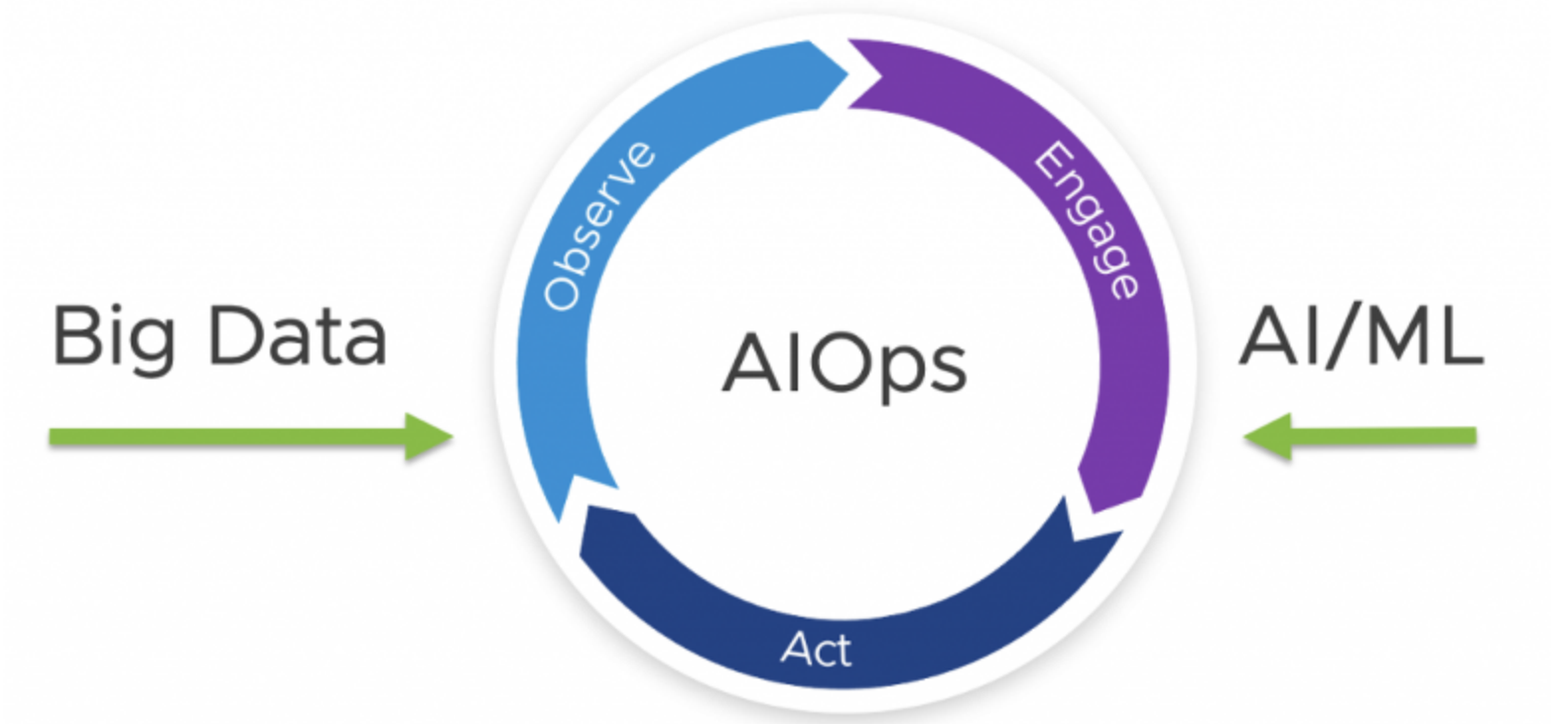
AIOps

Your Digital Operations Ally

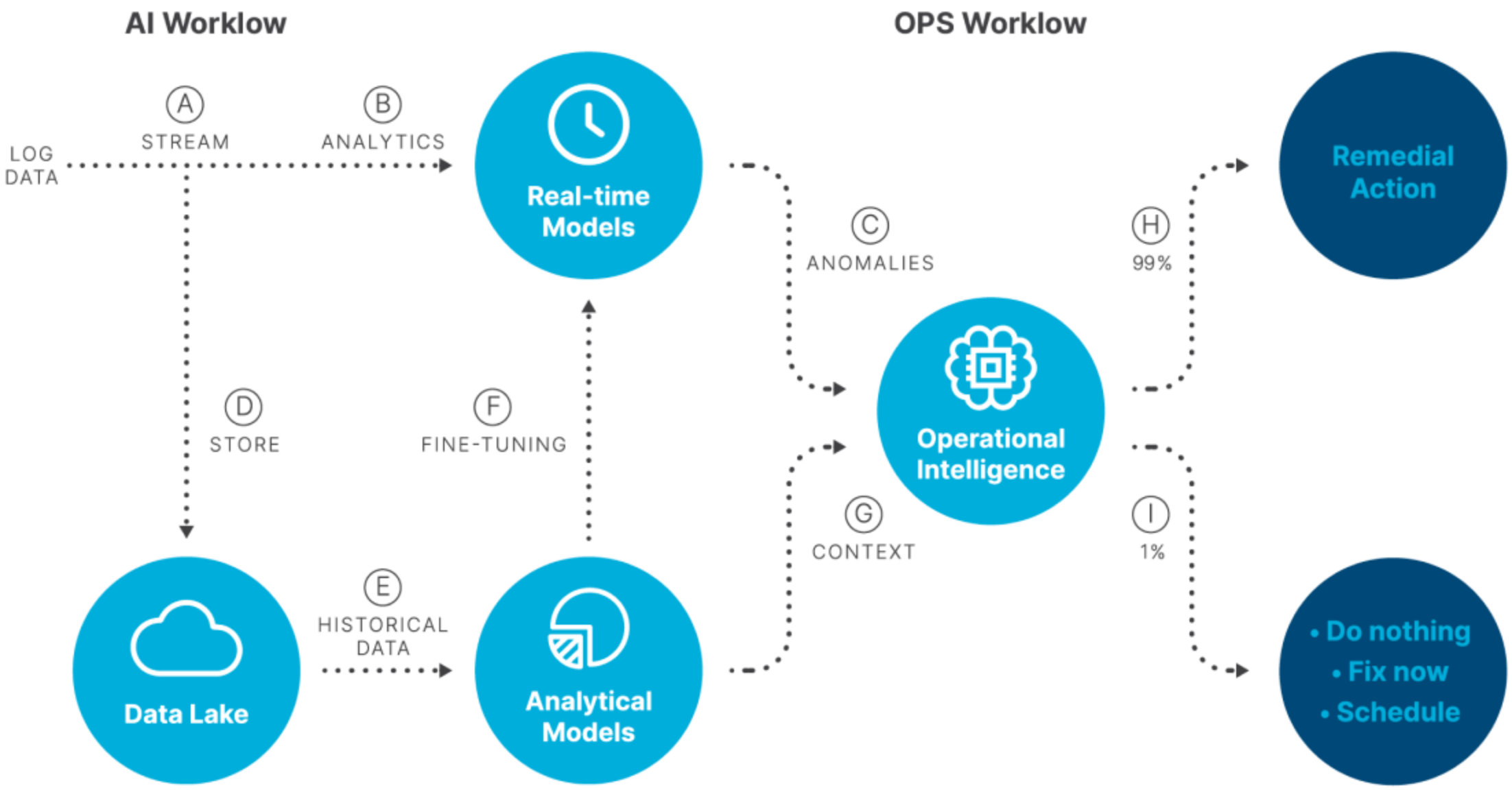


gart.

AI + Operations = A Brighter Future

In DevOps, teams work together to develop, test, and deploy software quickly and reliably.

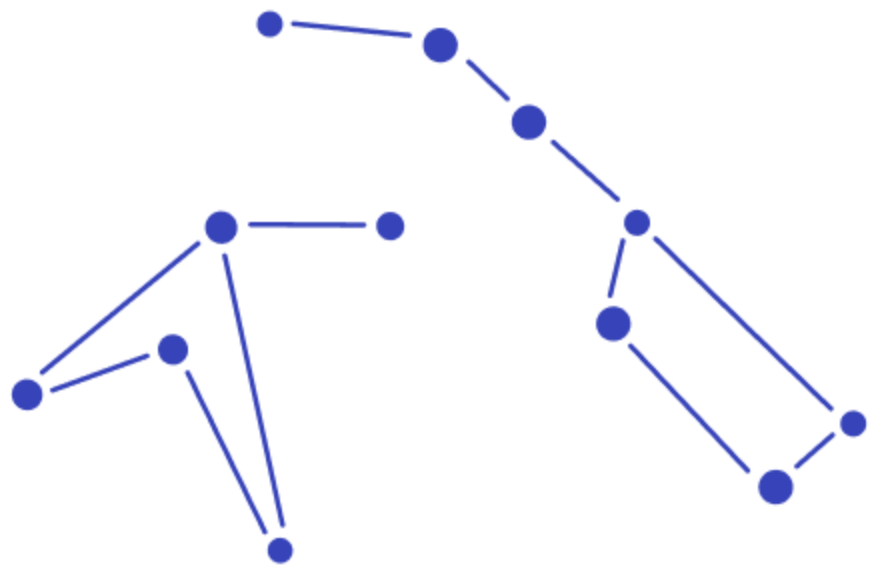
