SOLUTION GUIDE

BigPanda

AIOps Event Correlation and Automation

How to prevent and resolve outages in modern IT environments

Executive summary

Preventing and resolving outages is a major challenge for IT operations

Enterprises of all sizes have been transforming themselves digitally in recent years. In order to compete and grow market share in a constantly changing environment, they have been modernizing their applications, migrating to the cloud, adopting DevOps and SRE practices, and trying to embrace AI and automation.

These transformation projects are creating significant challenges and IT operations teams are feeling the heat like never before.

Saddled with legacy rules-based tools and technologies that weren't built for today's dynamic, hybrid environments, they are:

– drowning in IT noise

– lacking insights to determine root cause

– forever stuck in manual, reactive firefighting with an overwhelming number of painful incidents and outages

As a result, their businesses are suffering. Operating costs, performance and availability of critical applications and services, and business agility are all taking a hit.

It’s time for AIOps Event Correlation and Automation

AIOps Event Correlation and Automation help IT Ops, NOC, DevOps and SRE teams prevent and resolve outages at scale in modern IT environments. The adoption of AIOps ECA is a major milestone for customers on their IT operations maturity journey. AIOps Event Correlation and Automation provides three key capabilities:

Event Correlation for reducing noise and detecting incidents in real-time, before they escalate into outages

Root Cause Analysis for surfacing root cause in real-time and helping resolve outages rapidly

Level-0 Automation for automating various manual tasks and workflows to help resolve outages rapidly

AIOps Event Correlation and Automation helps operations teams support their digitally transforming businesses and their modern IT environments. This results in reduced operating costs, improved performance and availability and increased business agility.

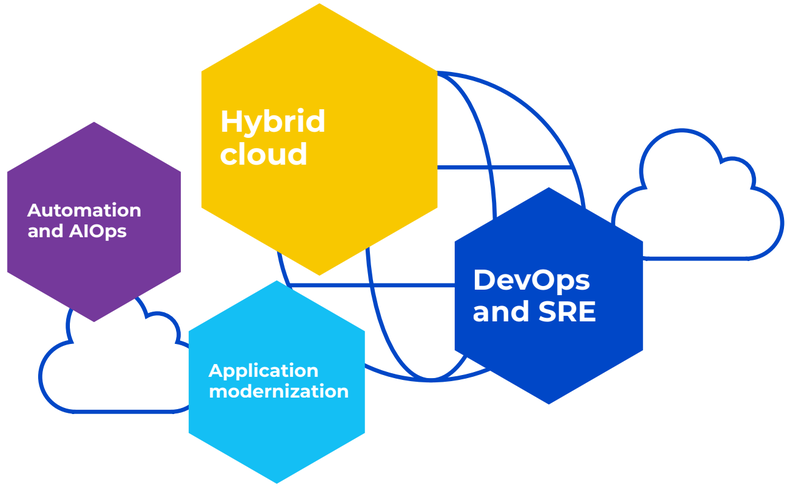
Prevent outages, reduce escalations and consolidate or eliminate tools that are not providing value in the incident management lifecycle.

“Tools like BigPanda really help us to reduce all our noise levels, get that aggregation done, get that enrichment done, and then produce actionable incidents so somebody can be paged to look at it.”

– Dan Grace, Global Technology Operations Leader, Equifax

Modern IT environments create challenges for IT operations

Companies are under immense pressure to adopt new technologies and processes that will enable them to move faster, remain competitive, and do more with less resources. As a result, they're embarking on one or more projects to drive the business forward:



These projects are complex, last several years and (almost by definition) disrupt the status quo. They also result in an overwhelming volume of heterogeneous IT noise and very little actionable insight, making it almost impossible for human IT Ops, NOC, DevOps and SRE teams to support them.

IT noise makes real-time incident detection extremely hard in modern IT environments

The typical enterprise has invested in 15 or more observability and monitoring tools. These tools were designed to provide IT Ops, NOC, DevOps and SRE teams with visibility into critical applications, systems, and infrastructure, both on-prem and in the cloud.

