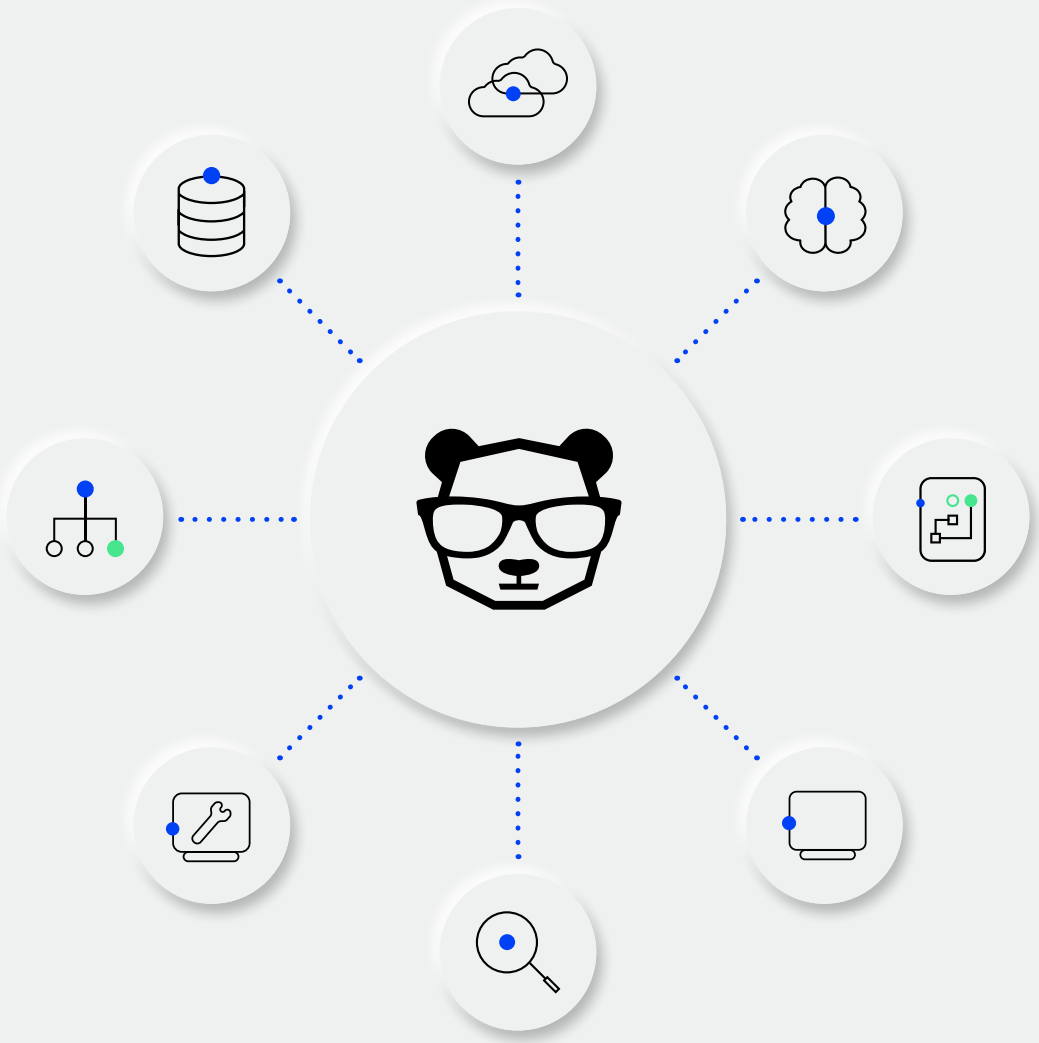
BigPanda

E-book

Full-context ops

Turn data into patterns, insights, and actions.



"An alert without context is just noise."