AIOps brings artificial intelligence and machine learning into this process to make it even better.



gart.

How does AI improve DevOps?

gart.



AIOps enhances DevOps by automating tasks and improving system monitoring

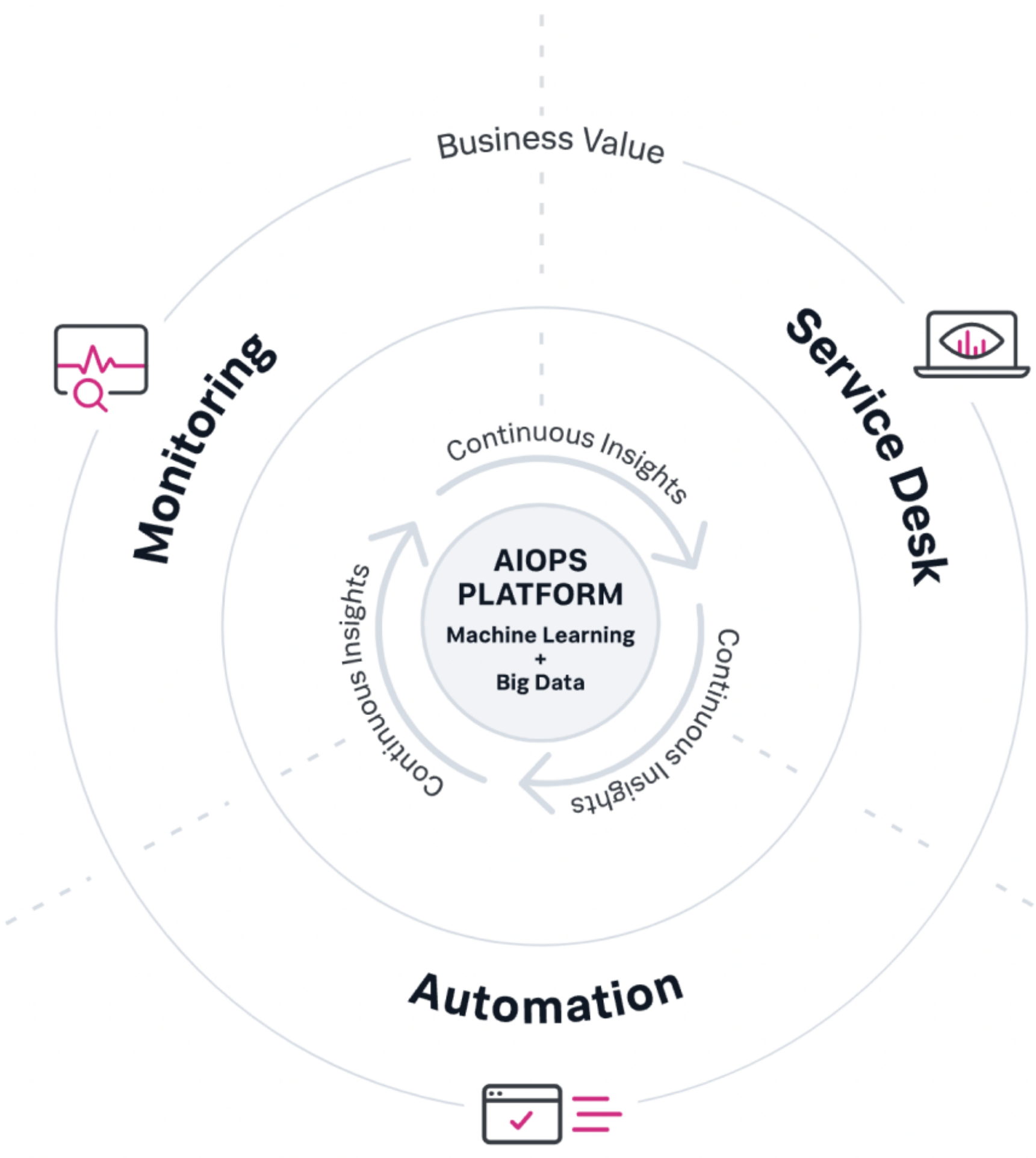
gart.

