AIOps | Beyond the Buzzword
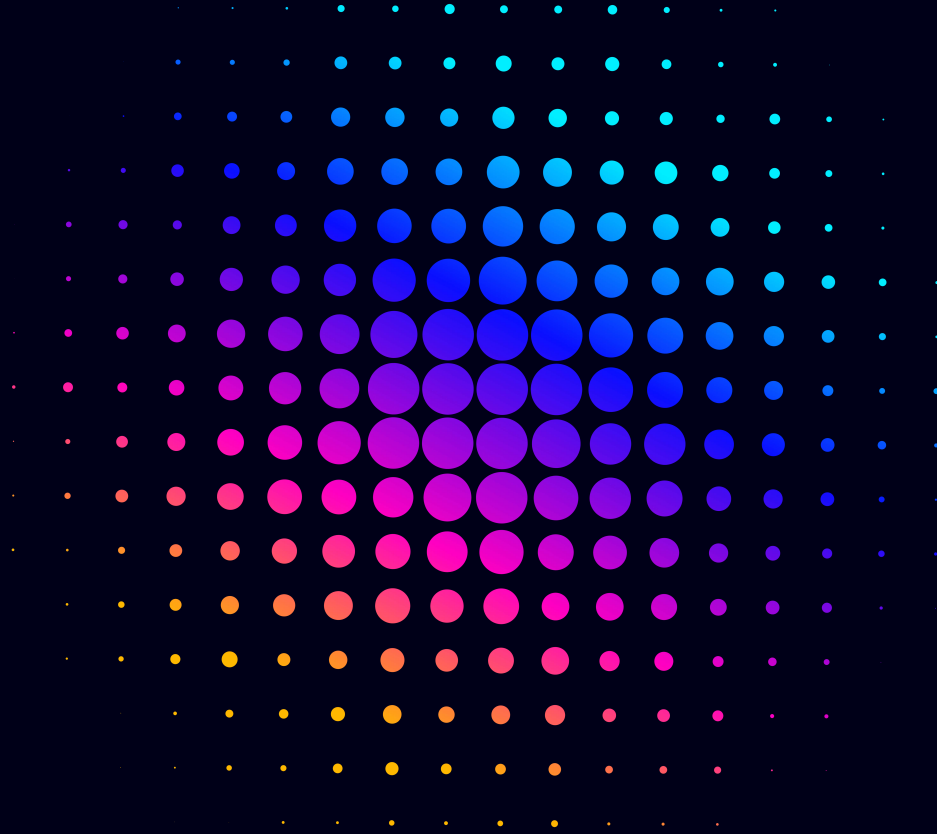
Improving IT Operations with Big Data,
Machine Learning, and Artificial Intelligence

compucom®
Technology Driven.
People Powered.

AIOps | Beyond the Buzzword

compucom.

Technology Driven.
People Powered.

In enterprise organizations with complex and vast IT ecosystems, it's becoming more challenging to maintain a firm grip on IT operations.

INTRODUCTION:
THE BIG DEAL ABOUT AIOPS

AI – Big benefits and some anxiety

How do you feel when you hear the term Artificial Intelligence (AI)? Excited? Anxious? Afraid? Suspicious? Were you an early adopter of ChatGPT, asking it to facilitate business brainstorming sessions, or find you a delectable apple crumble recipe for your family get-together? Will you enjoy using Microsoft Copilot as your productivity assistant? (Many early users do – 77% of current users said once they'd tried Copilot, they didn't want to give it up)

Or does the mention of AI make you think of disappearing jobs and shudder with thoughts of deep fakes and conspiracies, the voice of HAL 9000, SkyNet, and glitches in The Matrix? Frankly, for many of us, it's a bit of both.

There's no denying that there are valid concerns about our future with AI, and we need to stay clear-eyed and vigilant of its limitations and risks, but it's also not all doom and gloom like the movies. Whatever our trepidations, AI has rapidly moved from the realm of sci-fi to become part of our everyday lives. The abundance of practical and beneficial applications for AI in business is undeniable – freeing us from grunt work, augmenting our analytical capabilities, and saving us from costly human errors.