Jon Brown, Senior Analyst, Enterprise Strategy Group by TechTarget

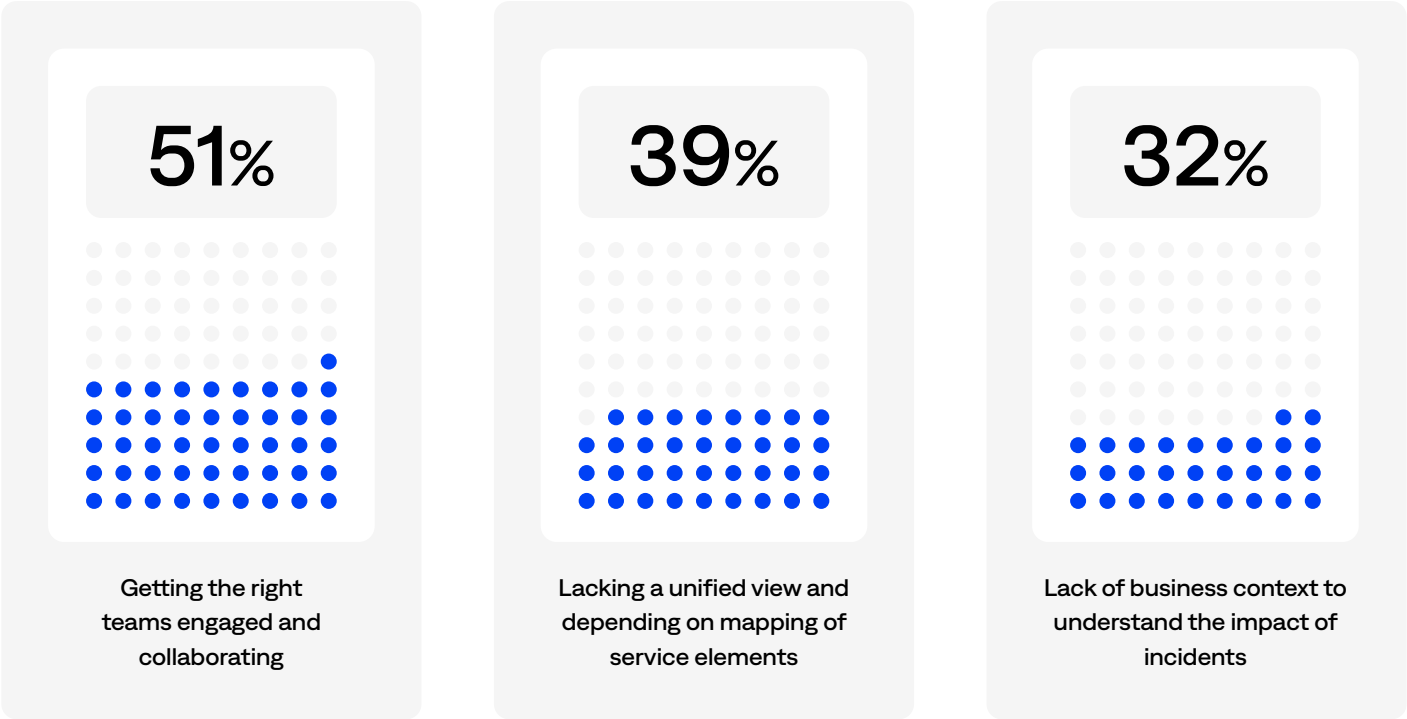
Table of contents

Achieve scalable, self-sufficient ITOps with full context

ITOps, DevOps, and SRE teams are often siloed. They employ different tools, possess varying experience levels, and operate disconnected incident-response workflows. Additionally, the constant evolution of IT environments has created an order-of-magnitude increase in complexity, which, combined with siloed teams, creates information gaps, unrealistic expectations, and immense stress for operators. Combined, these factors negatively impact business outcomes for many organizations.

As a result, organizations in every industry increasingly rely on technology to remain competitive. However, that reliance brings additional challenges, complexity, and risk of incidents and service disruptions.

In fact, 82% of respondents in a 2024 Enterprise Management Associates survey of more than 400 global IT leaders reported that incidents and outages are increasing every year. Respondents report the most significant challenges to effective incident response and management as:



The antidote lies in delivering all the information teams need, quickly and upfront, so they can better understand what happened, why, and what to do about it. This comprehensive view of every incident is the foundation of full-context operations.

Bloor

"Adding context to enrich alert data leads to more effective prioritization, resulting in faster problem resolution and fewer service disruptions."

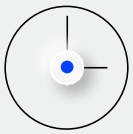
Paul Bevan, Research Director of IT Infrastructure,
Bloor Research

Without full context, ITOps and ITSM teams are challenged by inconsistent alert data, slow incident detection and response, and unsustainable incident triage processes. Operators require full context about incidents — information that builds on and goes beyond basic metrics, events, logs, and traces (MELT). The raw, very specific details of MELT data are helpful for forensics and triage. However, getting a complete picture of an incident and its impact requires additional information, including monitoring and observability, service maps, topology, CMDB, and change data. Context changes the game. A responder can immediately understand the business impact of a given alert and respond or assign appropriately, ultimately improving operational efficiency and service availability.

