platform.
- ESM solutions have to ensure data segmentation for sensitive and confidential information, particularly for HR, legal and finance functions.

User Recommendations

- Start by involving stakeholders from other enterprise functions that are expected to be part of the ESM program. Address organizational change management-related challenges by forming a cross-functional collaboration team that develops the ESM strategy, plans and business communications.
- Develop an ESM strategy that incorporates short- and long-term business demand for enterprise services and the current business challenges that ESM is expected to address.
- Build an ESM practice that aligns to the ESM strategy. This should include considerations around how process, workflow and collaboration challenges will be addressed.
- Leverage ESM practice components that support business outcomes for ESM platform selection. This reduces risks with overbuying and delivers expected value from the program.
- Identify business value in terms of digital UX and customer satisfaction scores as additional factors to support your ESM program, rather than being driven only by ROI justifications.

Sample Vendors

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

Gartner Recommended Reading

3 Keys to Enterprise Service Management Success

Market Guide for IT Service Management Platforms

Key Functional Considerations to Identify Your Next ITSM Platform

How to Build a Successful Enterprise Service Management Program

Threat Exposure Management

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

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Threat exposure management encompasses processes and technologies that allow enterprises to continually and consistently assess the visibility and validate the accessibility and exploitability of their digital assets. It must be governed by an effective continuous threat exposure management (CTEM) program.

Why This Is Important

The diversity of modern infrastructure and reevaluation of what threat exposure is affect organizations' ability to accurately assess cyber risks. Security teams often struggle to identify modern exposures, leaving security gaps in systems such as SaaS and cyber-physical systems (CPS) security. Threat exposure management addresses these challenges by enabling identification, prioritization and validation of issues across diverse attack surfaces and ensuring comprehensive visibility and mitigation.

Business Impact

Threat exposure management governs and prioritizes risk reduction for the modern enterprise. It requires assessment of all business-related systems, applications and subscriptions, broadening risk understanding for today's digital landscape. CTEM programs factor in business importance, likelihood of attack, visibility of vulnerability and validation of the existence of an attack path, enabling businesses to mobilize responses to genuine, impactful risks.

Drivers

- Organizations' vulnerability management programs often lack alignment with business criticality. Organizations focus on volume rather than scoping a target set based on their priorities, leaving them with too much to do regarding their exposure and little guidance on which action to prioritize. Threat exposure management provides business alignment through the scoping process and helps reduce volumes of irrelevant or non-business-critical issues.
- A programmatic and repeatable approach to answer the question "How exposed are we?" is necessary for organizations. Threat exposure management aims to allow reprioritization of treatments as environments shift in a rapidly changing and expanding IT landscape.
- Organizations commonly silo exposure activities such as penetration testing, threat intelligence management and vulnerability scanning. Siloed views provide little or no awareness of the complete picture of cyber risk.
- Modern IT infrastructure, including subscriptions, SaaS applications and cloud environments, has introduced a much wider, more varied set of potential exposures, making organizations susceptible. Current approaches focus too much on traditional IT and vulnerability, when a large percentage of the exposure problem is focused elsewhere.
- Vendor offerings to identify threat exposures are evolving and consolidating into exposure assessment platforms (EAP), which offer greater visibility. This means that end users will have access to new information about potential threats without having to purchase new subscriptions.

Obstacles

- The increased scope of CTEM programs over traditional VM introduces many new complexities often not previously considered or budgeted for.
- While evaluating new exposures is necessary, effective response and the ability to mobilize a gradient of countermeasures, such as threat monitoring and control configuration, is lacking. Patching is the de facto response to vulnerability discovery.
- Processes to manage end-to-end awareness (from visibility of attack vectors to response to breaches) are virtually nonexistent in most organizations, which often simply scan their networks for compliance reasons. Regulations rarely factor in the exploitability of exposures.
- Assessing the complexity of attacks requires new skill sets. Market areas, such as adversarial exposure validation (AEV), make it simple to test the out-of-the-box scenarios using simulation tools. But users need new skills to be effective at using these capabilities and customizing scenarios.

User Recommendations

- Create agreements on tackling exposure with various organizational stakeholders, as success depends on it. Automated remediation from tools is unlikely to have a significant impact.
- Communicate the risks to the board. Senior executives must be aware of existing risks, and allocate resources to prepare against potential threats.
- Implement wider, more multiplatform programs, such as CTEM, to manage exposure. Include scoping and directional exposure awareness that deals with business-critical issues, not just “fire and forget” approaches.
- Prepare response and reaction plans. Monitoring for threat exposure issues is critical to limiting the potential impact of attacks. Validating that those exposures genuinely exist and security controls are functioning as expected is useful. However, it is essential that organizations also prepare reaction plans for the issues they may find to ensure resolution paths are effective.
- Include, in your CTEM program, assets that your organization doesn’t directly own, such as social media accounts, SaaS and data held by supply chain partners.

Gartner Recommended Reading

Implement a Continuous Threat Exposure Management (CTEM) Program

Reduce Threat Exposure With Security Controls Optimization

Market Guide for Adversarial Exposure Validation

Sliding into the Trough

Swarming Support

Analysis By: Julian Edwards, 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 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 the time to collaborate. It is an alternative to assigning tickets to functional or hierarchical 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 temporary support teams for certain high-profile issues. Swarming is a key aspect of collaborative support hubs.

Business Impact

Swarming support:

- Enables real-time resolution by directly accessing skilled, available support resource
- Brings expertise together from subject matter experts across IT
- Allows for increased productivity, as higher-priority incidents are resolved more quickly
- Helps facilitate collaboration between the IT service desk and expert groups
- Helps create knowledge articles more easily, as the agent is part of the dialogue
- Improves efficiency, as fewer tickets are sequentially passed between teams

Drivers

- The use of swarming in agile teams to complete features and user stories is showcasing its potential to other stakeholders and generating interest in support circles.
- Swarming is used to respond to high-priority incidents when major incident managers form agile response teams.
- Swarming occurs organically in peer IT support.
- Increasing availability of intelligent swarming capabilities is prompting interest and driving experimentation and uptake. The adoption of agile capabilities and collaboration is also driving adoption, with a focus on collaboration and breaking silos.
- The emergence of AI capabilities, including intelligent swarming, and the integration with event intelligence may make swarming automation more accessible.