AIOps, or AI for IT Operations, is one such example. It uses Big Data, Machine Learning (ML), and AI to automate and improve how IT operations are managed. AIOps helps companies ingest and analyze the overwhelming quantity of data and alerts generated by IT operations to identify patterns, trends, and anomalies. It learns from these and then makes predictions, initiates automated remediations, or offers recommendations to aid IT teams in decision-making.
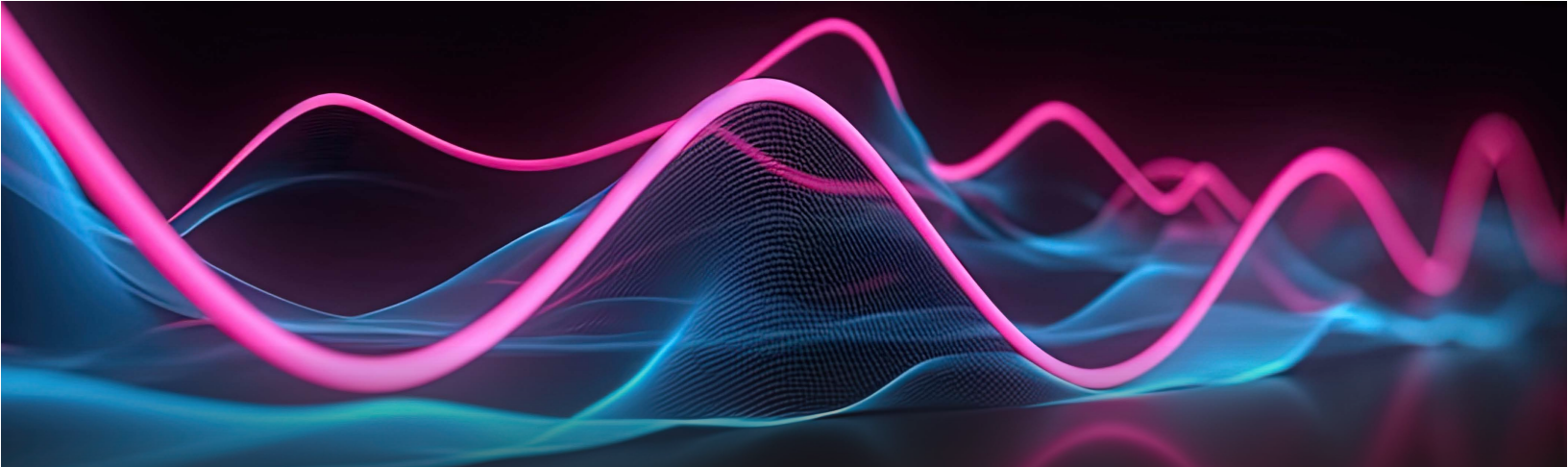
Today's complex and vast IT ecosystems need AIOps

In enterprise organizations with complex and vast IT ecosystems, it's becoming more challenging to maintain a firm grip on IT operations. A typical enterprise organization has numerous applications, services, and infrastructure components in varied locations, generating huge amounts of data and requiring constant monitoring and analysis.

Pair this with increased user expectations and dependence on technology, and it's easy to see the need for a system to help your IT teams cut through the noise to understand and predict which improvements are needed. And if this system can also automate some remedial actions, you'll greatly augment your capability to keep your IT operations running smoothly and efficiently.

Getting AIOps right

The end goals of implementing AIOps are boosted efficiency, less downtime, and cost savings. And who wouldn't want to achieve those? However, implementing AIOps is not as simple as buying a platform like Moogsoft or Splunk.

Whatever the origin of data collected, it's vital that the AIOps framework can handle the volume and scale as your organization grows.

The key to a successful implementation is integrating the right toolsets with your infrastructure to enable three main functionalities:

- Data ingestion (from multiple sources across the infrastructure)
- Analysis, correlations, and recommendations
- Proactive remediation (the fix)

Getting started with AIOps can seem daunting, but a solid first step is to understand what it is and how it works and then identify the areas where it can bring value to your IT operations. In the following sections, you'll gain a big-picture understanding of AIOps, learn how to go beyond the buzzword to a successful implementation, and read about some real-world examples.

UNDERSTANDING HOW AIOPS WORKS

Leveraging Big Data and Machine Learning

Big Data for AIOps refers to large, diverse sets of information sourced from monitoring systems and engagement data such as events, logs, performance, availability, and capacity.

ML is a subset of AI that focuses on algorithms that can learn from data and improve their performance without being explicitly programmed. In AIOps, ML can help discover patterns, trends, and correlations in the data, using them to make predictions and recommendations. It also enables AIOps to adapt to evolving environments and user needs by using feedback loops and reinforcement learning.