AIOps give your operators the context and insights they need to instantly uncover vital incident and root-cause details that allow them to identify and resolve incidents.

Benefits of providing full context

Your organization can reap benefits including:

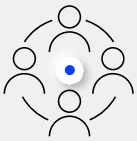


Faster mean time to resolution

By instantly ingesting events from across your IT stack to centralize and correlate meaningful insights across services, applications, tags, and more, you can significantly reduce MTTR and minimize downtime and service disruption.

Reduced manual effort

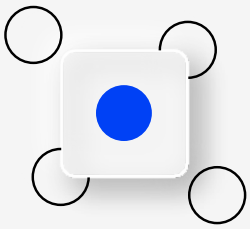
Centralized knowledge and processes ensure data is actionable, making operators more effective at incident response workflows and more satisfied.



Streamlined collaboration

Unified incident management across teams eliminates friction and duplication, reduces unnecessary escalations, and boosts coordination and resource utilization.

Add context to build ITOps consistency



ITOps teams frequently face a mountain of alerts without context. High volumes of alert data lead to manual, time-consuming, and error-prone workflows. Siloed teams, tools, and knowledge impede your team's ability to identify and prioritize incidents quickly, resulting in prolonged, massive bridge calls and slow, labor-intensive investigations for each incident resolution.

Legacy event management, monitoring, and even modern observability tools alone are not up to the task. In fact, 32% of ITOps respondents report that the biggest challenges in incident response and management are the lack of business context and understanding the full impact. In short, you're in trouble if all you have is disconnected raw data. If there is no way for responders to identify what's important or where to focus their remediation efforts, you're creating extremely stressful conditions for your team.

A lack of context and accountability is a massive problem in incident response. In the EMA report, 27% of respondents stated that more than half of MTTR is wasted time, and 69% said about a quarter. Rather than actively spending time reviewing alert data to understand the issue, operators are left waiting for other team members to add context before they can take meaningful action to resolve the incident.

> *"Our AIOps strategy with BigPanda bridged our on-premises and cloud environments, delivering a unified platform for ecosystem management."*
>
> **Steve Liegl, Director of Infrastructure and Operations, WEC**

ITOps and ITSM teams face several challenges without the critical context they need to understand the full scope and impact of outages, let alone resolve them.

The most significant of these obstacles and the factors contributing to them include the following:

Siloed IT operations teams, tools, and knowledge: When ITOps and ITSM teams each have their own tools and experience levels, they lack a shared language or platform to identify actionable, important alerts. This prevents them from exchanging information, collaborating around remediation efforts, or finding critical context around an alert or incident. Instead, they have to wait for other teams or manually sift through alerts, wasting time and effort on time-intensive and error-prone processes.

Noisy, unactionable data: ITOps and ITSM teams are expected to manage volume from a huge variety of tools. In fact, the average BigPanda customer uses about 20 observability and monitoring tools. Significant variations in ITOps tools, data, alerting, and resolution processes leave operators with a mountain of noise. And without context and normalization across incident-response milestones. Critical issues are lost in the deluge of alerts, leaving operators without a framework to prioritize nor a clear understanding of the problem, whether it's the impact or how to resolve it. In fact, 47% of the EMA survey respondents reported that less than half of their alerts are actionable.

Unsustainable pace of work: Siloed teams typically lack a unified view of alert data or even standardized and agreed-upon approaches to data quality and naming. This hinders the identification of affected applications and root causes, which escalates the Mean Time to Innocence (MTTI). It also increases stress and fatigue among IT teams subjected to duplicative processes, repeat escalations and re-escalations, inconsistent approaches, and manual, repetitive, and frustrating processes. The end result is low team morale and over-reliance on experienced employees.

It's 10 p.m. on a Thursday: Why context matters

How does lack of context play out in a real-world incident? It's Thursday night. Your observability tools just informed you that the data center network is down. A flood of angry customer tickets confirms the situation, but you don't have all the details about what happened, much less why it happened. You have no hints about how to remediate the problem. In short, you're lacking context.