Ironically, the result is the inability to detect incidents in real-time because of the following:

Fragmented monitoring, change and topology data. Forces manual "swivel-chair" strategies

Disparate and inconsistent data formats. Confuse and slow down teams

Barrage of IT noise and false positives. Overwhelm IT operations teams

Siloed monitoring tools. Prevent end-to-end, cross-stack visibility

Inability to easily analyze or report on historical data across silos. Causes recurring incidents

Root cause analysis is broken in modern IT environments

Identifying the root cause of an outage or a poorly performing application is one of the biggest challenges that IT organizations face today. In modern, hybrid and cloud-native environments, problems have moved up the stack from infrastructure to complex application architectures, databases, and the cloud. Modern IT environments can experience thousands of changes every week and each change has the potential to cause unintended outages or disruptions.

IT teams must deal with:

- **Broken dependency models.** Traditional dependency-driven RCA is no longer effective
- **Fragmented diagnostic information.** Multiple-source log files, traces, metrics, and more, complicate root cause analysis
- **A single outage or incident causing hundreds of alerts.** Difficulty in detecting patterns that point to root cause, across alert storms
- **Out-of-date and/or incomplete topology models.** Impacted ability to correlate alerts and identify root cause
- **Difficulty visualizing incident evolution over time.** Hard to understand what triggered a chain of alerts that creates an incident

Ineffective automation makes MTTR unacceptably high in modern IT environments

As the number of tools organizations adopt increases, IT environments become more complex and IT operations teams grapple with a growing number of incidents and outages.

Incident response workflows are still mostly manual, time-consuming, error-prone and tedious—also sapping the productivity and morale of IT Ops, NOC, DevOps and SRE teams:

- **Slow and manual incident triage.** Low team productivity and high MTTR
- **Manual IT ticket creation.** Tedious, error prone and costly
- **Manual war-room creation.** Wastes time, leaves out relevant experts, prevents automatic sharing of critical information
- **Dangerous gaps in communication.** Lack of timely, targeted outage notifications and escalations to expert teams exacerbates issues

The state of IT operations today

$740K

Average cost of a data center outage

Source: Trace3 Research

40%

CIOs who will lose their jobs within 5 years due to failure to deliver business outcomes

Source: Gartner

65%

Organizations reporting growing frequency of alerts in the last 12 months

Source: IDG

32%

Organizations who plan to use AIOps

Source: Gartner

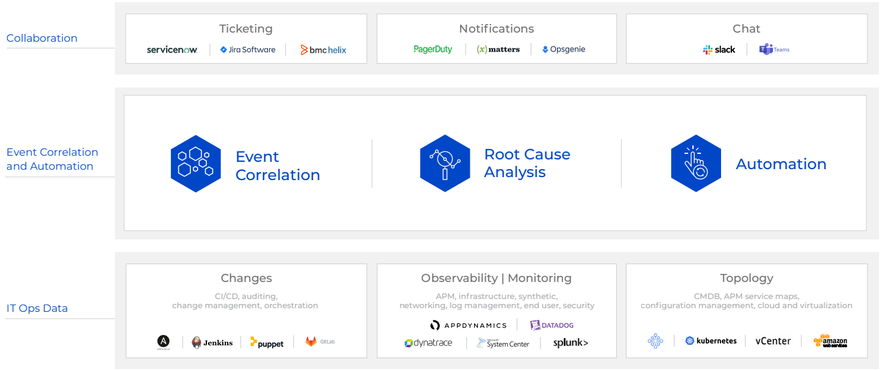
“There is no future of IT operations that does not include AIOps. This is due to the rapid growth in data volumes and pace of change (exemplified by rate of application delivery and event-driven business models) that cannot wait on humans to derive insights.”

– Market Guide for AIOps Platforms, Gartner Research, April 2021

AIOps can help

AIOps is the application of AI/ML to handle the overwhelming volume, variety, and velocity of IT Ops data endemic to modern IT environments. AIOps augments and scales the fixed capacity of human IT Ops, NOC, DevOps and SRE teams – allowing them to slash the frequency, duration and impact of incidents and outages. But where should enterprises start their AIOps journey?

