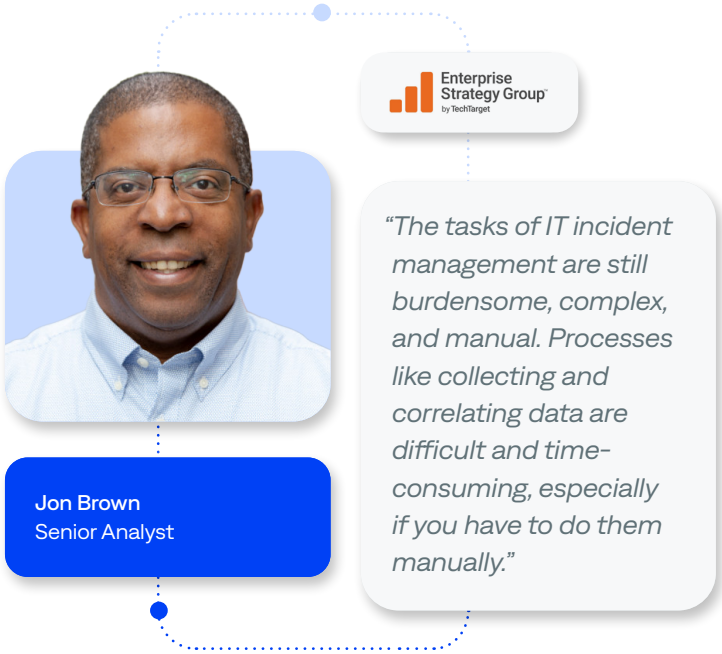
BigPanda

E-book

Laying the data foundation for agentic ITOps:

A strategic guide for enterprise IT leaders

Contents



The rise of agentic ITOps

Adopting hybrid cloud infrastructures and modern software development practices such as continuous integration/continuous delivery (CI/CD), microservices, and agile methodologies revolutionized enterprise IT. These innovations power the modern world, but introduced unprecedented challenges in scale, fragmentation, and operational complexity.

To manage this complexity, enterprises invested billions into observability tools, IT Service Management (ITSM) platforms, and L1 operations teams. However, incident detection remains poor despite a 20% year-over-year increase in spending on observability and IT Service Management (ITSM) platforms.

End-users, rather than system telemetry, still report 65% of all incidents. Enterprises continue to rely on human-driven workflows to manage these systems, where responders must interpret data manually to diagnose issues and take action. The result is spiraling headcount, observability, and ITSM costs to sustain cumbersome ITOps workflows and slow, reactive incident response.

Legacy tools and processes designed for monolithic systems and static infrastructures cannot meet these challenges. Enterprise ITOps requires a more agile and intelligent approach that leverages advances in AI and automation to remain scalable, effective, and sustainable.

Agentic ITOps offers a path forward by transforming manual and reactive ITOps processes into intelligent, autonomous systems. These systems can adapt to changing environments, learn from experience, and collaborate with humans to detect, respond to, and prevent incidents at machine speed. With intelligent, automated workflows, enterprises stand to gain faster mean time to resolution (MTTR), reduced L1 spend, fewer escalations, and improved SLAs and uptime.

Taking advantage of these advancements requires a fundamental shift in how enterprises approach their IT data strategy. This approach requires moving beyond static configuration management databases (CMDBs) and embracing AI-powered insights from diverse data and knowledge sources. Critically, agentic AI doesn't require highly structured inputs to function, and can transform messy, scattered inputs into adaptive intelligence.

"We've reached peak frustration with getting your ITOps or ITSM teams all the fragmented, siloed CIs into a CMDB," said Jason Walker, Chief Innovation Officer at BigPanda. "GenAI can ingest and index all the valuable, unstructured data from your organization and convert it into data that can be leveraged to improve your operations."

This e-book is a strategic guide to help enterprises understand the capabilities and lay the foundational data strategy to deploy and see rapid value from agentic ITOps.