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 in 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 counterculture 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.
- Product availability can be lacking in swarming-enabled solutions.

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 select set of applications and associated tickets to establish their viability and 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.

Gartner Recommended Reading

How to Integrate ITSM Teams With Product Teams

Quick Answer: How Can I Reduce the Impact of Major Incidents?

Innovation Insight: Collaborative Support Hubs

Essential Roles and Competencies for a Collaborative Support Hub

Observability

Analysis By: Padraig Byrne, Gregg Siegfried

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Observability is the characteristic of software and systems that enables them to be understood based on their outputs and enables questions about their behavior to be answered. Platforms that facilitate software observability enable observers to collect and explore high-cardinality telemetry using techniques that iteratively narrow the possible explanations for errant behavior.

Why This Is Important

The complexity of modern applications and the rise of practices such as DevOps has left organizations frustrated with legacy monitoring tools and techniques. These can do no more than collect and display external signals, which results in monitoring that is, in effect, only reactive. Observability acts like the central nervous system of a digital enterprise. Observability platforms surface data that allows system behavior to be better understood and anomalies to be detected and triaged.

Business Impact

Observability platforms have the potential to reduce both the number of service outages and their severity. Their use by organizations can improve the quality of software because previously invisible (unknown) defects and anomalies can be identified and corrected before service is degraded. By enabling stakeholders to better understand how their products are used, observability also supports the development of more accurate and usable software.

Drivers

- The term “observability” is now ubiquitous, with uses extending beyond the domain of IT operations. Care must be taken to ensure the term retains relevance when used beyond its original range of reference.
- OpenTelemetry’s progress and continued acceptance as the “observability framework for cloud-native software” raises observability and its toolchain.
- Traditional monitoring systems capture and examine signals in relative isolation, with alerts tied to threshold or rate-of-change violations that require prior awareness of possible issues and corresponding instrumentation. Given the complexity of modern applications, it is unfeasible to rely on traditional monitoring alone.
- Observability platforms enable an observer, a software developer or a site reliability engineer to explain and predict unexpected system behavior more effectively, provided enough instrumentation is available. Integration of observability with AI applications to automate subsequent actions is now becoming a reality for many observability platform vendors.
- Observability is an evolution of longstanding technologies and methods, and established monitoring vendors are well on their way to incorporating observability into their products. New companies are also creating innovative observability offerings at a fast rate.
- Expectations of IT services have evolved, driving enterprise software vendors to consider user experience as a key component of application success.

Obstacles

- In many enterprises, the role of IT operations has been to “keep the lights on,” despite constant change. This, combined with the longevity of existing monitoring tools, means that adoption of new technology is often slow.
- Enterprises have invested significant resources in their existing monitoring tools, which exhibit a high degree of “stickiness.” This creates organizational barriers to adopting new practices, such as those related to observability.
- Costs associated with observability platforms have grown as companies struggle to keep up with the explosion in volume and velocity of telemetry.
- Lack of skilled resources and a steep learning curve continue to be a constraint in implementing observability, particularly for less familiar techniques such as distributed tracing and continuous profiling.

User Recommendations

- Assess observability platforms’ ability to integrate into continuous integration/continuous delivery pipelines and feedback loops.
- Investigate problems that cannot be framed by traditional monitoring by using observability to add flexibility to incident investigations.
- Encourage observability practices by focusing on vendors that make it easy to use open standards for collection, such as OpenTelemetry.
- Tie service-level objectives to desired business outcomes using specific metrics and use observability platforms to understand variations.
- Ensure IT operations and site reliability engineering teams are aware of updates to existing observability platforms and how they may take advantage of them. Many traditional application performance monitoring vendors are starting to incorporate observability features into their products.
- Understand that even with observability, some services are still not possible to instrument, particularly third-party SaaS services. Organizations should use alternative methods, such as digital experience monitoring, to close such visibility gaps.

Sample Vendors

Chronosphere; Coralogix; Dynatrace; Grafana Labs; Honeycomb; Observe

Gartner Recommended Reading

Magic Quadrant for Observability Platforms

Critical Capabilities for Observability Platforms

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 collaborate with customers or product owners, using operational data and feedback, to define service-level indicators (SLIs) and service-level objectives (SLOs). Site reliability engineers work with product or platform teams to design, operate and continuously optimize systems that meet defined SLOs.

Why This Is Important

SRE has evolved reactive and proactive engineering practices that enable customer-focused reliability while supporting effective and efficient scaling. Individual organizations implement SRE in widely varying ways, depending on their goals. SRE teams can work with product and platform teams to help them achieve the levels of reliability that the product and platform owner are accountable for.

Business Impact

The SRE approach to improving reliability is intended for critical products and platforms that need to deliver customer value at speed and at scale while managing risk. Within each product or platform, the critical customer journeys, processes or transactions must be addressed also. The exact impact depends on the business driver impacted, for example, time to market, revenue and customer satisfaction.

Drivers

- Organizations are under pressure to meet customer requirements for reliability while scaling their digital services and are looking for guidance to help them.
- SRE has evolved since its initial implementations. Reliability remains the focus and integrates a rich body of knowledge that complements agile, DevOps and platform engineering approaches.
- Organizations that have adopted highly skilled automation practices (usually DevOps) and usage of infrastructure-as-code capabilities to deliver digital business products expand to incorporate reliability into these products.
- The most common use case, judging from inquiry calls with Gartner clients, is to leverage SRE concepts to improve the reliability of existing systems that are not meeting customer requirements for availability or performance or proving difficult to scale.

