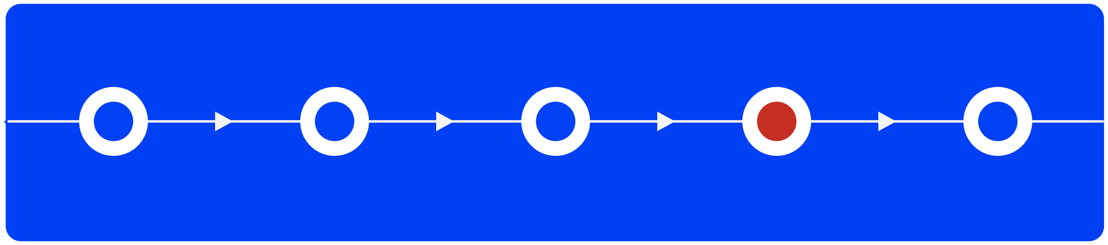
BigPanda

E-book

Three ways to simplify root cause discovery

Contents



Why automated root-cause investigation matters
(Hint: You can reduce MTTR by 50%)

Picture this: It's 9:30 p.m. on a Tuesday. Your observability tools just informed you that the data center network is down. A flood of angry customer tickets confirms the situation. For smaller organizations, critical outages like this can cost nearly $7,000 per minute. But for larger companies like yours, it's probably closer to $24,000 per minute, according to recent figures from EMA Research[1].

You don't know what caused the outage, and your CEO is eager to resolve it. Needless to say, it's all hands on deck. With dozens of people now on a high-stress bridge call to investigate the problem, one question is top of mind. Almost on cue, the director of ITOps joins the call and asks, "What changed?"

Next time you chase a customer-impacting incident or outage, ask yourself: How long will your users wait until they switch to a competitor's product or outsource to a service provider? Will they wait while your hard-working ITOps, DevOps, and SRE teams scramble to isolate the problem and identify root cause?

Constantly evolving IT environments have increased complexity on a massive scale. Containers, CI/CD, microservices, and cloud-native applications deliver alert and change data across a multicloud IT stack, making identifying incident root cause extremely difficult. Legacy event management, monitoring, and observability tools aren't up to the task of efficiently collecting and analyzing the deluge of ITOps data to identify what likely caused an incident.

Instead, most organizations still rely on expensive, skilled staff members to hunt through log files, change-management systems, and code repositories to find the issue that started it all. This manual, time-intensive process is fraught with potential misses due to human error, especially if your staff lacks the skills or access to the data they need.

A **50% reduction in MTTR** could mean thousands of labor hours saved annually.

[1] "It outages: 2024 costs and containment," Enterprise Management Associates, 2024.

IHG
HOTELS & RESORTS

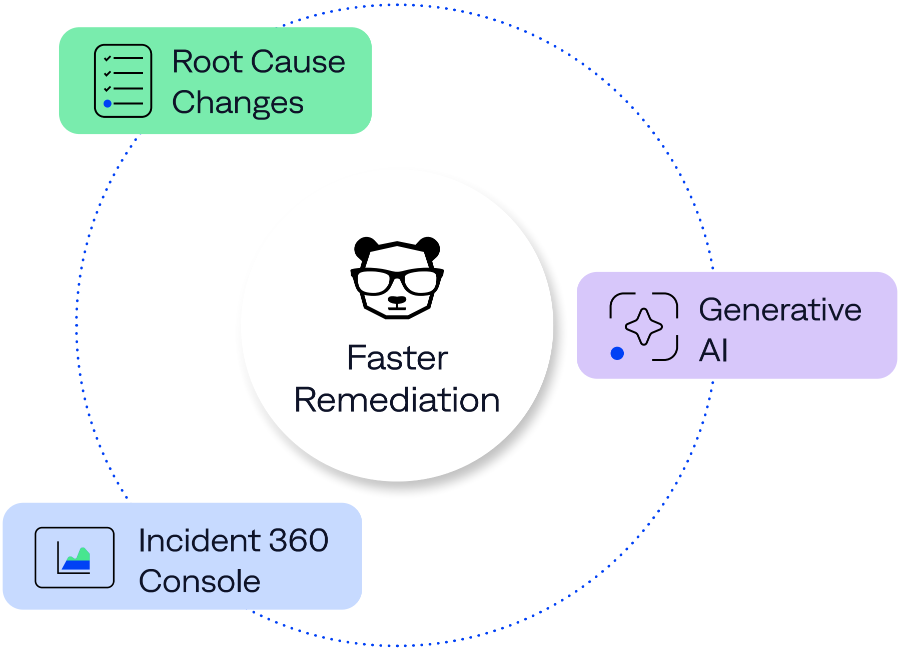
> *"If we are unable to identify and understand the root cause of an incident, we are at a tremendous disadvantage. With BigPanda, we are now taking advantage of machine learning automation and AI to further decrease the mean time to identify an incident, which gives us more time to resolve the operational incident, reducing MTTR and keeping our services running."*