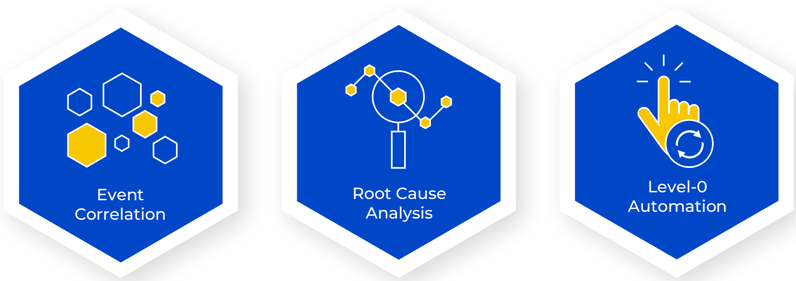
To answer that question, let's look at the three layers in today's AIOps landscape:



Start with AIOps Event Correlation and Automation, to solve your most urgent and critical problem

AIOps Event Correlation and Automation (ECA) focuses on applying AIOps to overcome the overwhelming noise and alert data generated by the plethora of observability, monitoring, change and topology tools used by enterprises. It turns IT Ops noise into insights, which helps prevent and resolve outages, as well as automate manual tasks, all in real-time. AIOps ECA helps human teams increase service availability, while driving operational costs down and giving them the bandwidth they need to focus on innovation.

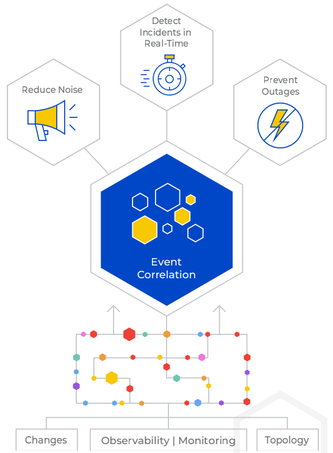
AIOps ECA does this by delivering three key capabilities:



Event Correlation prevents incidents from escalating to outages

Event correlation aggregates, normalizes and enriches data from across your fragmented observability, monitoring, change and topology tools. When enhanced with AIOps, it uses AI/ML to correlate the data into actionable insight.

The main attributes of Event Correlation with AIOps are:



- **Aggregation of events from different sources**
- **Normalization of events to a standard taxonomy**
- **Enrichment of events with topology and operational context**
- **AI-guided impact analysis and prioritization**
- **AI-guided noise reduction and correlation**
- **Reporting and analytics**

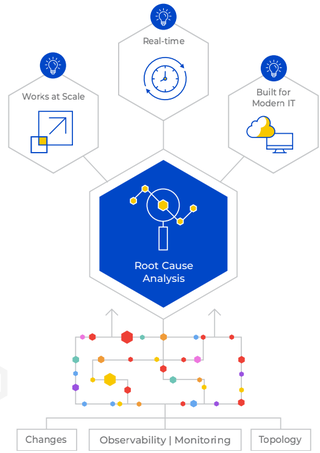
This helps your IT operations teams detect incidents as they form, in real-time, before they escalate into painful outages.

Root Cause Analysis enables rapid resolution

Root Cause Analysis lets you quickly isolate the root cause of incidents, and automatically identifies changes to infrastructure and applications that cause most issues in today's dynamic, hybrid infrastructures.

The main attributes of Root Cause Analysis are:

- **Identification of environment changes that cause problems**
- **Incident timelines, linking to other IT Ops tools**
- **Topology-based root cause analysis**

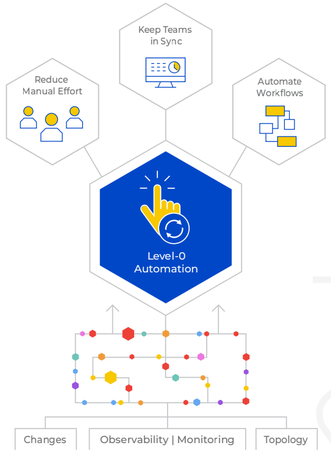


Instead of wasting hours or days on bridge calls trying to find the root cause of outages, IT Ops teams can identify root cause in minutes and act quickly.

Level-0 Automation eliminates manual tasks to speed up incident response

Automation streamlines the incident response lifecycle with automatic bi-directional ticketing, notifications and war room creation. Advanced implementations can also connect to third-party Runbook Automation tools to run workflow automations.