Obstacles

- Belief that reliability is an I&O responsibility only, rather than being a shared organizational goal.
- Organizations have difficulty shifting mindsets from service-level agreements with blanket availability statements to defining and measuring reliability in terms of customer-focused SLOs.
- Defining appropriate SLOs that reflect both business needs and user expectations can be complex.
- Finding SRE role candidates with the right mix of development, operations and people skills is a challenge for clients. This impacts initial adoption and scaling efforts.
- Rebranding of a traditional operations team without changing to adopt SRE practices leaves teams as SRE in name only, without the benefits.
- Clients have voiced problems with product owners who overly focus on functional requirements and not nonfunctional requirements, thus hampering improvements.
- SRE requires close collaboration between development and operations teams. Organizational silos can make it difficult to implement SRE effectively.
- SRE initiatives require executive sponsorship and investment to effectively scale.

User Recommendations

- Define your goals for SRE.
- Begin your SRE journey with a small focused initiative and then iteratively grow adoption. Demonstrate value to gain organizational commitment.
- Select opportunities that are politically friendly, will demonstrate sufficient value and have an acceptable risk profile.
- Automate for SRE efficiency. Identify repetitive tasks and automate them. This frees up engineers to focus on more strategic work.
- Work with the product owner to identify the SLIs and SLOs necessary to make customers and users happy — not to perfection.
- Implement monitoring and improve observability to objectively report on actual performance relative to error budgets and SLOs.
- Ensure product owners treat SLOs as a feature and are accountable for them.
- Instill collaboration among site reliability engineers, developers and other stakeholders.
- Create a community and leverage organizational learning practices while evolving SRE practices.
- Cultivate a blameless culture where mistakes are seen as opportunities for learning and improvement.

Sample Vendors

Datadog; FireHydrant (Blameless); Harness; New Relic; Nobl9; Sedai; ServiceNow; Splunk

Gartner Recommended Reading

7 Steps to Start and Evolve Your SRE Practice

Improve Customer Experience and Reliability With SLIs and SLOs

Tool: Sample Job Description for Site Reliability Engineer (SRE)

Market Guide for Site Reliability Engineering Tooling

Generative AI

Analysis By: Svetlana Sicular

Benefit Rating: Transformational

Market Penetration: More than 50% of target audience

Maturity: Adolescent

Definition:

Generative AI (GenAI) 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

GenAI is becoming real in enterprises. AI leaders from the 2024 Gartner AI Mandates for the Enterprise Survey reported an average spend of $1.9 million in fiscal year 2024 on GenAI initiatives, which reflects a belief in further GenAI potential. Governments are committing large funds to GenAI; vendors continue fast innovation, advancing model performance, multimodality, reasoning and agentic capabilities. Research of training data, explainability, fine-tuning, distillation and other aspects of GenAI exploitation is fast-paced and is reflected in commercial and open-source solutions.

Business Impact

GenAI has a strong momentum for expansion and deeper integration into business workflows across various business functions and industries. Fully integrated tools, accompanied by AI governance practices, robust education and IT support, enable enterprises to tackle critical business processes. Multimodal GenAI opens new opportunities in life sciences, transportation and education. The current focus for GenAI application is on productivity, automation and evolving job roles.

Drivers

- GenAI is proving its worth in life sciences, manufacturing, finance, law and entertainment. It is becoming more specialized and optimized for domains such as coding assistance, scientific discovery, research, diagnostics, legal analysis and financial modeling. Additionally, 78% of enterprises surveyed by Gartner have integrated or are planning to integrate the use of GenAI into some areas (see Technology Spending Drivers, Business Outcomes and Challenges for CIOs Across Industries for more information).
- Businesses aim to automate tasks, generate content and enhance customer experience by integrating GenAI into their processes. Prompt engineering is the main approach for custom GenAI use cases.
- Governments, spurred by the GenAI promise, are increasing investments in national AI strategies.
- Agentic AI is a top driver of a GenAI value proposition this year due to automation benefits and combining GenAI with other techniques.
- Fierce GenAI model competition continues. GenAI providers are introducing model quality and performance improvements, as well as more sophisticated reasoning and handling of image and video inputs. Galloping leaderboards list hundreds of large language models (LLMs), including a variety of smaller models that demonstrate precision and cost-effectiveness in specific domains and tasks, such as time series. Distillation, truncation and other methods to derive smaller models from large ones result in reduced latency and lower costs. Open-source LLMs democratize access to GenAI and stimulate ecosystem innovation.
- Technology vendors and service providers compete on GenAI applications and model offerings, and their enterprise readiness, pricing, infrastructure, safety and indemnification. Vendors and open-source communities offer better tooling for training, fine-tuning, evaluation and life cycle.
- Infrastructure innovations and investments are on the rise. Hyperscalers and some enterprises are building supercomputing systems that combine innovations in computational accelerators, high-speed networks and performance-optimized storage. Meanwhile, innovations like DeepSeek stimulate ideas efficiently with less advanced chips and lower costs.

Obstacles

- Estimating GenAI's value is challenging, with less than 30% of the AI leaders from the 2024 Gartner AI Mandates for the Enterprise Survey reporting that their CEOs praise AI investment returns. Organizations face productivity leakage, where GenAI adoption doesn't directly yield value.
- Technical challenges include security, model evaluation, data availability and quality, and managing compute for inferencing.
- Low maturity organizations have difficulty in identifying suitable use cases and face unrealistic expectations for GenAI initiatives.
- Advanced organizations struggle to find skilled professionals. New users necessitate GenAI literacy.
- Governance challenges include hallucinations, bias, fairness and establishing a governance operating model. Government regulations may impede GenAI initiatives.
- GenAI licensing and pricing are inconsistent among providers. Pricing remains confusing and constantly evolving, often catching customers by surprise.

