

Benefits

- ✓ **Proactive incident detection**
Correlate alerts from internal and external observability, CMDB, and service desk sources to help automate early L1 detection of potential incidents.
- ✓ **Comprehensive incident diagnosis**
Enrich every incident with critical context from historical, change, and internal and external observability data to accurately diagnose issues.
- ✓ **Precise incident triage**
Automatically categorize, prioritize, and diagnose incidents using historical data and operational context to suppress noisy alerts and validate next steps.
- ✓ **More automation, less escalation**
Empower L1 teams to resolve incidents with suggested and automated remediation. When escalation is required, automatically assign and equip L2 teams with complete incident context.
- ✓ **Clearly-defined ownership**
Establish clear ownership and impact to help in-house operations and outsourced MSPs quickly identify the right contacts.

Get started with BigPanda AI Detection and Response.

[Request a demo](#)

BigPanda AI Detection and Response

Take control of incidents before they escalate with autonomous detection, diagnosis, triage, and response.

Reactive, human-driven IT operations (ITOps) workflows—where siloed teams manually detect, diagnose, and respond to incidents generated by monitoring and observability tools and end-user complaints—can cost enterprises over US\$200 billion annually through in-house operations and outsourced managed service providers (MSPs).

Despite significantly investing in observability tools, many organizations still struggle with inadequate detection, often learning of incidents from customers.

Even after detecting incidents, a lack of operational context frequently delays resolution, leading to L1 bottlenecks during triage, misguided responses, and needless escalations.

Poor detection and visibility

Most L1 teams must manually sift through massive volumes of fragmented, incomplete, noisy data from observability, change, topology, and CMDB tools during incident triage. Without centralized visibility and data-driven insights, it's extremely challenging for L1 operators to identify the impacted service or application and make informed decisions, negatively impacting incident resolution times and accuracy.

Documentation gaps

Outdated, incomplete, or missing runbooks, knowledge base articles, and incident documentation create critical knowledge gaps during response. Without reliable runbook guidance or historical context on how similar incidents were previously handled, L1 teams struggle to take confident action, hindering first-contact resolution and increasing escalations, often to the wrong L2 specialists.

MSP blind spots

Enterprises often rely on MSPs to scale network and service desk operations. However, MSPs frequently have limited access to and integration with their clients' broader observability stack, creating coverage blind spots. In addition, poor communication about infrastructure changes outdated standard operating procedures, and high turnover results in an inconsistent, delayed and error-prone alert response.

How BigPanda can help

The BigPanda agentic ITOps platform enables enterprises to keep their digital world running by transforming manual, reactive, human-driven processes into automated, proactive, AI-driven IT operations that quickly detect, investigate, respond to, and prevent incidents.

BigPanda AI Detection and Response enables L1 teams to identify incidents early, before they impact businesses. It automatically detects potential incidents by analyzing real-time information from internal and external observability, CMDB, and service desk sources. It uses AI to correlate multiple data points, determine whether issues are connected to a broader incident, suppress noise, and differentiate true signals from false positives so teams can proactively prioritize and respond.

Teams can enrich incidents with critical context from historically similar incidents, change data, and internal and external observability data to diagnose issues and accurately validate the next steps during runbook and knowledge base article execution.



They can accelerate triage by categorizing, prioritizing, and diagnosing incidents automatically and precisely. They can also suppress low-impact alerts and surface actionable incidents enriched with impact, priority, and root cause analysis.

With AI that learns, teams can automate more and escalate less during incident response. AI agents recommend or automate remediation actions based on the context of an incident using institutional and informal knowledge, even if it's undocumented. This improves first-contact resolution and delivers informed response recommendations to L2 escalation teams. The AI agent continuously learns from resolved incidents and adapts to new situations in real time so teams can rely less on manual escalation.

	Detection	Triage	Response
Challenge	Visibility gaps delay incident detection, often resulting in customers reporting issues to the service desk.	IT blind spots lead to slow, error-prone triage, missed SLAs, and teams incorrectly categorizing, prioritizing, and assigning incidents.	A lack of documentation and historical insights creates gaps in resolution paths, delaying L1 response and leading to frequent L2 escalations.
Solution and business value	Identify early indicators of potential incidents, regardless of where they originated, and uncover whether individual issues are part of a broader problem.	Instantly surface high-impact issues and automatically categorize, prioritize, and diagnose incidents, based on root cause and historical analysis, to enable rapid response.	Confidently drive more first-contact resolutions with AI-powered actions tailored to the context of each incident—even as that context evolves.



"BigPanda has enabled us to get more real-time, relevant data about a specific incident. This has significantly reduced our mean time to resolution (MTTR)."

Steve Liegl
Director of Infrastructure and Operations
[WEC Energy Group](#)



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

Paul Bevan
Research Director, IT Infrastructure
Bloor Research