IT Crisis Management: How AIOps Cuts Costly Downtime and Supports Teams

bigpanda | CIO DIVE

Custom content for BigPanda by **CIO Dive's Brand Studio**

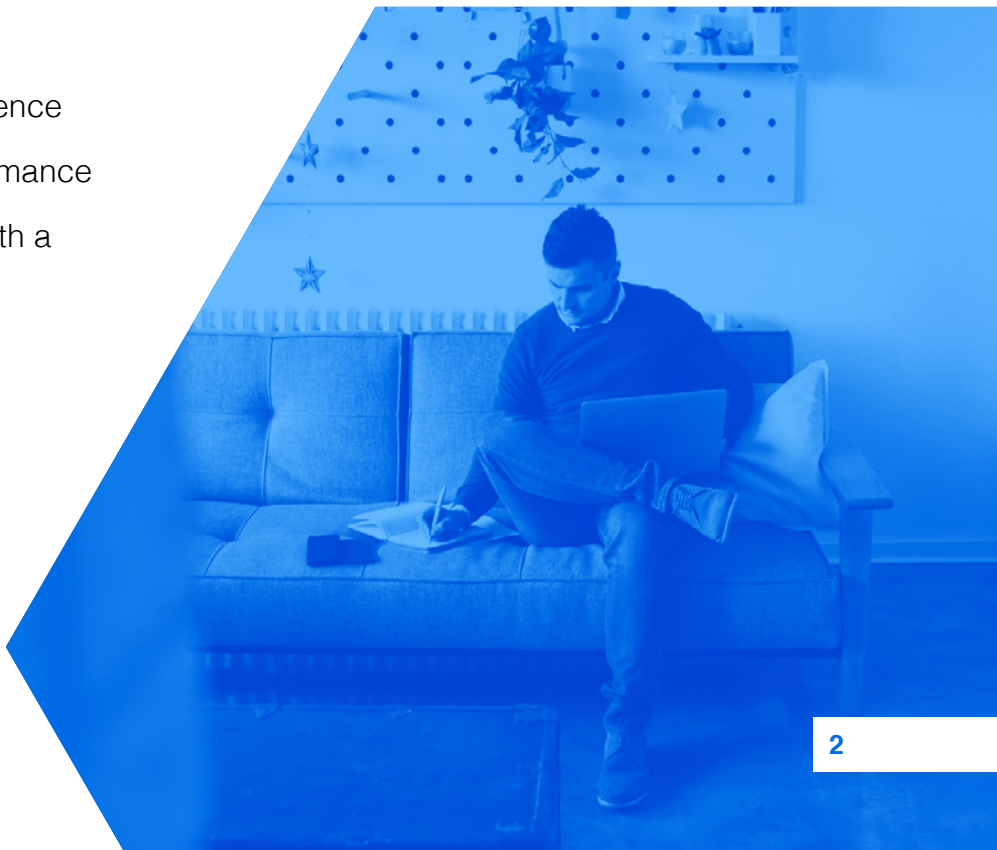
Introduction

The cost of downtime is higher than ever, amplifying pressure on teams for IT operations (ITOps), network operations centers (NOCs), and DevOps to minimize outages. Meanwhile, it keeps getting harder to maintain system reliability. Augmenting IT operations with artificial intelligence (AIOps) can help relieve this pressure and enhance reliability, by helping IT teams keep ahead of shifting, multilayered challenges.

ITOps challenges can shift dramatically and suddenly. For instance, nearly instantly, the COVID-19 pandemic changed technology priorities for 95% of companies, shifting their focus to immediate problems related to:

- Traffic spikes
- Multichannel customer experience
- Visibility into tech stack performance
- Resolving incidents quickly with a remote IT workforce.

The number and duration of outages significantly colors the customer experience. When COVID-19 sent people throughout North America home to work, this sharply spiked both demand for digital services and user expectations for reliability (as homes became schools and workplaces, and as personal digital devices became vital hubs for social and family connections). Under these conditions, even brief outages or slowdowns can cause big problems for customers, possibly eroding their loyalty.



This disruption occurred against a backdrop of generally rising IT complexity. For years, more enterprises have been adopting hybrid infrastructure. While this can be proactive, many organizations were effectively forced to distribute IT operations to accommodate remote work. This move has tradeoffs. When parts of an organization's IT systems and applications reside in the cloud — worlds apart and managed differently from legacy on-premise systems — incident management becomes vastly more complicated.

IT professionals, on any team and working from any location, are more critical than ever for maintaining service reliability. To ensure that they can keep performing well in their essential roles (while also significantly reducing the expense and risk of outages), these people need support from artificial intelligence.

According to Gartner, "AIOps platforms enhance technology leaders' decisions by contextualizing large volumes of varied and volatile data." AIOps platforms and tools leverage machine learning algorithms and data analytics to process large datasets drawn from existing ITOps systems. This allows AIOps to automatically spot and address problems, and also to promptly and fully inform decisions made by IT teams. This can prevent outages, or at least minimize their duration and cost.