In DevOps, AIOps offers:

- Continuous monitoring for real-time performance.
- Swift anomaly detection, like a vigilant guardian.
- Instant alerts for quicker issue resolution.
- Deep-dive root cause analysis.
- Task automation for seamless operations.
- Predictive maintenance to prevent failures.
- Performance and cost optimization insights.

gart.

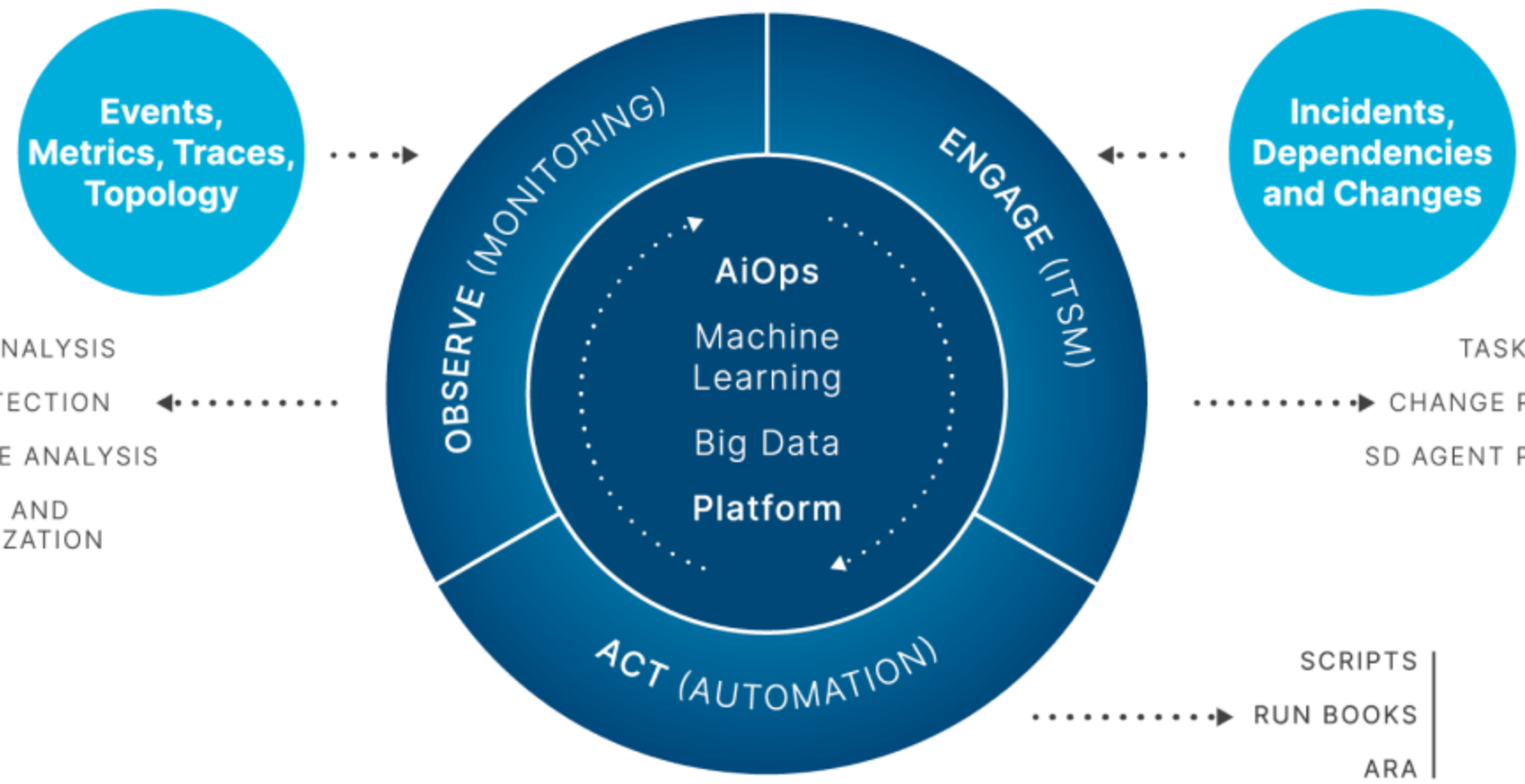
AIOps Basics



gart.