User Recommendations

- Focus on problems that GenAI can solve effectively. Develop methods to identify impactful GenAI use cases that align with business objectives and offer tangible benefits.
- Design solutions to be loosely coupled with GenAI models to enable flexible model selection and combinations. Investigate GenAI vendor roadmaps to avoid spending your own resources on the capabilities that vendors will deliver in the future.
- Develop an AI-ready data strategy around your GenAI portfolio. Plan to incorporate your proprietary data into GenAI via retrieval-augmented generation or similar methods. Ensure data is relevant, clean, and accessible for GenAI models.
- Invest in AI literacy and talent upskilling for working with GenAI tools and technologies.
- Establish GenAI governance operating model, policies, controls and technical oversight. Consider both your and your vendors’ responsible AI practices.
- Plan for the cost of running GenAI initiatives, including infrastructure, compute resources and ongoing maintenance.

Sample Vendors

Alibaba Cloud; Amazon Web Services; Anthropic; DeepSeek; Google; Hugging Face; IBM; Meta; Microsoft; OpenAI

Gartner Recommended Reading

Generative AI: The Basics

Solution Path for Implementing Generative AI Systems

AI Technology Sandwich: A Conceptual Framework for Executing AI

10 Best Practices for Scaling Generative AI Across the Enterprise

Technology Change Automation

Analysis By: Chris Laske

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

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 delivery (CI/CD) tools and event intelligence platforms enable rapid delivery 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 using technology change automation to autogenerate change records, assess change risk, streamline approval processes and enable better visibility to changes, resulting in improved change velocity and quality while minimizing business disruption.

Business Impact

Technology change automation delivers value to I&O, as well as agile, organizations by:

- Integrating ITSM platforms with CI/CD pipelines tools to streamline change record creation.
- Leveraging AI for intelligent risk advisory to streamline and ensure proper classification.
- Automating change approval workflows to reduce delays.
- Automating conflict checks to avoid change collisions.
- Ingesting change record data into event intelligence 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.
- Inaccurate assessment of change risk can lead to numerous business disruptions.
- Poor visibility to production changes leads to delays in service restoration during major incident events.
- Need for audit compliance often requires some type of change record.
- Several AI apps in ITSM vendors are expanding beyond IT support use cases to automate change risk analysis and analyze historical change cases to identify standardization opportunities.

Obstacles

- Development teams that have adopted independent 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 and leverage AI effectively.
- 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 (such as value enablement and 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 (such as rapid business value enablement and delivery and cost of business disruption due to failed changes).
- Define request-for-change review criteria to utilize for converting policy to code. This approach identifies patterns in change evaluator decisions and converts them into policies that can be embedded in the change evaluation workflow.
- Build automated approval workflows for standard changes to include dynamic routing to enable autonomy and avoid bottlenecking. Use ITSM platform change management capabilities such as conflict checking, preapproved change-window validation and CI/CD tool integration.
- Enable integrations between ITSM and event intelligence platforms for change management data to improve correlation between incidents and changes.
- Begin leveraging intelligent risk advisory to utilize predictive analytics of prior releases for risk and impact assessments.

DEX Tools

Analysis By: Dan Wilson, Autumn Stanish, Stuart Downes, Tom Cipolla, Lina Al Dana

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital employee experience (DEX) management tools measure and help continuously improve the performance and employee sentiment related to company-provided technology. Near-real-time processing of data from endpoints, applications, employee sentiment and organizational context surfaces actionable insights and drives self-healing automations, optimized support and employee engagement. Insights and self-healing also enhance interactions with self-service portals and chatbots.

Why This Is Important

Despite increased investment in digital workplaces, gaps remain with measuring and improving DEX. Client interest in DEX has remained steady in recent years but primary use cases are IT operations focused. Mature digital workplaces increasingly invest in more strategic, experience-focused use cases with cross-functional DEX teams that target reduced IT overhead, and help the company retain and attract top talent.

Business Impact

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

- Reduced employee productivity-zapping digital friction
- Improved IT efficiency, visibility and automation
- Enhanced IT support, with quicker resolutions
- Improved endpoint configuration and patch compliance
- Better balance of objective and subjective success measures
- Optimized device costs by embracing performance-based refresh cycles
- More proactive, predictive and human-centric IT

Drivers

- A DEX strategy and DEX tools play a significant role in shaping the overall employee experience.
- Today's workforce relies heavily on technology to carry out their job responsibilities.
- When employees silently endure or find workarounds for issues they encounter, IT is unaware and unable to resolve them, leading to negative sentiment for IT.
- IT leaders demand broader measurement to supplement internally focused activity KPIs that have proven incomplete.
- IT administrators are looking for better visibility into how devices and applications 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.
- Desired for faster support interactions require service desk and other IT support analysts to have faster access to device configuration and performance data.
- Increasing threat of cyberattacks demands faster identification and remediation of configuration issues and missing patches.
- Companies are looking to reduce costs, e-waste and greenhouse gas emissions by replacing scheduled device life cycle strategies with performance-based strategies that increase life spans and maximize ROI.
- Increased importance of IT sustainability goals is driving demand for better visibility into endpoint power consumption, automation to adjust power settings, and ways to communicate directly with employees to encourage sustainable behaviors.
- AI and machine learning have significantly increased the perceived value and capability of SaaS-based DEX tools.

Obstacles

- Legacy IT cultures distrust the tool's insights and are threatened by automation.
- Cloud-averse organizations will be limited to less capable on-premises offerings.
- Low-maturity end-user services organizations will gain only partial value from a DEX tool's IT operations capabilities, and are unlikely to use experience-focused capabilities.
- An "ignorance is bliss" mindset, fearing that a sudden unveiling of the massive volume of issues will make themselves and overall IT leadership look bad.
- Developing a ROI story requires an organizational value on employee experience.
- Cost to acquire, implement and integrate new tools is often unbudgeted or perceived as high.
- There are often insufficient staffing levels, no clear owner for or skills required to operate a DEX tool.
- Limited ability to address organizational change management work can hinder reinforcing new behaviors and DEX tool adoption.
- Complexity involved with implementing DEX tools may deter organizations with limited technical expertise.