How agentic ITOps deliver the promised value of AIOps

Agentic ITOps represents a significant advancement in traditional artificial intelligence for IT Operations (AIOps) capabilities, incorporating autonomous decision-making and action. Advances in agentic AI can transform ITOps and IT service management (ITSM) and bring orders of magnitude improvements in efficiency and capability. By harnessing these advancements, enterprises can reduce costs and risks and accelerate growth.

AIOps platforms, which Gartner calls event intelligence solutions (EISs), apply artificial intelligence (AI) and machine learning (ML) to IT operations to streamline and optimize IT processes. The primary outcomes of traditional AIOps are noise reduction, correlation, accelerated root cause analysis, and improved incident workflows.

AIOps relies on structured data housed in a CMDB and processed through rule-based systems. This makes it challenging to keep ahead of tech stack visibility with an accurate CMDB. CMDBs also omit most of your organization's institutional knowledge. Vital information and operational knowledge, such as team expertise, unstructured tickets, and chat logs, remain buried and unusable. This lack of information leaves your responders without the actionable context to detect, triage, and respond to IT incidents quickly and effectively.

"A CMDB was sold as an inventory and up-to-date map of the entire universe of your services and components, and it almost always falls short of that," said Walker. "Now you can take in information from all sources and convert it into usable data that an agentic AI assistant can incorporate into its assistance with day-to-day operations."

Agentic ITOps significantly expands the capabilities of AIOps by eliminating the need for structured data and rules. This opens the floodgates to various unstructured data sources that can provide unprecedented understanding and visibility. Agentic ITOps creates autonomous systems that can make decisions and perform tasks without constant human intervention. These systems, also known as AI agents, can adapt to changing environments, learn from experience, and collaborate with humans to detect, respond to, and prevent incidents at machine speed.

These AI agents can do more than analyze data. They can automatically detect potential issues, rapidly diagnose them, assess impact, prioritize accordingly, trigger automated fixes or suggest next steps, and even predict and prevent IT incidents.

By taking advantage of advances in AI and previously untapped data sources, agentic ITOps can help enterprises:

Massively improve incident detection capabilities with real-time visibility into external dependencies, end-user issues, and real-world events such as power or internet outages and social media signals.

Automate L1 operations by autonomously detecting, triaging, and responding to incidents across complex and distributed environments and providing AI-driven insights and guided actions for responders.

Augment incident management teams with an AI assistant to automate workflows, accelerate resolution, and boost service reliability.

Automate IT change management with change analysis and risk mitigation. Provide clear guardrails to help teams predict and prevent change-related failures, reduce incidents, avoid escalations, and shift from reactive firefighting to proactive reliability.

Agentic ITOps marks a shift towards delivering on the promise of AI-powered, proactive IT operations. Your teams can automatically detect potential issues, rapidly diagnose them, assess impact, prioritize accordingly, and trigger automated fixes or suggest next steps.

In short, agentic ITOps transforms AI from a tool to improve efficiency into an autonomous digital operator that allows your organization to reduce costs, limit risk, and accelerate growth. The following table shows that agentic ITOps represents several critical capability improvements compared to traditional AIOps.