AIOps concept

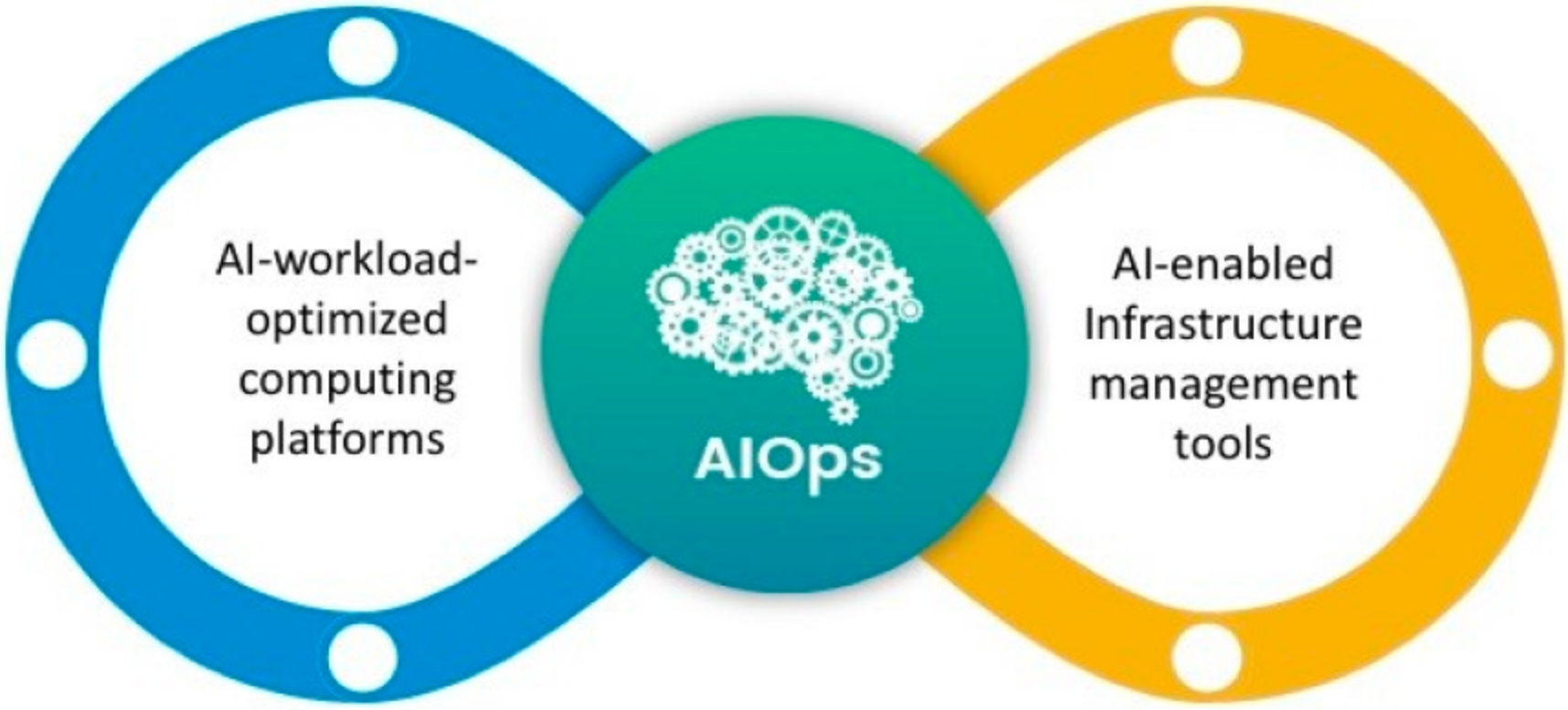
The concept (and practice) of AIOps is aimed at transcending the growing array of tools and API-based integrations to create a unified and centralized framework for managing the entire infrastructure.



gart.

The Transformative Power of AIOps in IT Operations

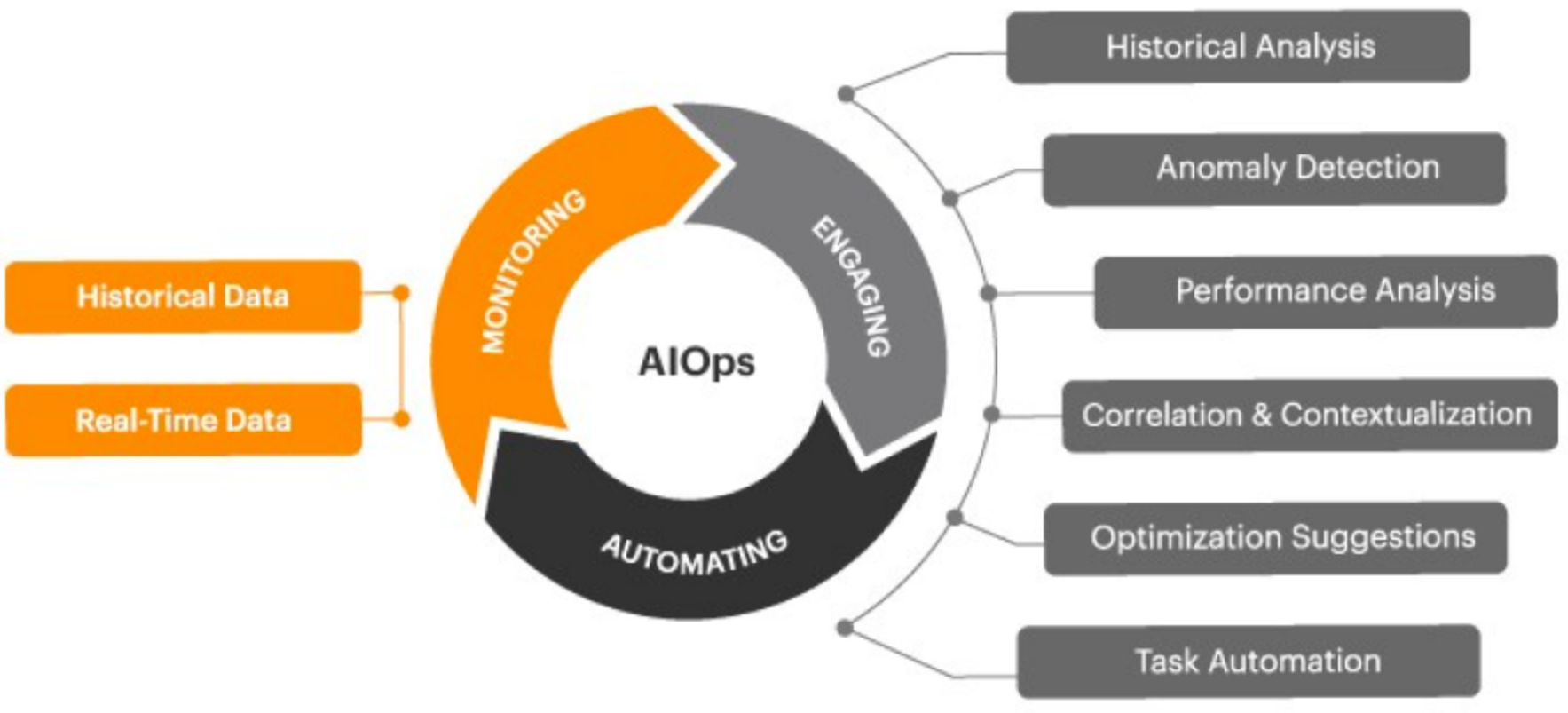
1. **Reduced IT Complexity:** AIOps frameworks come with predefined metrics, procedures, policies, and process templates.
2. **Automation of Work Processes**: AIOps gathers information on all systems within a network, tracking business process execution.
3. **Real-time Company Infrastructure Overview**: AIOps continuously updates a real-time overview of a company's entire infrastructure, covering physical servers, workstations, multi-cloud environments, data repositories, applications, and services.



gart.