Alvin Smith
Vice President of Global Infrastructure and Operations,
IHG Hotels & Resorts

Fast-paced organizations don't have the luxury of figuring out what happened after the fact. The pace of change in IT has made it imperative that you determine root cause in real-time and remediate incidents in moments. A solid AIOps platform can help your organization get to the root cause of incidents and outages faster and more reliably than humans will ever be able to alone.

BigPanda takes a pragmatic approach to AI and machine learning to remove the barrier between human and machine collaboration, enhancing an operator's ability to instantly uncover the vital root cause details that are essential for identifying and resolving incidents. In fact, organizations that combine correlated and enriched event data with capabilities such as generative AI and Root Cause Changes are achieving up to a 50% reduction in mean time to resolution (MTTR).

Three core elements of the BigPanda platform uncover crucial details to resolve incidents and reduce MTTR: Incident 360 Console, Root Cause Changes, and Generative AI for Automated Incident Analysis.



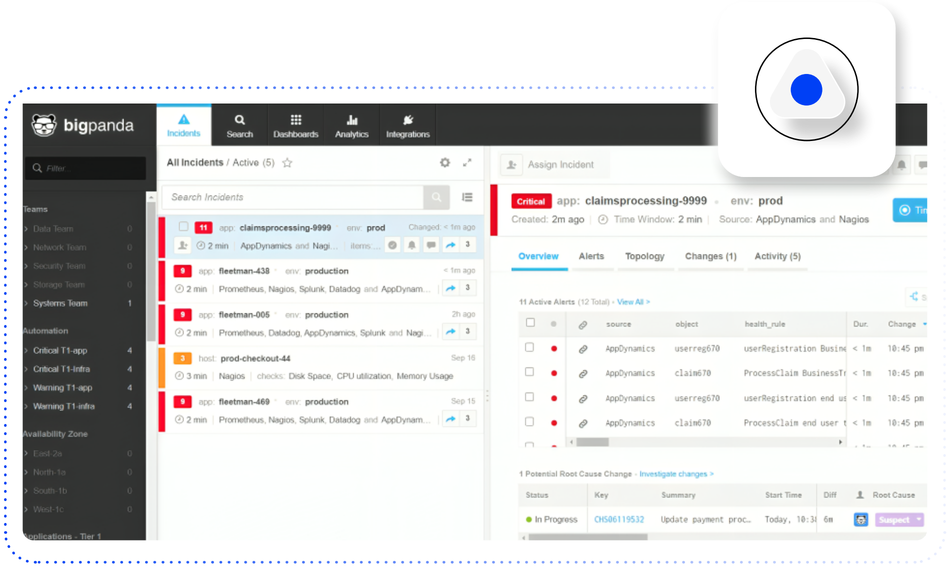
Gartner

> *"Integrating change and incident management will help identify issues caused by change to improve incident response time and collaboration to improve service reliability."* [2]

BigPanda Incident 360 Console

Historically, teams conducted root-cause analysis only after incidents were resolved. Teams often met days later to discuss what went wrong and how to avoid a recurrence. But as outage costs skyrocket and incidents increase, it's critical to get to root cause in near-real-time. And that takes the right data.