	AIOps	Agentic ITOps
Core capabilities	Reduce noise and accelerate incident triage with AI-driven event correlation.	Automate L1 operations, accelerate major incident management, and predict and prevent incidents.
Primary use case	Help teams make faster, smarter decisions during incident detection and triage.	Automate the full incident lifecycle—from L1 detection and response to L2/L3 resolution.
Improve ITOps efficiency	Reduce alert noise and improve prioritization, allowing IT teams to focus on critical issues.	Proactively identify and prevent issues before they impact services, significantly lowering operational overhead.
Augment IT team experience	AI-enhanced context for human-driven workflows.	AI agents proactively assist, coordinate, and guide actions across team workflows
Correlation	Aggregate and analyze vast amounts of data to identify relationships between events, reducing alert fatigue and pinpointing critical issues.	Agents perform contextual cross-domain correlation across all structured and unstructured, internal and external data, enabling autonomous decision-making and remediation.
Incident Management	Faster incident resolution by correlating events, identifying root cause, and providing solutions.	Automatic incident remediation, automated incident investigation, root cause analysis, and evidence-based response and remediation.
Improved IT Team Productivity	Helps responders be faster and better informed.	Eliminate repetitive, duplicative work and supercharge SMEs so teams can move faster, stay focused, and resolve confidently.
Time to Resolution	Reduce alert noise and accelerate incident investigation with AI-powered root cause analysis.	Automated incident investigation and root cause analysis, evidence-based response, and remediation steps.
Post-incident learning	Makes incident timelines and learnings more accessible.	Transforms every incident into institutional knowledge to improve future responses.
Prevention and Risk Management	Surface insights to help reduce repeat incidents.	Predict and prevent incidents through change analysis and systemic pattern recognition.
Strategic Business Outcome	Improve MTTR, reduce escalations, and boost operational efficiency.	Enhance those gains by reducing incident volume, protecting revenue, and scaling team capacity.
Cost Efficiency	Reduce IT spending by minimizing downtime and associated costs through event detection and streamlined troubleshooting. This process reduces alert fatigue and enhances observability and monitoring tools.	Agentic ITOps automates high-volume L1/L2 tasks, lowers IT software licensing costs, reduces L1 headcount, and reduces outsourced L1 spend.

BigPanda

"There are $200 billion worth of manual ITOps workflows *ripe for intelligent automation. With agentic ITOps, we're helping enterprises move beyond manual, slow incident management toward intelligent systems that free up talent and reduce operating costs."*

Assaf Resnick, CEO, BigPanda

How to lay the foundation for agentic ITOps with an incremental approach to revising your data strategy

You might be worried that implementing an AI-first data strategy will be too difficult, or that your enterprise isn't ready to deploy agentic ITOps. You can get started right away with agentic ITOps using your existing data. In fact, one of the key capabilities that agentic AI offers enterprise IT is the ability to aggregate, analyze, and correlate data from previously diverse and unstructured data sources. There is no need to clean your data first; agentic AI is designed to work with and handle messy, incomplete data, regardless of its state.

Agentic ITOps allows enterprises to harness a broad, differentiated dataset that unlocks the vital information buried in chat histories, call transcripts, ITSM logs, manual workflows, and more. The key to success is identifying and adopting a phased implementation approach that will allow your organization to progressively expand its agentic capabilities while reducing adoption friction.

The data sources that feed agentic ITOps

This rich, tacit data holds the keys to transforming ITOps and ITSM. By providing your teams instant and contextual access to the full spectrum of information your organization possesses, your organization can significantly improve operational efficiency and deliver exceptional service reliability.

Observability and monitoring tools.

Real-time visibility into IT environments.

ITSM platforms.

Incident, KB, runbook, and change management records offer insights into IT trends and recurring issues.

Data about past incidents.