AIOps uses Big Data, AI, and ML capabilities to:

- Collect ever-increasing volumes of data from multiple IT infrastructure components.
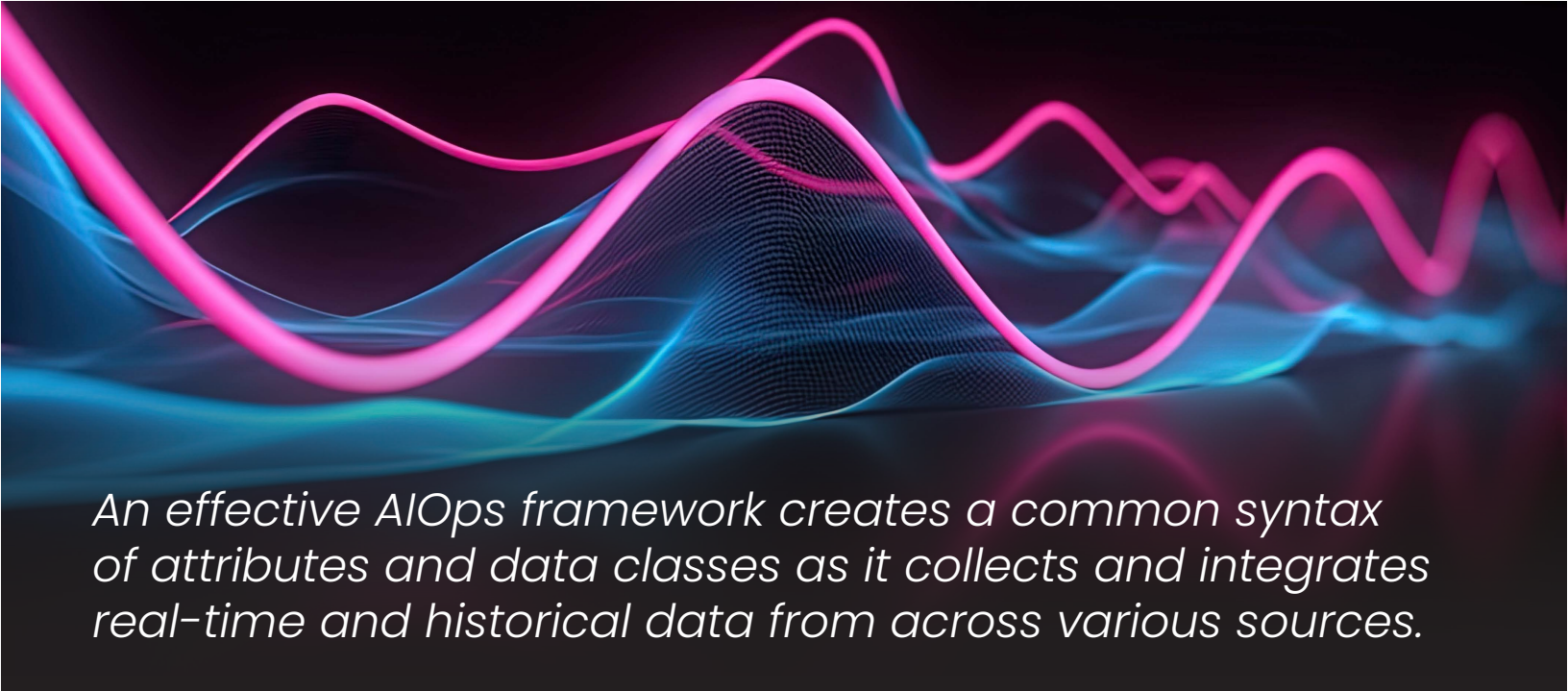
- Intelligently pinpoint significant events and patterns related to performance and availability.
- Diagnose the root cause for automatic or human resolution.

The three functions of an AIOps implementation

According to a recent study, 67% of enterprise infrastructure is now cloud-based. A typical infrastructure can often be a combination of on-premises, private, and public cloud components and may be managed by multiple IT teams.

A successful **AIOps implementation** will carefully integrate several toolsets to help teams collaborate to observe, analyze, and act proactively to fix IT operations issues. These toolsets can be categorized into three functions:

1. **Data Ingestion:** Observability tools handle the ingestion, aggregation, and analysis of performance data from your applications, infrastructure, and network.
2. **Analysis, Correlation, and Recommendations:** AIOps solutions analyze, correlate, and enrich the data for better insights and automated actions, enabling IT teams to filter out the noise from alerts and zero in on anomalies, patterns, and trends in resource requirements to get the big picture of your IT operations in real-time.
3. **Proactive Remediation:** AIOps tools can execute automated processes in response to recommendations, rectifying issues such as slowdowns promptly, sometimes before they even happen.

An effective AIOps framework creates a common syntax of attributes and data classes as it collects and integrates real-time and historical data from across various sources.