The Transformative Power of AIOps in IT Operations

4. **Business Continuity and Productivity Growth**: AIOps frameworks help maintain strict Service Level Agreements (SLAs) for both internal and external users.
5. **Quick ROI (Return on Investment)**: AIOps frameworks improve IT operations, supporting high service availability.
6. **Differentiation in the Competitive Landscape**: As AIOps adoption is not universal, organizations implementing these systems gain a competitive edge. Users appreciate the rapid response of applications and services, a natural outcome of AIOps implementation.



gart.

Why Working in an AIOps-Enabled Company is game Changer

1. **Faster Onboarding for New Hires:** AIOps simplifies the onboarding process for new employees, regardless of their skill level. While it doesn't mean hiring just anyone, it certainly reduces the learning curve and associated costs.
2. **Reduction in Routine Tasks:** A higher level of automation with AIOps frees IT personnel from manual operations. This efficiency not only saves specialists' time but also allows them to focus on higher-level tasks, reducing errors associated with human factors. AIOps frameworks come with built-in automation processes for workflows, such as managing service tickets, vulnerabilities, recovery processes, compliance assessments, reporting, and more.
3. **More Resources for Innovative Processes:** While salary and work schedules are primary motivators for employment, the prospect of engaging in more interesting work than routine processes is appealing.

gart.

Three-phased AIOps approach

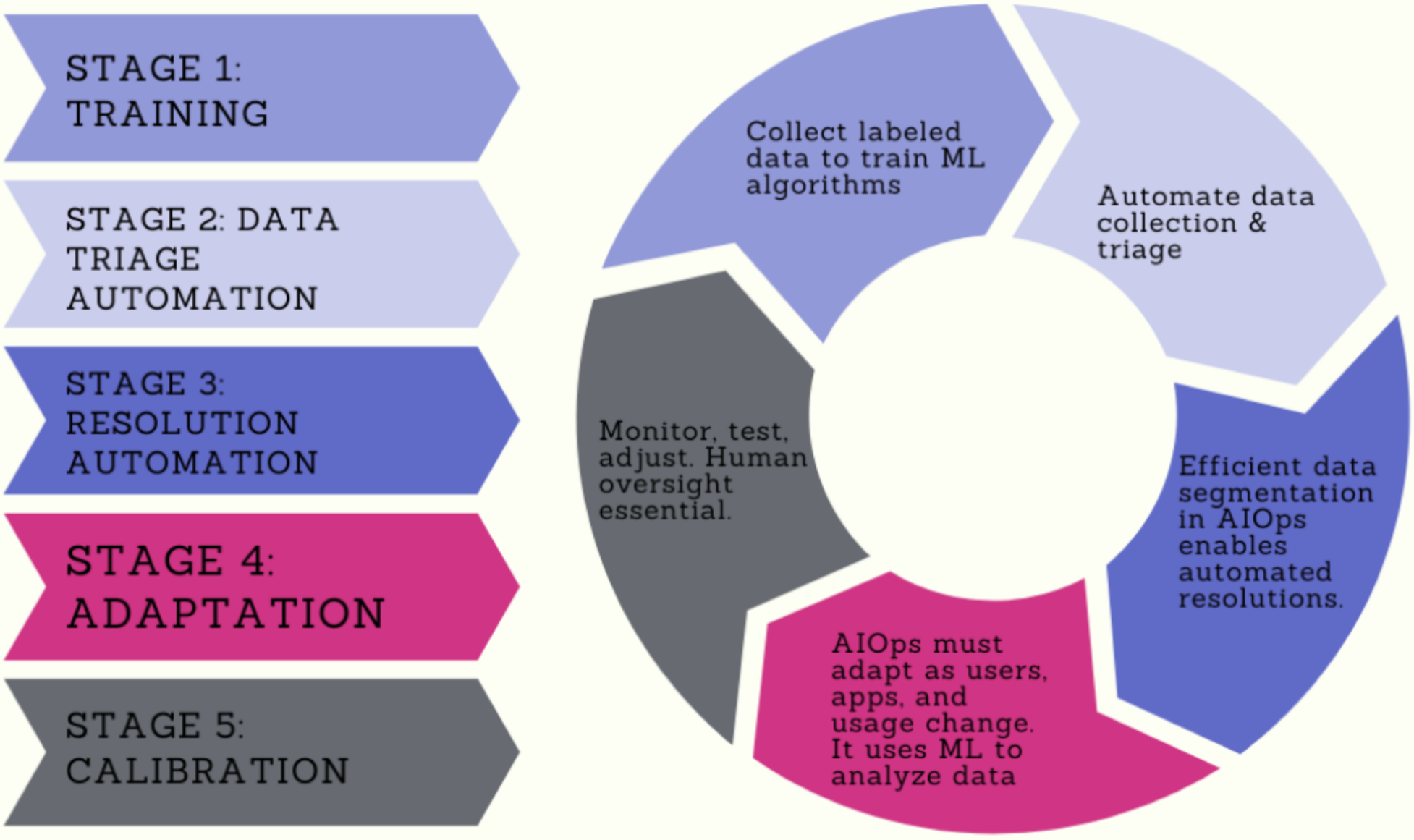
An effective approach to AIOps should consist of three phases.

1. Predicting issues before they occur
2. Preventing impact to end users
3. Automating remediation and resolution

gart.