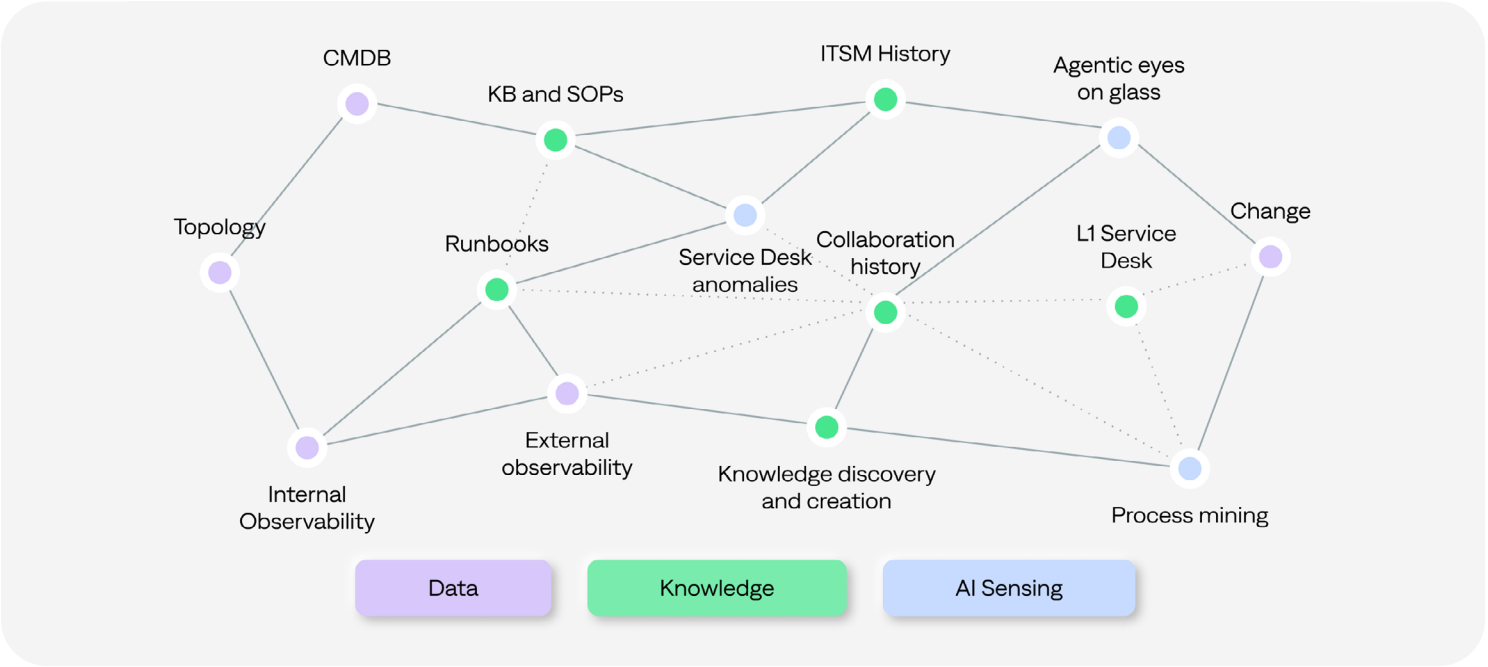
Gather comprehensive insights from previous incidents to accelerate investigation, including classification, priority, duration, assignments, runbook, service impact, and closure codes of comparable incidents.

Collaboration and communication platforms.

Unstructured data from chat platforms, emails, meeting transcripts, and documentation can reveal patterns in incident resolution and operational workflows.

By unifying these diverse data sources, agentic IT operations platforms like BigPanda can build a continuously evolving knowledge base that powers end-to-end operational visibility, predictive insights, and intelligent automation capabilities.

We call this real-time intelligence engine the BigPanda IT Knowledge Graph. Designed to enable an AI-first data strategy, the IT Knowledge Graph continuously ingests and connects data that lies buried in fragmented systems and silos across large enterprises. This data is used to build an intelligent model of your IT environment, allowing your enterprise to evolve from reactive IT operations to proactive, agentic AI-powered decisions.



The BigPanda IT Knowledge Graph unifies siloed and fragmented data, systems, and communications to enable powerful, agentic IT operations and automation.

The IT Knowledge Graph mirrors how real-world teams operate. As new signals, incidents, and human feedback emerge, the IT Knowledge Graph adapts to changing conditions to bridge the gaps between tools, teams, and knowledge. This unified intelligence gives AI agents and IT teams the confidence to predict, prevent, and agentically automate incident workflows, and evolve to meet changing business and technology requirements.

