# Hype Cycle for IT Management Intelligence, 2023

Published 20 July 2023 - ID G00792530 - 138 min read

By Analyst(s): Cameron Haight

Initiatives: I&O Operations Management

IT organizations are increasingly turning to IT management intelligence technology to improve IT operations, service management and cybersecurity. I&O leaders should leverage this Hype Cycle to assess the intelligent services, processes and technologies available to improve IT delivery capabilities.

**More on This Topic**

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

## Strategic Planning Assumptions

- By 2025, the use of synthetic data will reduce the volume of real data needed for machine learning (ML) by 70%.
- By 2026, generative artificial intelligence (AI) technology will account for 20% of initial network configuration, which is an increase from near zero in 2023.
- By 2026, augmented FinOps will have improved cloud cost optimization and reduced budget planning efforts by as much as 40%.
- By 2027, 90% of enterprises will use AI functions to automate Day 2 network operations, compared with fewer than 10% in 2023.
- By 2027, 80% of enterprises will have integrated AI-augmented testing tools into their software engineering toolchains, which is a significant increase from 10% in 2022.
- By 2027, AI-powered innovation teams will deliver projects that are as much as 75% more successful, compared with traditional human teams, leading to accelerated value generation from applied innovations.
- By 2028, the combination of humans and AI assistants working in tandem could reduce the time required to complete coding tasks by 30%.

# Analysis

## What You Need to Know

*This document was revised on 22 August 2023. The document you are viewing is the corrected version. For more information, see the* Corrections *page on gartner.com.*

AI empowers IT infrastructure, service, security and other operations teams to optimize processes, enhance performance and reduce risks in the delivery of IT services. Functions that can benefit from AI augmentation include:

- **Infrastructure deployment and management:** AI can assist in generating or suggesting portions of infrastructure templates. This includes analyzing patterns, understanding best practices, and leveraging historical data to provide recommendations or to generate code "snippets" for templates, manifests, playbooks, etc.
- **Observability and anomaly detection:** Teams using observability tools can benefit in multiple ways from AI. This includes reducing the volume of telemetry by intelligently filtering and enriching operational data. In addition, using natural language processing (NLP) allows operators to ask questions in a natural language, rather than interfacing through predefined dashboards or domain-specific query languages. Other technologies involve analyzing telemetry to identify the root causes and the impact of outages, and the ability to translate such information into human-readable output, rather than reading computer-generated log files.
- **Security and threat intelligence:** AI can reduce security-related risks through the analysis of network traffic, user behavior and system logs. It can correlate the data with threat intelligence to detect patterns that may represent behavioral anomalies that indicate a cyberattack or an unauthorized access.
- **Cost optimization and forecasting:** AI-based analysis may be able to provide recommendations with respect to cloud-based pricing — i.e., potentially leveraging the use of spot and/or reserved instances, instead of on-demand alternatives based on analysis of usage patterns. Clients can extend these capabilities to perform a future workload and pricing pattern analysis to inform budget planning efforts and cost optimization opportunities.

- **IT service support:** Enhance service capabilities leveraging chatbots and/or virtual assistants leveraging ML, enabling rapid and personalized support for a wide range of infrastructure and operations (I&O) and other requirements. AI-oriented systems such as these can understand and respond to user and administrator queries and assist in troubleshooting common issues. This reduces the burden on IT support teams, while enhancing user satisfaction by offering quick resolutions.

AI has an increasingly broad (and sometimes overlapping) array of scenarios in which it can be applied. Gartner recommends that IT organizations collaborate to develop an integrated "IT management intelligence" approach that focuses on the creation of an operating framework to establish a shared vision on the impact of AI in IT. This framework can be used to identify the most promising models, use cases, key performance indicators (KPIs) and mechanisms of governance. By harnessing the power of AI in a combined manner, IT organizations can optimize the unlocking of new possibilities and increasingly drive innovation in their respective functional areas.

## The Hype Cycle

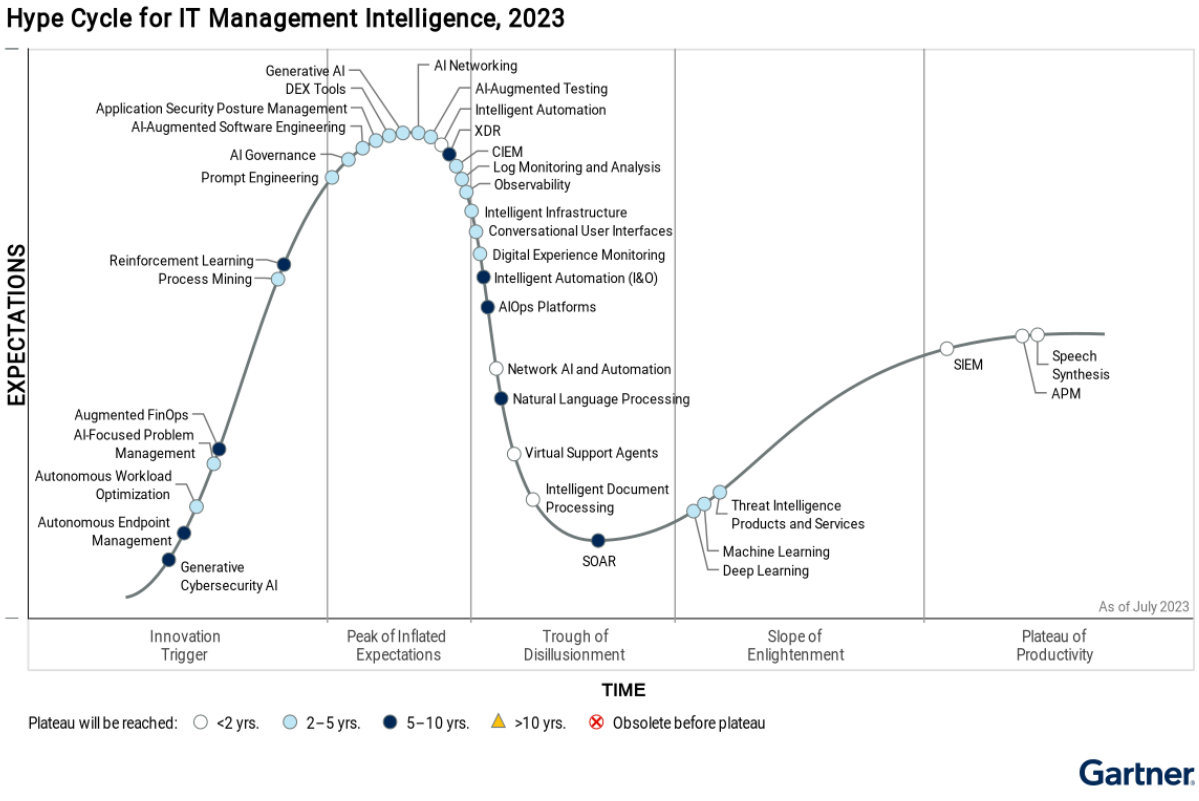
This Hype Cycle is designed to provide an integrated, cross-functional perspective on the application of AI and ML technologies, which is spread across several operationally focused and function-specific Hype Cycle representations. The points on the Hype Cycle for IT Management Intelligence are distilled from the following:

- The Hype Cycle for I&O Automation
- The Hype Cycle for Monitoring, Observability and Cloud Operations
- The Hype Cycle for ITSM
- The Hype Cycle for Agile and DevOps
- The Hype Cycle for Security Operations
- The Hype Cycle for Emerging Technologies

One of the driving forces behind the development of this Hype Cycle has been the emergence of generative AI, which is AI that assists in the development of content through the use of large language models (LLMs). Although LLM-based technology has been around for several years, it is the recent introduction of Generative Pre-trained Transformer (GPT) 3.5, followed rapidly by the availability of GPT 4.0 by Open AI that "GenAI" has taken the industry by storm. Enterprise IT organizations have begun to experiment with this technology, with a few already piloting applications using the approach. However, there remain many challenges in regard to production use of the content that is created, and there are initiatives underway in several governmental entities looking for ways to regulate its development.

Gartner believes that the adoption of increasingly sophisticated AI as an integral part of IT products, services and solutions will continue. This will include the creation of specialized or domain-centric AI models to improve infrastructure and application observability, enhance DevOps automation and improve self-service support.

## Figure 1: Hype Cycle for IT Management Intelligence, 2023



## The Priority Matrix

The Priority Matrix maps the time Hype Cycle entries are likely to require to achieve mainstream adoption against the level of benefit they can be expected to provide. As a result, this graphic is designed to answer two important questions:

1. How much value will an organization derive from an innovation?

2. When will an innovation be mature enough to provide this value?

During the next few years, generative AI will become a key enabler in the development of new, intelligent capabilities spanning across the I&O (including IT service management [ITSM]), software engineering and cybersecurity domains. As generative AI and NLP technology matures, use cases in one domain will grow in acceptance in other areas, such as where the functionality found in AI-augmented software engineering coding assistants is also leveraged in infrastructure-as-code (IaC) scenarios.

Generative AI technology will increasingly be leveraged to improve resource-intensive anomaly detection and remediation activities across a diverse spectrum of tooling. This includes AIOps Platforms, Log Monitoring and Analysis, APM and Observability, Problem Management and Threat Intelligence. Additional ML/AI technologies will be leveraged to improve IT's workload management ability via adjacent tooling, such as augmented FinOps and autonomous workload optimization technologies.

I&O and other IT domain leaders should increasingly collaborate on their investments in AI-infused IT management intelligence technologies to enhance their overall organizational ML skills, as well as limit potential AI technology procurement overlap.

## Table 1: Priority Matrix for IT Management Intelligence, 2023

(Enlarged table in Appendix)

| Benefit | Years to Mainstream Adoption | | | |
|---|---|---|---|---|
| ↓ | Less Than 2 Years ↓ | 2 - 5 Years ↓ | 5 - 10 Years ↓ | More Than 10 Years ↓ |
| Transformational | | AI-Augmented Software Engineering<br>Application Security Posture Management<br>Conversational User Interfaces<br>Deep Learning<br>Generative AI<br>Machine Learning<br>Observability | Augmented FinOps<br>Generative Cybersecurity AI<br>Natural Language Processing | |
| High | APM<br>Intelligent Automation<br>Intelligent Document Processing<br>Network AI and Automation | AI-Augmented Testing<br>AI Governance<br>Autonomous Workload Optimization<br>DEX Tools<br>Digital Experience Monitoring<br>Intelligent Infrastructure<br>Log Monitoring and Analysis<br>Process Mining<br>Prompt Engineering<br>Threat Intelligence Products and Services | AIOps Platforms<br>Autonomous Endpoint Management<br>Reinforcement Learning<br>SOAR<br>XDR | |
| Moderate | SIEM<br>Speech Synthesis<br>Virtual Support Agents | AI-Focused Problem Management<br>AI Networking<br>CIEM | Intelligent Automation (I&O) | |
| Low | | | | |

Source: Gartner (July 2023)

## On the Rise

### Generative Cybersecurity AI

**Analysis By:** Jeremy D'Hoinne, Avivah Litan, Mark Horvath, Wilco van Ginkel

**Benefit Rating:** Transformational

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

**Maturity:** Embryonic

**Definition:**

Generative cybersecurity AI technologies generate new derived versions of security-related and other relevant content, strategies, designs and methods by learning from large repositories of original source data. Generative cybersecurity AI can be delivered as a public or privately hosted cloud service or embedded with security management interfaces. It can also integrate with software agents to take action.

**Why This Is Important**

Enterprises witness many applications leveraging foundation models that can read multimodal objects (such as sensory data and images), following the first applications based on large language models (LLMs).

Cybersecurity technology providers can exploit generative cybersecurity AI to improve existing workflows, be a proxy of existing analytics, and generate security configuration or realistic attack data. Soon, applications will include autonomous agents, which can work using high-level guidance without a need for frequent prompting.

**Business Impact**

Existing vendors and new startups will add generative cybersecurity AI, expanding or replacing features. They will start implementing it with resource-intensive tasks, such as incident response, exposure or risk management, or code analysis.

Organizations will benefit from generative cybersecurity AI as it can improve efficiency and shorten response times to cybersecurity risks and threats. The pace of adoption will vary across industries and geographies due to security and privacy concerns.

**Drivers**

- ChatGPT is one of the most hyped and fastest-adopted AI technologies ever. It relies on generative AI foundation models, which are largely trained on massive internet datasets.
- Security operations center (SOC) teams cannot keep up with the deluge of security alerts they must constantly review, and are missing key threat indicators in the data.
- Risk analysts need to speed up risk assessments, and be more agile and adaptable through increased automation and prepopulation of risk data in context.
- Organizations continue to experience skill shortages and look for opportunities to automate resource-intensive cybersecurity tasks. Use cases for the application of generative AI include: synthesizing and analyzing threat intelligence; generating remediation suggestions for application security, cloud misconfigurations and configuration changes to adjust to threats; generating scripts and codes generation; implementing secure code agents; identifying and graphing key security events in logging systems; conducting risk and compliance identification and analysis; automating the first steps in incident response; tuning of security configuration adjustment; creating general best practice guidance.
- Generative cybersecurity AI augments existing continuous threat exposure management (CTEM) programs by better aggregating, analyzing and prioritizing inputs. It also generates realistic scenarios for validation.
- Generative AI offerings include the ability to fine-tune models, develop applications using prompt engineering and integrate with prepackaged tools and plugins through APIs. These possibilities open up a path for providers to add generative cybersecurity AI.
- Microsoft has already demonstrated a preview version of its security co-pilot feature, which is expected to drive competitors to embed similar approaches.
- Security program performance solutions and activities can solve their increasing demand for business alignment. Further, they can perform scenario planning for budget (re)allocation, and efficiency and effectiveness indicators and corrections.

**Obstacles**

- The cybersecurity industry is already plagued with false positives. Early examples of “hallucinations” and inaccurate responses will cause organizations to be cautious about adoption or limit the scope of their usage.

- Best practices and tooling to implement responsible AI, privacy, trust, security and safety for generative AI applications do not fully exist yet.
- Privacy and intellectual property concerns could prevent sharing and usage of business- and threat-related data, reducing the accuracy of generative cybersecurity AI outputs.
- As generative AI is still emerging, establishing the trust required for its wider adoption will take time. This is especially true for the skill augmentation use cases, as you would need the skills you are supposed to augment, in order to ensure the recommendations are good.
- Uncertainty on laws and regulations related to generative AI may slow down adoption in some industries, for example regulated industries in EU countries subject to GDPR compliance.

### User Recommendations

- Pick initial use cases carefully. First implementations might have a higher error rate than more mature techniques already in place.
- Monitor the addition of generative AI features from your existing providers and beware of “generative AI washing.” Don’t pay a premium before obtaining measurable results.
- Choose fine-tuned models that align with the relevant security use case or fine-tune in-house models from base models offered by the providers.
- Refrain from sharing sensitive and confidential data with hosted models until verifiable privacy assurances are provided by the host.
- Apply AI security frameworks, such as AI TRiSM. Work with your legal team on data privacy and copyright issues.
- Implement a documented approval workflow for allowing new generative cybersecurity AI experiments.
- Make it mandatory from a policy standpoint that any content (that is, configuration or code) generated by an AI is fully documented, peer-reviewed by humans and tested before it is implemented. If not possible, consider any AI-generated content as “Draft Only” when used for critical use cases.

### Gartner Recommended Reading

4 Ways Generative AI Will Impact CISOs and Their Teams

Innovation Insight for Generative AI

Market Guide for AI Trust, Risk and Security Management

### Autonomous Endpoint Management

**Analysis By:** Dan Wilson, Tom Cipolla

**Benefit Rating:** High

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

**Maturity:** Embryonic

**Definition:**

Autonomous endpoint management (AEM) represents the AI/ML-powered convergence of DEX and UEM tool capabilities. By automating endpoint and DEX management, AEM replaces traditional tools and architectures with lightweight, cloud-based, intelligence-powered capabilities. AEM supports agile approaches, reduces IT overhead and enables efforts to be redirected toward employee enablement and business-value-added work.

**Why This Is Important**

Increased dependence on technology and accelerated rate of change continue to overwhelm IT, undermine technology stability and degrade DEX. AEM uses cloud-powered intelligence to automate common endpoint and experience management tasks to free up IT for more value-added work. The overall goal is to improve device stability and compliance, and employee productivity and satisfaction to drive talent attraction and retention. IT will also be viewed as a business enabler rather than a hurdle or barrier.