AIOps stages

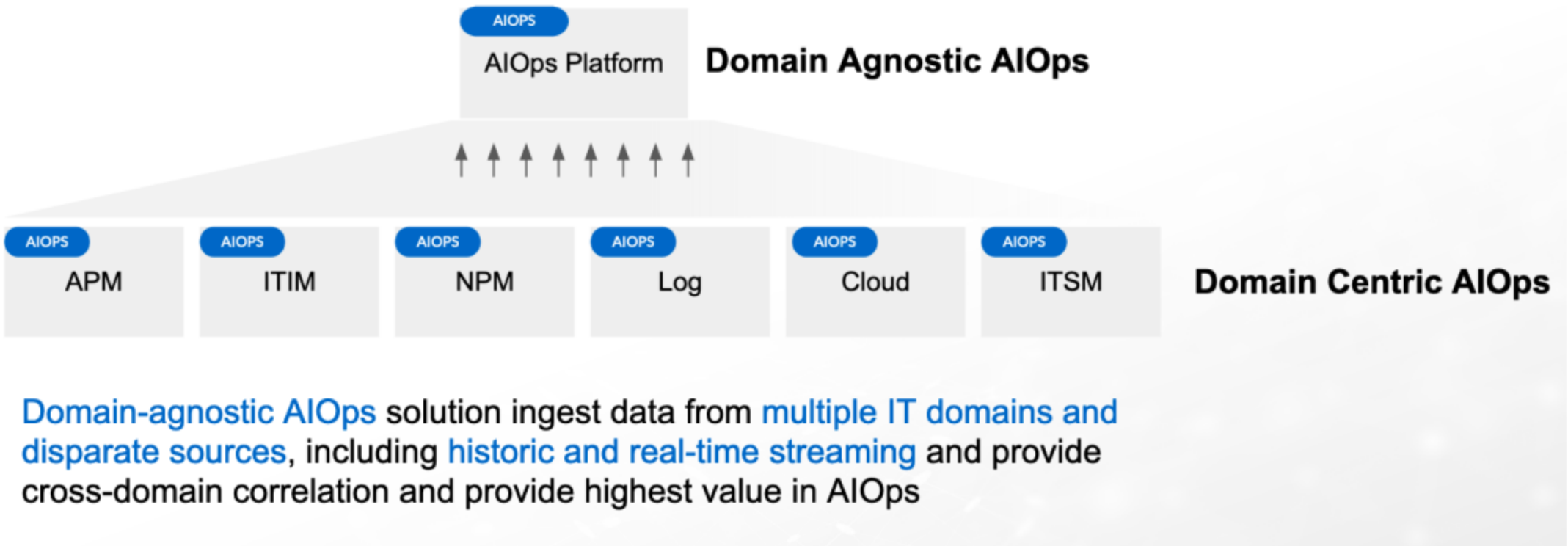
AIOps uses advanced analytical technologies such as machine learning to automate and optimize IT operations processes. AIOps typically works by following these steps:



gart.

Types of AIOps Solutions

1. **Domain-centric** tools focus on a specific area like log monitoring, while domain-agnostic tools operate broadly across domains such as monitoring, cloud, and infrastructure.
2. **Domain-agnostic** tools use vast IT data from across an organization to build models, offering flexible, accessible, and future-proof solutions.

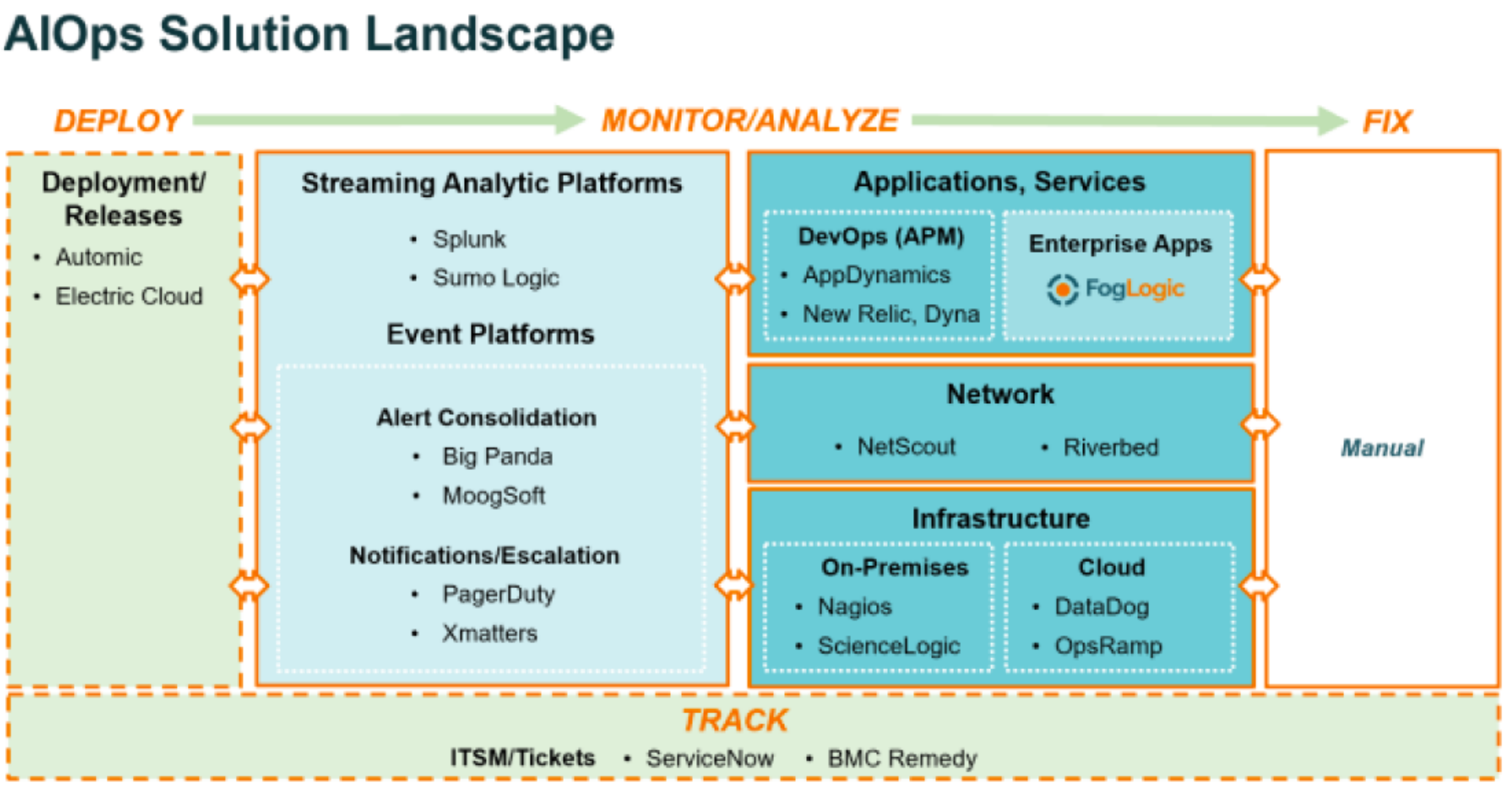


gart.

AIOps Landscape

One of the challenges for customers is to navigate and understand the AIOps landscape because most vendors do claim AIOps, but the application of AIOps is different. Following are some common themes I have seen:

1) Monitoring-centric AIOps (Domain-Centric)
2) ITSM centric-AIOps (Domain-Centric)
3) Data-Lake centric-AIOps (Domain-Centric)
4) Pure play AIOps: (Domain-Agnostic)



gart.