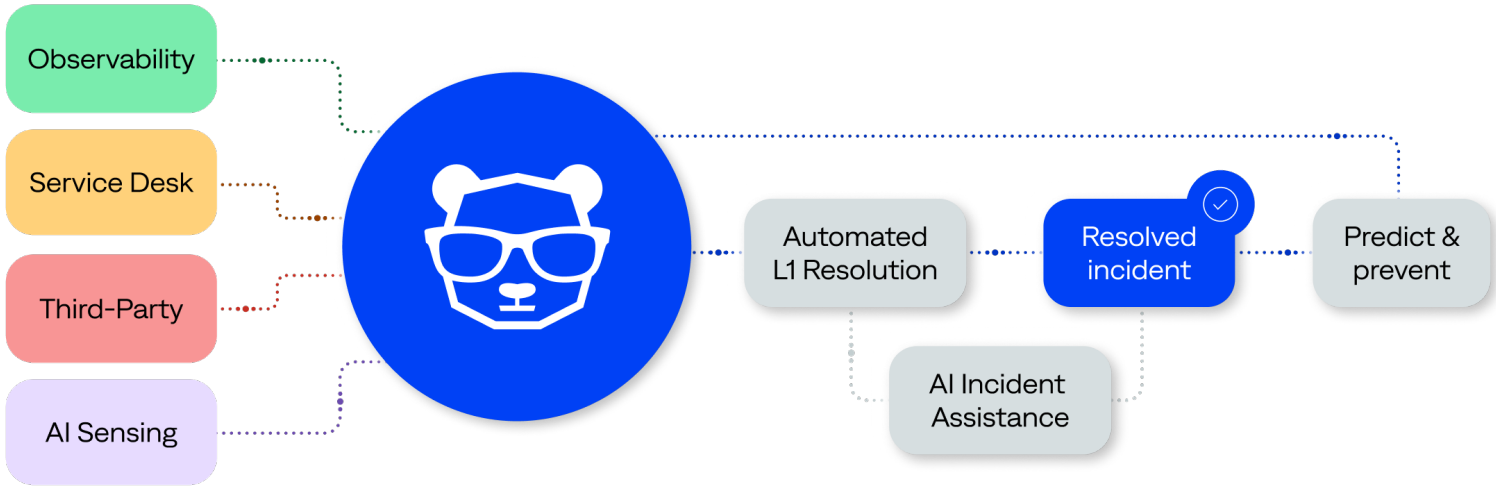
The IT Knowledge Graph is at the core of the BigPanda platform. It is a real-time intelligence engine that is purpose-built to enable an AI-first data strategy, forming the basis for agentic IT operations. Let's explore how different data types are utilized to address strategic IT operations challenges, unlock value in phases, and reduce adoption friction.

There are three main entry points to agentic IT operations, each based on your organization's specific requirements and goals.

Operational goal: Accelerate incident detection and response

Every incident starts as an alert, and it's the L1 network operations center (NOC) teams' job to monitor all alerts across the IT stack. However, in reality, L1s only see a fraction of the alerts firing in their enterprise. This is because they rely on service and application owners to forward their alerts - often manually. This results in a patchy and delayed picture of what's happening. And when alerts do flow in, teams are frequently overwhelmed by volume. NOCs often deal with a flood of alerts, many of which are false positives or low-priority notifications, and many lack the critical 'know-how' they need to take the next steps. Sorting through the noise to find critical alerts and digging for context takes time and delays response.

BigPanda AI Detection and Response changes the game by using real-time signals and automation to detect, diagnose, triage, and resolve issues quickly. It autonomously collects, correlates, and enriches alerts across silos—without waiting for human handoffs. Instead of seeing isolated symptoms, teams gain a complete, contextualized view of incidents as they unfold. This added visibility helps L1 teams detect issues earlier, understand their root cause faster, and route them intelligently. The result? Faster detection and triage, fewer escalations, and accelerated mean time to resolution (MTTR).



BigPanda AI Detection and Response filters out noise and surfaces early signals of potential issues before they impact your business.

AI Detection and Response achieves this by using AI-driven correlation across observability, service desk activity, and external service provider dependencies. You can learn more about the capabilities that are unlocked by adding more data sources in the table below. By ingesting observability, CMDB, and ITSM data, your organization can improve first-contact resolution, eliminate manual and duplicate L1 workflows, and prevent disruptive escalations.