The first challenge is sifting through the mass of related available events, alert, and change data. The data volume can be daunting. Striking a balance between too much and not enough data is difficult. The average BigPanda customer uses more than 21 sources of observability data. But relying on observability data alone isn't enough. Observability relies on data anomalies to identify an incident. When you combine observability data from one platform with third-party observability alerts, topology, service maps, and change-management tools, it becomes exponentially more difficult to make sense of what caused an incident. And especially in real time.



All Incidents / Active (5)

11 app: claimsprocessing-9999 · env: prod Changed: < 1m ago
2 min | AppDynamics and Nagi... | items:... 3

9 app: fleetman-438 · env: production < 1m ago
2 min | Prometheus, Nagios, Splunk, Datadog and AppDynam... | 3

9 app: fleetman-005 · env: production 2h ago
2 min | Prometheus, Datadog, AppDynamics, Splunk and Nagi... | 3

3 host: prod-checkout-44 Sep 16
3 min | Nagios | checks: Disk Space, CPU utilization, Memory Usage

9 app: fleetman-469 · env: production Sep 15
2 min | Prometheus, Nagios, Splunk, Datadog and AppDynam... | 3

Critical app: claimsprocessing-9999 · env: prod
Created: 2m ago | Time Window: 2 min | Source: AppDynamics and Nagios

11 Active Alerts (12 Total) · View All >

☐	●		source	object	health_rule	Dur.	Change
☐	●		AppDynamics	userreg670	userRegistration Busine	< 1m	10:45 pm
☐	●		AppDynamics	claim670	ProcessClaim BusinessTr	< 1m	10:45 pm
☐	●		AppDynamics	userreg670	userRegistration end us	< 1m	10:45 pm
☐	●		AppDynamics	claim670	ProcessClaim end user t	< 1m	10:45 pm

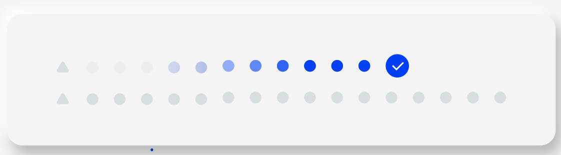
1 Potential Root Cause Change · Investigate changes >

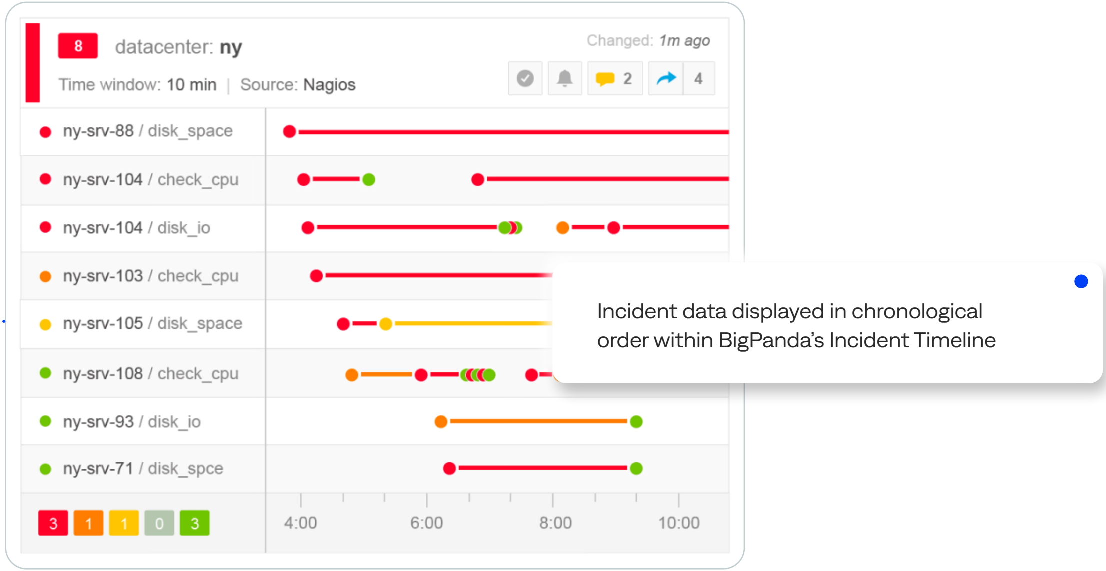
Status	Key	Summary	Start Time	Diff	Root Cause
● In Progress	CHS06119532	Update payment proc..	Today, 10:3	6m	Suspect