**Business Impact**

I&O leaders can automate endpoint and DEX management tasks and reallocate efforts toward business value-added work. Specific impacts include:

- Reduced IT overhead through automatic resolution of issues that disrupt and impede employee productivity.
- Maintaining 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, persona or similar.

**Drivers**

- IT staff are overwhelmed with the growing number of endpoint devices, operating systems and applications.
- 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 UEM tools and modern management has reached critical mass as clients favor location-agnostic, cloud-based tools.
- Adoption of DEX practices and tools is growing rapidly.
- Cloud-based UEM and DEX tools are starting to demonstrate how ML-powered intelligence can quickly process a significant amount of data, provide actionable insights and recommendations, and execute automations.
- Expanding automation to perform other common administrative tasks or to apply standard policies and configurations is the next step in building toward AEM.
- Convergence could include other management tools and agents installed on endpoints.
- AEM directly supports the IT leader's goal of speed and agility.
- AEM use cases are promising in addressing the management of applications and replacing human execution of 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 mid-maturity 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 tools are unlikely to address niche use cases due to insufficient data to train ML and AI models to perform the automated activities.
- AEM is not possible on-premises, so cloud-averse organizations will not be supported.
- Organizations that lack experience with agile methodologies and automation skills, and operate under a legacy mindset that focuses on control and customization.

### User Recommendations

A few endpoint management vendors now offer AEM capabilities, so hype has moved slightly beyond the Innovation Trigger. Time to Plateau remains 5-10 years based on the historical adoption ramp for UEM and DEX tools. When reviewing long-term strategic plans, IT leaders should:

- Avoid lock-in by ensuring that strategic endpoint and DEX management vendors have a roadmap that directly provides or includes necessary partnerships to provide AEM capabilities.
- Reduce location dependence by migrating endpoint management, security, and identity solutions to the cloud.
- Prepare your organization by annually assessing current and future skill requirements, updating existing and defining new roles, and implementing strategies for upskilling and professional development.

- Eliminate inertia by evangelizing human-centricity and an enablement mindset, and embracing modern management principles and agile approaches.

### Sample Vendors

Ivanti; VMware

### Gartner Recommended Reading

Market Guide for DEX Tools

Magic Quadrant for Unified Endpoint Management Tools

## Autonomous Workload Optimization

**Analysis By:** Pankaj Prasad, Manjunath Bhat, Hassan Ennaciri

**Benefit Rating:** High

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

**Maturity:** Embryonic

### Definition:

Autonomous workload optimization tools maximize performance while minimizing resources through one or more of the three approaches. First, resource and cost optimization, including minimizing compute resources. Second, performance, including optimizing code for running applications, e.g., fine-tuning configuration of the underlying runtime. Third, dynamic workload placement, including reshuffling jobs and allocating resources to workflows for maximum utilization and minimizing idle time.

### Why This Is Important

Optimizing IT costs has always been on the agenda for infrastructure and operations (I&O) leaders. Additional pressures include becoming energy efficient and simultaneously ensuring optimal performance to customers. For the results to be impactful, this has to be done at scale while also dealing with the trade-offs required to optimize across the dimensions of cost, performance and energy. The scale and trade-off challenge is better addressed via autonomous operations and algorithms.

### Business Impact

Automated workload optimization tools enable organizations to optimize their IT costs, and avoid wastage of IT resources, while balancing the performance requirements of applications to ensure that customers are not impacted. These tools can enable organizations to become more energy efficient, and in the process, take a step closer toward their sustainability goals.

### Drivers

Once organizations achieve their targets for availability and performance, the next goal is optimization along a few dimensions:

- **Optimize performance:** Enterprises should aim for an optimal range of performance where cost is balanced while avoiding negative impact to customer experience, for example, by leveraging error budgets.
- **Optimize workloads and cost:** Mapping application resource utilization to demand patterns, especially in virtualized and cloud-native architectures, enterprises can dynamically project resource requirements thereby also optimizing their IT spend.
- **Energy efficiency:** I&O leaders are committing to sustainability goals and achieving greater energy efficiency is one of their primary targets. This is also a driver for sustainable software engineering.
- **Speed and scale:** Manual intervention in optimization goals will not be sustainable in the long run. The need to speed and scale is a driver for autonomous tools and processes.

Obstacles

- **Lack of maturity:** Ad hoc workloads and lack of appropriate tools to capture the right metrics are inhibitors toward realizing the full potential of workload optimization tools.
- **Standardization:** Many enterprises have a nonstandardized IT architecture where these tools will only tackle simple optimizations and require high efforts for significant results.
- **Collaboration challenges:** Data sharing between customer-facing, preproduction and production teams is crucial to ensure no negative impact due to optimization efforts. For e.g., to identify the appropriate error budgets and to ensure trade-offs do affect other operation areas like increase in errors.
- **Disconnect with business:** Business leaders' buy-in is crucial for continued investment, and is hampered due to a lack of appropriate reporting, i.e., translating resource optimization gains in dollar terms, proper tracking and trend analysis for comparisons.
- **Narrow focus:** Most of the tools in this space have a narrow focus on virtual operating systems or Kubernetes, limiting their adoption to workloads that leverage such architectures.

### User Recommendations

- Start small and get some perspective on resource utilization vs. performance to identify patterns and correlations. Use this data to pilot autonomous optimization for non-mission-critical workloads to prove value and capability before rolling out autonomous optimization for all applications.
- Use autonomous optimization as a driver for improving maturity in monitoring metrics and to speed up standardization initiatives across IT architectures and processes to maximize the value of optimization objectives.
- Improve collaboration across customer-facing, preproduction and production teams to ensure regular review and appropriate data exchange, including, but not limited to customer engagement, performance, IT resource requirement and utilization patterns, and capacity.
- Collaborate with business leaders and IT stakeholders to ensure measurements and benefits are suitably conveyed and business and technical objectives are appropriately captured.
- Optimize continuously, which means reviewing results, revisiting targets and refining goals since this has to be an ongoing effort.

### Sample Vendors

Akamas; CAST AI; Cisco Systems (Opsani); Control Plane; Google; Granulate; IBM; Sedai; StormForge

### Gartner Recommended Reading

Market Guide for Digital Platform Conductor Tools

Market Guide for AIOps Platforms

## AI-Focused Problem Management

**Analysis By:** Mark Cleary

**Benefit Rating:** Moderate

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

**Maturity:** Emerging

**Definition:**

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

**Why This Is Important**

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

**Business Impact**

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

- Reduces end-user frustration by reducing repetitive incidents.
- Reduces incident volume and cost by identifying underlying issues.
- Creates a more efficient problem management practice as the discipline becomes embedded.
- Helps understanding the health of the products and services provided by IT better.

**Drivers**

Organizations are attracted to the ability to:

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

### Obstacles

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

### User Recommendations

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

### Sample Vendors

Aisera; BMC Software; ServiceNow

### Augmented FinOps

**Analysis By:** Adam Ronthal, Dennis Smith

**Benefit Rating:** Transformational

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

**Maturity:** Embryonic

### Definition:

FinOps applies the traditional DevOps concepts of agility, continuous integration and deployment, and end-user feedback to financial governance, budgeting and cost optimization efforts. Augmented FinOps automates this process through the application of artificial intelligence (AI) and machine learning (ML) practices — predominantly in the cloud — to enable environments that automatically optimize cost based on defined business objectives expressed in natural language.

### Why This Is Important

In the cloud, it is now possible to assess the cost of a specific workload or collection of workloads assigned to a project. However, price/performance — the primary measure of cloud efficiency — is difficult to assess due to the complexity and diversity of choice in underlying cloud infrastructure and service offerings and a lack of consistency in pricing models. Augmented FinOps can automate this process by applying AI/ML techniques.

### Business Impact

The automation of cloud budget planning and financial operations will allow businesses to express their objectives — ideally in natural language — and allow their cloud ecosystems to automatically optimize the underlying cloud resources to meet those objectives. This will result in more efficient use of resources and, therefore, optimal spend by reducing/eliminating misaligned or poor use of cloud infrastructure and service offerings.

**Drivers**

- Practitioners are increasingly realizing that cloud is fundamentally a complex cost optimization exercise.
- Cloud adopters have a strong desire for transparency into cloud spending.
- Buyer inexperience is leading to either under-provisioning and associated resource contention or overprovisioning and spending more than is needed.
- Vendors are positioning cost-effectiveness as a competitive differentiator in their go-to-market strategies.
- Practitioners need to reduce the unpredictability of cloud spending when using cloud infrastructure and services for analytics, operational database management systems (DBMSs), data lakes and other applications, including custom IT infrastructure.
- Consumption-based usage remains common in earlier stages of cloud adoption, driving the need for augmented FinOps, although commit-based usage mitigates some unpredictability.
- Cost overruns are often obscured, downplayed, or dismissed by line of business implementers, requiring augmentation to achieve holistic and comprehensive cost optimization.
- Automation of financial governance controls in cloud environments provides increased predictability and cost optimization with less operational effort.
- Solid financial governance frameworks are positioning organizations to take advantage of FinOps.
- Emergence of specific roles — like FinOps practitioner or cloud economist — focused on FinOps practices and cost optimization means organizations have the expertise to address augmented FinOps.
- Owing to their complexity, cloud environments are ideally suited for the application of ML and AI methods to automate processes and track price and performance.
- Core FinOps capabilities are being delivered in three ways: Homegrown solutions, cloud service provider (CSP) instrumentation and third-party vendors. Increasingly practitioners are seeking out third-party or CSP tools to address their needs. All of these have a broad objective of adopting augmented capabilities as a means of competitive differentiation.

### Obstacles

- Cloud service provider pricing models remain needlessly complex and diverse.
- Cloud ecosystems are (and will remain) open to third-party participants, which implies multiple commercial arrangements with multiple providers.
- Standards for cloud cost, usage and billing data like the FinOps Foundation's FOCUS proposal have yet to be broadly adopted. APIs for communicating performance data within the context of a broader ecosystem have yet to emerge. Both of these are required to assess the primary measure of success: price/performance.

### User Recommendations

- Seek out service offerings to automate (via AI/ML) performance, consumption and pricing options. Increasingly, incorporate these capabilities into cloud data ecosystems that will learn from consumption patterns as they seek to optimize the underlying resources, and by extension, cloud spending through orchestration and optimization.
- Apply Gartner's FinOps Maturity Model to assess FinOps offerings in terms of their ability to address the following core capabilities: Observe, report, recommend, predict and optimize. The last three introduce augmented FinOps capabilities.
- Plan to use multiple tools to address the full scope of requirements. Many tools are broad in reach, but do not go deep into prescriptive recommendations. Others are tightly scoped and provide very targeted optimizations. Expect to spend time combining multiple tools to achieve broad and deep capabilities.

### Sample Vendors

Acceldata; Anodot; Apptio; Capital One Software; Densify; Enteros; Finout; OtterTune; Sync Computing; Unravel Data

### Gartner Recommended Reading

How to Identify Solutions for Managing Costs in Public Cloud IaaS

A Guidance Framework for Selecting Cloud Management Tools

Emerging Tech: Data Management Product Leaders Must Implement Augmented FinOps in Their Cloud Solutions

CDAOs and CFOs Must Drive Business Value in the Cloud Through Collaboration

Financial Governance Is Essential to Successful Cloud Data and Analytics

### Process Mining

**Analysis By:** Marc Kerremans

**Benefit Rating:** High

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

**Maturity:** Adolescent

**Definition:**

Process mining tools are designed to discover, monitor and improve business operations and processes by extracting knowledge from events captured from systems, applications and devices, in order to deliver visibility, understanding and insights. Process mining includes automated process discovery, conformance checking, social network/organizational mining; automated construction of simulation models, model extension, model repair, case prediction, and history-based recommendations.

**Why This Is Important**

Process mining provides visibility, analysis and understanding about business operations by providing near-real-time information to all end users about how they are currently performing, whether their processes are compliant, and what could be improved. If process mining tracks clients and their interactions, and their touchpoints with the organization as the main object rather than an order, invoice or request, then this can be seen as customer journey mining. These customer interactions are subsequently connected to internal operations.

**Business Impact**

Process mining provides a deeper understanding of previous customer contacts and underlying processes in order to enhance current and future interactions by understanding and aligning the customer's intent and the objective of the business. Showing which process improvements are necessary to meet and exceed customer expectations, process mining helps organizations in addressing how they can actively impact customer experience and customer retention through internal operational improvements.

### Drivers

- **Digital business:** In this era of digital business, business and sales leaders need a way to reflect on how new technological capabilities can provide value to the business and, ultimately, to the customer. Process mining can show how and where to activate these capabilities to create business value. Aligning and adapting these processes with client interactions is imperative to achieve targeted business outcomes.
- **Artificial intelligence (AI):** With the use of AI and advanced machine learning algorithms, data acquires meaning, and new and powerful insights can be derived from it. A powerful example of this data science in action, process mining shows how algorithms can be used as a mechanism to capture knowledge and insight in a packaged form that can be simply reused in a consistent fashion.
- **Task automation (RPA):** Process mining can complement RPA perfectly by assessing the processes to which tasks belong, and identifying “hot areas” in the organization, where a lot of effort is wasted in repetitive tasks. This results in long-term sustainable business value and averts the shortcomings of a short-term perspective focused on large, one-off cost savings.
- **Hyperautomation:** Not only is process mining a fundamental part in creating visibility and understanding before you automate. It also visualizes how different islands of automation are connected, and how continuously implemented and connected automation can be improved through its monitoring capabilities.
- **Business operations resilience:** Business operations resilience is the ability to alter operations in the face of changing business conditions based on a seek-model-adapt model. The techniques underlying process mining provide a new and enhanced way to encompass the sense and model capabilities. Based on available day-to-day operational data, the advanced process mining algorithms provide an accurate model of the ways of work in a format that can be understood by anyone in the organization.

### Obstacles

Obstacles that have kept process mining from a faster adoption can be classified into two main categories: Lack of awareness and misunderstandings.

Lack of awareness:

- After being considered for years as a purely academic technique, the collaboration of emerging process mining vendors with well-known enterprise applications, such as SAP, have heavily promoted process mining and shaped the process mining market.
- Recently process mining has moved into areas other than process discovery, such as customer interactions and social networks. It has even spread into areas such as Internet of Things (IoT), manufacturing and logistics distribution networks, supply chains, which have demonstrated sustainable value-creating capabilities of process mining.

Misunderstandings:

- Process mining needs application log files.
- Our organization is not mature enough.
- It is all about IT.
- Process mining itself improves processes
- Employees are monitored.
- Our organization has many manual activities.
- Our organization doesn't have the data.
- Our organization already has process maps.
- It is hard to justify the investment.

### User Recommendations

- Improve visibility and understanding of the actual performance of business operations, by investing in process mining. Actual quantitative data is delivered in a context that not only reveals information about a process, but connects this data to other constituents in a value chain, such as data about clients.
- Create awareness and inspire business and operational colleagues by introducing small, short-term pilots. Start a pilot on activities where the data is easily available. This starter project will already deliver value and will provide insights in where the next iteration needs more detailed data.
- Explore use cases that go beyond traditional mining use cases by targeting business operations and interactions with external parties such as customers. This can be seen as customer journey mining.

### Sample Vendors

ABBYY; Appian; Apromore; BusinessOptix; Celonis; IBM; Microsoft; QPR Software; SAP Signavio; Software AG

### Gartner Recommended Reading

Magic Quadrant for Process Mining Tools

Critical Capabilities for Process Mining Tools

Business Case for Implementing Process Mining

### Reinforcement Learning

**Analysis By:** Peter Krensky, Shubhangi Vashisth

**Benefit Rating:** High

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

**Maturity:** Emerging

**Definition:**

Reinforcement learning (RL) is a type of machine learning (ML) where the learning system receives training only in terms of positive feedback (rewards) and negative feedback (punishments). During problem solving, the system fosters actions or situations so that the overall reward is maximized while minimizing punishments.

**Why This Is Important**

Some problems can best be solved with RL, especially when other ML approaches are not feasible due to a lack of labeled training data.

**Business Impact**

The primary potential of RL is in industrial control and design, marketing and advertising, recommendation systems, and gaming industries. The technology can lead to significant improvements in self-driving cars, robotics, vehicle routing, warehouse optimization, logistics, predictive maintenance and other industrial control scenarios.