Phased data strategy for BigPanda AI Detection and Response

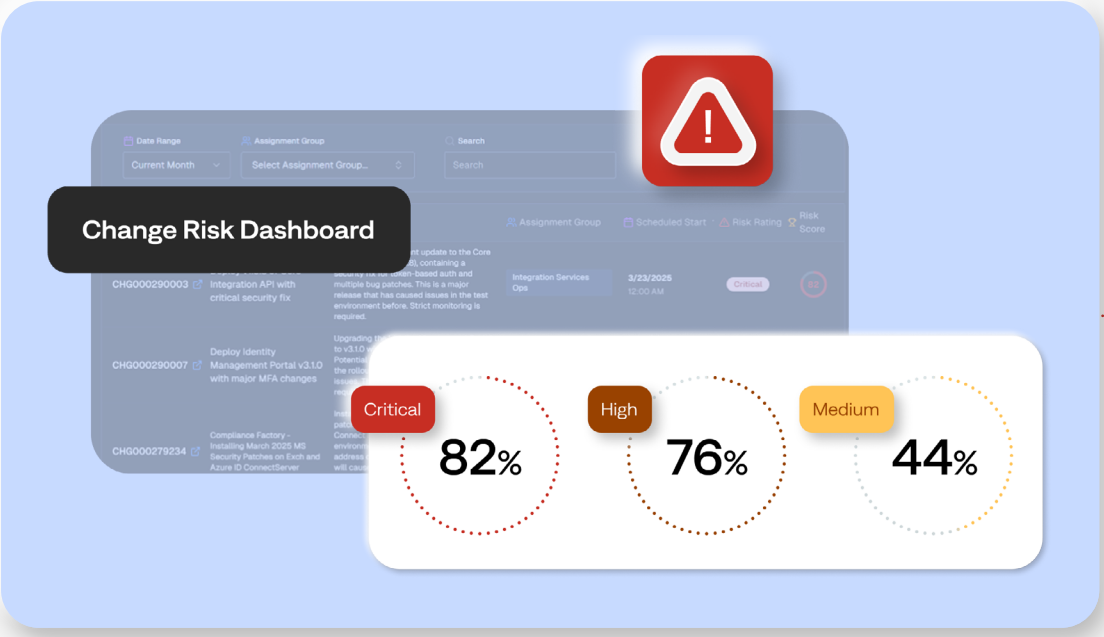
	Data Sources	Results	Key Metrics
Detection Level 1: Real-time operational data.	• Observability • CMDB • Topology • ITSM integration	Reduce noise, ticket and incident volume, and manual analysis. Identify signals early and detect incidents before they escalate.	**Workload Reduction** ↓ Mean time to detect. ↓ Alert and incident volume. ↓ Ticket volume. ↓ Manual workload. ↓ Service desk generated tickets.
Diagnosis and triage Level 2: Institutional and team knowledge.	• Change data • KB Articles/Wikis • Runbooks/SOPs • ITSM ticket data	Guide L1s on next steps accurately with impact, priority, and root cause to improve prioritization and reduce escalations. Automatically enrich ITSM tickets with context to accelerate response.	**All of the above and:** + First contact resolution rate + Resolution SLA Percent ↓ Mean time to assign ↓ Escalation rate ↓ Reassignment rate ↓ Bridge call volume, size, and duration
Response Level 3: Agentic application of L1/2 data and knowledge.	• No new data sources needed	Eliminate guesswork and empower L1 teams to resolve incidents confidently with AI-suggested and automated remediation.	**All of the above and:** + Zero-touch response rate + Automated remediation + Automated L1

Operational goal: Reduce the volume and risk of change-related incidents

Change-related incidents can feel like an endless cycle for change managers, release managers, and ITSM leaders. High volumes of change requests, no clear way to analyze risk systematically, costly rollbacks, and constant firefighting after the fact strain resources and exhaust teams.