Data Ingestion: A closer look

In an enterprise organization, the applications, infrastructure, and network are often siloed, perhaps even delivered by multiple providers. This makes it challenging to gain a comprehensive overview of all IT domains in order to best manage them.

To complicate issues further, each component of IT operations may come with its own "language" or terminology for attributes. An effective AIOps framework creates a common syntax of attributes and data classes as it collects and integrates real-time and historical data from across a company's various sources to build greater visibility and allow for cross-domain analysis of issues.

The sources could be different hosting models, such as on-premises, private cloud, public cloud, or hybrid. The systems needing monitoring might include the following:

- Point of Sale (PoS)
- Internet of Things (IoT) devices
- PCs and servers
- Infrastructure, applications, middleware, databases, and backup

Collecting the data for AIOps may mean plugging in existing monitoring tools, ticketing systems, and incident management systems, leveraging performance monitoring from service providers, or instrumenting the environment with monitoring tools. Whatever the origin of data collected, it's vital that the AIOps framework can handle the volume and scale as the organization grows.

Analysis, Correlation, and Recommendations: Taming the data, identifying incidents, and finding the root cause

Event analysis

Once the data is ingested, the AIOps platform applies machine learning algorithms to filter, remove duplicates, normalize, and correlate events across multiple siloes, boiling the data down into more manageable "incidents."

The algorithms used in incident analysis continuously improve over time in two ways: learning from results applied to previous incidents and through manual training by operators.
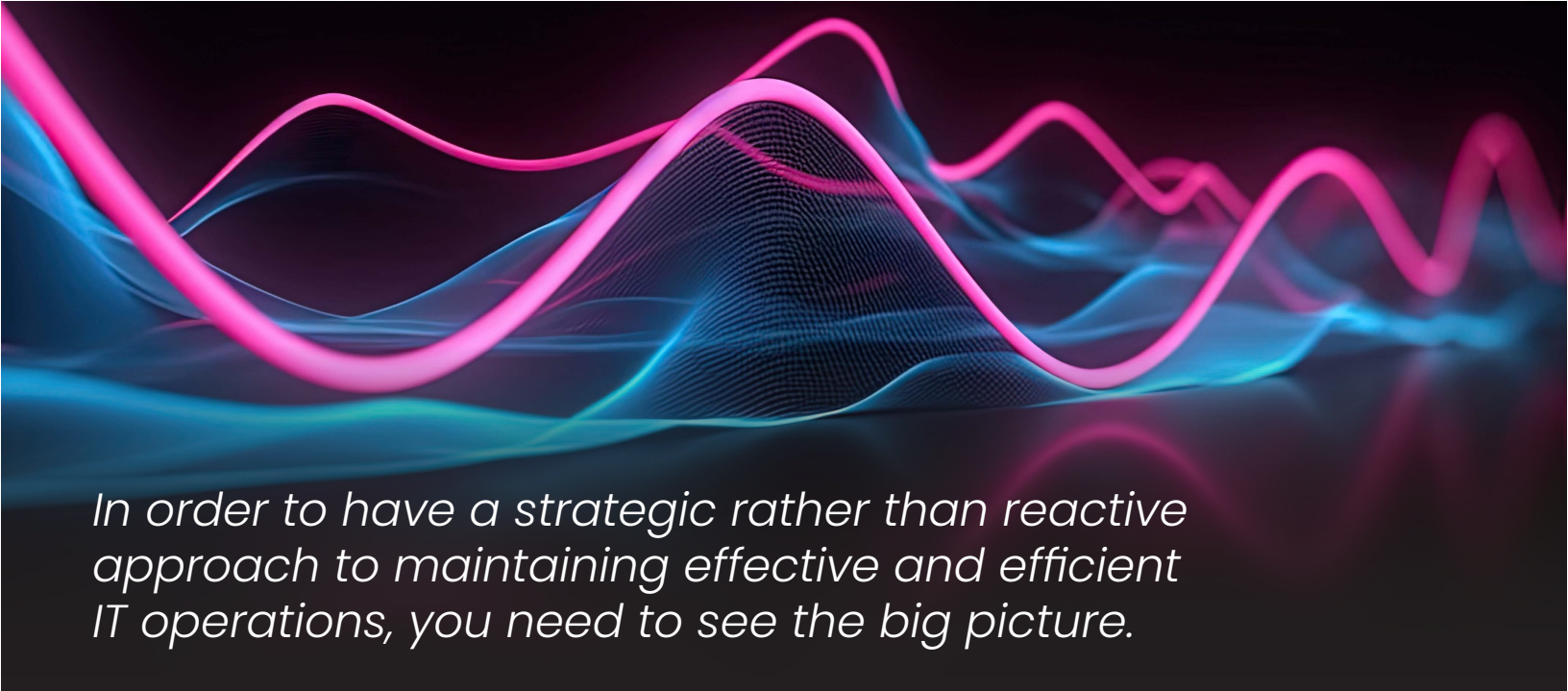
Incident enrichment and management

Alerts and incidents can be enriched with data and details from external sources such as ITSM tools, financial systems, and business databases to aid in the diagnosis and remediation process.