Monitoring-centric AIOps (Domain-Centric)

Observability or monitoring tool vendors are now claiming AIOps, but this is often a limited, domain-centric application of AI. While suitable for smaller IT estates, it falls short for large enterprises using multiple tools, common in industries like healthcare and finance where organizations may employ 15 or more tools.

Sample vendors: AppDynamics, Dynatrace, NewRelic, Datadog, LogicMonitor, ScienceLogic etc.

dynatrace

Science Logic

gart.

Logic Monitor

ITSM centric-AIOps (Domain-Centric)

Incident management-focused vendors, initially centered on event and incident data, are now integrating AI/ML for incident-specific applications. This form of AIOps is localized to incidents, primarily serving reactive roles for service desk, NOC, and ITOps teams. While some vendors expand into the broader IT operations space due to their extensive footprint, choosing them for easier data access may not be optimal in the long run.

Sample vendors: ServiceNow, PagerDuty, Cherwell

Data-Lake centric-AIOps (Domain-Centric)

Initially known for serving as extensive data stores or data lakes for log data, these vendors expanded to include various data types. While offering AI/ML for predicting patterns and providing analytics on their data, a significant gap in this type of AIOps is the lack of understanding and context of the application stack, topology, serviceability, supportability, and the connection between apps and business or service.

Sample vendors: Splunk, Elastic, Graylog

Pure play AIOps: (Domain-Agnostic)

These vendors are truly domain-agnostic, operating on IT data from all domains (apps, microservices, infra, incidents, cloud ...) and provide aggregate intelligence and augmented decisions taking into consideration a very wide spectrum of IT data, thus yielding better results than purely domain-centric platforms. One major advantage of such platforms is also the notion of understanding the application and business context that allows for driving better ML decisions and reducing false positives and unintended consequences that may be prevalent in machine driven decisions.

Sample vendors: CloudFabrix, BigPanda, Moogsoft

AIOps as a Cybersecurity Tool

1. **Data Classification and Monitoring**: AIOps helps categorize data and classify the resources collecting and storing it. This enables the application of cybersecurity measures in line with established policies.
2. **Early Detection of Threats**: AIOps automatically establishes a baseline template for user activity and system performance. Real-time monitoring facilitates the detection of deviations and anomalies. When integrated with cybersecurity or Security Information and Event Management (SIEM) systems, this allows for the rapid identification of malicious activity.
3. **Contextual Threat Management**: Suspicious signals about system states can be cross-referenced with data from other sources, including the company's knowledge base or external threat intelligence services. This approach helps identify threats posing real risks to the company, allowing security or IT teams to focus efforts on addressing the most critical vulnerabilities.
4. **Enhanced Incident Response Capabilities**: Automated AIOps processes notify the appropriate personnel of suspected threats. The responsible party receives immediate information about the severity of the incident, the affected infrastructure segments (along with dependent elements), and even guidance on how to respond to the threat.

gart.

Key AIOps use cases

Alert Noise Reduction
AIOps streamlines alert management by correlating alerts, reducing redundancy, and leveraging AI/ML to offer recommendations, patterns spotting, and forecasting to minimize alert volume.

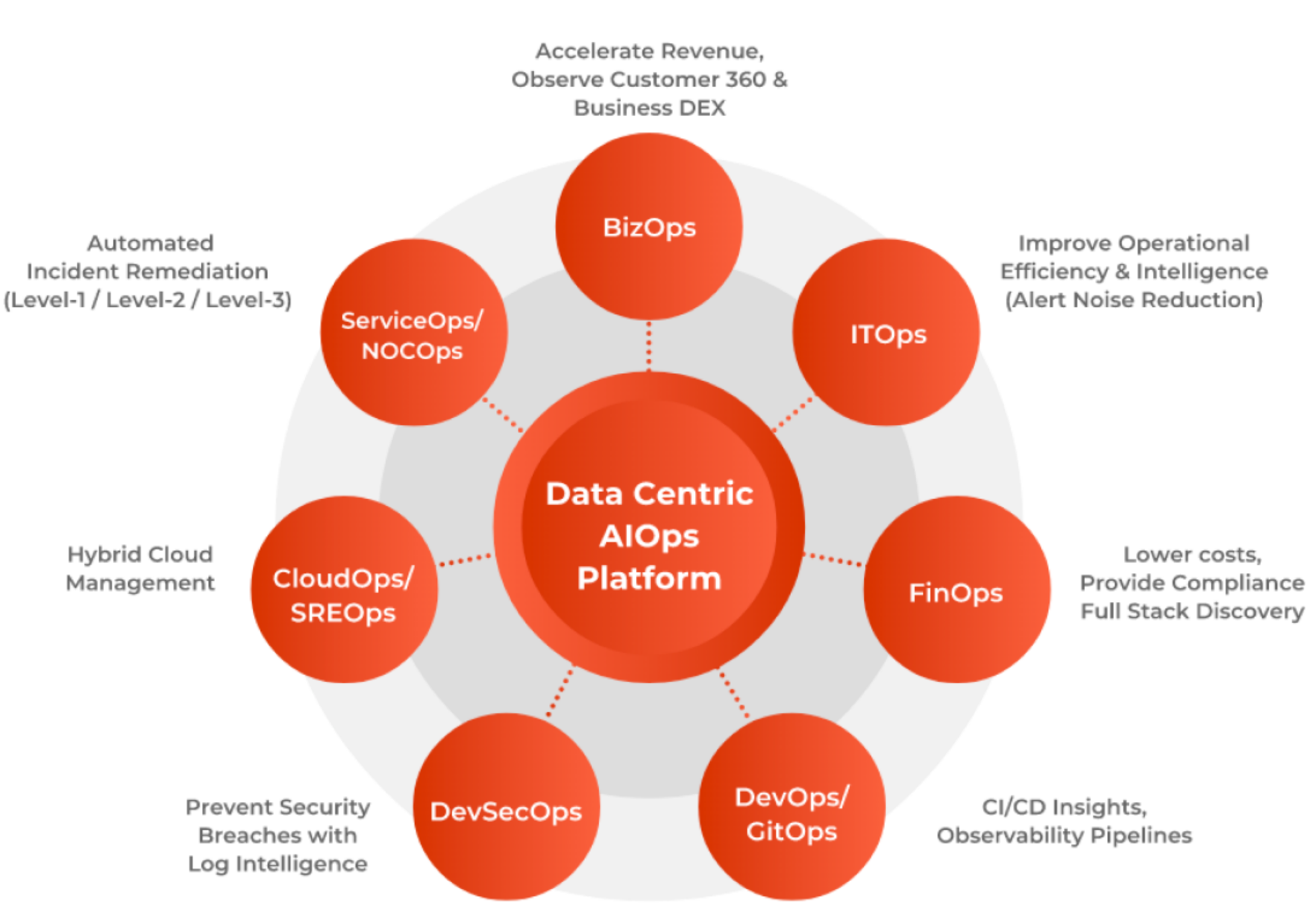
Incident Room
AIOps enhances incident management with AI/ML recommendations, quick root cause identification, and streamlined communication through channels like Slack or Teams, improving metrics like Mean Time to Resolution.