Changes are still the most significant contributor to IT outages. One global enterprise processes over 30,000 changes per month, supported by more than 10 Change Advisory Board (CAB) meetings per week, and still sees 15–20% of major incidents caused by changes. Even more telling: 60% of those incidents are linked to changes previously assessed as "low risk."

The problem isn't just the volume of changes. Manual processes and a lack of critical context make it difficult to assess risk and make informed decisions accurately.



BigPanda AI Incident Prevention allows you to view all change management requests in your environment instantly and assess their associated risks..

BigPanda AI Incident Prevention offers a way to break this cycle. By simply ingesting ITSM data—such as ticket history, change records, and CMDB—into BigPanda, teams can automatically analyze the relationship between changes and incidents, and prevent incidents from happening.

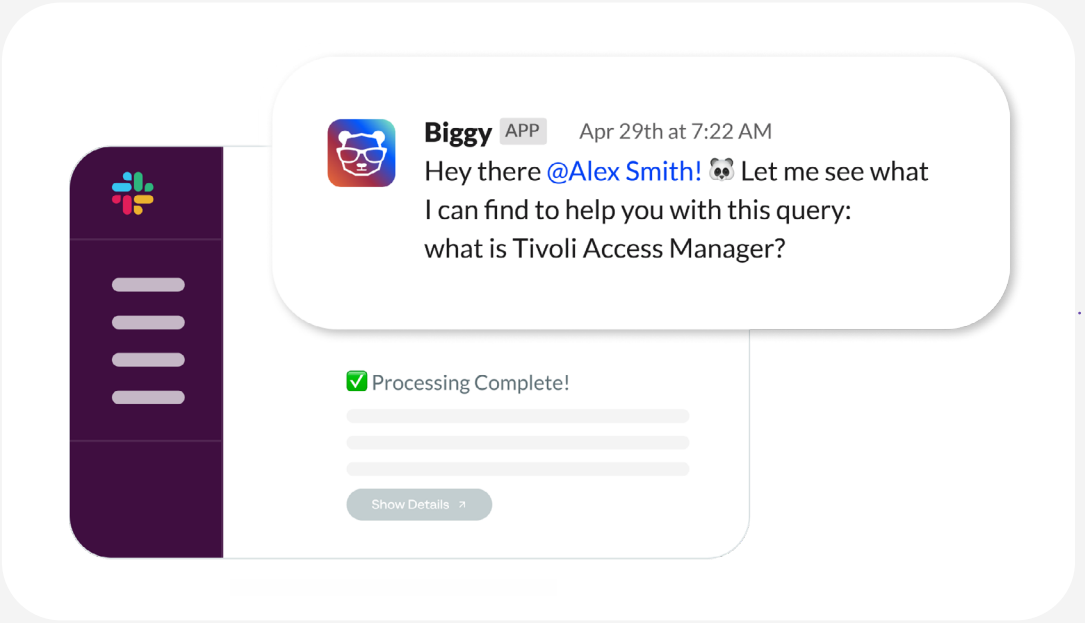
ITSM data contains information, such as affected CIs, team owners, and past impact, allowing AI Incident Prevention to quickly identify patterns, flag high-risk changes before they go live. This unified, AI-driven approach means you don't have to build complex data integrations across dozens of tools to see results. You can quickly start reducing incident volume, improving stability, and freeing up resources for strategic initiatives—turning change management from reactive damage control into proactive, risk-aware decision-making.

Phased data strategy for BigPanda AI Incident Prevention

	Data Sources	Results	Key Metrics
Change analysis and risk mitigation Operational data.	• ITSM real-time integration (ticket history, CMDB, change records)	Automate change analysis and prevent change-related risks with clear risk thresholds and guardrails across teams.	**Change Success Rate** + Changes pushed in a month. ↓ Number of incidents caused by change. ↓ CAB review time, size, meeting frequency. ↓ Change cycle time.
Advanced change analysis and risk mitigation Additional institutional knowledge.	• Runbooks • Wikis • SOPs • Chat History	Provides additional context and enhances risk reasoning and suggested mitigations.	Higher degree of all of the above, and expansion to additional teams.