**Drivers**

- Recent successes across various industries (For example, text summarization and machine translation, real-time bidding for marketing and advertising, creation of dynamic treatment regimes in healthcare, optimized design of chip layouts in manufacturing, and optimization of robotic players in gaming.)
- Commercial vendors launching new RL products and products with embedded RL
- Sustained data scientist interest in the RL framework because it involves much less training data and supervision than currently dominant supervised learning schemes
- Faster compute capabilities are enabling more application scenarios for RL
- Better simulation capability is also an enabler of RL scenarios
- Reinforcement Learning from Human Feedback (RLHF) in which feedback from an AI community or user group is used to train better models
- Increased attention, interest and potential recognition due to generative AI hype

### Obstacles

- Limited RL capabilities offered by current data science and machine learning (DSML) platforms
- Often exceedingly high computational requirements
- Lack of good-enough simulations in many business situations
- Difficulty in designing the reward structure of the RL model for most business scenarios
- Often brittle or difficult-to-implement solutions with applicability in limited use cases
- Lack of staff with reinforcement learning experience
- Lack of explainability

### User Recommendations

- Apply RL in use cases requiring frequent model retraining with traditional techniques, because RL can adapt to new environment and circumstances
- Apply RL when the business outcomes and constraints are clear but you lack sufficient labeled data to build robust ML models.
- Acquire special expertise or engage a service provider with risk management support. The application of RL is currently riskier than most traditional techniques.
- Leverage off-the-shelf capabilities available from major vendors in the market, and seek out embedded reinforcement learning.

### Sample Vendors

AgileSoDA; Amazon Web Services (AWS); Dataiku; MathWorks; Microsoft; Pathmind; RISELab; TensorFlow

### Gartner Recommended Reading

Innovation Insight for Generative AI

Innovation Insight: AI Simulation

Go Beyond Machine Learning and Leverage Other AI Approaches

## At the Peak

### Prompt Engineering

**Analysis By:** Frances Karamouzis, Afraz Jaffri, Jim Hare, Arun Chandrasekaran, Van Baker

**Benefit Rating:** High

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

**Maturity:** Emerging

#### Definition:

Prompt engineering is the discipline of providing inputs, in the form of text or images, to generative AI models to specify and confine the set of responses the model can produce. The inputs prompt a set that produces a desired outcome without updating the actual weights of the model (as done with fine-tuning). Prompt engineering is also referred to as "in-context learning," where examples are provided to further guide the model.

#### Why This Is Important

Prompt engineering is the linchpin to business alignment for desired outcomes. Prompt engineering is important because large language models (LLMs) and generative AI models in general are extremely sensitive to nuances and small variations in input. A slight tweak can change an incorrect answer to one that is usable as an output. Each model has its own sensitivity level, and the discipline of prompt engineering is to uncover the sensitivity through iterative testing and evaluation.

#### Business Impact

Prompt engineering has the following business impacts:

- **Performance:** It helps improve model performance and reduce hallucinations.
- **Business alignment:** It allows subject data scientists, subject matter experts and software engineers to steer foundation models, which are general-purpose in nature, to align to the business, domain and industry.
- **Efficiency and effectiveness:** Alternative options, such as building a model from scratch or fine-tuning, can be much more complex, drive longer time to market and be more expensive.

#### Drivers

- **Balance and efficiency:** The fundamental driver for prompt engineering is it allows organizations to strike a balance between consuming an "as is" offering versus pursuing a more expensive and time-consuming approach of fine-tuning. Generative AI models, and in particular LLMs, are pretrained, so the data that enterprises want to use with these models cannot be added to the training set. Instead, prompts can be used to feed content to the model with an instruction to carry out a function.

- **Process or task-specific customizations or new use cases:** The insertion of context and patterns that a model uses to influence the output generated allows for customizations for a particular enterprise or domain, or regulatory items. Prompts are created to help improve the quality for different use cases — such as domain-specific question answering, summarization, categorization, and so on — with or without the need for fine-tuning a model, which can be expensive or impractical. This would also apply to creating and designing new use cases that utilize the model's capability for image and text generation.

- **Validation and verification:** It is important to test, understand and document the limits and weaknesses of the models to ensure a reduced risk of hallucination and unwanted outputs.

Obstacles

- **Embryonic nature of the discipline:** Prompt engineering processes and roles are either unknown or enterprises have a low level of understanding and experience. Gartner webinar polling data (over 2,500 responses; see Executive Pulse: AI Investment Gets a Boost From ChatGPT Hype) revealed that approximately 60% of respondents self-reported that they had not heard of prompt engineering. And 90% of those same respondents revealed that their organization did not currently have prompt engineers.

- **Role alignment:** Data scientists are critical to understanding the capabilities and limits of models, and to determine whether to pursue a purely prompt-based or fine-tuning-based approach (or combination of approaches) for customization. The ultimate goal is to use machine learning itself to generate the best prompts and achieve automated prompt optimization. This is in contrast to an end user of an LLM who concentrates on prompt design to manually alter prompts to give better responses.

- **Lack of business alignment:** There is often a lack of consensus on prompt engineering's business approach, as well as agreed-upon standards, methodology and approaches. This has led to fierce debates on the value of prompt engineering and how to establish governance.

- **Risk:** Beyond the early stages of awareness and understanding, the biggest obstacle may be that prompt engineering is focused on verification, validation, improvement and refinement; however, it's not without risk. Prompt engineering is not the panacea to all of the challenges. It helps to manage risk, not remove it completely. Errors may still occur, and potential liability is at stake.

### User Recommendations

- Rapidly build awareness and understanding of prompt engineering in order to quickly start the journey of shape-shifting the appropriate prompt engineering discipline and teams.

- Build critical skills across a number of different team members that will synergistically contribute critical elements. For example, there are important roles for data scientists, business users, domain experts, software engineers and citizen developers.

- Communicate and cascade the message that prompt engineering is not foolproof. Rigor and diligence need to permeate and work across all the enterprise teams to ensure successful solutions.

### Sample Vendors

FlowGPT; HoneyHive; LangChain; PromptBase; Prompt Flow; PromptLayer

### Gartner Recommended Reading

Quick Answer: How Will Prompt Engineering Impact the Work of Data Scientists?

Quick Answer: What Impact Will Generative AI Have on Search?

Accelerate Adoption of Generative AI by Offering an FMOps- or a Domain-Specific Partner Ecosystem

Glossary of Terms for Generative AI and Large Language Models

### AI Governance

**Analysis By:** Svetlana Sicular

**Benefit Rating:** High

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

**Maturity:** Emerging

**Definition:**

AI governance is the process of creating policies, assigning decision rights, and ensuring organizational accountability for risks and investment decisions for the application and use of artificial intelligence techniques. AI governance is part of adaptive data and analytics governance, addressing the predictive and generative nature of AI.

**Why This Is Important**

With AI now delivering value in the enterprise, data and analytics leaders observe that scaling AI without governance is ineffective and dangerous. Generative AI and applications, like OpenAI's ChatGPT, make AI governance a necessity, as using pretrained AI models billions of times sharpens risk concerns. The leaders want to balance AI's business value and the need for appropriate oversight. AI draws the attention of legislators worldwide, who mandate actions by clarifying AI governance priorities.

**Business Impact**

AI governance, as part of the organizational governance structure, enacts responsible AI, and provides common implementation and adherence mechanisms across the business ecosystem when it comes to:

- Ethics, fairness, and safety to protect the business and its reputation,
- Trust and transparency to support AI adoption via explainability, bias mitigation, model governance, operationalization, and collaboration norms and capabilities.
- Diversity to ensure the right technology and roles for each AI project.

**Drivers**

- AI governance is in the peak area of the Hype Cycle. Enterprise practitioners are taking steps toward establishing AI governance. Leading organizations in various industries establish AI governance by addressing standards for AI development and operations, providing best practices, guidelines for model management and monitoring, data labeling and interpretation, explainability, fairness, bias mitigation, security, and legal.

- Regulations around the globe target AI directly and affect AI practices indirectly, making AI governance goals more concrete. The U.S. Blueprint for an AI Bill of Rights provides governance pathways, from principles to practice. The objective of the EU AI Act is to "enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems." The Algorithmic Impact Assessment is a mandatory risk assessment tool intended to support the Treasury Board of Canada. Singapore's Model AI Governance Framework guides organizations in developing appropriate governance structures and mechanisms.

- Trust and transparency of AI solutions are crucial for AI adoption. The probabilistic and opaque nature of AI is new to audiences familiar with deterministic outcomes. AI governance can minimize misinterpretations of AI results by scrutinizing trust in data sources and the explainability of AI decisions. It provides specific testing and validation guidelines, differentiating "life-critical AI."

- AI governance is necessary to establish AI accountability. It is difficult to achieve because use cases differ in terms of their data, solution and outcome requirements. It outlines reactive responsibilities, actions and procedures in the case of unanticipated and unintended consequences. It ensures that ethics are considered for each use case.

### Obstacles

- Often, AI governance is stand-alone from mainstream governance initiatives, which stalls its progress. The best method is to extend existing governance mechanisms to take advantage of recognizable policies and methods, such as in data governance. AI governance benefits from a conversation with the security, legal and customer experience functions.
- Many governance initiatives assume command and control. Instead, adaptive governance supports freedom and creativity in AI teams but also protects the organization from reputational and regulatory risks. Little or no governance in AI teams to facilitate freedom and creativity is an acceptable approach if this is a conscious governance decision.
- AI value assurance and model risk management are new in AI. While methods exist — for example, in the financial industry — they are largely unknown to others, and every governance organization is inventing its own.
- Technologies to support AI governance are fragmented and are often designed for a single industry.

### User Recommendations

- Extend to AI your existing governance mechanisms, such as risk management or data and analytics governance.
- Establish and refine processes for handling AI-related business decisions. Blend processes, people and technology to succeed.
- Aim to align your AI governance framework with the laws and regulations in your jurisdiction(s) to directionally assure your efforts amid evolving AI-specific considerations. Gain agreement on AI risk guidelines that are driven by the business risk appetite and regulations.
- Decide on the organizational structure and accountability for propagating responsible AI — for example, what to centralize and what to do locally.
- Implement tools for AI review and validation. For each AI use case, require an independent AI model validator, a data scientist whose job is to assure model explainability and robustness. Have all parties in the process defend their decisions in front of their peers and validators.
- Ensure that humans are in the loop to mitigate AI deficiencies.

### Sample Vendors

Arthur; Chatterbox Labs; Credo AI; DarwinAI; FICO; Google; IBM; Prodago; SAS; Weights & Biases

### Gartner Recommended Reading

Applying AI — Governance and Risk Management

4 AI Governance Actions to Make a Swift Business Impact

Artificial Intelligence Primer for 2023

## AI-Augmented Software Engineering

**Analysis By:** Arun Batchu, Hema Nair, Oleksandr Matvitskyy

**Benefit Rating:** Transformational

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

**Maturity:** Emerging

### Definition:

The use of artificial intelligence (AI) technologies (e.g., machine learning [ML] and natural language processing [NLP]) to help software engineers create, deliver and maintain applications is designated AI-augmented software engineering (AIASE). This is integrated with engineers' existing tools to provide real-time, intelligent feedback and suggestions.

### Why This Is Important

Today's software development life cycle includes such routine and repetitive tasks as boilerplate functional and unit-test code and docstrings, which AIASE tools automate. AI-powered automation enables software engineers to focus their time, energy and creativity on such high-value activities as feature development. Emerging AI tools discover the configurations that meet operational goals. Software builders who use these tools remain productive and engaged, and they stay longer in their jobs.

### Business Impact

AIASE accelerates application delivery and allocates software engineering capacity to business initiatives with high priority, complexity and uncertainty, helping quality teams develop self-healing tests and nonobvious code paths. These tools automatically generate test scenarios previously created manually by testers, and detect test scenarios often missed by test teams. AIASE tools detect issues with code security, consistency or maintainability and offer fixes.

### Drivers

Demand drivers include:

- The increasing complexity of software systems to be engineered
- Increasing demand for developers to deliver high-quality code faster
- Increasing numbers of application development security attacks
- Optimizing operational costs

Technology solution drivers include:

- The application of AI models to prevent application vulnerabilities by detecting static code and runtime attack patterns
- The increasing impact of software development on business models
- The application of large language models to software code
- The application of deep-learning models to software operations

**Obstacles**

- Hype about the innovation has caused misunderstandings and unrealistic expectations about the benefits of AIASE.
- There is a lack of deep comprehension of generated artifacts.
- There is limited awareness about production-ready tools.
- Software engineers who fear job obsolescence have shown resistance.
- There is a lack of transparency and provenance of data used for model training.
- Uneven, fragmented solutions that automate only some of the tasks in the software development life cycle (SDLC).
- AI skills such as prompt engineering, training, tuning, maintaining and troubleshooting models.
- High model training and inference costs at scale.
- Intellectual property risks stemming from models trained on nonpermissive licensed code.
- Privacy concerns stemming from code, and associated proprietary data leaking as training data for AI models.
- Technical employees' fear of jobs being automated by AI.

### User Recommendations

- Pilot, measure and roll out tools only if there are clear gains.
- Verify the maintainability of AI-generated artifacts, including executable requirements, code, tests and scripts.
- Track this rapidly evolving and highly impactful market to identify new products that minimize development toil and improve the experience of software engineers, such as those that ease security and site operations burden.
- Reassure software engineers that AIASE is an augmentation toolset for human engineers, not a replacement.
- Pick providers (including open-source vendors) that supply visibility to training data and transparency on how the model was trained.
- Establish the correct set of metrics, such as new release frequency and ROI, to measure the success of AIASE.

### Sample Vendors

Akamas; Amazon Web Services; Diffblue; Google; IBM; Microsoft; OpenAI; SeaLights; Sedai; Snyk

### Gartner Recommended Reading

Innovation Insight for ML-Powered Coding Assistants

Infographic: Artificial Intelligence Use-Case Prism for Software Development and Testing

Market Guide for AI-Augmented Software Testing Tools

## Application Security Posture Management

**Analysis By:** Dale Gardner

**Benefit Rating:** Transformational

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

**Maturity:** Adolescent

**Definition:**

Application security posture management (ASPM) tools continuously manage application risk through collection, analysis and prioritization of security issues from across the software life cycle. They ingest data from multiple sources, correlate and analyze findings for easier interpretation, triage and remediation. They enable the enforcement of security policies and facilitate the remediation of security issues while offering a comprehensive view of risk across an application.

**Why This Is Important**

Modern applications are complex, and siloed data sources make visibility and control exceptionally difficult. ASPM supports integration and interoperability between application security and the DevOps environment, enabling organizations to implement DevSecOps policies and processes in their software development life cycle (SDLC). Orchestration enables specific test regimens and release controls. Prioritization and triage supports the ability to focus on the most critical issues while assessing risk in terms meaningful to all stakeholders.

**Business Impact**

ASPM aids security and software engineering teams by integrating and orchestrating application security tools and controls, improving visibility and control, and enabling the measurement and management of risk. Triage of application security data (including test findings and monitoring) brings increased productivity by prioritizing resources to focus on the most critical issues. ASPM delivers clarity and improved insights — both from an operational and risk-oriented view — into application security status.

**Drivers**

- ASPM evolved from and replaces application security orchestration and correlation (ASOC), adding breadth of coverage and additional features. Because of this, and the state of the market, its position on the Hype Cycle has been reset.
- AppSec and software delivery teams struggle with prioritizing remediation and mitigation efforts throughout the SDLC, given increased application complexity and the rapidly growing volume of data provided by application security tools. ASPM solves this challenge by ingesting information from multiple sources, correlating results and automating triage.
- Prioritization capabilities aid in gaining acceptance and support for security efforts among engineering teams. Too often, these teams are inundated with data from multiple tools. Consolidating information, evaluating its validity, and prioritizing remediation is a cumbersome process that doesn't scale to address the amount of data and the speed of engineering processes. Ensuring security concerns are addressed becomes more time-consuming and error prone, which fuels the perception that security is a barrier, not a benefit. ASPM can help validate warnings, ensuring teams focus on tasks offering the greatest risk reduction.
- Security and engineering teams have difficulty in reporting the business and other risk postures of applications, absent meaningful business metrics and threat intelligence. ASPM products can assist in translating raw vulnerability data into a form more relevant to executives and application owners.
- In organizations with diverse development and deployment processes, establishing automated controls for policy enforcement is complex, leading to a tendency to establish and enforce "one size fits all" approaches to policy definition. ASPM's integration and intermediation capabilities between application development and deployment processes and security controls offer the ability to centralize management of those controls and allow for more granular approaches to enforcement.