It would be helpful to have information from all your network services, including cloud-based services. You might also want data on impacted hosts and services that are down, information about recent network or server changes, and details on how teams resolved previous, similar incidents.

Without this information readily accessible — or even available — you can't fully assess the challenge or identify the next steps. Still, with your CEO anxious for an update, it's all hands on deck for your team. You feverishly message your team, sending them to manually dig through reams of log data, change data, knowledgebase articles, and runbooks to identify the outage's root cause.

Fragmented systems impede your team's efforts. Some systems are outdated, lack documentation, or simply don't have the right access. Others require past knowledge from long-term team members. Vital contextual information may be lost or spread across change management systems and your CMDB. Combined, this means your team misses potentially relevant and critical connections, which increases investigation time and results in unnecessary escalations to the wrong teams. And time is money. For smaller organizations, critical outages like this may cost more than $12,000 per minute, but for larger companies like yours, it's probably closer to $25,000 per minute, according to Enterprise Management Associates.

PlayStation

"With BigPanda, our IT noise is not only reduced, but we are able to identify the root cause in real time. We see who the responsible team is, who owns the service that's alerting, and more, which is significantly reducing our MTTR."

Priscilliano Flores, Staff Software Systems Engineer,
Sony Interactive Entertainment

Go beyond MELT and observability data

Alerts without context are just noise. And an incident without context isn't a priority. Most ITOps teams look to observability data to gain the full context of an incident. MELT data provides part of the picture; adding more observability data doesn't always give you more insight. Slogging through high-volume observability data requires assigning expensive, skilled staff members to hunt through log files, change management systems, and code repositories to locate the issue that started it all.

Ultimately, alerts without context and the additional flood of data can make taking the next right action more challenging for several reasons, including:

Lack of actionability

On its own, the sheer volume of MELT data is unactionable and can lead to missed signals and wasted time, exacerbating alert fatigue and prolonging MTTR.

Communication issues

There are no insights into or mechanisms for cross-team collaboration using MELT data.

No clear cross-source connections

MELT can pinpoint specific issues but not reveal broader patterns, making determining root cause or understanding relationships between systems far more difficult and worsening the stress of incident response.

Other ITOps teams also look to observability tools, frequently adding more specialized tools and alerts for deeper context into their infrastructure. But no single tool provides comprehensive observability across the entire technology stack. And different tools excel at different tasks, forcing you to combine tools to achieve end-to-end visibility. Even with so-called "full-stack" observability tools, the average organization still uses 10 to 20 additional tools to fill observability gaps.

This "observability sprawl" creates massive complexity, increasing the noise to monitor without providing an understanding as to **why** the alerts are being sent. Without context on the alerts from each observability tool, you're actually making full-stack observability harder and more time and resource-intensive for operators. In fact, the Enterprise Strategy Group reports that 91% of organizations struggle when deploying observability solutions.

CAMBIA HEALTH SOLUTIONS

"BigPanda has helped significantly with deduplicating, correlating, and automating our processes, and we now have the full context around what is impacted throughout the organization and how to fix it quickly."

Mark Peterson, IT Operations Supervisor,
Cambia Health Solutions

Clean up messy data with correlation

Messy data is a reality. Data will never be perfect in ITOps. But that doesn't mean you have to be satisfied with less than a comprehensive picture of your infrastructure. You can get a holistic picture by bringing together existing data from across your entire operational environment, including monitoring, topology, CMDB, and change data. When you correlate that multidimensional data and augment it with AI, you uncover meaningful connections in a single place where operators can collaborate to resolve incidents quickly.

Four steps to strong correlation

Establish the following to get to this state:

1

Centralize knowledge across the infrastructure and IT tech stack

By ingesting available service mapping and discovery tools, CMDB, change, and monitoring data, operators can see the total impact across environments, identify relational patterns, escalate directly to the right teams. This lets them get ahead of issues that may otherwise remain obscured.

2

Standardize siloed data with multisource, multidimensional correlation

By correlating data across both source (i.e., topology, CMDB, change data) and dimension (i.e., physical topology, cluster, check, tags), you can derive a deeper understanding of incidents across the tech stack. This helps identify relational patterns hidden within disparate data, even if the data isn't completely clean.