The main attributes of Level-0 Automation are:



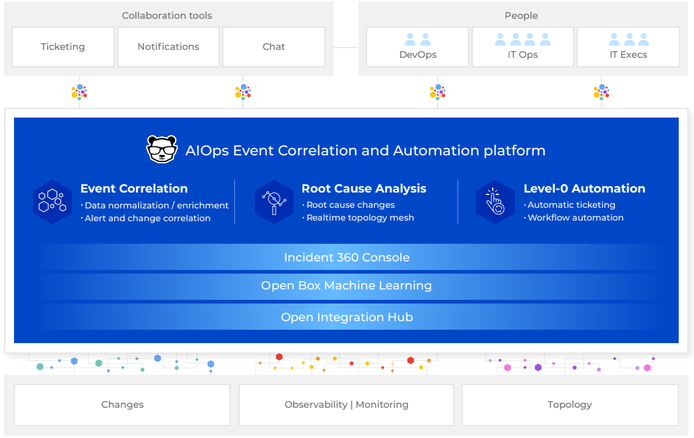
- **Automatic incident triage**
- **Automatic notifications**
- **Automatic ticket creation**
- **Automatic war-room creation**
- **Workflow and automation**

These automations eliminate errors and shave critical minutes off the incident management lifecycle, driving faster incident resolution.

BigPanda's AIOps Event Correlation and Automation platform

BigPanda's AIOps Event Correlation and Automation platform

BigPanda's SaaS-based AIOps Event Correlation and Automation platform, helps enterprises prevent and resolve outages. Purpose-built for large, complex and modern IT environments, BigPanda helps IT Ops, NOC, DevOps and SRE teams supporting their enterprises reduce the frequency, duration and impact of incidents and outages.

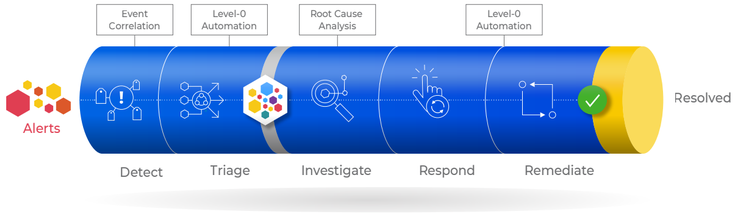


BigPanda's vendor-agnostic approach to AIOps delivers value in just 10–12 weeks, even for the largest and most complex enterprises in the world.

Incident pipelines

Before BigPanda

After BigPanda



BigPanda provides AIOps Event Correlation, Level-0 Automation, and Root Cause Analysis that help shorten the different stages of the IT incident management lifecycle and eliminate residual effects between them.

How BigPanda does Event Correlation

1

BigPanda aggregates, normalizes and enriches data from all your fragmented tools for observability, monitoring, change, and topology, regardless of their domain or vendor.

2

BigPanda's unique Open Box Machine Learning (OBML) is then applied to correlate that data into actionable insight. OBML allows your IT Ops team to easily test and tune ML-based correlation patterns before they go into production.

3

BigPanda also provides IT executives, service owners and team managers with powerful analytics to track incident trends, KPIs and metrics to increase long-term operational efficiencies.

Key advantages of Event Correlation in BigPanda

Aggregation

BigPanda connects to all your monitoring, change and topology tools and aggregates their data in real time (over 300 unique tools to date).

Normalization

BigPanda then translates these diverse IT datasets into one consistent taxonomy, in real time.

Enrichment

BigPanda's cross-domain Event Enrichment Engine uses contextual data from all operational and topology sources of to enrich monitoring alerts and make correlation more effective.

Noise reduction

BigPanda uses its Open Box Machine Learning to correlate alerts, changes and topology data together and reduces IT noise by more than 95%. This makes it possible to detect evolving incidents as they happen, before they escalate.

Impact analysis

BigPanda's Incident 360 Console provides cross-stack views that filter incidents by severity and displays business context such as affected services and potential customer impact for each incident The Real-time Topology Mesh shows dependencies between applications/ services and low-level infrastructure.