### Obstacles

- Effective automation of security testing presumes an organization understands the overall risk posture of an application, the types of testing needed and how best to respond to findings. If the underlying activities needed to develop this understanding have not been undertaken, efforts to articulate policies on which prioritizations and triage efforts will rely are complicated, potentially leading to reduced benefits from ASPM tools.
- Vendors tend to emphasize integration with either development or operations security tools. This presents a barrier to delivering a “full stack” view of an application’s security risks, spanning both developed code and infrastructure components. Progress to more broadly integrated products is evident.
- ASPM tools work by aggregating and analyzing data, and some level of abstraction is inherent. That poses a risk that critical information may be inadvertently overlooked in processing, yielding the potential for false positives, or a false sense of security.

### User Recommendations

- Prioritize ASPM in organizations with diverse development teams and a wide assortment of security tooling.
- Identify key stakeholders who will use an ASPM solution. Because underlying processes and outputs will affect many parts of the organization, stakeholder support is crucial to success in implementation and use.
- In particular, ensure the integration of ASPM with the development pipeline will provide a good developer experience, which will be a key to success.
- Evaluate the ability of tools to scale to process the amount of data generated across the application life cycle.
- Evaluate support for legacy applications, since many offerings focus on cloud native applications.
- Examine native ASPM capabilities (for example, as a feature of application security testing or other security tools) as an alternative to an investment in a dedicated solution. Such offerings may be effective in more homogeneous environments.

**Sample Vendors**

Apiiro; Bionic; Dazz; Enso Security; Kondukto; Legit Security; Rezilion; Synopsys; Tromzo; Wabbi

**Gartner Recommended Reading**

Innovation Insight for Application Security Posture Management

Guide to Application Security Concepts

How to Select DevSecOps Tools for Secure Software Delivery

Market Guide for Continuous Compliance Automation Tools in DevOps

Adapting Cybersecurity to the Agile Enterprise

**DEX Tools**

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

**Benefit Rating:** High

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

**Maturity:** Early mainstream

**Definition:**

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

### Why This Is Important

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

### Business Impact

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

- Fewer IT issues that disrupt and impede employee productivity.
- Reduced IT overhead through automation.
- Improved endpoint configuration and patch compliance.
- Better balance of objective and subjective success measures, including technology adoption, performance and employee sentiment.
- IT becoming more proactive and human-centric.
- Increased ability to retain talent.

**Drivers**

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

### Obstacles

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

### User Recommendations

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

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

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

### Sample Vendors

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

### Gartner Recommended Reading

How to Successfully Deploy a DEX Tool

Market Guide for DEX Tools

Employee Enablement Is Key to Digital Workplace Services Leaders' Survival

### Generative AI

**Analysis By:** Svetlana Sicular, Brian Burke

**Benefit Rating:** Transformational

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

**Maturity:** Adolescent

**Definition:**

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

### Why This Is Important

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

### Business Impact

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

**Drivers**

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

**Obstacles**

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

### User Recommendations

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

### Sample Vendors

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

### Gartner Recommended Reading

Innovation Insight for Generative AI

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

Emerging Tech: Venture Capital Growth Insights for Generative AI

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

ChatGPT Research Highlights

## AI Networking

**Analysis By:** Jonathan Forest

**Benefit Rating:** Moderate

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

**Maturity:** Adolescent

### Definition:

AI networking uses AI and machine learning (ML) to deliver granular and specific actionable network insights. AI networking can be a feature within a network vendor's management platform, a stand-alone multivendor platform or a part of an AIOps platform. It can also be delivered as part of a managed network service. AI networking primarily delivers Day 2 network insights. Further, it offers recommendations to accelerate incident resolution, and prevent outages and trouble tickets.

### Why This Is Important

AI networking can improve network availability and end-user experience, reduce operational resources required to manage networks, and decrease time to resolve incidents. Stronger AI networking products offer predictive management and simplified troubleshooting recommendations. They improve network performance which can't reasonably be achieved through manual resources. Ultimately, the goal is to provide a better experience for end users and more efficient network management for organizations.

### Business Impact

AI networking drives operational management savings of up to 25% by reducing the number of support calls, enabling a quicker incident response, improving network availability and optimizing the end-user experience. It simplifies network management so that the network team won't need deep configuration and troubleshooting skills. However, new data science skills may be needed. The adoption rate within campus networks appears to be higher than it is for other networking domains such as SD-WAN.

**Drivers**

- There are a handful of vendors that are actively investing in and promoting AI networking capabilities in the market.
- Many networking capabilities are becoming commoditized. In order to differentiate their offerings, some vendors are overhyping their capabilities and claiming that predictive analytics can eliminate most trouble tickets.
- Organizations are looking at how to optimize Day 2 operations by reducing incidents and accelerating the resolution of network incidents.
- Organizations want to improve network availability and network or application performance to enhance end-user application experience.
- Organizations seek to simplify networking and reduce reliance on deep skills by networking teams. They have had trouble finding staff to manage their network in-house and often choose to source network operations with a managed network services (MNS) provider. For some organizations, AI networking offers an alternative approach that allows organizations to manage the network in-house with fewer networking skills required.
- AI networking is seen as an approach to reduce the management costs of network operations, because it can reduce the amount of personnel required to manage the network. Since many recommendations are done automatically, the time to resolve incidents is shortened, which translates to fewer resources required.
- Platform teams and cloud teams are having a greater influence on networking decisions. They are preferring to use modern automation and data science techniques versus traditional approaches to network operations.
- AI networking helps to simplify managing increasingly complex network, security and application infrastructures. They now come with heterogeneous environments — think multicloud, data center, colocation and edge — and more layers of abstraction, such as containers and Kubernetes.
- The hype around ChatGPT promises to expand AI networking to include Day 0 and Day 1 operational tasks.

**Obstacles**

- Overzealous marketing creates confusion and makes it more difficult to select an offering that adds demonstrable value, slowing down overall adoption.
- Network operations personnel are generally risk-averse. They do not fully trust the AI networking recommended actions to remediate network incidents, or they need to validate the outcomes first, which minimizes the value.
- Core networking features and capabilities remain more important in customer buying decisions than AI networking.
- Many AI networking products or features are nascent, unproven and rather immature.
- AI networking vendors generally struggle to link capabilities to strong business cases, and enterprises struggle to determine a clear ROI.
- Enterprises already have trouble managing existing tools. Adding more tools will just exacerbate tool sprawl.
- Some network personnel are concerned about losing their jobs or having to change their way of working.

### User Recommendations

- Start small and iterate your use of AI networking solutions by validating and tracking the accuracy of the recommendations. When more recommendations and predictions prove accurate, you can start using the more automated recommendations over time.
- Start with a handful of high-priority use cases, such as ticketing or hardware. Minimize the risk by starting with noncritical production tasks or processes with a high chance of success.
- Investigate AI networking solutions that are integrated with broader network vendor offerings. Most mainstream networking vendors will have meaningful offerings in the next 12 months.
- Require vendors to deliver a concrete roadmap over the next one to two years, with specific details such as feature descriptions and timelines.
- Prefer multivendor solutions to avoid siloed tools and address broader use cases.
- Focus on the business case you are trying to solve by evaluating potential cost savings, time savings, agility benefits and end-user performance improvements.

### Sample Vendors

BigPanda; Cisco Systems; HCLTech; Hewlett Packard Enterprise (HPE); Huawei; Juniper Networks; MetTel; Palo Alto Networks; ScienceLogic; VMware

### Gartner Recommended Reading

Quick Answer: What Functionality Should I Expect From Network AIOPs Features?

Market Guide for AIOps Platforms

## AI-Augmented Testing

**Analysis By:** Joachim Herschmann, Jim Scheibmeir

**Benefit Rating:** High

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

**Maturity:** Adolescent

### Definition:

AI-augmented testing comprises AI- and machine learning (ML)-based technologies and practices to make software testing activities more independent from human intervention. It continuously improves testing outcomes by learning from the data collected from performed activities. It extends traditional test automation beyond the automated execution of test cases to include fully automated planning, creation, maintenance and analysis of tests.

### Why This Is Important

Software engineering leaders seeking to release faster without degrading quality are looking for more efficient ways of testing across all phases of the software life cycle. AI-augmented testing enables the automation of a broad set of testing activities related to requirement quality, design quality, code quality, release quality and operational resilience. This increases the degree of autonomy of those activities.

### Business Impact

The adoption of AI-augmented testing has the potential to significantly improve an IT organization's ability to serve and delight its customers. It can enable the adjustment of testing scenarios and overall software quality parameters as part of a continuous quality strategy aimed at optimizing the end-user experience. It will also help to constitute a closed-loop system that provides continuous feedback about critical quality indicators and helps to reduce the costs of creating and maintaining tests.

### Drivers

- A high dependency on human expertise and interaction limits how quickly modern digital businesses can design, build and test new software.
- Where automated testing is already in place, current levels of automation often remain below expectations due to a continued dependency on human intervention to maintain the automation as applications under test (AUT) evolve.
- The pressure to innovate quickly for market differentiation without compromising on quality relies on both a higher velocity and a higher degree of autonomy of the related activities.
- While delivery cycle time is decreasing, the technical complexity required to deliver a positive user experience and maintain a competitive edge is increasing. The answer is not more testing, but more intelligent testing enabled by AI technologies.

### Obstacles

- Currently available tools are still relatively new, have a narrow scope and still need to prove their value. Generative AI, in particular, is the latest and most disruptive example. Hallucinations (content that is nonsensical or untruthful in relation to certain sources), subpar training data, potential copyright violations and security issues are the main risks associated with that particular set of AI technologies.
- Waiting until better AI-augmented testing solutions are available leads to a loss in competitive advantage and fewer innovations. It also incurs greater testing costs and the risk of undertesting.
- Underestimating the time required to acquire new skills and setting wrong expectations about the time required to become successful can be obstacles.
- Gathering, cleaning and processing data and training the model are not trivial tasks, and require adequate skills. Moreover, they are not yet autonomous processes.

### User Recommendations

- Set the right expectations about the potential and limitations of AI-augmented testing and ensure that humans are always in the loop to verify the results produced by AI-augmented testing tools. This is particularly relevant for tools employing generative AI to automatically create tests, as generated tests may be completely useless or create false positives or negatives.
- Build a pilot team to map the cases where AI can provide the biggest benefits for software testing to the areas of greatest need in your organization. Evaluate opportunities to use it for test planning and prioritization, test creation and maintenance, test data generation, visual testing and test and defect analysis.
- Maximize the impact of AI-augmented testing by using it to enable a systematic approach to achieve the quality goals of business and development. Focus on key business value enablement and determine where it can help reduce cost and manage risk.

### Sample Vendors

ACCELQ; Applitools; Avo Automation; CodiumAI; Diffblue; Functionize; mabl; ProdPerfect; testRigor

### Gartner Recommended Reading

Market Guide for AI-Augmented Software-Testing Tools

Quick Answer: How Can AI Provide Benefits for Software Testing?

Innovation Insight for Continuous Quality

Improve Software Quality by Building Digital Immunity

Infographic: Artificial Intelligence Use-Case Prism for Software Development and Testing

### Intelligent Automation

**Analysis By:** Peter Liu

**Benefit Rating:** High

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

**Maturity:** Adolescent

**Definition:**

Intelligent automation (IA) is a combination of process automation and artificial intelligence (AI) technologies, which together empower rapid and continuous improvements in end-to-end process automation. It also contemplates the use of analytics and AI (especially machine learning) to make automated and intelligent decisions, and case management to provide processes with enough flexibility for end-to-end case management success.

**Why This Is Important**

IA enables fast end-to-end automation of business and operational processes leveraging AI/ML technologies. IA ecompasses various forms of automation for operation and business processes, including data centers, workplace services, networks, the edge and application availability. IA improves efficiency, scalability and reliability while reducing operating costs, human errors and enhancing productivity.

**Business Impact**

Business impacts are:

- Improves the productivity of employees, getting rid of repetitive tasks and enabling employees to focus on tasks that add value for the company, like innovation and creativity.

- Optimizes operational efficiency, enhances agility and reduces costs and response times by leveraging AI/ML techniques to perform event correlations and determines optimal actions using CSPs data.
- Uses analytics and AI to make automated and intelligent decisions.

**Drivers**

- Economic headwinds and shocks place an even greater importance on automation for CSPsto provide the required agility and efficiencies while retaining skilled talent.
- Technology vendors are increasingly embedding intelligent automation capability into their radio, network operation and management, BSS and CRM solutions to address the operation efficiency and complex challenges.
- Operation efficiency and lower operational costs are accelerating intelligent automation adoption in CSPs. Customers are also demanding SLA guarantees and higher availability, which are easier achieved by augmenting operations with AI-based automation.
- Maturing and expanding data science initiatives are leading to better AI/ML algorithms, new capabilities from Generative AI and LLM, more cost-effective computing power and a substantial increase in available data to support the emergence of intelligent techniques.
- The use of intelligence automation will transform how IT and network infrastructure is delivered and supported, including delivering more agility to address resource demand, which is attractive for CSPs building next-generation operation and management platforms.

**Obstacles**

- Although automation is not a new idea in the telecom space, adding artificial intelligence and reducing human intervention in the process cycle is a relatively new concept in the telecom space. Many CSPs have misconceptions about what to expect as IA becomes part of their work life.
- Building the right vendor strategy and integrating overlapping but disperate tools together to orchestrate, reinvent or recalibrate processes is increasingly challenging, with an abundance of choice of solutions and technologies for insurers to sift through.
- Employees lack skill sets to work effectively with the new tools that are now part of their workflow.
- Lack of executive support and business user involvement. Many intelligent automation projects are treated as a technology project without a business user involvement in the beginning.
- The accuracy of algorithm models is limited by the completeness and accuracy of the data being used. Fragmented data and data quality are always a major concern of a successful intelligent-based automation adaptation.

### User Recommendations

- Focus on improving the efficiency of the process before introducing intelligent automation — this is critical. Introducing intelligence and automation on top of an inefficient process tends to lead to a worse situation.
- Build a transformational mindset with respect to AI and automation across the company through accelerating your AI skills and talent development.
- Enhance context-awareness through establishing cross-team visibility and a strong data foundation for intelligence.
- Establish an automation roadmap through requesting intelligent capabilities into vendors' products — or consider how internal capabilities can be developed that can create this intelligent automation.
- Establish a new governance structure in business which has oversight of decisions made by AI. Create a safety net of what resources are allowed by AI to control and what are not.
- Avoid accelerating too fast with automation, build solid foundations in governance, organization structures and skills and competencies by growing from simpler use cases in a phased approach.

### Sample Vendors

Amdocs; B-Yond; Ciena; Ericsson; Guavus; Huawei; IBM; Juniper Networks; SS&C Blue Prism; Tupl

### Gartner Recommended Reading

Communications Industry: 2023 Top Tech Trends for CSP CIOs

Market Guide for AI Offerings in CSP Customer and Business Operations

Market Guide for AI Offerings in CSP Network Operations

The Gartner 2023 Predictions: Hyperautomation (Inclusive of AI, RPA & Low Code)

The Executive Guide to Maximizing Hyperautomation

## XDR

**Analysis By:** Eric Ahlm, Thomas Lintemuth, Franz Hinner

**Benefit Rating:** High

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

**Maturity:** Early mainstream

**Definition:**

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

**Why This Is Important**

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

**Business Impact**

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

### Drivers

- XDR platforms appeal to organizations with modest maturity needs due to the detection logic, mostly vendor-provided, that generally requires less customization and maintenance.
- XDRs appeal to organizations looking for improved visibility across the security stack, as well as those looking to lower the administration requirements of more complex incident response (IR) solutions.
- Midsize organizations that struggle to correlate and respond to alerts generated from disparate security controls appreciate the productivity gain from centralized XDR interfaces.
- Staff with the required skills to maintain and operate an extensible detection stack are hard to recruit and retrain.
- Purchasing a systemic detection stack in the form of XDR can simplify product selection and acquisition.

### Obstacles

- Single-vendor systemic XDR solutions may take years to replace in the case of effectiveness or efficiency issues.
- XDR's lack of extensibility for custom detections and other use cases could cause some clients to need both an XDR and a classic SIEM solution to meet multiple needs.
- Expanding an XDR detection stack's capabilities through the addition or replacement of security controls may be limited by the vendor.
- An XDR product alone does not always meet all needs for long-term log storage for use cases other than incident response, such as compliance, application monitoring and performance monitoring. XDR may also be a poor choice for a forensically sound system of record for things such as access data.