Diagnosis and recommendations

The AIOps platform runs diagnostics to identify the root cause. For example, it may run an automation to collect more information from an endpoint. It then determines how an incident can be resolved and builds recommendations.

If the diagnostics cannot determine a resolution, AIOps escalates the incident and may dispatch a technician to perform further diagnostics.

In order to have a strategic rather than reactive approach to maintaining effective and efficient IT operations, you need to see the big picture.

Proactive Remediation: Enable your IT teams with automated remediation and better insights

Automated remediation

Some AIOps implementations only provide monitoring and make recommendations. A more sophisticated implementation includes the capability for automated responses through an execution engine.

This provides some key advantages:

- Rather than waiting on human engineers to respond, incidents can be resolved more quickly, helping improve IT operations and, by extension, the user experience.
- AIOps tools can use historical data to improve automated remediation over time, growing more effective the longer the tools are in place.

This doesn't mean handing over complete control for incident response. Policies can be set to configure how AIOps tools respond in various scenarios. For example, adjustments to specific infrastructure components, such as a critical server, could require review and approval from a human engineer.

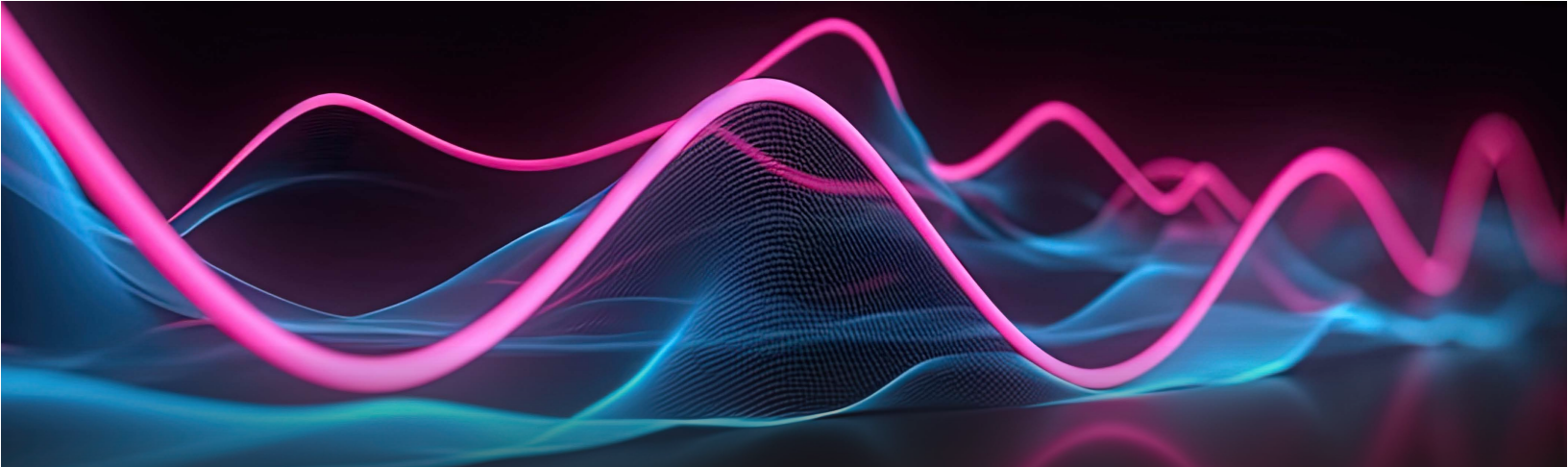### Better decision-making and proactive remediation

In order to have a strategic rather than reactive approach to maintaining effective and efficient IT operations, you need to see the big picture. Today, that's almost impossible without AIOps. The days of searching through log files to identify possible issues are gone. It's no longer humanly possible to deal

with the vast amounts of data from the metrics, logs, traces, emails, and tickets in a typical enterprise infrastructure, especially when functions may be siloed and perhaps come from different providers.