3

Use AI to augment correlation with structured and unstructured data

Generative AI provides the opportunity to supplement multidimensional enrichment and correlation with large language models to deliver incident summaries rapidly in plain language. This helps operators to understand the impact and identify possible paths for resolution more quickly, allowing them to handle more incidents in less time and scale incident response processes.

4

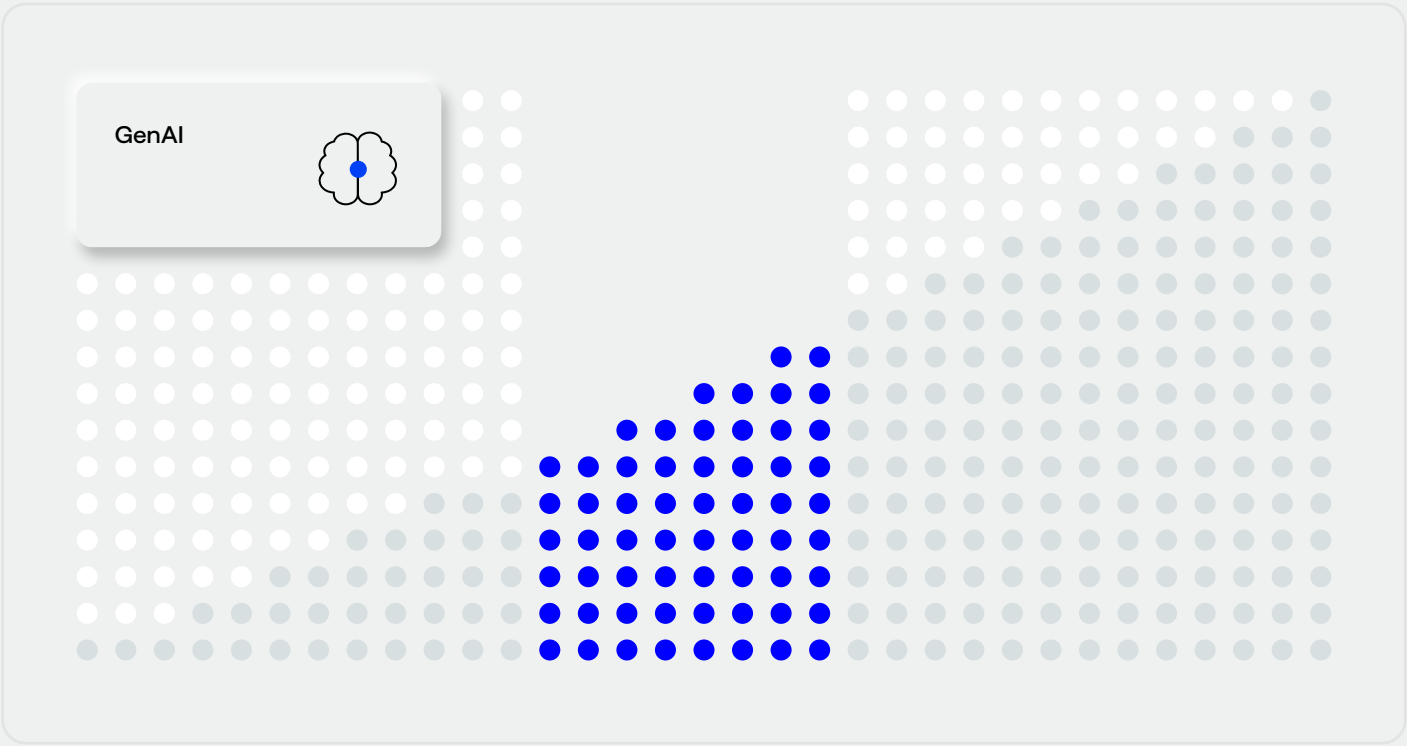
Deliver a unified, full-context view of incidents

AIOps platforms like BigPanda allow you to normalize, enrich, and correlate alert and incident data; add meaning and value to it; and centralize it in one place. With a more holistic view, you can automate root-cause analysis and issue prioritization, uncover patterns that would be otherwise hidden and disconnected, free experienced resources, and scale incident response.

A robust observability practice is essential, but it's only one component of a fully modern event-management and incident-response strategy. To ensure reliable performance, maximum uptime, and improve MTTR, teams need AIOps-powered actionability within their monitoring and performance management workflows. Applying advances in generative AI to enrich and correlate alert data allows operators to extract meaningful insights from complex IT data in real time.