### User Recommendations

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

### Sample Vendors

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

### Gartner Recommended Reading

Market Guide for Security Orchestration, Automation and Response Solutions

## CIEM

**Analysis By:** Henrique Teixeira

**Benefit Rating:** Moderate

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

**Maturity:** Emerging

**Definition:**

Cloud infrastructure entitlement management (CIEM) capabilities help enterprises manage cloud access risks via administration-time preventive controls for the governance of entitlements in hybrid and multicloud infrastructure as a service (IaaS) and platform as a service (PaaS). They use analytics, machine learning (ML) and other methods to discover anomalies in account entitlements, such as accumulation of privileges, and dormant and unnecessary permissions.

**Why This Is Important**

Multicloud entitlement management is challenging, given the rapid increase in the number and complexity of entitlements, and the inconsistent cloud provider approaches to their definition and configuration. This challenge is getting worse given the proliferation of machine identities, which are orders of magnitude more numerous than human identities in cloud infrastructure. Managing cloud entitlements continues to be a responsibility of the client organization alone.

**Business Impact**

CIEM can help organizations to:

- Reduce the risk of misconfiguration by simplifying the effort to manage entitlements in multiple clouds.
- Reduce cloud attack surface and access risks posed by excessive permissions of machine identities.
- Improve agility in DevSecOps use cases by giving visibility to unnecessary developer privileges without disrupting developer flows.
- Extend privileged access management (PAM) use cases with easy-to-apply least privilege approaches.
- Simplify compliance with regulations like SOX and GDPR.

**Drivers**

- Cloud infrastructure and platform services (CIPS) providers keep adding more services, which in turn leads to a rapid increase in the number and complexity of entitlements to be managed.
- The proliferation of machine identities led to a volume of entitlements which is now orders of magnitude bigger than the number of human entitlements. It is estimated that the percentage of dormant machine identities has doubled in the last two years.
- CIEM has become a useful example of applied identity analytics for security posture management, and an enabler of the identity fabric immunity (see Top Trends in Cybersecurity 2023).
- CIEM capabilities that were originally only available from pure-play vendors, are now also being made available as optional modules embedded in cloud security posture management (CSPM) and converged cloud-native application protection platforms (CNAPP). In the identity and access management (IAM) space, a number of PAM vendors and a few identity governance and administration (IGA) vendors have developed or integrated CIEM functionality in their products. Cloud providers — except for Microsoft — have not invested in multicloud permission management capabilities.
- More mature CIEM providers have started to expand their scope beyond IaaS and PaaS, into SaaS, Kubernetes, access management (AM) tools and other identity providers (IdPs).
- Some CIEM providers have added more traditional IAM capabilities and configuration management, such as lightweight user and entitlement life cycle management, via integrations with Jira and ServiceNow for access requests and remediation.
- Some CIEM providers have broadened their scope into identity threat detection and response (ITDR), and security posture dashboards.

### Obstacles

- Per its original definition, CIEM is meant to address risks of multicloud permissions in CIPS only. More mature CIEM providers are expanding into SaaS, and AM targets, and adding PAM, CSPM or ITDR features. However, vendors and customers are still experiencing early challenges in understanding what CIEM can provide today, and what this technology may become in the future.
- CIEM has two possible buying centers in the organization — IAM or cloud security — which need to align. The uncertainty about which of these two areas should be accountable for the CIEM initiative can delay adoption.

### User Recommendations

- Adopt a pragmatic approach to evaluate CIEM functionality that starts with basic actionable intelligence to remove dormant entitlements.
- Use CIEM to manage entitlements of machine identities as well as for people.
- Maximize CIEMs value by capitalizing on its analytics capabilities to optimize posture management after removing unnecessary entitlements. Leading CIEM capabilities enforce least-privilege policies and remediate violations.
- Check if existing or prospective PAM, IGA and cloud security vendors offer CIEM capabilities to avoid redundant investments. Inversely, if choosing a CIEM stand-alone product, check how it may save you money by bundling CSPM, CNAPP and ITDR features.
- Use CIEM as part of a broader IAM and cloud security strategy to supplement IGA, PAM and CSPM technologies. CIEM will add identity visibility.

### Sample Vendors

Authomize; Britive; Ermetic; Microsoft; SailPoint; Sonrai Security

### Gartner Recommended Reading

Innovation Insight: Cloud Infrastructure Entitlement Management

Top Trends in Cybersecurity 2023

Emerging Tech: CIEM Is Required for Cloud Security and IAM Providers to Compete

Quick Answer: Cloud, Kubernetes, SaaS — What's the Best Security Posture Management for Your Cloud?

Magic Quadrant for Privileged Access Management

### Log Monitoring and Analysis

**Analysis By:** Pankaj Prasad, Gregg Siegfried

**Benefit Rating:** High

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

**Maturity:** Early mainstream

#### Definition:

Log monitoring and analysis solutions provide log ingestion, storage, interactive search, dashboards, alerts and advanced diagnostic analysis. Log-monitoring solutions apply advanced analytics or machine learning (ML) to reduce the operator's cognitive load through contextualization, correlation and analysis of large volumes of log data from multiple data sources.

#### Why This Is Important

Storing and searching log files is reactive and relies on human operators, which is not effective for IT architectures currently being deployed. The focus of traditional log monitoring is entity-centric anomaly detection and manual diagnosis. Automated log analytics uses statistical analysis, pattern recognition, correlations and machine learning to accelerate identification and resolution of service-impacting anomalies.

#### Business Impact

Log monitoring and analysis will impact:

- **Customer journeys** — Log analysis can help in behavior analysis and mapping user journeys, enabling better decisions.
- **Enhanced anomaly detection** — This enables monitoring of logs for patterns, which provides better insights into potential anomalies over static thresholds.
- **Operational efficiency** — Logical and temporal correlations of log data across multiple data sources enables better diagnosis and faster root-cause analysis.

### Drivers

- Data explosion with modern architectures — As organizations adopt geographically distributed, container- and microservice-based architectures, the amount of log data generated — already in the petabyte per day range at some organizations — will start approaching exabyte levels. At scale, collection, storage and gaining insights from logs is not feasible without automated analysis.
- Operational challenges — I&O organizations need to improve mean time to repair (MTTR) by reducing manual correlation effort time.
- Root cause analysis — I&O and site reliability engineering (SRE) teams looking for ways and means to enhance the resilience of their IT architectures need a faster way to identify correlating patterns and relevant logs beyond the system of interest.

### Obstacles

- Implementation — ML models demand heavy investment for either supervised or unsupervised training to be accurate over time, thus increasing the time to value for these solutions. The noncentralized nature of log data in many organizations further hampers the quality of outcomes.
- Basic use cases — These products do not enable ease of higher-order use cases beyond I&O due to the lack of an advanced interface that can be used by a data-scientist-type persona.
- Cost — Whether a log-monitoring solution is deployed on cloud or on-premises (as either an open-source or proprietary option), the licensing or maintenance costs increase with the volume of log data and data-retention policies. Balancing total cost of ownership (TCO) for log monitoring solutions and preserving historical information for analysis is a prevalent problem for I&O organizations.

### User Recommendations

- Simplify log analysis by establishing a log governance model that standardizes field names and data formats throughout multiple sources of log data. This facilitates the pooling of log data from multiple sources and results in more efficient queries.
- Evaluate advanced analysis and out-of-the-box capabilities and use cases during product assessment for log monitoring and analysis.
- Choose a solution that supports multiple sources of logs and broad use cases, and deploy them centrally. Log collection and analysis should not be deployed in silos.

**Gartner Recommended Reading**

Guidance Framework for Deploying Centralized Log Monitoring

Market Guide for AIOps Platforms

Infographic: AIOps Architecture for Analyzing Operational Telemetry

**Observability**

**Analysis By:** Padraig Byrne, Gregg Siegfried

**Benefit Rating:** Transformational

**Market Penetration:** 5% to 20% 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. Tools that facilitate software observability enable observers to collect and quickly explore high-cardinality telemetry using techniques that iteratively narrow the possible explanations for errant behavior.

**Why This Is Important**

The inherent complexity of modern applications and distributed systems 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 tools enable a skilled observer to explain unexpected system behavior more effectively.

**Business Impact**

Observability tools 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. By enabling product owners to better understand how their products are used, observability supports the development of more accurate and usable software, and a reduction in the number and severity of events affecting service.

### Drivers

- The term “observability” is now ubiquitous, with uses extending beyond the domain of IT operations. Although the 2020s are now the “decade of observability,” 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 (possibly adaptive) 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 tools enable a skilled observer, a software developer or a site reliability engineer to explain unexpected system behavior more effectively, provided enough instrumentation is available. Integration of software observability with artificial intelligence for IT operations (AIOps) to automate subsequent determinations is a potential future development.
- Observability is an evolution of longstanding technologies and methods, and established monitoring vendors are starting to reflect observability ideas in their products. New companies are also creating offerings based on observability.

### Obstacles

- In many large 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 nontechnical, cultural barriers to adopting new practices such as those based on observability.
- Costs associated with observability tools have grown as companies struggle to keep up with the explosion in volume and velocity of telemetry.

### User Recommendations

- Assess software observability tools to integrate into their continuous integration/continuous delivery (CI/CD) pipelines and feedback loops.
- Investigate problems that cannot be framed by traditional monitoring by using observability to add flexibility to incident investigations.
- Enable observability by selecting vendors that use open standards for collection, such as OpenTelemetry.
- Tie service-level objectives to desired business outcomes using specific metrics, and use observability tools to understand variations.
- Ensure IT operations and site reliability engineering teams are aware of updates to existing monitoring tools and how they may take advantage of them. Many traditional application performance monitoring vendors are starting to incorporate observability features into their products.
- Avoid the conclusion that observability is synonymous with monitoring. At minimum, observability represents the internal perspective, rather than external.

### Sample Vendors

Chronosphere; Grafana; Honeycomb; Lightstep; Observe; VMware

### Gartner Recommended Reading

Monitoring and Observability for Modern Infrastructure and Applications

Magic Quadrant for Application Performance Monitoring and Observability

### Intelligent Infrastructure

**Analysis By:** Philip Dawson, Nathan Hill

**Benefit Rating:** High

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

**Maturity:** Emerging

### Definition:

Intelligent infrastructure is built from simple, repeatable infrastructure building block components, integrated and managed in a standardized, automated manner. It optimizes infrastructure resources for application consumption through infrastructure machine learning (ML) and tuning as software overlays through an automated software intelligence plane.

### Why This Is Important

Intelligent infrastructure encapsulates generative AI and ML into the infrastructure configuration. Building on the capabilities of virtualization, it adds the dynamic hardware composition capability of a composable infrastructure to deliver a hardware configuration that is optimized for a specific application. Intelligent infrastructure additionally adds or feeds the generative AI/ML automation functions to the intelligence plane.

### Business Impact

Intelligent infrastructure is an innovation in delivering automated optimized systems for application delivery. It builds on earlier innovations, including converged, hyperconverged, software-defined and composable infrastructures, helping deliver hybrid cloud-like infrastructure on-premises or with a provider. It feeds off the application API-led programmable infrastructure that tunes infrastructure through system calls and requests, which improves application and infrastructure integration.

### Drivers

- IT leaders now recognize that cloud infrastructure, cloud platforms and cloud-native applications drive the overall composable, programmable and intelligent infrastructure journey.
- Cloud delivery and edge expansion are fueling the standardization of infrastructure, design and architecture and the expansion of the three areas to edge and Internet of Things (IoT) locations beyond remote offices/branch offices (ROBOs).
- Adding generative AI and automation on top of this infrastructure composition capability ensures that infrastructure is always optimized for the application load.
- In intelligent infrastructure, the “control plane” is enhanced with automation driven by infrastructure analytics ML, to become an automated “intelligence plane.”

### Obstacles

- The intelligence plane automates infrastructure and workload provisioning to application consumption. Intelligent infrastructure should not be tied to hardware features, but rather software functions.
- As with software-defined and composable infrastructures, traditional system vendors often tie intelligent infrastructure to hardware-related features, which can propel lock-in.
- Cloud management platforms are used as overlays for cloud migrations. Intelligent infrastructure has to adapt to hybrid cloud and multicloud delivery, delivering client value whether on-premises, with a provider or public cloud through anything as a service (XaaS).

### User Recommendations

- Select infrastructure solutions based on their ability to meet the current business requirements while still offering the flexibility to exploit the integration and automation of intelligent infrastructure innovations to be delivered over the next five years.
- Increase agility and business alignment by integrating application, asset management and sourcing information into the infrastructure intelligence and control planes as a drive to platform- and infrastructure-driven consumption models.
- Prepare for the evolution of application delivery and workload provisioning by incorporating intelligence/ML infrastructure functions with intelligent fabrics into your future system requirements.

### Sample Vendors

Cisco; CU Coding; Hewlett Packard Enterprise; IBM; Intel; Microsoft; Tintri; VMware

### Gartner Recommended Reading

How to Evolve Your Physical Data Center to a Modern Operating Model

Market Guide for Servers

Quick Answer: How Can I Optimize the Use of Programmable Platforms for Effective Software Delivery?

## Sliding into the Trough

### Conversational User Interfaces

**Analysis By:** Gabriele Rigon, Stephen Emmott, Van Baker, Bern Elliot, Frank O'Connor

**Benefit Rating:** Transformational

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

**Maturity:** Adolescent

#### Definition:

Conversational user interfaces (CUIs) are human-computer interfaces that enable natural language interactions for the purpose of fulfilling a request, such as answering a question or completing a task. The sophistication of a CUI can vary from understanding basic queries to handling complex multiturn dialogs, so CUIs range from Q&A bots to more advanced virtual assistants (VAs). CUIs fundamentally shift the interaction medium from traditional point-and-click to natural-language-driven.

#### Why This Is Important

UIs provide direct control between the user and the applications they are operating. In a CUI, this responsibility shifts from application-specific controls to conversational controls, and the CUI is determining the intent and acting upon it. This makes CUIs more widespread as agent (acting) UIs for software, devices and the Internet of Things. AI-enabled CUIs can provide a single, intuitive, common interface to multiple application functions across the entire organization.

#### Business Impact

Training, onboarding, escalations, productivity, empowerment and responsibility all change with CUIs and need to be embraced as part of CUI projects. AI-enabled CUIs can dramatically standardize and improve the usability of a variety of applications across all business functions, such as CRM, the digital workplace and ERP, hence improving efficiency. They can also benefit customer experience when used to automate support in the form of self-service chatbots or VAs.

#### Drivers

- **Users' expectations and generative AI:** Users increasingly expect to be able to hold conversations with and ask natural language questions of the applications they use. CUIs are beginning to complement or even replace traditional interfaces in a variety of applications, such as search and insight engines, business intelligence platforms and productivity software, such as document and spreadsheet applications. The trend toward the enablement of interactions in natural language between users (customers and employees) and software has been significantly accelerated by the hype around generative AI and ChatGPT.

- **Conversational AI platforms:** The underlying technology supporting custom-developed CUIs (like chatbots and VAs) built on top of conversational AI platforms (CAIPs) has matured significantly in the last few years. Vendors are investing in core AI technologies, such as large language models (LLMs), to improve components such as natural language understanding. They are also expanding their capabilities to support broader use cases beyond self-service chatbots and toward broader B2C and B2E automation.

- **Search:** CUIs will be increasingly used for knowledge search and retrieval based on document ingestion. Some technologies driving this include LLM-enabled enterprise applications, such as Microsoft 365 Copilot, as well as ChatGPT-like Q&A chatbots and LLM-powered VAs. This is also causing the market to be flooded with dedicated add-ons and even new vendors.

- **Multimodal interactions:** Generative AI methods are increasing the availability of multimodal interactions, such as those based on images, videos, audio and other sensory data. As a matter of fact, beyond text, voice is emerging as a primary modality of interaction between users and CUIs. This can add a powerful enhancement to the communications. Multimodality can solve some of the problems of the current generation of LLMs. Multimodal language models will also unlock new applications that were impossible with text-only models.

### Obstacles

- Developing CUIs is intrinsically complex and requires more effort than graphical UIs. More sophistication has to be built into VAs' conversational capabilities to deal with a range of users and edge cases. CUIs' predictions about users' intents can be wrong, so the CUI designer has to keep ambiguity in mind.

- Lack of CUI personality, poor accuracy and conversational design, as well as unreliability of answers generated by LLMs, can affect user sentiments negatively and, as a consequence, adoption and ROI.

- CUIs are available from many sources, whether offered by applications, CAIPs or through separate augmentation. For example, transactional conversational AI use cases require capabilities that only platforms can provide. Q&A scenarios may also be supported by architectures primarily leveraging search and LLMs. Understanding the sophistication and the limitations of these and other approaches is not trivial. This may lead buyers to choose the wrong tooling and many CUIs to fail.