[2] Gartner, 2024 Planning Guide for IT Operations and Cloud Management, Gregory Murray, Ang Troy, et al., 4 October 2023
Gartner is a registered trademark and service mark of Gartner, Inc. and/ or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

BigPanda helps teams find root cause quickly by consolidating all relevant observability and monitoring data in the BigPanda Incident 360 Console. The console uses a powerful open AI pattern-matching algorithm to automatically group alert data from multiple sources for quick access and analysis. During this process, it removes up to 90% of noise, normalizing and organizing information based on patterns that you can tune to meet your specific requirements.

Once an incident's alert data is correlated, it's much easier for first responders to identify root cause. The Incident Details Pane shows a timeline, visually arranging alerts in chronological order. The timeline simplifies identification of which alerts occurred at the beginning of an incident — which are often those most closely associated with the root cause.





8 datacenter: **ny**

Changed: *1m ago*

Time window: 10 min | Source: Nagios

2 4

ny-srv-88 / disk_space
ny-srv-104 / check_cpu
ny-srv-104 / disk_io
ny-srv-103 / check_cpu
ny-srv-105 / disk_space
ny-srv-108 / check_cpu
ny-srv-93 / disk_io
ny-srv-71 / disk_spce

3 1 1 0 3

Incident data displayed in chronological order within BigPanda's Incident Timeline

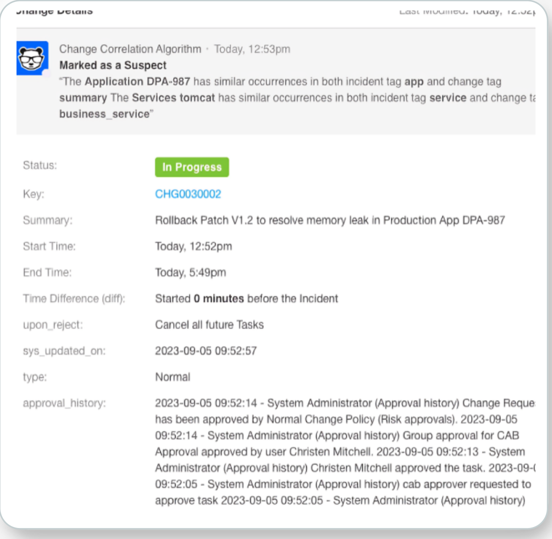
The visual elements of the Incident 360 Console enable responders to find root causes visually, expediting investigation, escalation, and resolution. It also helps teams working on post-mortem root-cause analysis, as all the data necessary is in a single place and ready for analysis.

Consolidating, cleaning, and organizing data into correlated incidents is an important part of using advanced generative AI to automatically identify root causes. Without the right data correlation, even the most advanced algorithms fail to deliver reliable insights.

Bloor

"Observability, by itself, does not identify root cause the way BigPanda does."

Paul Bevan
Research Director, IT Infrastructure, Bloor Research



Change Details — Last Modified: Today, 12:52p

Change Correlation Algorithm · Today, 12:53pm
Marked as a Suspect
"The **Application DPA-987** has similar occurrences in both incident tag **app** and change tag **summary** The **Services tomcat** has similar occurrences in both incident tag **service** and change ta **business_service**"