User Recommendations

- Develop well-rounded requirements, use cases and success metrics by collaborating with business and IT peers.
- 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 needs and budget by reviewing the Magic Quadrant and Critical Capabilities for Digital Employee Experience Management 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.
- Transform the IT operations culture to incorporate proactive support and 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

ControlUp; HP; Ivanti; Lakeside Software; Nexthink; Omnissa; Riverbed Technologies; ServiceNow; Tanium; TeamViewer (1E)

Gartner Recommended Reading

Magic Quadrant for Digital Employee Experience Management Tools

Critical Capabilities for Digital Employee Experience Management Tools

How to Successfully Deploy a DEX Tool

Digital Employee Experience

Analysis By: Tori Paulman, Dan Wilson

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Digital employee experience (DEX) refers to the employees' perceptions of, and interactions with, the technology they use for work, including applications, devices, services and, increasingly, AI agents. A DEX strategy empowers employees to adopt new ways of working by minimizing technology friction, supporting meaningful adoption, applying usage and performance metrics, and driving continuous improvement.

Why This Is Important

Across nearly every role, workers are spending an increasingly outsized portion of time working with applications, wearables and/or devices. Additionally, organizations continue to explore and deploy AI capabilities, making the state of their digital employee experiences critical to their productivity and satisfaction. A strategy for continuously understanding, measuring and improving DEX is essential to attracting and retaining talent, improving employee engagement, reducing total cost of IT operations and maximizing workforce productivity.

Business Impact

DEX strategies use experience best practices, such as personas, journey mapping, observability and employee listening, to identify and minimize digital friction. A holistic, coordinated approach to DEX across IT and non-IT partners can reduce silos and maximize benefits, which include improved workforce digital dexterity and well-being, ability to attract and retain valuable talent and help employees deliver against business outcomes. Workers who say that their relationship with IT transcends basic support are twice as likely to recommend their organization as a good place to work and want to grow their careers.

Drivers

- IT leaders must understand how workers and leaders perceive and value their relationship with IT and improve partnerships.
- Attention to improving DEX has been working. The Net Promoter Score, which measures whether workers believe they are working with modern technology and an engaged IT team, has risen dramatically from 22 in 2022 to 28 in 2024, according to the 2024 Gartner Digital Worker Survey.
- The proliferation of applications, devices and services has resulted in a workforce frequently toggling between applications. DEX strategies must reduce friction and improve the productivity of workers by helping them spend more of their time doing their core work functions.
- There is a wealth of data about employees' workstyles, productivity and friction. A DEX listening strategy turns the noise of telemetry and sentiment into insights — what we call workstyle analytics — while protecting employee privacy.
- Workers with the highest level of satisfaction with applications provided for work purposes are 1.2 times more likely to stay in the same company, according to the 2024 Gartner Digital Worker Survey.
- Personas, journey mapping, experience design and effective listening can ensure technology investments deliver expected benefits.
- Business leaders are increasingly looking for guidance on how technology can help boost employee productivity, engagement, well-being and digital dexterity.
- IT leaders are increasingly investing in DEX tools that collect, combine and derive actionable insights from employee feedback with measurements of technology performance, stability and use. These tools generate actionable insights and drive self-healing automations and optimized support.
- A focus on DEX often leads to reduced operational costs as large systemic issues are removed from the environment, enabling IT to shift focus from resolving technical issues to higher-value employee enablement initiatives.

Obstacles

- A strategy for DEX is an intentional shift from a focus on technology to a focus on humans, which can be difficult for tech-centric IT leaders to connect with.
- Focusing too much on DEX tools as an all-in-one fix often leads to suboptimal outcomes where stakeholders cannot see the value of your DEX investments.
- Proving a return on investment for investing in DEX tools requires rethinking traditional IT metrics.
- Trying to improve DEX is nearly impossible without HR partner buy-in to connect overall employee experience to DEX strategy.
- Software, services and staffing costs to acquire, implement and integrate DEX tools often require collaborative funding from both IT, HR and line of business.
- Many workers still see IT as a transactional break/fix service provider, so DEX leaders must more effectively communicate the value they are providing.
- Low-maturity IT organizations often discover their DEX ambitions are impossible if they are still working toward consistent backlog management and reliable service delivery.
- A cornerstone of DEX is digital dexterity and many IT organizations do not see it as their job to drive digital worker enablement.

User Recommendations

- Appoint (or volunteer to become) a DEX leader responsible for establishing a charter and vision that connects to mission-critical priorities.
- Strengthen key partnerships with IT peers, HR, communications, facilities and business leaders by connecting digital to the overall employee value proposition and developing broader success metrics.
- Catalyze employee engagement by assembling an influencers network to facilitate bidirectional feedback.
- Guide the focus of DEX strategies toward the highest-value activities by developing a listening strategy that blends quantitative experience scores and telemetry from devices, services and applications, with qualitative insights from surveys and voice of the employee.
- Prioritize high-impact personas, for example, revenue-generating roles or product developers, and connect DEX improvements to critical organizational outcomes by developing value stories.
- Develop high-impact DEX personas (for example, revenue-generating roles or product developers). Identify key moments in an employee journey, such as a worker's interaction with a customer or citizen, rather than trying to improve a less critical experience, such as viewing paid time off for all workers.
- Relentlessly pursue digital friction by looking for activities that require excessive effort, result in pain points or wait times and lead to worker questions or errors.
- Mine insights from interactions with self-healing, self-service portals and chatbots for opportunities to improve DEX at scale.