A well-integrated AIOps platform can help with these challenges by:

- Determining a model of normal operating parameters for a system and then monitoring for anomalies. Anomalies can then either alert the right IT operators so they can work to resolve an issue before it happens or trigger an automation, for example, starting other instances of an in-demand application during predicted spikes in use.
- Creating an accurate topology that provides real-time insight into the state of critical systems and services so IT teams can focus on innovation rather than just responding to the everyday problems inherent to complex IT operations.

As you can see from the descriptions of the three AIOps functions, the "GIGO" (Garbage In, Garage Out) principle is relevant to effective AIOps implementation. You can buy fancy AI tools, but they won't help your IT operations unless the algorithms can be trained on accurate data. In the next section, we'll talk about how properly integrating the right toolsets with your IT systems is the key to reaching the full potential of AIOps.

To go beyond the buzzword, cut through the hype, and realize the benefits, AIOps components must be properly integrated with your IT systems.

GOING BEYOND THE BUZZWORD

As with any buzzword-worthy trend, ensuring a new technology aligns with your business's specific needs and strategic goals before diving in is essential. But once you've determined that AIOps is a fit for your company — to go beyond the buzzword, cut through the hype, and realize the benefits, AIOps components must be properly integrated with your IT systems.

Early AIOps adoption and expertise

Gartner coined the term AIOps in 2017. But even before then, Compucom's delivery teams were investigating ways to help customers cope with the increasing complexity and scale of IT infrastructure combined with the exploding volume of real-time data. As an early adopter of AIOps capabilities, we recognized the urgent need to help our customers better handle their IT operations.

Since they were initially introduced, AIOps tools have matured, becoming more scalable. Through experience, we've refined a set of combined tools that can readily integrate our customers' existing capabilities and customize them to suit their needs and preferences.

To date, we have retail, finance, and healthcare customers that are benefiting from our AIOps expertise. We provide AIOps as part of our Infrastructure Management and Cloud Technology services, and we can support on-premises, cloud, and hybrid environments.

Our AIOps approach

Compucom's approach integrates toolsets to handle five AIOps components.

1. The **Event Management** component monitors and manages network, server, storage, application, and IoT data, passing events to the Situational Awareness component.

2. The **Situational Awareness** component correlates events to determine an "incident," reducing event noise by 98%. The incident is enriched with relevant data to help understand system and business impact in virtual situation rooms that enable collaboration across multiple domains. Algorithms are applied to determine the root cause, learning from previous results and from manual training by the operators.

3. The **Engage** component (IT Service Management or ITSM) manages and records all actions and results from the Situational Awareness and Orchestration Services components. This dramatically improves record and ticket quality, allowing for much more effective Problem Management.

4. The **Orchestration Services** component is instructed by the Situational Awareness component when additional information or action from an endpoint or service is needed. It enables operators to design workflows for diagnosis and remediation, which may include steps asking for human input.

5. The **Execution Services** component directly interacts with the endpoint devices. It executes the commands from the Orchestration Services component and returns the results.

Your organization's topology provides context for AIOps, and visualizations and dashboards show the big picture of your applications and infrastructure.

Monitor the right sources. Use the right tools.

Sophisticated AIOps monitors and ingests data from three layers. Events from these layers can then be correlated to create context and a better understanding of inefficiencies or bottlenecks:

- **Hybrid IT Infrastructure:** Sources such as compute, network, storage, IoT, logs, and databases are typically monitored by Element Management Systems (EMS). Our AIOps solution ingests these sources and can integrate events from other Managed Services Providers (MSPs).
- **Applications**: These include all in-scope business applications hosted within the Hybrid IT Infrastructure. This is typically accomplished through Application Performance Management (APM).
- **Business Transactions:** This includes monitoring transactions within the environment, like real-time order volume. This is also accomplished with APM.

As we put together our version of AIOps, we prioritized the following:

- **"Plug and Play" Flexibility:** Our flexible interface (Enterprise Service Bus) enables us to easily integrate Compucom and customer tools for various application and infrastructure support requirements — such as monitoring tools, ticketing systems, and incident management systems — switching them out as needs evolve.
- **Better Visibility into Applications and Infrastructure:** Your organization's topology provides context for AIOps, and visualizations

and dashboards show the big picture of your applications and infrastructure.
- **Enhanced Diagnosis and Incident Remediations Capabilities:** Incident diagnosis is enhanced through advanced intelligent event aggregations, filtering, correlation, and machine learning. Remediations are optimized with artificial intelligence and business process automation.
- **A Minimal Footprint Within Your Managed Environment:** The AIOps platform and associated execution engine have a small footprint to minimize the burden on your computing environment.