Status:	In Progress
Key:	CHG0030002
Summary:	Rollback Patch V1.2 to resolve memory leak in Production App DPA-987
Start Time:	Today, 12:52pm
End Time:	Today, 5:49pm
Time Difference (diff):	Started **0 minutes** before the Incident
upon_reject:	Cancel all future Tasks
sys_updated_on:	2023-09-05 09:52:57
type:	Normal
approval_history:	2023-09-05 09:52:14 - System Administrator (Approval history) Change Reque has been approved by Normal Change Policy (Risk approvals). 2023-09-05 09:52:14 - System Administrator (Approval history) Group approval for CAB Approval approved by user Christen Mitchell. 2023-09-05 09:52:13 - System Administrator (Approval history) Christen Mitchell approved the task. 2023-09-(09:52:05 - System Administrator (Approval history) cab approver requested to approve task 2023-09-05 09:52:05 - System Administrator (Approval history)

Root Cause Changes

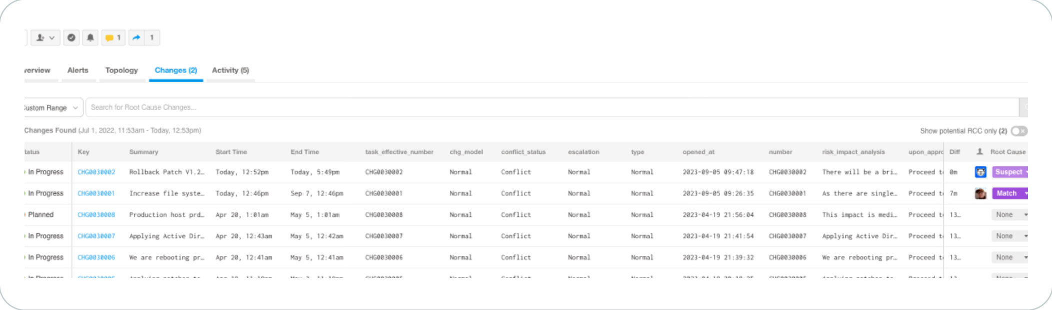
Tracking system changes has become infinitely more complicated. Gone is the monolithic Java application querying a centralized Oracle RDBMS and running on a single IBM server. The modern IT environment is a complex maze of Java, .Net, Python, Go, and JavaScript-based microservices, communicating with MongoDB, PostgreSQL, Snowflake, and Amazon S3 while running on elastic clouds and container clusters.

Your tech stack is now so diverse and complex that changes are both constant and extremely difficult to track accurately. Any changes could result in an incident or outage, whether code deployments, system setting adjustments, server provisioning and de-provisioning, third-party library updates, database configuration changes — the list goes on.

BigPanda calls changes that result in an incident or outage, root-cause changes. These changes are the single most important element for ITOps to investigate, isolate, and resolve when looking for root cause. BigPanda Root Cause Changes radically simplifies and speeds these steps using advanced AI. The component performs real-time correlative analysis, comparing change data to the organized set of data from a given incident. It clearly describes incidents, their priority, and what changes are likely responsible.

BigPanda autonomously captures significant real-time incident-related change data. Utilizing 29 unique vector dimensions, the advanced AI distinguishes high-confidence alert matches, illuminating likely root causes without limiting the suspects to a single result with the highest score. This relieves Level 1 responders to work on incidents instead of wasting time interpreting data.

The result? BigPanda automatically reveals the changes most likely to have caused incidents in only a few seconds. Response teams can focus immediately on the most relevant system changes and resolve incidents far faster.



Changes Found (Jul 1, 2022, 11:53am - Today, 12:53pm)

tatus	Key	Summary	Start Time	End Time	task_effective_number	chg_model	conflict_status	escalation	type	opened_at	number	risk_impact_analysis	upon_appro	Diff		Root Cause
In Progress	CHG0030002	Rollback Patch V1.2…	Today, 12:52pm	Today, 5:49pm	CHG0030002	Normal	Conflict	Normal	Normal	2023-09-05 09:47:18	CHG0030002	There will be a bri…	Proceed t	0m		Suspect
In Progress	CHG0030001	Increase file syste…	Today, 12:46pm	Sep 7, 12:46pm	CHG0030001	Normal	Conflict	Normal	Normal	2023-09-05 09:26:35	CHG0030001	As there are single…	Proceed t	7m		Match
Planned	CHG0030008	Production host prd…	Apr 20, 1:01am	May 5, 1:01am	CHG0030008	Normal	Conflict	Normal	Normal	2023-04-19 21:56:04	CHG0030008	This impact is medi…	Proceed t	13…		None
In Progress	CHG0030007	Applying Active Dir…	Apr 20, 12:43am	May 5, 12:42am	CHG0030007	Normal	Conflict	Normal	Normal	2023-04-19 21:41:54	CHG0030007	Applying Active Dir…	Proceed t	13…		None
In Progress	CHG0030006	We are rebooting pr…	Apr 20, 12:41am	May 5, 12:41am	CHG0030006	Normal	Conflict	Normal	Normal	2023-04-19 21:39:32	CHG0030006	We are rebooting pr…	Proceed t	13…		None