Gartner Recommended Reading

Nationwide Thrives With a Data-Driven Level 4 Digital Workplace

Design a Human-Centric Digital Employee Experience (TransUnion)

Tool: Digital Employee Experience Journey Map

Evolve the Digital Workplace to Improve DEX

Event Intelligence Solutions

Analysis By: Matt Crossley, Matthew Brisse

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Gartner defines event intelligence solutions (EIS) as the application of AI/machine learning (ML) and data analytics at the event management level to augment, accelerate and automate manual efforts in the event management process. EIS 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 of events from these tools has shifted the challenge from gathering data to interpreting and responding to it. EIS apply AI/ML and data analytics techniques to classify and cluster cross-domain events in near real time, at scale, and in ways that exceed human capacity. The resulting insights can augment human analysis, accelerate human response or automate a process to help resolve issues.

Business Impact

EIS deliver value through:

- **Agility and productivity:** By reducing alert fatigue through identification and correlation of related events so operators can focus on fewer, yet more relevant and 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 EIS capabilities is accelerating and fueled by:

- **Increasing complexity:** Organizations rely on a growing portfolio of monitoring and observability solutions to ensure the reliability and resilience of increasingly complex and distributed, hybrid and multicloud workloads.
- **Increasing monitoring expectations:** Investments and improvements in monitoring, and the pursuit of observability, generate more data from more sources. Increasing demand and advances in monitoring trends in areas, such as observability and digital experience monitoring, present operators with extremely detailed views into their applications, business services and the end-user experience. Effective use of this additional data requires near-real-time analysis and correlation of events from related assets and services.
- **Demand for reliability:** Shifts in roles and responsibilities are driven by modern operating models, like DevOps and site reliability engineering, in the pursuit of greater availability and faster incident resolution. EIS enable agility by offloading some mechanical tasks of event triage, root cause analysis and solution identification, accelerating response to common issues and freeing up human creative capacity for novel events and business priorities.

Obstacles

- **Unrealistic expectations:** Hype is a major obstacle to EIS adoption. Clients struggle to separate claims of AI and automation from achievable use cases. This impacts demonstrating the value of EIS, specifically, quantifiable return on investment.
- **Maturity of dependencies:** Benefits of EIS beyond event correlation, such as root cause analysis and remediation, require maturity in dependencies such as change management and automation.
- **Market complexity:** Monitoring and observability vendors are moving up the stack, EIS vendors are reaching into monitoring and observability domains, and AI applications in IT service management allow vendors to use AI capabilities to extend their reach.
- **Disruptive AI:** AI developments continue at pace, resulting in a proliferation of generative AI-based capabilities, moving toward agentic AI solutions and associated expectations. As these developments evolve, expect further changes in the definition of “state of the art,” and equal pressure on existing ways of working.

User Recommendations

- Establish clear, realistic use cases for an EIS 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 cross-domain analysis of an EIS with a mature monitoring and observability strategy. This approach creates a solid foundation of valuable data for ingestion and analysis, and the surfacing of insights across domains.
- Do not focus solely on automated remediation; this is rarely achieved at scale. Accelerating response and augmenting human decision making has tremendous value. These approaches often avoid the challenge of the probabilistic uncertainty, combined with automated change in production environments.

Sample Vendors

BigPanda; BMC Software; Dell Technologies; Digitate; Grokstream; Hewlett Packard Enterprise; IBM; Interlink Software; PagerDuty; Selector

Gartner Recommended Reading

Market Guide for Event Intelligence Solutions

Infographic: Using AIOps to Manage Operational Telemetry

Climbing the Slope

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, platform, 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 services are then made available through automation workflows, specialized platforms, self-service catalogs, direct invocation and API integrations.

Why This Is Important

IA delivers velocity, quality, efficiency and reliability through scalable, declarative approaches for deploying and managing infrastructure. These tools integrate into delivery pipelines targeting deployments that range from on-premises, hybrid and to the cloud, enabling infrastructure consumers to build what is needed when needed. Once deployed, IA provides day-two-and-beyond operational automation, and extends to policy compliance and policy enforcement capabilities.

Business Impact

IA services enable:

- **Agility and collaboration** — Fostering teams' autonomy by delivering what product teams need with security, cost and compliance requirements.
- **Productivity** — Version-controlled, declarative, repeatable, efficient deployments.
- **Cost improvement** — Reductions in manual efforts via increased automation.
- **Risk mitigation** — Compliance driven by standardized configurations and governance.

- **Quality assurance** — Removal of human error with automated repeatable deployments.

Drivers

IA tools support maturation beyond simple deployments through:

- Multicloud/hybrid cloud infrastructure delivery that is vendor- and platform-neutral
- Support for immutable and programmable infrastructures
- Predictable delivery, enabling automated operations
- Self-service and on-demand environment creation
- Integration into DevOps and Platform 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

- Combining the 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 overinvestment.
- Steep learning curves can cause developers and administrators to revert from familiar imperative methods using scripts for infrastructure-as-code-based declarative approaches.

- Demonstrating the return on investment (ROI) of automation projects can be challenging, especially in the short term.

User Recommendations

- Identify existing IA tools used to catalog capabilities. Recognize 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. Evaluate the use of GenAI as a means to upskill teams.
- Baseline how managed systems and tooling will be consumed (e.g., by engineers, self-service catalog, API or on-demand).
- Integrate security and compliance requirements into the scope for automation and delivery activities.
- Develop an IA tooling strategy that incorporates current needs and evolution of the near-term roadmap.

Sample Vendors

Amazon Web Services; Broadcom (VMware); IBM (HashiCorp); Microsoft; Perforce; Progress Software; Pulumi; RackN; Spacelift; Upbound

Gartner Recommended Reading

Market Guide for Infrastructure Automation and Orchestration Tools

How to Start and Scale Your Platform Engineering Team

Virtual Support Agents

Analysis By: Julian Edwards, 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 resetting passwords, deploying software, escalating support requests and executing scripts to restore IT services.