Predictive Analytics
AIOps converts unstructured data into time-series data, running predictive analytics by identifying key data points through correlation with high-level KPIs, continuously monitoring critical observability data, and initiating preventive measures.

Asset Intelligence
Real-time asset intelligence in AIOps provides rich contextual information for IT monitoring, aiding Ops teams in identifying issues, managing risk and compliance, offering a 360-degree view of asset inventory, and supporting dependency mapping in complex IT infrastructures.

gart.

Who is using AIOps and Why?



gart.

Who is using AIOps and Why?

AIOps is embraced across diverse teams like DevOps, SRE, ITOps, cybersecurity, and business leaders, impacting all aspects of business and IT.

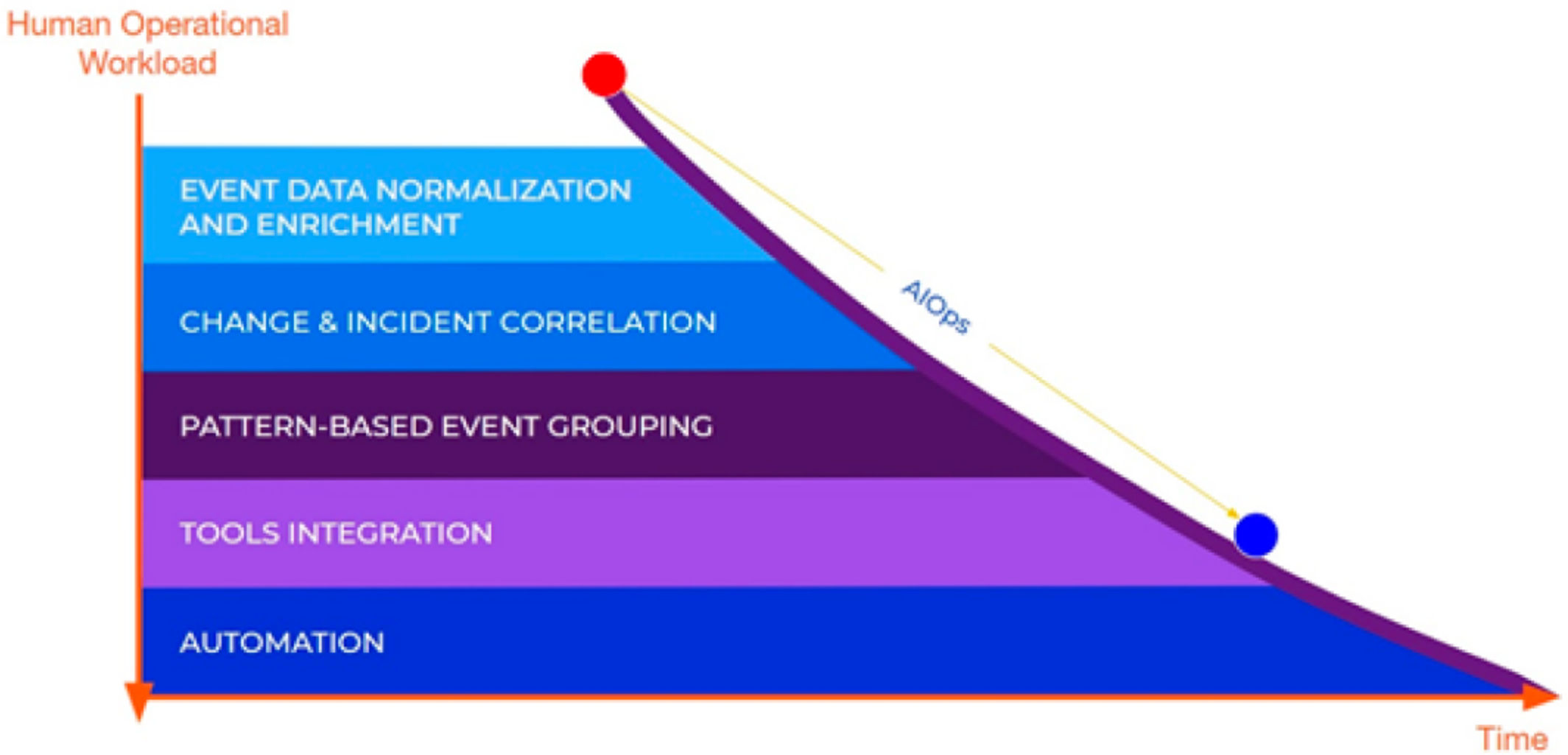
- **DevOps:** AIOps supports DevOps with metrics, traces, and log analysis, evolving to focus on production metrics like user engagement and business relevance as DevOps practices mature.
- **ITOps:** ITOps teams start with event correlation and expand into metrics, logs analysis, and behavioral analytics, aiming for anomaly detection, diagnostics, root cause analysis, and automation of actions.
- **SRE:** SRE objectives align with ITOps and DevOps, emphasizing resilience. While event correlation and log analytics aren't primary, AIOps platforms provide real-time insights for topology and dependencies, aiding SRE teams.
- **Business Teams:** AIOps caters to business leaders focusing on efficiency, user engagement, and productivity, emphasizing both quantitative IT metrics and qualitative KPIs for people, processes, and technology.

gart.

The Cost Impact of AIOps

Assessing the cost impact of AIOps goes beyond technology-driven cost reduction. Leaders should consider qualitative benefits like enhanced flexibility, risk reduction, prevention of disruptions, and faster anomaly resolution.

AIOps optimizes revenue, enhances customer satisfaction, protects brand reputation, and has direct and indirect impacts on business performance and the bottom line.



gart.

If you like the content

Share

Like

Comment

gart.