### User Recommendations

- Treat CUIs as transformative, and plan on them becoming the dominant interaction model between users and applications.
- Prioritize the requirements of your custom CUIs in terms of sophistication, integration and control. Do not underestimate the risks of building CUIs that do not meet enterprise-grade performance, accuracy and security standards.
- Develop your strategy for consolidation upon one or few conversational AI platforms or approaches, avoiding challenges that derive from the proliferation of CUIs deployed by different business units in different regions.
- Educate stakeholders around benefits and limitations of generative-AI-enabled CUIs, and encourage well-informed employees to experiment with such CUIs.
- Prepare for new roles and skills in the enterprise. Dialogue designers and AI trainers, for example, are needed to enable custom CUI initiatives. Citizen developers will acquire prompt engineering and model management skills to leverage generative-AI-enabled CUIs effectively.

### Sample Vendors

Amelia; Avaamo; Cognigy; Google; IBM; Kore.ai; Omilia; OneReach.ai; OpenAI

### Gartner Recommended Reading

Magic Quadrant for Enterprise Conversational AI Platforms

Critical Capabilities for Enterprise Conversational AI Platforms

Competitive Landscape: Conversational AI Platform Providers

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

## Digital Experience Monitoring

**Analysis By:** Mrudula Bangera, Padraig Byrne

**Benefit Rating:** High

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

**Maturity:** Mature mainstream

### Definition:

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

### Why This Is Important

DEM helps organizations address visibility in two key areas:

- **Remote employees' experience:** Instrumenting the corporate network is relatively easy. Doing the same for a home or coffee shop network ranges from challenging to impossible.
- **Web applications:** Visibility into the performance of as-a-service-based applications (including e-commerce) presents a unique challenge, due to the location of the application and difficulty in instrumenting cloud-based environments.

### Business Impact

RUM and STM technologies in DEM allow businesses to understand how the users (customers) are interacting with the brand across mobile and web. The endpoint monitoring technology gives organizations increased flexibility to gain visibility into the endpoint, network and service of the user, irrespective of where workers are located, and without requiring extensive instrumentation of the physical environment.

Drivers

- **User experience:** Organizations are coming to the realization that metrics tell only part of the story. If the user is having a less-than-ideal experience, then whatever the metrics say are meaningless. DEM can help provide visibility into not just the metric-based performance, but also the subjective portion of the user experience.
- **SaaS:** As organizations move from on-premises-based applications to SaaS-based applications, they lose visibility into, and control over, the performance of these applications. A user of a SaaS-based application in one location using a specific endpoint (such as a laptop or mobile) may have a totally different experience from a different user at a different location using a different endpoint. Even the same user at the same endpoint may have very different experiences, depending on where they are located at the time. DEM enables organizations to understand where the performance bottlenecks are, so they can be addressed.
- **Work from anywhere:** The massive changes in workforce location brought on by the COVID-19 pandemic are driving infrastructure and operations (I&O) teams to adopt endpoint monitoring technologies to analyze and optimize remote workers' access to, and use of, applications.
- **"Last mile" in full-stack observability:** Monitoring of applications from the server side is important, but I&O teams need to understand the end-user journey and the corollary experience. Endpoint monitoring through DEM tools allows I&O teams to track performance from the endpoint's connectivity to Wi-Fi through service provider networks and beyond.
- **Commercial off-the-shelf (COTS) and virtual desktop infrastructure:** Organizations often rely on COTS applications for critical business operations. The very nature of these solutions makes them difficult (if not impossible) to instrument from an application perspective. I&O teams rely on the visibility provided by DEM tools to provide information on performance from the end user's perspective.

### Obstacles

- There are very few DEM vendors that provide functionality across all three pillars of DEM (synthetic monitoring, endpoint visibility and real-user monitoring), making it difficult to choose a vendor that can provide a complete solution.
- Most DEM visibility comes from an agent installed on the endpoint, which can represent a challenge for organizations that are already running numerous endpoint agents.
- Large organizations may struggle with the management of tens or hundreds of thousands of endpoints via a DEM tool user interface.
- Due to the sheer volume of data generated by DEM tools, organizations without a robust analytics approach may struggle to make sense of all the data. Few vendors use analytics to enable a proactive approach in this space.
- User experience can be enhanced through autorectification of anomalies. However, very few DEM vendors provide the ability to automate remediation.

### User Recommendations

- Gain a holistic view of digital experience by choosing and deploying DEM solutions that gather sentiment alongside other data points.
- Minimize endpoint performance impacts by evaluating DEM capabilities from vendors and tools you already own (for example, DEM capabilities from a unified endpoint management , security or remote access vendor).
- Enable insight-driven automation by choosing DEM solutions that provide analytics and remediation functions.
- Measure SaaS application performance by choosing DEM solutions that can perform real-user monitoring and synthetic transaction monitoring.
- Gain transparency into employee experience by monitoring as many endpoints as possible.

### Sample Vendors

Apica; Catchpoint; Cisco; Fortinet; Kadiska; Lakeside Software

### Gartner Recommended Reading

Market Guide for Digital Experience Monitoring

How to Monitor and Troubleshoot Remote Workers' Application Performance

3 Ways to Optimize Observability and Monitoring of Digital Services in the Cloud

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

Use Synthetic Monitoring to Enhance User Experience for Hosted and SaaS Applications

### Intelligent Automation (I&O)

**Analysis By:** Chris Saunderson

**Benefit Rating:** Moderate

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

**Maturity:** Emerging

#### Definition:

Intelligent automation (IA) for infrastructure and operations (I&O) is the application of AI techniques, advanced rule engines, heuristics and machine learning (ML) to automate decision making and execute actions for I&O activities. It involves collection, analysis, recommendations, and actions based on data gathered from human and machine-based sources. IA is increasingly being used to improve business agility and reduce outage impact, and is driving more advanced I&O service enablement.

#### Why This Is Important

I&O leaders are increasingly looking to ML-based analytics and augmented decision making to improve operational resiliency and responsiveness, address complexity and process increasingly large amounts of data through automation. In keeping with the demand in the market, technology providers are adjusting their product focus to apply analytics techniques, such as decision trees, knowledge graphs, clustering, regression and classification.

#### Business Impact

I&O teams should be in lockstep with their business to ensure performance, reliability and resilience needs are met. IA drives data collection, updates, analysis and automation of actions. This enables new automated capabilities that deliver:

- Predictive capabilities: maintenance/failure effects, cost/delivery forecasting.

- Staff efficiency: value-added work rather than manual work, root cause analysis.
- Insight generation: trends, recommendations for next automation actions, unhandled event analysis.

**Drivers**

- IA is an approach that is being investigated by clients to optimize their service operation costs by eliminating manual tasks, and to enable scalable operational support at a manageable cost.
- Technology providers that offer best-of-breed tools for artificial intelligence for IT operations (AIOps), application performance monitoring (APM) and robotic process automation (RPA) will influence IA. AIOps and stand-alone RPA technology providers may expand their offerings to deliver IA, through acquisitions or organic development. Typically, infrastructure managed service providers (MSPs) source third-party IA solutions to expand capabilities in their service offerings.
- Maturation of the use of automation will increase reliability and velocity of delivery, and cost optimization, and reduce toil for operations teams and cognitive loads on platforms and operations teams.
- Three factors drive synergy among IA, AIOps and RPA: the buying segment (I&O leaders) overlaps across these technologies; the objectives (increasing efficiency, scale and agility) are aligned; and the future of these innovations will increasingly be driven by AI technologies.

### Obstacles

- Successful implementation of IA will leverage a high degree of cooperation and trust between business, I&O, data and analytics teams, and technology providers.
- IA for I&O has significant overlaps with multiple automation domains that present challenges in identifying suppliers that can fill distinct I&O use cases without duplication. IA tool providers offer the underlying algorithmic implementations, connectors and data repositories, but the implementation still requires significant setup and refinement, and is never “out of the box.”
- There is pressure to use existing automation solutions to address IA use cases, even if only partially successful. The costs of these solutions, especially related to the skills investment needed, are challenging to justify.
- Required cross-domain skills for developing solutions to meet the challenges of the complex environment into which these platforms are targeted may place the I&O organization at a disadvantage in securing the talent and skills needed.

### User Recommendations

- Define use cases by analyzing gaps in existing automation that can benefit from augmented decision making and execution.
- Collaborate with data and analytics teams to adapt best practices that include data preparation, cleansing and data lakes to glean insights from a centralized knowledge repository. Development of skills to identify root cause for AI-derived exceptions will be key.
- Leverage I&O procedures and documentation to help train and sustain AI models. Leverage investments in infrastructure MSPs that offer IA solutions or partner with stand-alone IA tool providers.
- Roadmap the adoption of IA as an evolution of your automation journey, keeping humans in the loop until confidence is built, and transition your team to an automation engineering role,

### Sample Vendors

arago; AutomationEdge; Coretex; CSS Corp; HCL Technologies; NTT DATA; Perpetuuiti; Tata Consultancy Services

### AIOps Platforms

**Analysis By:** Matt Crossley, Matthew Brisse

**Benefit Rating:** High

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

**Maturity:** Early mainstream

#### Definition:

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

#### Why This Is Important

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

#### Business Impact

AIOps platforms deliver value through:

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

#### Drivers

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

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

Obstacles

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

### User Recommendations

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

### Sample Vendors

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

### Gartner Recommended Reading

Market Guide for AIOps Platforms

Deliver Value to Succeed in Implementing AIOps Platforms

Infographic: Artificial Intelligence Use-Case Prism for AIOps

Infographic: AIOps Architecture for Analyzing Operational Telemetry

How Do I Plan for Migrating My Data Center Infrastructure Into an XaaS Model?

## Network AI and Automation

**Analysis By:** Pulkit Pandey

**Benefit Rating:** High

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

**Maturity:** Mature mainstream

**Definition:**

Network AI and automation combine multiple technologies including but not limited to data analytics, artificial intelligence (AI), machine learning (ML), orchestration, robotic process automation (RPA) and artificial intelligence for IT operations (AIOps). Together, these technologies enable CSPs to use deep knowledge about the network to power the adaptive automation of their services and operations.

**Why This Is Important**

Network intelligence empowers rapid end-to-end business or operation process automation complemented by sophisticated algorithms, leading to better efficiency, faster response and improved productivity. In addition, it introduces scalability and flexibility to meet the diversified requirement of more complex and dynamic network technologies. It also enables the extraction of actionable insights to provide better customer experiences and support new businesses with precision and in adaptive ways.

**Business Impact**

Network AI and automation benefit CSPs in:

- Enabling real-time network optimization, predictive maintenance and more adaptive networks to support business agility.
- Improving the productivity of employees, minimizing repetitive tasks and enabling employees to focus on innovation and creativity.
- Improving operational efficiency and agility, lowering operating costs, and shortening the time of response.
- Gaining customer insight that might lead to improved customer satisfaction and revenue.

**Drivers**

- More network equipment vendors have started to embed “intelligent and automation” capabilities into their solutions. The emergence of the relevant algorithm, tools and technologies accelerates the adoption.
- The adoption of AI in networks is gaining speed, as CSPs are accepting a shift from a use-case-based approach to a more stable platform-based approach.
- CSPs’ network environment is growing increasingly complex with the introduction of such technologies as network function virtualization (NFV), software-defined networking (SDN) and cloud-native distributed architecture enabling the development of on-demand services and network slicing. Existing network management and operation systems lack the scale and flexibility to meet the requirements of these more dynamic network technologies.
- The COVID-19 pandemic and headwinds in the economy refocused network infrastructure on resilience, which for many resulted in accelerating the intelligent automation agenda.
- Maturing and expanding data science initiatives, better algorithms, more cost-effective computing power, and a substantial increase in available network data support the emergence of intelligent techniques.
- The use of intelligent automation will transform how IT and network infrastructure is delivered and supported, including delivering more agility to address resource demand, which is attractive for CSPs that are building next-generation operation and management platforms.
- The rise in connected endpoints driven by the IoT, as well as 5G, will also require automation to improve network KPIs and allow automation of maintenance tasks and energy savings.

### Obstacles

- Although automation is not a new idea in the telcos, adding AI to the process cycle is a relatively new concept. Management and frontline employees sometimes have misconceptions about what they should expect as AI becomes part of their work lives.
- Lack of skills in either IT or telecom processes acts as a hurdle in the process.
- The accuracy of algorithm models is limited by the completeness and accuracy of the data being used. Fragmented data and data quality are always major concerns of successful intelligent-based automation adoption.
- The multivendor, multilayer and cross-domain environment challenges network automation and intelligent implementation.
- Most of today's network AI and automation projects have a tactical approach that is difficult to scale due to the lack of cross-domain orchestration and collaboration, thus creating internal-technology-based silos. In addition, data unification and lack of sufficient data is also a challenge among vendors and CSPs.

### User Recommendations

- Select initiatives that align with your organization-level strategy by including BU heads to ensure transparency and accountability.
- Enhance network intelligence and automation capabilities through investments in advanced technologies like analytics, AI/ML, low-code platforms, API-centric SaaS and decision intelligence (DI) and generative AI.
- Improve the efficiency of the network automation process before introducing AI, because introducing intelligence on top of an inefficient automation process nearly always leads to a worse situation.
- Build a transformational mindset for AI and automation across the network operation and management team by accelerating AI skills and talent development.
- Establish an automation roadmap by requesting intelligent capabilities in vendors' products, or consider how to develop internal capabilities that can create this intelligent automation.
- Enhance context awareness by establishing cross-siloed visibility and a strong data foundation for intelligence.

### Sample Vendors

Amdocs; AsiaInfo Technologies; Cisco Systems; Ericsson; Huawei; Juniper Networks; Netcracker; Nokia; P.I. Works; ZTE

### Gartner Recommended Reading

Market Guide for AI Offerings in CSP Network Operations

How Can The Telecom Sector Be Successful With AI?

AI Vendors Selling to CSPs: Your Guide to an Effective Solution Packaging

## Natural Language Processing

**Analysis By:** Bern Elliot, Erick Brethenoux

**Benefit Rating:** Transformational

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

**Maturity:** Emerging

### Definition:

Natural language processing (NLP) enables an intuitive form of communication between humans and systems. NLP includes computational linguistic techniques aimed at parsing, interpreting and, sometimes, generating human language. NLP techniques deal with the pragmatics (contextual), semantics (meanings), grammatical (syntax) and lexical (words) aspects of languages. The phonetic part is often left to speech-processing technologies that are essentially signal-processing systems.

### Why This Is Important

NLP enables the automated processing and leveraging of vast quantities and types of text-based information. These can include documents, literature, email, text messages, invoices and receipts. With speech-to-text, NLP can process speech, including livestreams of text and speech. As a result, NLP enables a vast array of applications and automation that was previously unachievable by machine, offering businesses significant process improvement.

### Business Impact

- NLP is an enabler that is typically useful when built into applications that support business workflows.
- Because so many tasks involving text rely on human labor, the potential for savings and new business processes is vast.
- Business value reported from some applications using NLP, such as machine translation, are thousandfold efficiency improvements and operational cost savings.

### Drivers

- Growth in transcription and translation services.
- Language-generation applications (chatbots, text summarization) that produce natural language descriptions of tabular data, making it easier for many to understand.
- Keyword tagging in documents, making it easier to determine relevant sections or to extract other information, such as intent and entities.
- Autocorrect and autocompletion tools and services.
- Content moderation services that analyze user-generated content (text or images) to flag potentially offensive content or identify fake news in social media.
- Sentiment analysis to identify the effective states and subjective information in statements — for example, from negative to neutral to positive.
- Search improvements through better understanding of the intent of a search query or through summaries of the retrieved content.
- Text analytics and intelligent document processing (IDP) to quickly process large numbers of an organization's documents and determine compliance or legal validity.
- Advances in insight engine text capabilities combined with more-advanced NLP functionality.
- The introduction of new machine learning (ML) techniques, including transformer-based large language model (LLM) approaches, such as BERT and GPT-3. This has enabled new use cases and improvements to existing use cases, with special regard to those involving text generation.