Justifying investment in a key technical resource that can sound somewhat abstract can be challenging, especially during a crisis. This paper offers guidance to build the business case for AIOps.

> **"AIOps platforms enhance technology leaders' decisions by contextualizing large volumes of varied and volatile data."**
>
> Gartner

Downtime Costs Are Up

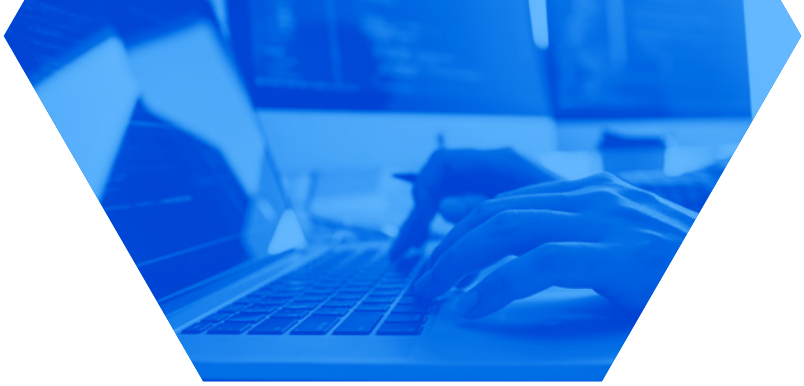
For the past several years, financial losses attributable to technology downtime have been rising steadily, according to the latest Global Server Hardware, Server OS Reliability Survey from Information Technology Intelligence Consulting (ITIC). Nearly all (98%) of the 1,000 organizations surveyed in 2019 said that one hour of downtime cost them at least $100,000. For the vast majority (86%), each hour of downtime cost them at least $300,000 (up from 81% in 2018).

ITIC observed: “In today’s Digital Age of ‘always on’ interconnected networks, businesses demand near-flawless and uninterrupted connectivity to conduct business operations. When the connection is lost, business ceases.” Note that this statement was made in May 2019, well before the COVID-19 pandemic.

Such high costs and criticality have made AIOps an essential part of any organization’s suite of monitoring tools and event correlation platforms. AIOps enables businesses to alleviate the financially crippling effect of downtime by streamlining incident detection, investigation, and resolution.

Nearly all (98%) of the 1,000 organizations surveyed in 2019 said that one hour of downtime cost them at least $100,000. For the vast majority (86%), each hour of downtime cost them at least $300,000 (up from 81% in 2018).

Global Server Hardware, Server OS Reliability Survey, Information Technology Intelligence Consulting (ITIC)



Streamline Distributed IT Work

Today's IT workforce is more distributed than ever, with more responsibilities than ever. IT professionals cannot afford to waste time by having to figure out, incident by incident, who needs to do what. When it's easy and fast to understand which change probably caused an incident, only the most relevant teams get involved in fixing the problem.

Also, a centralized, intelligent system for incident management and resolution supports accountability, especially when the IT workforce is highly distributed.

AI can be used to detect problems, identify their root cause, and automate incident management steps.

"The organization must pinpoint why a certain incident happened, what the cause was, and who owns it," said Eyal Efroni, VP of Customer Success at BigPanda. "Every organization has some finger-pointing, and the problem only gets bigger when multiple parties are involved."

AI can be used to detect problems, identify their root cause, and automate incident management steps (suggesting and executing corrective actions) These capabilities make it more likely that problems will be resolved at the first line of defense (L1 layer). By contrast, once an incident has already escalated, its hourly cost increases and L3 or DevOps engineers must step in. BigPanda provides robust support for cross-team, real-time collaboration, giving everybody a common platform, a common view, and common access to intelligence and context about the situation.

What Kind of AIOps Does Your Organization Need?

In his April 2020 Infoworld article, Not All AIOps Tools are Created Equal, David Linthicum, chief cloud strategy officer for Deloitte Consulting noted:

"Some AIOps tools are very data driven, capable of analyzing historical data. Others focus on real-time monitoring. Data-oriented tools look for patterns in the data (typically assisted by an AI engine) in order to find cause and effect. They get to the root cause of an issue without staff having to cull through gobs of data. ...The trouble is that many products in this space are actually old technology made new. We've been using operational tools for years. Those tools were redone to support public clouds; now they have been rebranded as AIOps tools with some built-in AI capabilities."

The least costly outage is the outage that never happens. Real-time data monitoring can quickly detect incidents when they occur. Organizations that require predictive capabilities to prevent outages should explore AIOps solutions that ingest and analyze historical data. While both capabilities are helpful, data oriented AIOps are needed to prevent outages by illuminating systemic root causes.

Preventing outages supports IT teams by combating alert fatigue. In the last few years, the quantity of ITOps alerts has been multiplied considerably. Gartner's 2019 Market Guide for AIOps Platforms lists three key reasons for this:

- **Volume.** The quantity of data generated by the IT systems, networks, and applications has grown exponentially.
- **Variety.** Events, metrics, traces (transactions), wire data, network flow data, streaming telemetry data, customer sentiment, and more all must be analyzed.
- **Velocity.** Data is now generated faster than ever. Also, the rate of change within IT architectures is accelerating, as are observability challenges.