“Change-related incidents are one of the biggest generators of unnecessary alert noise. We’ll use the BigPanda Root Cause Changes tool to gain a clearer understanding of the underlying causes behind incidents so we can respond more effectively.”

Mark Peterson
Supervisor of IT Operations, Cambia Health Solutions

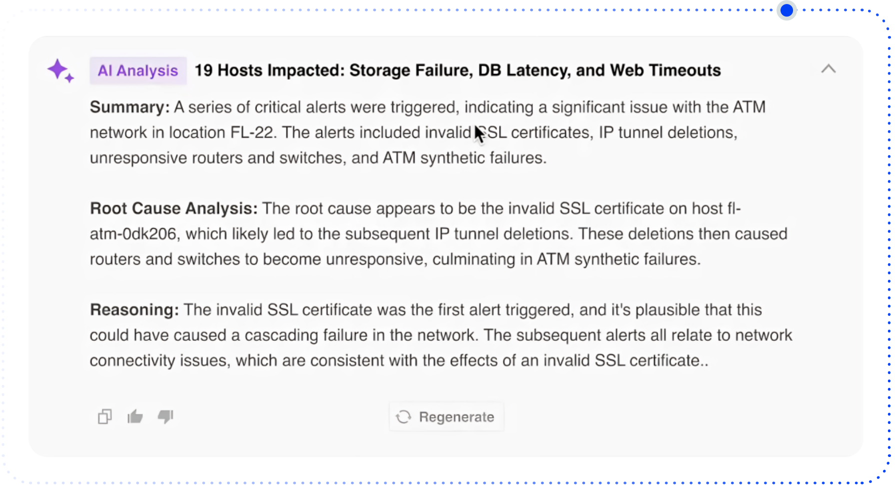
Generative AI

A seismic shift in the sophistication of AI systems, particularly large language models (LLMs), has created a significant opportunity for ops teams tasked with investigating root cause. Provided with the right details, BigPanda Generative AI for Automated Incident Analysis suggests root cause in a fraction of the time of human first responders.

BigPanda Generative AI ingests incident data and instantly identifies the root cause, relevance, and impact across distributed IT systems. It describes incidents in clear, natural language and can explain its findings, making results easily verifiable. This makes escalations faster, easier, and more consistent, scaling the impact of first responder teams and reducing the burden on more technically skilled staff As a result of AI-generated impact estimates, users report cutting incident triage times in half as well as reducing incident escalations.

Generative AI can be an extraordinarily powerful way to save ITOps time and effort,” said Jon Brown, senior analyst at Enterprise Strategy Group. “But Generative AI works best when it is given good data such as alert information enriched with other data types to help AI develop accurate conclusions.”

It’s important to note that generative AI relies on rich, clean data sets. Without clearly delineated incident data, GenAI results are far less accurate and reliable. BigPanda provides clean, consolidated, collated incident data so that BigPanda Generative AI can quickly return accurate root-cause estimates.