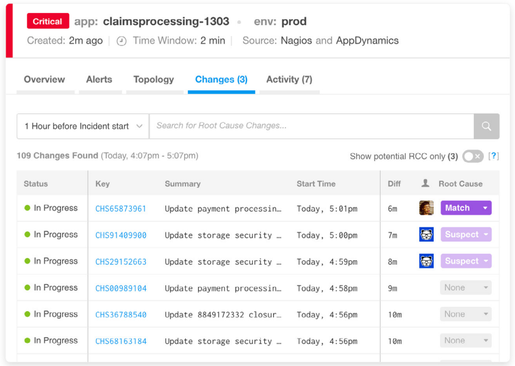
Analytics

BigPanda's Unified Analytics is based on a robust, fully customizable and scalable reporting and visualization back-end that can handle IT operations data at any scale. It displays key performance indicators, metrics and trends and supports data export to all widely used BI and DW platforms.

How BigPanda does Root Cause Analysis

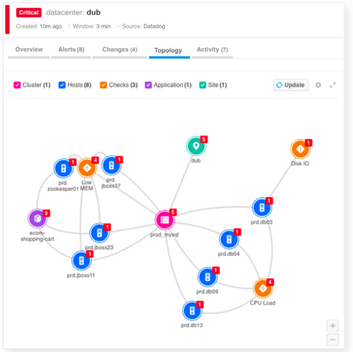
BigPanda gives organizations the ability to quickly drill down and isolate the root cause of incidents and outages. This includes automatically identifying changes to infrastructure and applications that cause most outages and incidents today, as well as lower-level infrastructure problems. Instead of wasting hours or days on bridge calls trying to find the root cause of outages, IT operations teams can now identify the root cause in minutes and take action quickly.

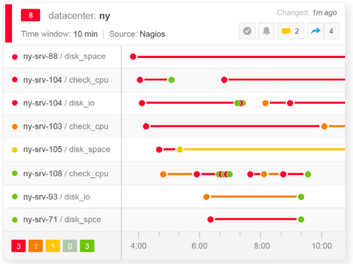
Key features of Root Cause Analysis in BigPanda



Root cause changes

BigPanda surfaces the problem change right alongside the incident, based on analysis performed by its Open Box Machine Learning technology.



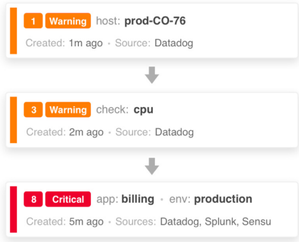


Incident timelines

Incident timelines show the evolution of an incident over time, to help operations teams understand when an incident started and how it evolved.

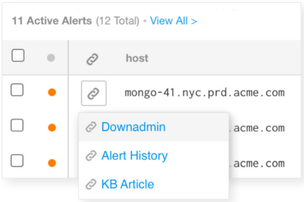
Real-time topology

BigPanda's Real-time Topology Mesh creates a full-stack, topology model that captures dependencies between networks, servers, clouds and applications.



Dynamic titles

Dynamic incident titles display probable root cause at a glance. As new alerts are collected and added to the incident, the incident title is updated.



Deep links

The Deep Links feature turns BigPanda into an intelligent gateway for operational context and can link to investigation or root cause info collected from other systems or tools.

How BigPanda does Level-0 Automation

BigPanda's Level-0-Automation gives IT operations teams time back that was once spent on manual tasks, shaves critical seconds and minutes off the incident management lifecycle, eliminates IT Ops process errors, and drives faster incident resolution.

Key features of Level-0 Automation in BigPanda

Automatic triage
BigPanda uses custom tags that capture business context and metrics for every incident. These are presented alongside the incidents within BigPanda's Incident 360 Console, so teams can easily and quickly conduct triage and decide what to do next.

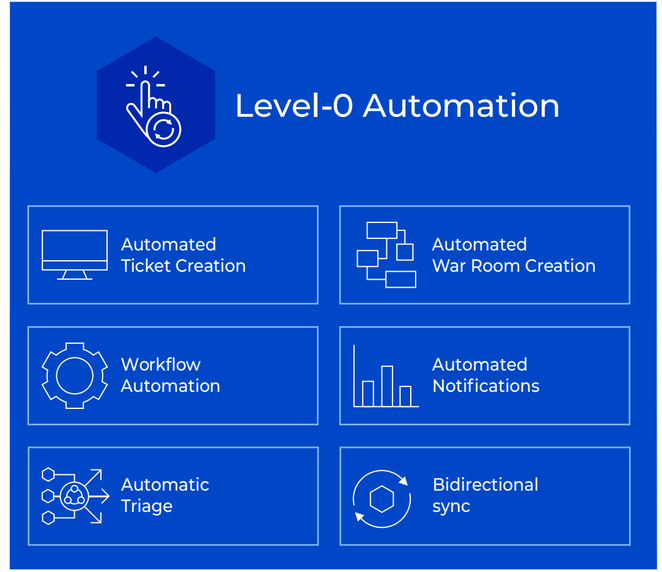
Ticket creation
BigPanda's out of box integrations with ticketing solutions (including ServiceNow, JIRA, BMC and Remedy) allow automatic ticket creation as soon as incidents are detected.