Why This Is Important

ITSM vendors leverage simple capabilities to meet chatbot requirements, which require manual effort to manage. A submarket of third-party vendors specializing in VSAs that integrate into ITSM platforms has emerged, claiming to have more sophisticated AI capabilities and competing against ITSM vendors. Large language models (LLMs) and GenAI dominate this topic, comprehending language nuances, generating relevant responses, adapting to conversational styles and revolutionizing virtual agents.

Business Impact

VSAs reduce support costs by handling incoming calls and live chats through knowledge-based articles transcribed into Q&A. They can also handle complex task-based actions like software requests and installations. VSAs save time by leveraging contextual information and offering extended support hours. Additionally, spikes in business user demands do not affect VSAs like they do IT service desk (ITSD) agents.

Drivers

- Cost optimization drives infrastructure and operations (I&O) leaders to identify new efficiencies, while necessitating cuts to services using human agents.
- According to the 2024 Gartner Digital Worker Survey (n = 5,141), reliance on IT for more than just solving a technical problem increased in 2024 over 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. Many have launched or are about to deploy LLM technologies, including GPTs.
- Many vendors have LLM-enabled conversational AI solutions, including ones tailored to the IT support use case of a VSA. Some even provide their own LLMs trained in IT support use cases.

Obstacles

- The 2024 Gartner Digital Worker Survey found fewer workers prefer VSAs over traditional IT support methods involving human interaction such as phone, chat and email.
- Security obstacles for VSAs include ensuring robust access controls and data protection measures to prevent unauthorized actions and safeguard sensitive information.
- 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.
- IT support users may decline to engage with VSAs if they are not enabled with both the capability and authority to take action on user requests.
- Add-on VSA products can be expensive, and this cost will be in addition to ITSM platforms that may already have similar but fewer features.
- Genuine VSA offerings are rare, as many marketed as IT support chatbots are general-purpose AI platforms that need further development. Often, their NLP capabilities and AI benefits for enhancing 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.
- Focus on high-impact use cases, supported by sufficient data, to ensure ongoing commitment toward VSAs.
- Invest in VSAs that offer multiple ways to engage with users (i.e., being accessible in the portal and 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 hallucinations (i.e., generated errors or nonsense) and privacy.
- Consider a general-purpose AI solution for call deflection or general case needs as a cost-effective alternative to ITSM-specific agents.

Sample Vendors

Aisera; Avaamo; Cognigy; Leena AI; Moveworks; Rezolve.ai; Serviceaide

Gartner Recommended Reading

Market Guide for Conversational AI Solutions

Applying AI — Business Domains

AI Use-Case Assessment for IT Service Desk

Market Guide for Artificial Intelligence Applications in IT Service Management

Magic Quadrant for Artificial Intelligence Applications in IT Service Management

Automated Incident Response

Analysis By: Pankaj Prasad, Padraig Byrne, Tanmay Bisht

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Automated incident response (AIR) centralizes the routing of events or incidents through a policy- or rule-based engine, on-call scheduler and streamlined collaboration. AIR improves operational efficiencies with action-oriented insights, shorter incident durations and automated workflows for event routing, seamless collaboration, remediation and escalations.

Why This Is Important

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

Business Impact

AIR solutions deliver value through:

- Quick incident resolution, minimizing customer impact
- Insights into incidents and their responses, which help improve process and operational efficiency
- Driving a collaborative approach for I&O and DevOps by integrating with multiple tooling categories
- Automated workflows that eliminate fatigue and human errors, and reduce the turnaround time
- Efficient dissemination of near-real-time information across the organization, especially the relevant stakeholders

Drivers

- **Streamlined and automated notification:** AIR automates communication across distributed teams, ensuring quick and accurate responder engagement. It enables organizations to overcome challenges of geographically distributed teams, remote workforce, complex on-call schedules and notification channel preferences, especially when dealing with incident triage when time is of essence.
- **Efficient data contextualization:** AIR tools enrich events, support remediation through run book automation and collect background context thereby saving time and enriching data that responders require for troubleshooting and incident resolution.
- **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 between various teams, and the time and action taken at each step of the incident. This provides vital information for postincident review (PIR) and process review, thus enabling further enhancements.
- **Workflow automation:** AIR tools can automate workflows that are part of processes like converting actionable alerts into incidents, opening a communications channel in instant messengers for collaboration, updating the real-time status on a web-portal and one-click remediation for existing run books.
- **Wider reach:** Use of AI, including generative AI and agentic AI, can drive adoption for a wider audience by translating technical jargon into easily understandable language, making it accessible for relevant stakeholders.

Obstacles

- **Overlapping capabilities:** The differentiating features of AIR solutions overlap with observability, ITSM and event intelligence solutions (EIS), making it difficult to articulate the value of investing in AIR.
- **Service definitions:** Service definitions are a complex part of AIR onboarding, necessary to connect alerts to responder teams, but challenging to configure. Configuration involves interpretation of a problem based on the event to accurately identify the domain experts that need to be engaged.
- **Portability between solutions:** Migrating from one AIR tool to another is a reset process. The integrations, team and service definitions, responder preferences, workflows 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 the impact of time lost in the process of manually contacting the right personnel for incident resolution to justify investing in these tools.

User Recommendations

- Evaluate the necessity of discrete AIR capabilities in a stand-alone solution by reviewing the features in your current observability, EIS and ITSM solutions.
- 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 observability and ITSM platforms leveraging bidirectional interface 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.
- Integrate incident workflow processes with ChatOps tools, such as Slack or Microsoft Teams, to improve incident communication and collaboration. Leverage AIR solutions' GenAI-based capabilities for data collection and summarization for post-incident review and analysis.

Sample Vendors

AlertOps; Datadog; Derdack; Everbridge; FireHydrant; Grafana Labs; incident.io; PagerDuty; Resolve.ai; Rootly

Gartner Recommended Reading

Innovation Insight: Increase Availability With Automated Incident Response

Entering the Plateau

Software Asset Management Tools

Analysis By: Yolanda Harris, Jaswant Kalay

Benefit Rating: Moderate

Market Penetration: More than 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, rationalize and downgrade software, monitor its consumption and provide key data to support software and cloud negotiations. SAM tools aggregate an organization's entitlement and consumption data, reconciling it to establish an effective license position (ELP) and reporting to properly govern software use.