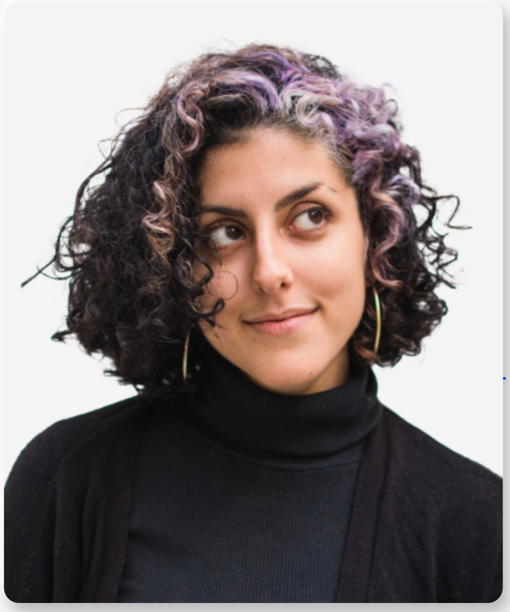
19 Hosts Impacted: Storage Failure, DB Latency, and Web Timeouts

Summary: A series of critical alerts were triggered, indicating a significant issue with the ATM network in location FL-22. The alerts included invalid SSL certificates, IP tunnel deletions, unresponsive routers and switches, and ATM synthetic failures.

Root Cause Analysis: The root cause appears to be the invalid SSL certificate on host fl-atm-0dk206, which likely led to the subsequent IP tunnel deletions. These deletions then caused routers and switches to become unresponsive, culminating in ATM synthetic failures.

Reasoning: The invalid SSL certificate was the first alert triggered, and it's plausible that this could have caused a cascading failure in the network. The subsequent alerts all relate to network connectivity issues, which are consistent with the effects of an invalid SSL certificate..

> *"Beyond augmentation, AIOps platforms can manipulate huge volumes of data to perform tasks much faster than humans. AI-driven root cause analysis, for example, makes ticket routing much faster."*
>
> **Gartner, Deliver Value to Succeed in Implementing AIOps Platforms,** Matt Crossley, 23 March 2023



The importance of keeping people in the process

When a Level 2 engineer escalates an incident, the Level 3 engineer typically verifies the findings before proceeding. The verification step isn't due to a lack of trust in the L2 engineer's abilities. It's all about the burden of accountability. An engineer knows that an incorrect call could result in significant costs and reputation damage for the organization — and turn a prolonged incident or outage into an emergency. Simply put: Two heads are better than one.

In much the same way, BigPanda AI-powered root-cause discovery enhances the abilities of frontline IT professionals. BigPanda designed and built the platform with expertise in IT infrastructure and systems. The platform provides operational awareness and context to reliably identify a problem's origin, what changed, and the relationship between systems to suggest where and how to resolve issues.

By removing the barriers between human and machine collaboration, the AI and ML help your IT department scale exponentially in capacity and experience.

BigPanda greatly simplifies the identification of an incident's origin by reducing thousands of events into dozens of incidents, providing accurate causality. Using the power of AI, it does this in seconds and frees ITOps, DevOps, and SRE teams to work on remediation instead of wasting time interpreting data. Your teams can focus their efforts and experience on more difficult tasks, such as putting the people, processes, and technology in place to prevent future incidents. Implementing these processes and technology successfully can deliver huge benefits.

Get to root cause with BigPanda

Based on conversations with BigPanda customers, we estimate the pace of change for most enterprises has already grown by at least a factor of 10 in the last five years alone. And analysts expect it to grow by another factor of ten in the next five. These numbers create an unprecedented challenge for IT organizations and their teams. Assuming radical increases in change volumes — and the fact that changes often break things — how can you expect IT teams to provide highly available, performant applications and services at all times?

The bottom line is that they can't do it alone. Without help from automation tools, the level of complexity and sheer volume of data is simply growing beyond human capacity. In short, automation is the future.

> *"We are able to identify 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. One of the biggest drivers that we have right now is auto-remediation."*
>
> **Priscilliano Flores**
> Staff Software Systems Engineer, Sony Interactive Entertainment

Learn more about the BigPanda AIOps platform.

Root-cause analysis is difficult, but it's not optional. When things go wrong, you need to know exactly what led to the problem so you can restore operations quickly and ensure outages and incidents don't happen again. The BigPanda platform include the tools to scale the skills and experience of your team and identify root cause so you can stay ahead.

BigPanda

bigpanda.io