Targeted notifications
BigPanda automates the sharing of incidents with notification tools (such as PagerDuty, OpsGenie and others) so that DevOps/Level-3 and other teams can start working on incidents upon detection.

Automatic war rooms
BigPanda can automate the creation of war rooms by sharing relevant incidents and inviting the right DevOps/Level-3 team members.

Bidirectional sync
All automation integrations are bi-directional, so updates inside BigPanda or other tools are automatically synchronized even after an incident has been shared.

Workflow automation
By leveraging BigPanda's powerful, easy to use REST API, organizations can easily integrate BigPanda with automation tools such as Rundeck, StackStorm, and Resolve Systems to run workflow automations.



BigPanda's impact on the business

The vast majority of BigPanda's customers are able to go-live in just 10-12 weeks. In production, these BigPanda users are able to:

Reduce operating costs

By boosting efficiency, reducing escalations, slashing downtime, eliminating or shortening bridge calls, flattening headcount, reducing SLA penalties, and consolidating tools, BigPanda customers can reduce operating costs by up to 50%.

Increase performance and availability

BigPanda helps organizations improve performance and availability of their critical business applications and systems, reducing MTTR by 50% or more. This helps IT operations teams preserve user experiences, automate different aspects of incident management, collaborate more effectively, eliminate noise and reduce constant firefighting.

Increase business velocity

By preventing outages and reducing noise in the incident management lifecycle, BigPanda gives IT operations teams time to focus on their strategic digital transformation initiatives, which significantly improves their agility and rate of innovation. The result is happy, loyal customers and business services that drive revenue.

What our customers are saying

"The BigPanda Open Box Machine Learning suggests correlation patterns much faster than we could do on our own. We can review suggested patterns and see the projected results."

– **Brian Kendall**
VP Service Assurance

Rise Broadband

"With the BigPanda Platform, we perform incident management in an autonomous way. Using Unified Analytics, we make informed decisions to avoid future issues and improve overall performance."

– **Sam Pereira**
Director of Technical Integration

ENDURANCE International Group

"We needed a platform that scales and allows for growth. We did not want the burden of infrastructure and maintenance costs."

– Kevin Johnson
VP Cloud & Application Operations

News Corp

"Tools like BigPanda really help us to reduce all our noise levels, get that aggregation done, get that enrichment done, and then produce actionable incidents so somebody can be paged to look at it."

– **Dan Grace**
Global Technology Operations Leader

EQUIFAX

"The NOC was dying before automation because the stuff we were doing, people don't do anymore. So being able to automate manual operations and workflows, it gave us the ability to do new, more exciting work."

– Ben Narramore
Senior Manager of Operations

PlayStation.

About BigPanda

BigPanda helps businesses prevent and resolve IT outages with their AIOps Event Correlation and Automation platform. Without BigPanda, IT Ops, NOC, DevOps and SRE teams struggle with manual and reactive incident response capabilities that are badly suited for the scale, complexity and velocity of modern IT environments. This results in painful outages, unhappy customers, growing IT headcount and the inability to focus on innovation.

Fortune 500 enterprises such as Intel, Cisco, United, Nike, Marriott and Expedia rely on BigPanda to prevent outages, reduce costs, and give their teams time back for digital transformation. BigPanda helps organizations take a giant step towards Autonomous IT Operations by turning IT noise into insights and manual tasks into automated actions.

BigPanda is backed by top-tier investors including Sequoia Capital, Mayfield, Battery Ventures, Greenfield Partners and Insight Partners.

BigPanda

Visit www.bigpanda.io for more information

(650) 562-6555 | info@bigpanda.io | www.bigpanda.io