Why This Is Important

SAM tools discover, inventory, normalize and reconcile on-premises, cloud and SaaS software consumption with entitlement data, allowing organizations across any industry and geography to streamline software licensing management. SAM tools provide near-real-time usage data, cost optimization opportunities and noncompliance risk reduction. These capabilities 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, SaaS licenses and subscriptions is a universal challenge that becomes more difficult with larger software estates, decentralized purchasing, complex licensing and hybrid environments.
- SAM tools help IT and procurement leaders govern the software asset life cycle by providing a consolidated view of an enterprise's software estate. They also support decision making and the ability to mitigate software compliance and security risks, optimize software spend and usage, and improve life cycle management.

Drivers

- Growth of cloud computing, SaaS and AI adoption has increased the complexity of SAM, with expanding requirements on cloud cost management, complex licensing rules, new and evolving consumption metrics and business-led technology buying.
- IT sourcing, procurement and vendor management (SPVM) leaders who invest in SAM tools gain visibility into software inventory and usage and improve the enterprise's ability to negotiate with software vendors and proactively manage risks.
- SAM tools help IT finance and budget owners gain insights into software expenditures for improved demand and forecasting, cost allocation and IT financial management.
- SPVM leaders are under pressure to minimize software licensing costs and 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. Enriched information, such as known vulnerabilities and exposures, end of life and end of support, becomes available, which enables enterprises to mitigate risks and plan for upgrades.
- SAM tools, within infrastructure and operations, have become valuable because they help consolidate and normalize data from various discovery and inventory sources. This cleansed data is essential for a robust configuration management database and accelerates adoption and value for IT service delivery.
- Management of the SaaS life cycle to reduce sprawl and security risks drives the need for tools that expand traditional SAM tool capabilities or replace them with SaaS management platforms and SaaS security tools. SaaS management platforms and SaaS security tools address cloud licensing challenges.

Obstacles

- Most sourced software fails to comply with ISO/IEC 19770-3:2016 standards, which provide guidance for software entitlement tags. Nonstandardized software entitlement tags may not integrate well with SAM tools. Furthermore, absence of standardized tags necessitates manual tracking and management of licenses. Such issues hinder adoption of AI-enhanced SAM tool features that remove manual effort and increase data sharing and integration with adjacent tools like IT service management or a configuration management database.

- Cloud services, hybrid environments and evolving compliance standards change the criteria for SAM tool features and leave gaps in their tool coverage. This often requires manual intervention and SAM managed service providers (MSPs) or additional data collection tools to produce an effective license position.
- Organizations often struggle to identify, differentiate and prove the value of SAM tools because of specific use cases and preexisting software tools that have adjacencies or significant overlapping capabilities with SAM tools.

User Recommendations

- Establish a clear, realistic scope by determining which three to five publishers you initially want to manage with your SAM tool. Prioritize them by compliance risks, spend volume, business criticality and/or renewal schedule. Develop a set of publisher management use cases the tool must deliver against and build on that to add publishers.
- Determine what license metrics and environments — for example, infrastructure 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 confirm data accuracy with data owners.
- Evaluate SAM MSPs that can complement investments in the SAM tool, support the tool implementation and address its limitations. Augment resources for tool administration and operations, such as entitlement loading, ELP creation, and actions to address noncompliance and savings opportunities.

Sample Vendors

Eracent; Flexera; Matrix42; ServiceNow; USU; Xensam

Gartner Recommended Reading

4 Keys to Unlock SAM's Strategic Value

The Future of the Software Asset Manager Is About Governance, Not Counting Licenses

Toolkit: 6-Step Business Case for Software Asset Management

Magic Quadrant for Software Asset Management Managed Services

Appendixes

See the previous Hype Cycle: Hype Cycle for ITSM, 2024

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

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

Source: Gartner (June 2025)

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 (June 2025)

Table 4: Maturity Levels

(Enlarged table in Appendix)

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

Source: Gartner (June 2025)

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 2024 Hype Cycle Builder

Market Guide for IT Service Management Platforms

AI Use-Case Assessment for IT Service Desk

Market Guide for Artificial Intelligence Applications in IT Service Management

A Blueprint for Modernizing Your ITSM Practice to Drive Digital Transformation

The IT Service Management Leader's First 100 Days

3 Keys to Enterprise Service Management Success

Key Functional Considerations to Identify Your Next ITSM Platform

Table 1: Priority Matrix for ITSM, 2025

Benefit	*Years to Mainstream Adoption*			
↓	*Less Than 2 Years* ↓	*2 to 5 Years* ↓	*5 to 10 Years* ↓	*More Than 10 Years* ↓
Transformational	Digital Employee Experience	Generative AI Infrastructure Platform Engineering Observability Service Response Site Reliability Engineering	Agent-Native I&O Threat Exposure Management	
High	Automated Incident Response XLA	AI-Powered IT Agent Advisory DEX Tools Infrastructure Automation Policy as Code Technology Change Automation	AI Applications for IT Service Management Autonomous Endpoint Management Enterprise Service Management Multiagent System Technology Dependency Hub	Natural Language Case Extraction
Moderate	Software Asset Management Tools Virtual Support Agents	AI-Focused Problem Management Continuous Endpoint Engineering Event Intelligence Solutions IT Knowledge Generation	Collaborative Support Hub Swarming Support	

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 to 5 Years*** ↓	***5 to 10 Years*** ↓	***More Than 10 Years*** ↓
Low		Operations Assistant		

Source: Gartner (June 2025)

Table 2: Hype Cycle Phases

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

Source: Gartner (June 2025)

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 (June 2025)

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 (June 2025)