Effective AIOps delivers serious advantages

Through anomaly detection, event correlation, and enhanced root cause analysis, Compucom's AIOps equips IT teams to:

- Improve root cause analysis across IT system silos.
- Reduce network congestion.
- Remedy the increased average response time for an application.
- Cut down the overwhelming volume of alarms.
- Identify issues during change management processes.
- Lower Mean Time to Detect (MTTD) and Mean Time to Remediate (MTTR).
- Dramatically reduce ticket counts and improve ticket quality.

Even the most dedicated system or network administrator will learn to tune out alerts if too many have turned out to be false alarms.

REAL-WORLD AIOPS: EXAMPLES AND BENEFITS

If you're reading this, perhaps you're trying to figure out if Artificial Intelligence for IT Operations (AIOps) could help your company, or maybe you're just brushing up on the latest IT lingo with a coffee in your hand, or if you're fancy, perhaps a double-shot, venti, non-fat, no-whip mocha with caramel drizzle. Either way, it helps to have some real-life examples of how AIOps can help IT teams improve the efficiency and lower costs of their IT operations.

AIOps Benefit: Anomaly detection for better troubleshooting

Today's complex IT environments make monitoring very noisy, with frequent or irrelevant alerts crowding out the most important ones. Anomaly detection uses machine learning algorithms to identify patterns and trends in data and detect deviations from normal behavior. This means monitoring can more easily adapt to seasonal or cyclical variation without manual tuning to avoid false positives or negatives.

A significant advantage of anomaly detection is that it can help you discover unknown or hidden issues you may not have anticipated or defined thresholds for, enabling proactive action before users are impacted.

Example
A retail business implements AIOps for more proactive troubleshooting. Normal operational baselines are built, accounting for spikes in ordering patterns during seasonal changes.

One day, AIOps detects an increase in average response time for a crucial ordering application, indicating a spike in demand outside the expectations for the time of year. Happily, stakeholders identify the likely cause as the introduction of a new line of unexpectedly and wildly popular products – they're riding the latest TikTok fad!
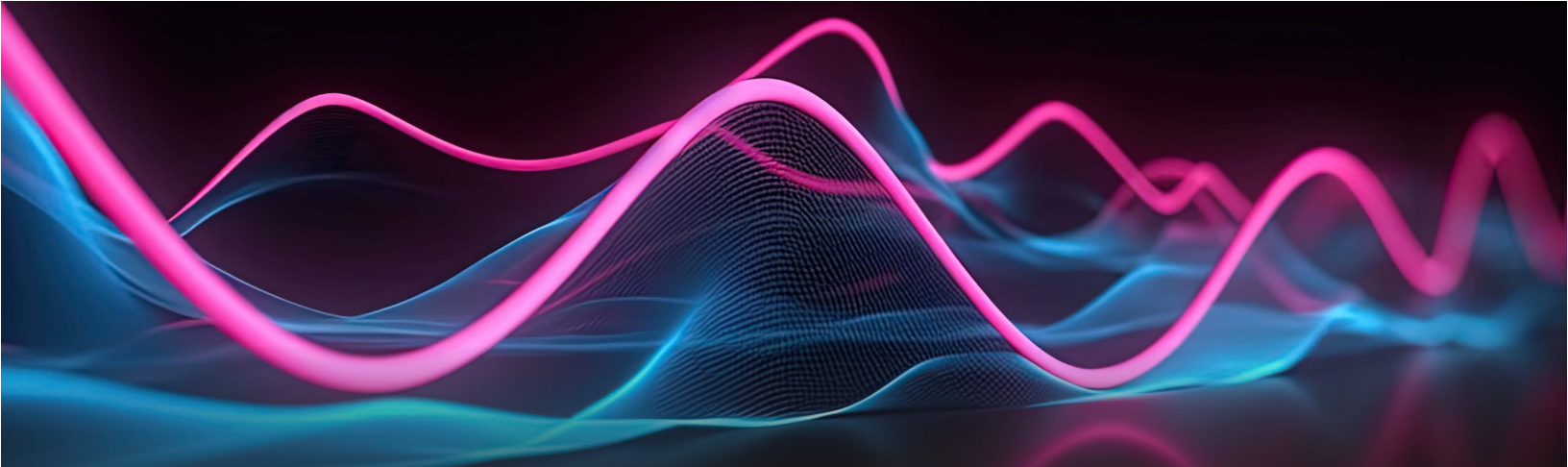
Since AIOps is trained in handling an increase in usage corresponding to seasonal changes, it recommends an automation to create new instances of the application so that ordering processes are not impacted.