### Obstacles

- Despite progress made in NLP methods, many subtle nuances properly processing the complex and enormous variety found in human languages are deeply influenced by cultural and other idiosyncratic conditions. Significant customization of tools and products is often needed.
- Although recent NLP methods that leverage deep neural networks have provided significant and useful improvements to many applications, some are experimental and are not yet mature.
- Support for low-resource languages. Although common languages have support for templates, data and algorithms, lesser-used languages can be difficult to develop for, and require more custom-made effort.
- Despite advances in new techniques, the hyped expectations surrounding NLP may result in unrealistic expectations, leading to disappointing results.
- Many of the new use cases of emerging NLP opportunities are poorly understood and face issues with meeting expectations or defining a clear business value to companies.

### User Recommendations

- Select the strongest and most-immediate use cases for NLP. Examples include customer service (affecting cost, service levels, customer satisfaction and upselling) and employee support (including augmenting them as they perform tasks). Another example is automation of paper- and document-based tasks (e.g., contract analysis, compliance enforcement, document generation, translation and transcription).
- Demonstrate success in initial projects by starting with modest goals. As experience is obtained, projects should iterate, and scope can increase. As enterprises enhance their NLP initiatives, new skills should be explored that better leverage new NLP methods.
- Verify the effectiveness of solutions before making significant commitments, because the quality of NLP solutions can vary.
- Evaluate master metadata implications. Ensure that language assets are considered from a master metadata management point of view to ensure reuse and portability of assets between algorithms and systems.

**Sample Vendors**

Baidu; Expert.ai; Google; IBM; Microsoft; Narrative Science; NLTK; Openstream; Rasa

**Gartner Recommended Reading**

Applying AI — A Framework for the Enterprise

Applying AI — Techniques and Infrastructure

Tool: Vendor Identification for Natural Language Technologies

Use-Case Prism: Artificial Intelligence for Customer Service

Cool Vendors in Natural Language Technology for Processing Enormous Volumes of Unstructured Data

Cool Vendors in Conversational and Natural Language Technology

**Virtual Support Agents**

**Analysis By:** Chris Matchett

**Benefit Rating:** Moderate

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

**Maturity:** Early mainstream

**Definition:**

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

### Why This Is Important

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

### Business Impact

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

### Drivers

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

### Obstacles

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

### User Recommendations

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

### Sample Vendors

Aisera; Espressive; Moveworks; ServiceNow

### Gartner Recommended Reading

Innovation Insight for Virtual Support Agents

Leverage 4 Domains of AITSM to Evolve ITSM Tools and Practices

Critical Capabilities for Enterprise Conversational AI Platforms

Magic Quadrant for Conversational AI Platforms

Applying AI — Business Domains

## Intelligent Document Processing

**Analysis By:** Shubhangi Vashisth, Stephen Emmott, Anthony Mullen

**Benefit Rating:** High

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

**Maturity:** Adolescent

### Definition:

Intelligent document processing (IDP) solutions extract data to support automation of high-volume, repetitive document processing tasks and to provide analysis and insight. IDP uses natural language technologies and computer vision to extract data from structured and unstructured content, especially from documents, to support automation and augmentation.

### Why This Is Important

IDP is increasingly important to create operational efficiencies in business processes that need to extract information from semistructured and unstructured data as part of automation of any workflow. Such tasks are routine, repetitive and primarily dependent on human effort. IDP caters to a wide variety of use cases — from digitization initiatives to more complex processes such as document-centric taxation processing and pension fund management. IDP is one of the technologies within a spectrum of technologies that enable hyperautomation.

### Business Impact

IDP can benefit the business by:

- Reducing the human labor needed to process documents and improving document-based workflows
- Extracting relevant data from different input formats for further analysis, validation and/or automation
- Preprocessing unstructured data for analysis
- Automating document and email classification and extraction
- Enabling discovery and insight
- Creating workflows to support process automation or integration with existing automation solutions

### Drivers

Key drivers include:

- The desire to consolidate document processing across multiple applications into one component.
- The need to ingest data from diverse sources and formats (e.g., PDFs, images) and extract information from it.
- Pressure to improve the accuracy and efficiency of extraction and automation processes.
- The desire to leverage generative AI for document classification and data extraction. Many vendors are already contextualizing large language models (LLMs), such as BERT and GPT-3, for specific industries and use cases.
- Enhanced capabilities to denoise and preprocess semistructured and unstructured data. Many vendors are expanding with additional capabilities for intelligent content processing (ICP) to process various content types, such as video, audio and images.
- Support for additional capabilities, such as document classification, metadata extraction, knowledge graphs, search and natural language question answering.

- Increased leverage of human in the loop (HITL) training methods to simplify adoption, ease deployment and continuously improve automation accuracy.

Examples of use cases span many enterprise departments and vertical industries, including:

- **Accounts payable/receivable:** Processing of invoices, purchase orders, payments, expense reports and receipts.
- **Healthcare:** Processing of medical forms.
- **Banking and financial services:** Processing of loan applications, driver licenses and other collateral; customer onboarding; environmental, social and governance (ESG) initiatives; and compliance.
- **Government:** Processing of forms, driver licenses, passports and other IDs.
- **Manufacturing:** Processing of equipment maintenance records, RFPs, business contracts and operating agreements.
- **HR:** Employee onboarding, travel and expenses.

Obstacles

- **Complex, consolidating markets:** The market has a competitive vendor landscape, with dedicated solutions and offerings from adjacent technology markets. These markets include insight engine vendors, OCR vendors, RPA vendors, cloud providers and, increasingly, service providers. Selecting the right solution gets tricky, as vendors offer overlapping capabilities and differentiation is low.
- **Integration challenges:** Many organizations already have either a homegrown solution or an existing IDP tool, but are looking for enhanced features, such as sophisticated text analytics, to cater to wider use cases and growing business needs. However, a single tool may not be able to cater to all requirements, and integration complexity makes it challenging to have multiple tools.
- **Category bleed, which confuses buyers:** With semantic platforms, insight engines, RPA and conversational AI vendors all offering IDP-like solutions to interpret and mine document form factors, buyers may not feel compelled to purchase an additional format-specific (document) solution.

### User Recommendations

- Evaluate the entire business process to understand where and how IDP solutions can be integrated. Treat IDP as a component that integrates with other platforms/applications.
- Adopt industry- and/or business-domain-focused solutions for a quick time to implementation.
- Align with stakeholders on accuracy and efficiency baselines for the process.
- Investigate the difference between placed-framed extraction and semantic-framed extraction. The former is not IDP, and only the latter can scale to unstructured content. If you want to use IDP as a launchpad for broader handling of semistructured and unstructured data, evaluate insight engine or semantic AI platforms that offer IDP along with other services.
- Design the HITL validation process either by leveraging internal sources or by outsourcing the task to the IDP solution provider.
- Discuss specialized requirements, such as the ability to process documents in entirely new formats, data preprocessing needs and SLAs around processing time.
- Compare the ease of integration of new tools, if looking to complement the capabilities of an existing solution.

### Sample Vendors

Alkymi; Altilia; Applica; DocDigitizer; Eigen Technologies; Hyperscience; Infrrd; Indico Data; Kofax; OpenText

### Gartner Recommended Reading

Infographic: Understand Intelligent Document Processing

Market Guide for Intelligent Document Processing Solutions

Quick Answer: How to Prioritize Requirements in the RFP for Intelligent Document Processing

Tool: RFP for Intelligent Document Processing

Intelligent Document Processing Growth Opportunities: Top Strategies for Tech CEOs

## SOAR

**Analysis By:** Eric Ahlm, Craig Lawson

**Benefit Rating:** High

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

**Maturity:** Early mainstream

### Definition:

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

### Why This Is Important

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

### Business Impact

SOAR solutions can help clients:

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

### Drivers

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

### Obstacles

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

### User Recommendations

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

### Sample Vendors

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

### Gartner Recommended Reading

SOAR Will Not Make You Better at Running SIEM

Market Guide for Security Orchestration, Automation and Response Solutions

## Climbing the Slope

### Deep Learning

**Analysis By:** Mike Fang, Svetlana Sicular, Alexander Linden

**Benefit Rating:** Transformational

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

**Maturity:** Adolescent

#### Definition:

Deep learning (DL) is a variant of machine learning algorithms. It uses multiple layers to solve problems by extracting knowledge from raw data and transforming it at every level. These layers incrementally obtain higher-level features from the raw data, allowing the solution of more complex problems with higher accuracy and less manual tuning.

#### Why This Is Important

Deep learning often outperforms traditional machine learning or shallow learning techniques in the presence of complex and very high dimensional data, such as images, speech and text. It can reduce the need for tedious feature engineering.

#### Business Impact

Deep learning is key for a lot of breakthroughs in the field of AI in many domains. It allows organizations to generate insights from disparate, especially unstructured, data sources. All this success is rooted in the ability of DL algorithms to exploit weak signals in the dataset, which in isolation may not carry much meaning, but in a group may highlight results that would have been neglected or not even surfaced. DL applicability has been most successful in vision, speech and text domains.

#### Drivers

- Algorithmic breakthroughs, such as the recent advancements in natural language processing (NLP) techniques using DL methods, have propelled the use of foundational models that promise state-of-the-art results in conversational platforms.
- The performance improvement and affordability from vast computing architectures, such as graphics processing unit (GPU), clustered computing and cloud, are driving adoption.

- Availability of off-the-shelf solutions is also a driver for DL.
- The vast availability of huge training datasets, such as image, audio, video or text, is enabling the use of DL techniques to help organizations enrich their decision-making process.
- Methods such as reinforcement learning, transfer learning, deep belief networks and evolutionary learning are driving the use of DL.
- Graph neural networks, used to embed dependencies between nodes from the graph, together with the deep neural network, are increasingly being used in computer vision, recommender systems and industries, such as transportation and chemical.

### Obstacles

- The infrastructure investments required to create and maintain DL solutions are still high.
- DL methods are construed as a black box by nature, so governing and ensuring the explainability of these solutions is a constant challenge.
- AI energy consumption is particularly high for advanced DL models and is harmful to the environment.
- The skills required to create and manage DL solutions from scratch are hard to come by.
- Support and capabilities around security, privacy and governance for vendors providing DL capabilities as a service are limited, which adds a layer of complexity over already black-box implementations.

### User Recommendations

- Use DL techniques only when shallow learning techniques have failed to deliver a suitable AI solution.
- Examine and select business areas where deep learning can provide the best value, especially where there is wide and heterogeneous data and the back-box nature of DL isn't a concern.

- Explore prepackaged solutions first and then move on to custom-made solutions for the business using DL. Create a diverse talent pool from industry and academia to ensure interpretability, as well as privacy, compliance, ethics and governance in DL solutions.
- Connect symbolic systems with deep learning to pilot some state-of-the-art composite AI techniques, such as neural symbolic AI, graph neural networks, and deep reinforcement learning to reduce technical debt and promote reusability, consistency and explainability.

**Gartner Recommended Reading**

Innovation Tech Insight for Deep Learning

Market Guide for DSML Engineering Platforms

Market Guide for Multipersona Data Science and Machine Learning Platforms

Introducing Deep Learning Abstraction Methods

3 Types of Machine Learning for the Enterprise

**Machine Learning**

**Analysis By:** Shubhangi Vashisth, Peter Krensky

**Benefit Rating:** Transformational

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

**Maturity:** Mature mainstream

**Definition:**

Machine learning (ML) is an AI discipline that solves business problems by utilizing statistical models to extract knowledge and patterns from data. The three major approaches that relate to the types of observation provided are supervised learning, where observations contain input/output pairs (also known as “labeled data”); unsupervised learning (where labels are omitted); and reinforcement learning (where evaluations are given of how good or bad a situation is).

### Why This Is Important

Over the last few years, ML has gained a lot of traction and is entering mainstream adoption because it helps organizations to make better decisions at scale with the data they have. ML aims to eliminate traditional trial-and-error approaches based on static analysis of data, which are often inaccurate and unreliable, by generalizing knowledge from data.

### Business Impact

ML drives improvements and new solutions to business problems across a vast array of business, consumer and social scenarios, such as:

- Credit approval automation
- Price optimization
- Customer engagement
- Supply chain optimization
- Predictive maintenance
- Fraud detection

ML impacts can be explicit or implicit. Explicit impacts result from ML initiatives. Implicit impacts result from products and solutions that you use without realizing they incorporate ML.

Drivers

- Augmentation and automation (of parts) of the ML development process has improved productivity of data scientists and enabled citizen data scientists to make ML pervasive across the enterprise.
- Availability of quality, labeled data is driving ML adoption at enterprises.
- Pretrained ML models are increasingly available through cloud service APIs, often focused on specific domains or industries.
- ML education is becoming a standard at many academic institutions, fueling the supply of talent in this space.
- Active research in the area of ML in different industries and domains is driving applicability far and wide.
- Newer learning techniques — such as zero- or few-shot learning — are emerging, reducing the need to have high volumes of quality training data for ML initiatives, thus lowering the barrier to entry.
- New frontiers are being explored, including federated/collaborative, generative adversarial, transfer, adaptive and self-supervised learning — all aiming to broaden ML adoption.

Obstacles

- Conventional engineering approaches are unable to handle the growing volumes of data, advancements in compute infrastructure and associated complexities.
- ML is not the only popular AI initiative to emerge in the last few years. Organizations also rely on other AI techniques, such as rule-based engines, optimization techniques and physical models, to achieve decision augmentation or automation.
- Organizations still struggle to take their ML models into production. MLOps continues to be a hot trend and organizations look to specialized vendors and service providers for support in their journeys of better operationalizing ML models.
- Application of ML is often oversimplified as just model development. Several dependencies that are overlooked — such as data quality, security, legal compliance, ethical and fair use of data, and serving infrastructure — have to be considered in ML initiatives.

### User Recommendations

- Assemble a (virtual) team that prioritizes ML use cases, and establish a governance process to progress the most valuable use cases through to production.
- Utilize packaged applications that fit your use-case requirements to derive superb cost-time-risk trade-offs and significantly lower the skills barrier.
- Explicitly manage MLOps and ModelOps for deploying, integrating, monitoring and scaling analytical, ML and AI models.
- Adjust your data management and information governance strategies to enable your ML team. Data is your unique competitive differentiator, and adequate data quality — such as the representativeness of historical data for current market conditions — is critical for the success of ML.

### Sample Vendors

Amazon; ClearML; Databricks; Dataiku; Domino Data Lab; Google; H2O.ai; KNIME; Microsoft; MindsDB

### Gartner Recommended Reading

Market Guide for Multipersona Data Science and Machine Learning Platforms

Market Guide for DSML Engineering Platforms

How to Improve the Performance of AI Projects

Infographic: Common Layers of Data Science and Machine Learning Activity

Use Gartner's MLOps Framework to Operationalize Machine Learning Projects

## Threat Intelligence Products and Services

**Analysis By:** Jonathan Nunez

**Benefit Rating:** High

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

**Maturity:** Early mainstream

**Definition:**

Threat intelligence (TI) services provide buyers with knowledge about the cyberthreat landscape by documenting tactics, techniques and procedures; and by profiling threats and threat actors. TI products deliver tools to assist organizations in aggregating, collecting, curating and operationalizing their own TI and potentially sharing it with outside entities.

**Why This Is Important**

Security leaders have an obligation to understand the organization's threat landscape. They must ensure their security solutions are updated with the latest threat content and provide contextual information to their teams as it helps inform overall risk. TI provides the means for an organization to maintain visibility of their threat landscape, build timely, accurate and actionable insights that can be applied before, during and after threats present themselves to your organization.

**Business Impact**

- TI products and services are applicable in every industry, across security functions and controls, because every organization has a unique threat landscape.
- TI informs the business about current and potential future threats that pose risks to organizations.
- TI solutions can be applied as machine- or human-readable to enhance security technologies and an understanding of adversarial intentions and motivations.

**Drivers**

- Security platform vendors are investing in TI products and services either through organic development or acquisitions. These vendors are delivering an increasing amount of threat intelligence platform (TIP) functionality to aggregate TI and manage it within a single platform offering, accelerating the adoption and utilization of TI in the market.
- Organizations continue to look for security solutions that address multiple use cases. This has pushed TIP vendors to extend beyond the security orchestration, analytics and reporting (SOAR) functionality they have been advertising, to now offering threat detection and enhanced analytic platform features.
- TI service providers are now expanding their core use cases and features to include digital risk protection services (DRPS), offering organizations a single-vendor way to deliver highly curated external threat and risk information. Gartner continues to see an interest in DRPS capabilities and features, driving TI solution providers to add the capability to their portfolios.
- Organizations are putting more effort toward understanding their risk by aligning digital exposures with malign threats. Often informed by TI, these vendors are now starting to offer external attack surface management (EASM) in an effort to heighten curation and increase actionability.
- Curation is key for organizations as they grapple with increased volumes of data. Customers will continue to demand a deep understanding of the threat landscape as they work to synthesize TI into actionable insights.