By aggregating and processing monitoring data from public and private cloud environments, as well as from on-premise applications and infrastructure, AIOps helps dramatically reduce this distracting, nerve-wracking noise.

Five Essential AIOps Capabilities for Remote ITOps

Since the pandemic began, most organizations now manage an IT workforce distributed among dozens, hundreds, or thousands of individual homes. These are uncharted waters for even the largest and most sophisticated enterprises. With a distributed IT workforce, effective incident management requires four core capabilities.

1. Unified Event Management.

Over the years, most enterprises have accumulated a wide and varied legacy of ITOps tools. Alerts generated by all these systems have risen to an overwhelming cacophony. BigPanda's AIOps solution subdues this noise by first ingesting all alert data, regardless of its source, and then using machine learning to intelligently correlate alerts around a probable root cause (which might be a network failure, infrastructure change, or code push). Finally, a single, defined incident is routed to the to the most appropriate person or team via the organization's systems for ticketing, notification and collaboration.

2. Rapid Detection and Resolution.

Generally, customers and internal stakeholders are unwilling to wait for IT problems to be resolved. "When you cannot isolate root causes quickly, the clock runs out for mean time to repair or resolution," said BigPanda CEO Assaf Resnick. By normalizing information from fragmented monitoring tools in a common data model, BigPanda's AIOps solution can correlate alerts as soon as data flows into the system and isolate their root cause. Consequently, IT teams spend less time performing cumbersome manual processes, including tens of hours on bridge calls trying to manually find the root cause. This accelerates the incident -> insight -> action cycle.

3. Collaboration Tools.

Resolving serious or puzzling incidents requires the expertise of multiple teams. However, resolution is often delayed when each team or professional uses different tools and views different datasets. BigPanda's Open Integration Hub provides a common view, and common tools, for all participants. This can be displayed effectively on one monitor, which is common for work-at-home professionals. Several BigPanda customers have mentioned that previously, their IT teams sat side-by-side in a network operations or support center, facing 40 monitors. Now, each professional faces just one monitor at home, or two if they are lucky, and collaboration is simpler than before due to enhanced integration with ticketing, chat and notification tools.

4. Unified Analytics.

When ITOps managers, IT executives, and line-of-business owners all can access the same history and view of incidents and resolutions, they can discuss underlying issues more productively. A consistent picture of what went wrong, and why, can more easily reveal opportunities to further streamline and bullet-proof IT operations. In BigPanda's AIOps solution, users can view and generate reports on various ITOps key performance indicators, metrics and trends. In addition to preventing future outages, this analysis helps identify gaps and overlaps in the tool stack. It also informs benchmarks and best practices.

5. Vendor-agnostic platform.

Given the wide diversity of current and future ITOps tools, it's essential to choose an AIOps platform that integrates easily with other systems, but that does not interfere with vendors, tools, practices or systems. "BigPanda becomes an abstraction layer that integrates with any monitoring, change or topology tool, most ticketing and collaboration platforms, and all commonly-used incident response platforms," said Bryan Dell, Chief Revenue Officer for BigPanda. "That makes it easy for companies to add or remove tools and vendors without a massive impact to their operational workflows and processes."

Conclusion: Long-Term Benefits of AIOps

The current global condition is teaching us how connected we all are. Especially as most organizations pursue the goal of digital transformation, it's important to view technology vendors as strategic partners.

It's also important to recognize the IT workforce as an essential partner in business success. Without ITOps, NOCs, and DevOps, the ITOps-from-home movement that enabled so many people to keep their jobs during major global crises would not have been possible. The heroic efforts of IT professionals to enable remote working is particularly noteworthy at a time when they also bear a primary responsibility to support digital transformation. The least that any organization can do to support this valuable work is to reduce its stress — especially, stress from alert fatigue, prolonged and difficult incident management processes, and from constantly fighting fires rather than addressing root causes.

Without IT Ops, NOCs, and DevOps, the ITOps-from-home movement that enabled so many people to keep their jobs during major global crises would not have been possible.

bigpanda

BigPanda accelerates the incident management process with event correlation, powered by AIOps. BigPanda captures and combines alerts with change and topology data from all your tools, then uses machine learning to spot problems and patterns that identify the root cause of performance issues or outages in real-time. The result: faster resolution, reliable applications and services, and better user experiences.

LEARN MORE

BRAND**STUDIO**

Custom Content. Targeted Results.

Industry Dive's Brand Studio collaborates with clients to create impactful and insightful custom content. Our clients benefit from aligning with the highly-regarded editorial voice of our industry expert writers coupled with the credibility our editorial brands deliver. When we connect your brand to our sophisticated and engaged audience while associating them with the leading trends and respected editorial experts, **we get results.**

LEARN MORE