Using GenAI, you can identify incident titles, descriptions, and even probable root causes within seconds, enabling ops teams to review and verify auto-generated responses immediately, understand causality and impact quickly, and shorten time-to-resolution dramatically.

Arming teams with high-quality context on alerts allows operators to know where experienced team members may sit, or which teams to assign to an incident, ensuring they can triage, investigate, and resolve incidents as efficiently and effectively as possible.



Get a clear picture of your IT infrastructure

Alerts become actionable when with context. It's also easier to prioritize and remediate incidents with context. If you can give your teams full context in the form of monitoring normalization, topology, CMDB, and change data, you enable them to anticipate issues as they develop. From there, they can proactively detect, identify, and resolve incidents before they evolve into outages. Full-context operations provide the tools, information, and processes to make ITOps data accessible and valuable.

With full-context operations, your teams benefit from:

A clear view and deeper understanding of incident data

If your teams have the ability to see patterns, connections, and correlations within data across services, applications, and your IT stack, they can gain immediate insights into the affected services, dependencies, and recent changes. This enables faster problem identification and resolution, as well as the ability to prioritize critical incidents and ensure focus on the issues with the highest business impact.

Actionable alerts

When you enhance correlation with AI and historical analysis, you enable a shared understanding of the IT environment across teams. By breaking down silos with shared data to enable more effective incident response, you can expedite an incident's root-cause changes. In fact, 38% of respondents in the EMA report stated that if a real-time solution could accurately determine the impact of incidents across distributed systems and communicate it in clear language, the value would be transformative. Another 45% said it would be high value.

Scalable, resilient incident response and management

Ultimately, full-context ITOps make it faster to detect, respond to, and resolve incidents. By delivering clear insights in context and suppressing irrelevant and redundant alerts, you free up time and resources for more effective incident management.

"BigPanda's Operational Intelligence and Automation Platform shows fast time to value in providing IT with proactive insights on events and alerts in context with change, root cause, and business impacts," said Dennis Drogseth, vice president of EMA. "BigPanda stands out in making the multidimensional challenges of optimizing business service delivery affordable, accessible, and actionable through its Explainable AI and native automation."

Bring on full-context operations

Every minute counts for ITOps, ITSM, and DevOps teams working on resolving an incident. They need as much information as possible to respond to and resolve an incident quickly. However, human capacity for ingesting information and acting on it is finite. As the systems we operate grow more complex, we need to ensure that the technology we use presents us with only the relevant information we need, exactly when we need it.

BigPanda offers the only resilient and scalable AIOps platform that centralizes knowledge across data sources and dimensions to reveal potential relationships within incidents and accelerate detection, response, and resolution times. With BigPanda's unique ability to supply full context for every IT incident, organizations using BigPanda report up to a 50% reduction in MTTR. An open and agnostic platform, BigPanda uniquely delivers the full context around incidents through several capabilities, including:

- **Event Enrichment Engine**

  BigPanda can ingest any available data to include topology, CMDB, change, and service maps. It normalizes the data and makes it easy to interpret, enrich, and share across teams for smooth communication and collaboration.

- **Alert Intelligence**

  Multidimensional and contextual alert correlation provides deeper insights into your IT infrastructure. BigPanda correlates alerts across sources to include topology, CMDB, change, historical data, and dimensions — as well as services and applications. This gives operators a holistic picture of the connections between different areas of your systems and what the incident has affected. This helps clarify when one issue or service manifests as alerts in other applications.

- **Automated Root Cause Analysis**

  Correlating multisource alerts with all change data allows both ITOps and ITSM teams to quickly identify and roll back the specific changes that caused incidents — and prevent them from reoccurring.

- **AI-enhanced analysis**

  BigPanda uses AI-generated summaries to augment multi-dimensional correlation, giving operators a consistent, clear summary in plain language and enabling them to understand the incident quickly and identify possible paths for resolution. Operators can handle more incidents in less time, scaling incident response processes.

CAMBIA HEALTH SOLUTIONS

"We enrich our data through BigPanda, enabling better correlation and more insightful alert tags. We have full-context visibility into our inbound alerts and can now get the right teams involved immediately for a far faster resolution time."

Mark Peterson, IT Operations Supervisor,
Cambia Health Solutions

Learn how BigPanda can transform your ITOps practice with full-context operations.