### Obstacles

- Many organizations have no formal TI program or dedicated analysts to use TI solutions, like a TIP, or interpret the value from bespoke TI reports. They rather focus on indicators like IP addresses, domains and hash values, and allocate too few resources to human-readable or advanced TI solutions.
- Organizations struggle to measure and justify the value of TI solutions. Lack of TI performance reporting will increase the likelihood of TI budget cuts or prohibition of program maturation.
- Many organizations lack well-defined priority intelligence requirements (PIRs), which can lead to overinvestment in or underutilization of TI solutions.
- A saturated and seemingly undifferentiated TI marketplace creates buyer confusion and fatigue, especially in light of not having well-defined PIRs, which can aid in the vendor-selection process.

### User Recommendations

- Incorporate TI solutions and services into your overall security program. Define detailed requirements and expectations for TI service providers to deliver outcomes aligned to organizational threat concerns.
- Ensure PIRs are defined to drive TI solution needs before TI vendor engagement. This is a foundational requirement as it informs what to focus on, what to collect, who to track, and what it means to the business in terms of risk and exposure.
- Develop operational delivery metrics (ODMs) for the defensible maturation of your TI Program. These ODMs should focus on metrics and outcomes that drive faster detection and response, increased efficacy in security tools, and improved efficiency in incident response.
- Consider leveraging TI services through your existing managed security services or managed detection and response providers. These providers can decrease time-to-value while simultaneously scaling your TI program by providing technical collection, curation, analysis and reporting.

### Sample Vendors

Bfore.Ai; Cybersixgill; Cyware; DuskRise; GroupSense; Security Alliance; Silobreaker; ThreatConnect; ZeroFox

**Gartner Recommended Reading**

Market Guide for Security Threat Intelligence Products and Services

Tool: Vendor Identification for Security Threat Intelligence Products and Services

Emerging Technologies: Adoption Growth Insights in Digital Risk Protection Services

Innovation Insight for Attack Surface Management

Emerging Technologies: Critical Insights for Threat Intelligence Demand

## Entering the Plateau

### SIEM

**Analysis By:** Eric Ahlm, Mitchell Schneider

**Benefit Rating:** Moderate

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

**Maturity:** Mature mainstream

#### Definition:

Security information and event management (SIEM) is a configurable security system of record that aggregates and analyzes security event data from on-premises and cloud environments. SIEM assists with response actions to mitigate issues that cause harm to the organization, and satisfy compliance and reporting requirements.

#### Why This Is Important

Aggregating and normalizing data from various environments to centralize visibility is a core element of effective security programs. SIEM supports an organization's ability to identify, prioritize and investigate security events of interest, execute response actions and report on current and historical security events.

#### Business Impact

SIEM solutions can impact the business by:

- Allowing organizations to identify and respond to critical security events earlier in their life cycle to reduce risk.
- Creating overall situational awareness for security issues and events, providing an efficient and trusted system of record, which can be used for operational security and compliance reporting.
- Aligning disparate technology investments and reducing the operational staffing overhead of managing security issues and incidents.

#### Drivers

- Central monitoring of threats, as reported by multiple sources, is a primary driver for SIEM. A SIEM offers a central place to monitor and investigate security alerts, as well as supporting contextual information required to make an alert actionable.
- A SIEM can turn raw alert data into actionable intelligence, through whatever analysis method works best for a given monitoring objective.
- The need to expand detection workflow to include response activities with capabilities such as security orchestration, automation and response (SOAR).
- SaaS SIEM solutions in the cloud transfer the platform and infrastructure maintenance to the vendor and allow for more predictable linear budgeting for growth.
- As more assets move to cloud-centric environments, such as Microsoft Azure, Amazon Web Services (AWS), Google Cloud Platform (GCP), Oracle and many others, a SIEM must have awareness of the underlying environment to perform well.
- Organizations have a large quantity of both streaming and nonstreaming data, which is useful for security monitoring, and SIEM platforms provide a centralized place to store and interrogate this data.

### Obstacles

- Getting a SIEM to perform well against detecting attacks requires dedication and sufficient staffing. Undermanaged SIEMs continue to plague many organizations.
- SIEM budgets and resources are constrained; however, the types of threats to monitor tend to be rather endless. As such, deciding what to best monitor with the SIEM resources you have is concession engineering at best.
- SIEM threat detection performance is dependent on not only SIEM and its configuration, but also the detection stack and all supporting telemetry chosen to be sent to the SIEM.
- Gartner is tracking a number of non-SIEM solutions that provide value for a limited function of a traditional SIEM. This can cause increased buyer confusion or make the justification of a complete SIEM more challenging

### User Recommendations

- Preplan what monitoring objectives best meet your organization's security needs. Use those as design requirements to correctly identify important selection criteria such as analysis methods, performance, sizing and retention.
- Allow for a learning period of alerting to determine how best to operationalize detection and response as planning operational support of alert pipeline management without knowing how many alerts and how much work is required can be difficult.
- Ensure your cloud SIEM is aware of the underlying infrastructure which it monitors. A SIEM must understand the nuances of its native environment, such as AWS, Google Cloud or Microsoft Azure.

**Sample Vendors**

Elastic; Exabeam; IBM; LogRhythm; Microsoft; NetWitness; Rapid7; Securonix; Splunk

**Gartner Recommended Reading**

Magic Quadrant for Security Information and Event Management

Critical Capabilities for Security Information and Event Management

## APM

**Analysis By:** Padraig Byrne, Mrudula Bangera

**Benefit Rating:** High

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

**Maturity:** Mature mainstream

**Definition:**

Application performance monitoring (APM) enables the observation of an application's behavior, dependencies, users and business KPIs throughout its life cycle. The application being observed may be developed internally, as a packaged application or as software as a service (SaaS).

### Why This Is Important

The APM market continues to evolve beyond its core root of server-side application monitoring as organizations seek to optimize business outcomes, enhance user experience and improve application performance. It is no longer sufficient to monitor one aspect of the technology stack; nor is it enough to deploy proprietary technologies to collect performance data. Modern APM implementations are becoming more tightly integrated with observability platforms.

### Business Impact

APM solutions enable businesses to examine modern applications' end-to-end performance, coupled with detailed inspections to quickly identify service-impacting outages. As organizations continue to embrace digital transformation, their need increases for agility in order to succeed with their transformation initiatives. APM solutions can be perceived as more than another monitoring tool, supporting the need for agility and aiding in its acceleration and effectiveness.

Drivers

- **Unified monitoring:** New application monitoring and observability tools are becoming more unified. This approach requires platforms that share common data models to conduct correlation analysis and other critical functions of application performance monitoring.
- **Holistic monitoring:** Modern tools are becoming more holistic in terms of the types of data they can ingest, analyze and integrate. The continued adoption of new application development and operations technologies requires monitoring teams to constantly test the limits of their monitoring products.
- **Integration with DevOps and site reliability engineering (SRE):** Testing in preproduction and integration with continuous integration/continuous delivery (CI/CD) tools have become the new norm, increasing the quality and robustness of the finished product.
- **Intelligent monitoring:** The use of logs, traces, metrics and multiple other types of telemetry is enabling operations and monitoring teams to find unexpected patterns in high-volume, multidimensional datasets using artificial intelligence for IT operations (AIOps) technologies.
- **Business monitoring:** APM tools can be used to derive business metrics, such as abandoned shopping carts or average spend per customer for retailers. Representing such critical business information means an increased likelihood of further investment in these tools.

### Obstacles

- Traditional implementations of APM often fail to provide a complete solution, requiring organizations to pivot between tools, wasting time and resources, while struggling to find the root cause of the problem.
- Modern architectures such as containers and microservices and cloud-native environments are coming to IT operations environments faster than monitoring strategies are evolving to handle them. This is leading to visibility gaps and performance challenges.
- Clients increasingly cite cost as a significant challenge for implementation of APM tools. Costs for larger organizations can run into millions per year, representing a significant percentage of IT spend.
- Many IT monitoring teams still rely on manually invoked runbooks or scripts to remediate problems, hindering I&O leaders' ability to deploy and monitor new technologies. There is often a major disconnect between what I&O monitors and what the business cares about, which can have significant negative implications for the business.

### User Recommendations

- Choose vendors that assist in relating application performance to business objectives and serve not only IT operations (ITOps), but also DevOps, application owners and lines of business, providing value throughout the application life cycle. Select a vendor that provides actionable answers and not just endless drill-downs to more data.
- Choose products based on their ability to support: mapping and monitoring of customer and business journeys; bidirectional integration with the DevOps toolchain; new emerging standards in instrumentation, such as OpenTelemetry; cloud-native monitoring with an API-first approach; application security; and integrations with your existing or planned IT service management (ITSM) and configuration management database (CMDB) tools.

### Sample Vendors

Cisco; Datadog; Dynatrace; Elastic; Grafana; Instana; New Relic; Splunk

### Gartner Recommended Reading

Magic Quadrant for Application Performance Monitoring and Observability

### Speech Synthesis

**Analysis By:** Bern Elliot

**Benefit Rating:** Moderate

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

**Maturity:** Early mainstream

**Definition:**

Speech synthesis is the artificial production of human speech. Current methods synthesize voice using a variety of modeling approaches, including AI-based language and voice models. Enhancements allow models to mimic specific speech patterns of individuals by tuning the synthesis model based on recordings. Recent advances in generative AI are enabling additional capabilities, improving the ability to mimic specific voices with limited training.

**Why This Is Important**

High-quality speech synthesis allows vastly improved user experiences at a fraction of the cost of a human-recorded alternative. The current deep-learning-based approach uses acoustic models to produce waveforms and generate speech that is highly accurate. This approach was only developed in 2016. The rapid advancement of this technique is enabling new and useful applications.

**Business Impact**

Speech synthesis is most used in the following business areas and applications:

- High volumes of generated speech (e.g., real-time streaming multimedia content)
- Frequent updates to content or where audio-visual material is dynamically assembled (e.g., training material)
- Where imitation or mimicry of characteristics is desirable (e.g., reading books aloud)
- Hands-free environments with audio output
- To make avatars or animations more realistic

Drivers

- **Reading and communication aids for the blind and visually impaired.**
- **Improved user experiences with speech-enabled virtual assistants, chatbots and personal assistants;** modernization of contact center interactive voice response systems; clearer and more engaging narration of news or information drawn from data, such as sports or business events.
- **Better-quality and less-expensive audio narratives,** including audio books, such as read-aloud children's stories with fun voices, with interesting possible applications to e-learning activities.
- **Match voice personas to audiences.** Target audiences based on both content and voice characteristics in website and other commercial audio information. This can be coupled with visual personas such as avatars.
- **Hands free.** Improved usability of hands-free voice controls and interaction with voice assistants.
- **Markup expressivity.** Voice controls and markup to more effectively draw listeners' attention to specific details.
- **Gaming immersion.** More engaging characters and dialogues offered in computer games.
- **Media and entertainment industry.** Fast production of video and audio contents, such as audiobooks and multilingual training material.
- **Conversationally enabling large language models (LLMs).** On top of recent approaches for speech synthesis enabled by language models themselves, the intense interest in LLMs, and applications enabling LLMs such as ChatGPT, and similar styles of interaction, has raised interest in enabling speech-based interactions, including in consumer segments.

### Obstacles

- **Ethical issues.** Recent models can mimic a specific individual's speech to the point that it is very difficult to identify it as a fake (aka deepfake). While there are legitimate uses for mimicry, speech synthesis also poses ethical issues where it may be used to manipulate or deceive listeners.
- **Risk of taking digital recordings out of context.** While this is a risk, the introduction of "digital watermarks" makes it possible to better identify when generated speech has been taken out of context and/or used without proper licensing.
- **The "uncanny valley" experience.** Users may find overly realistic virtual assistants "creepy."
- **Cost and time for custom-made voices.** Custom speech synthesis models take expertise and time to develop and tune.

### User Recommendations

- Business leaders should review their current applications that use speech and consider how this low-cost approach to speech generation, which combines low cost with high quality, can be best leveraged. However, planners should evaluate solutions before committing, because quality and latency issues may make some solutions less desirable than others.
- Leaders and those responsible for risk and security should determine where there may be exposures to voice mimicking. This can include situations where significant actions are taken solely based on verbal commands via phone. Personnel, clients and employees should be warned of the risk and enlisted in identifying situations at risk for this sort of fraud.
- Leaders should not lock-in their applications to vendors generating voice. To be able to choose between different providers of voice and to reduce technical debt of natural language technology solutions, ensure that either you or your vendor allow voice generation services to be easily interchanged.

### Sample Vendors

Acapela Group; Amazon; DeepZen; Descript; IBM; LOVO; Microsoft; ReadSpeaker (rSpeak); SoundHound; Verbio Technologies

**Gartner Recommended Reading**

Best Practices for the Responsible Use of Natural Language Technologies

Critical Capabilities for Enterprise Conversational AI Platforms

Tool: Vendor Identification for Natural Language Technologies

# Appendixes

## Hype Cycle Phases, Benefit Ratings and Maturity Levels

### Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

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

Source: Gartner (July 2023)

Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

### Table 4: Maturity Levels

(Enlarged table in Appendix)

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

Source: Gartner (July 2023)

## Evidence

Recommending Root-Cause and Mitigation Steps for Cloud Incidents Using Large Language Models

ChatGPT-Based Design-Time DevSecOps

Machine Learning-Based Runtime DevSecOps: ChatGPT Against Traditional Approach

How Large Language Models Like ChatGPT Accelerate AIOps

Evaluation of ChatGPT Model for Vulnerability Detection

Exploring the Effectiveness of Large Language Models in Generating Unit Tests

Evaluating Large Language Models Trained on Code

Is ChatGPT the Ultimate Programming Assistant — How Far Is It?

Grounded Copilot: How Programmers Interact With Code-Generating Models

Cataloging Prompt Patterns to Enhance the Discipline of Prompt Engineering

## Recommended by the Author

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

Assessing How Generative AI Can Improve Developer Experience

Quick Answer: Should Software Engineering Teams Use ChatGPT to Generate Code?

Quick Answer: How Can Generative AI Tools Speed Up Software Delivery?

Quick Answer: How Can Security Operations Teams Leverage ChatGPT?

Quick Answer: What 3 Actions Should I&O Leaders Take Now On ChatGPT?

Innovation Insight: AI Networking Has the Potential to Revolutionize Network Operations

Innovation Insight for Generative AI

Innovation Insight for Autonomous Testing

Market Guide for AI-Augmented Software-Testing Tools

## Table 1: Priority Matrix for IT Management Intelligence, 2023

| *Benefit* ↓ | *Years to Mainstream Adoption* | | | |
|---|---|---|---|---|
| | ***Less Than 2 Years*** ↓ | ***2 - 5 Years*** ↓ | ***5 - 10 Years*** ↓ | ***More Than 10 Years*** ↓ |
| Transformational | | AI-Augmented Software Engineering<br>Application Security Posture Management<br>Conversational User Interfaces<br>Deep Learning<br>Generative AI<br>Machine Learning<br>Observability | Augmented FinOps<br>Generative Cybersecurity AI<br>Natural Language Processing | |

| *Benefit* | *Years to Mainstream Adoption* | | | |
|---|---|---|---|---|
| ↓ | *Less Than 2 Years* ↓ | *2 - 5 Years* ↓ | *5 - 10 Years* ↓ | *More Than 10 Years* ↓ |
| High | APM<br>Intelligent Automation<br>Intelligent Document Processing<br>Network AI and Automation | AI-Augmented Testing<br>AI Governance<br>Autonomous Workload Optimization<br>DEX Tools<br>Digital Experience Monitoring<br>Intelligent Infrastructure<br>Log Monitoring and Analysis<br>Process Mining<br>Prompt Engineering<br>Threat Intelligence Products and Services | AIOps Platforms<br>Autonomous Endpoint Management<br>Reinforcement Learning<br>SOAR<br>XDR | |
| Moderate | SIEM<br>Speech Synthesis<br>Virtual Support Agents | AI-Focused Problem Management<br>AI Networking<br>CIEM | Intelligent Automation (I&O) | |
| Low | | | | |

Source: Gartner (July 2023)

## Table 2: Hype Cycle Phases

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

| Phase | Definition |
| --- | --- |

Source: Gartner (July 2023)

## Table 3: Benefit Ratings

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

Source: Gartner (July 2023)

## Table 4: Maturity Levels

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

Source: Gartner (July 2023)