Operational goal: Augment your IT experts with AI assistance

Incident commanders, L2 and L3 engineers, Site Reliability Engineers (SREs), and service owners face a triple threat to effective incident response. Poor collaboration between stakeholders, missed handoffs that delay resolution, and a lack of access to critical information buried across siloed systems and teams.



The BigPanda AI Incident Assistant gleans actionable insights from across siloed systems, hidden data, and historical activities.

The BigPanda AI Incident Assistant is a real-time AI partner to help these teams overcome these challenges and investigate and resolve incidents faster. It surfaces hidden institutional knowledge across siloed teams, tools, and systems to quickly uncover what's happening, why, and how to fix it. Teams can now reduce reliance on long bridge calls, eliminate unnecessary escalations, and generate lasting institutional knowledge from untapped sources like conversations, tickets, and chat threads.

Getting started is fast—enterprises only need access to ITSM, on-call data, and chat tools connections. By integrating directly with Slack and Microsoft Teams, AI Incident Assistant centralizes collaboration and ensures nothing gets lost in side conversations or forgotten after the fact. It also learns from past incidents, automatically surfacing relevant history, context, and recommended next steps. Within days (or as soon as your next major incident occurs), teams can improve collaboration, accelerate resolution, and transform major incident management from reactive scrambling to proactive, orchestrated action.

Phased data strategy for BigPanda AI Incident Assistant

	Data Sources	Results	Key Metrics
AI-powered Collaboration and Troubleshooting Collaboration, bi-directional tool integration	• Slack/Teams App • ITSM (real-time integration + data) • On-Call	Eliminate manual coordination and accelerate team alignment, and automate major incident management workflows.	**Service Reliability:** + Reduced workloads. ↓ Major Incident MTTR.
Agentic investigation Real-time operational data, institutional and team knowledge	• Observability • BigPanda incidents (ADR) • KB Articles/Wikis • Runbooks/SOPs • Post-mortems/RCAs	Surface relevant insights in real-time, using automated observability data analysis, historical insights and institutional knowledge, to accelerate investigation and automate detection of new incidents with contextual listening.	**All the above and:** + Automated investigation.
Shared knowledge Conversational knowledge	• Redacted transcripts • Chat history • Call transcription	Supercharge investigation for faster remediation and operationalize shared knowledge for smarter operator response in the future.	**All of the above and:** ↓ Incident timelines. + Faster employee onboarding.

Mike Cervasio
Global Practice Manager for Observability and AIOps

World Wide Technology

"By delivering scalable, enterprise-ready AI that integrates seamlessly into existing environments, BigPanda enables a fundamental shift in how organizations manage IT operations towards greater confidence, control, and agility."

Agentic AI is the future of ITOps, and BigPanda powers that future

The BigPanda Agentic ITOps platform transforms how enterprises detect, respond to, and prevent incidents. Agentic ITOps represents a new paradigm, where technology works alongside humans to scale IT capacity to meet the speed, complexity, and demands of modern enterprise IT environments.

AI Detection and Response, AI Incident Prevention, and AI Incident Assistant from BigPanda allow enterprises to respond to and prevent IT incidents at machine speed, improving operational efficiency and delivering exceptional service reliability.

Your enterprise can start unlocking these capabilities today with a progressive, phased approach to an AI-first data strategy that unlocks value in phases and reduces adoption friction. Once you implement AI Detection and Response, you can continue to add data sources from various networks, applications, services, and business teams into the IT Knowledge Graph. This implementation unlocks the capabilities offered by AI Incident Prevention and AI Incident Assistant.

The more information the IT Knowledge Graph has access to, the more accurate and relevant the outcomes will be. Schedule a personalized demo to learn how your enterprise can lay the foundation for agentic AI and transform reactive IT operations into intelligent, autonomous systems.

DEMO

See the BigPanda agentic IT operations platform in action

Agentic AI transforms how enterprises detect, respond to, and prevent incidents.

Get a demo

bigpanda.io