Based on knowledge of the organization's topology, AIOps also provides operators with details of this remediation for cohort devices and applications so they can proactively ensure the unexpected spike will be handled smoothly.

AIOps Benefit: Event correlation to lower alert fatigue

Even the most dedicated system or network administrator will learn to tune out alerts if too many have turned out to be false alarms.

AIOps uses machine learning algorithms to analyze the alerts from different sources and find the patterns and dependencies among them. It then groups related alerts based on common attributes, such as time, location, source, or type, and filters out irrelevant or false alerts based on predefined thresholds. Then, natural language processing generates meaningful incidents that describe the issues' nature, severity, and impact.

AIOps augments your teams' abilities to find the source of an issue and collaborate to speed up Mean Time to Resolution (MTTR).

Example

A healthcare organization has a cloud-based electronic health record (EHR) system monitored by various tools for performance, availability, security, and compliance. However, many of the alerts are redundant or irrelevant.

AIOps helps their IT team:

- Group the alerts – for example, if the EHR system experiences a network outage that affects multiple servers and applications, AIOps groups all the alerts related to the network outage into one incident.
- Filter out irrelevant alerts, such as those expected due to routine maintenance or testing activities for the EHR system.
- Prioritize incidents based on their urgency, importance, or business impact. If the EHR system has some incidents that affect patient safety or privacy, such as data loss or breach, AIOps prioritizes these incidents and assigns them a critical status.

By using AIOps to group related alerts using event correlation, the healthcare organization successfully reduces alert fatigue and improves incident management for their EHR system.

AIOps benefit: Faster and more accurate Root Cause Analysis (RCA)

Getting to the root cause of a performance issue can take up a lot of time, especially when teams are siloed and have limited visibility into the complete picture.

AIOps augments your teams' abilities to find the source of an issue and collaborate to speed up Mean Time to Resolution (MTTR). By leveraging AIOps to detect the pattern of impact from an event, operators can use events and their root causes as modeled "fingerprints" within the time series data and logs, speeding up AIOps' ability to recognize and resolve incidents.

Example

A government organization implements AIOps, hoping to reduce service desk tickets and increase their quality:

1. Monitoring tools pick up a recurring CPU spike on a server at 2 AM every morning.
2. AIOps generates a ticket each time, but after checking for signs of the spike an hour later, closes the ticket with no known cause.
3. During Problem Management processes, an operator notes the recurring tickets and creates an automation to query the device as soon as the CPU spike is detected, taking a snapshot of running processes.
4. The operator identifies the pattern; an antivirus process runs daily on the server at 2 AM.
5. The operator trains AIOps that, before creating a CPU spike ticket for the server, it should check to see if it's just the antivirus process running.
6. This remediation is suggested to operators when other incidents match the fingerprint.

By enabling operators to investigate further and improve the quality of the tickets, AIOps helps them eliminate unnecessary tickets. This noise reduction ensures issues that need remediation will not get lost in a sea of meaningless alerts.

With AIOps spending expected to reach $40 billion by 2026, many companies are jumping on board the AIOps train.

GET A HANDLE ON YOUR IT OPERATIONS

So, is AIOps overhyped? Should system and network administrators start quaking in their Vans if their boss mentions AIOps because robots are coming to steal their jobs? Definitely not.

When the camera was invented in the 1800s, a critic decried photography as "the mortal enemy of all art," echoing fears of contemporary painters that it would make them irrelevant. Luckily, that was far from what happened — photography inspired Impressionism and the modern art movement. Just like photography spurred artists to new levels of creativity, AI is at its best when it builds on our human capabilities — freeing us from drudgery and allowing us more time for creative, challenging, and fulfilling work. AIOps isn't intended to displace IT teams but rather help them better cope with the significant issues they face today:

- Sorting through overwhelming infrastructure data from many sources
- Ever-present and escalating cyber threats
- An ongoing shortage of IT talent

To optimize IT operations, your IT team needs to understand the big picture by correlating metrics, events, and logs and then connecting the dots to figure out solutions. AIOps gives them automation and advanced tools to help them achieve that.

With AIOps spending expected to reach $40 billion by 2026, many companies are jumping on board the AIOps train. Ensuring you reach your goals rather than just paying for hype is essential. Going with an experienced provider like Compucom allows your IT talent to go beyond the buzzword and reap the benefits of truly effective AIOps.

At Compucom we are technology driven and people powered. Learn more about how we can help you with sourcing, integrating, and supporting your technology needs at compucom.com.

compucom.
Technology Driven.
People Powered.