

Everything you need to **master RCA for modern IT**

- ◆ Smarter RCA strategies for enterprise IT challenges

Table of contents

■	Introduction	3
■	From firefighting to future-proofing against downtime with conversational RCA	4
■	Stopping vulnerabilities before they spread with embedded security insights	9
■	Cracking the cause of service desk SLA violations with AI-driven contextual recommendations	15
■	Conclusion	18
■	About ManageEngine Analytics Plus	19

Introduction

Modern IT environments are more complex and vulnerable than ever.

With infrastructure growing at scale, threats evolving rapidly, and **digital downtime costing businesses as much as**^[1]

\$9,000 / minute

the ability to quickly pinpoint and mitigate the root cause of IT incidents has become mission-critical.

Yet, traditional root cause analysis (RCA) methods are struggling to keep up. Manual investigations are hamstrung by data silos, alert overload, slow correlation of events, and the sheer scale of analysis. **A recent study by IBM**^[2] shows that it still takes organizations an average of 69 days to contain a breach after discovering it and nearly 200 days to identify one in the first place. Slow, manual RCA can lead to IT outages and service degradations dragging on for hours, disrupting operations and eroding trust. Root causes go undiscovered or misdiagnosed, and teams react rather than resolve proactively. The lack of speed and precision in RCA has become a critical inhibitor to IT resilience.

AI-powered analytics offers a transformative solution. By infusing RCA with GenAI-assisted insight, context, and automation, analytics reduces investigation times, isolates the real contributing factors, and enables proactive mitigation.

In this e-book, you'll discover three game-changing strategies to revolutionize modern RCA. Together, these approaches reveal how AI empowers IT teams not only to solve incidents faster but to build a foundation for resilient, future-ready IT operations.

01

From firefighting to future-proofing against downtime with conversational RCA

News of critical downtime can quickly plunge even the most seasoned IT team into chaos. Inevitably, every team has gone through this chaotic and dreaded cycle of an unexpected system outage. What follows is a frantic scramble by cross-functional teams to fix the issue and restore service as quickly as possible.

In these high-pressure moments, the true adversary isn't just the outage—it's the ticking clock and the complexity of retracing the series of events that caused it. Identifying the root cause often requires endless log checks, war room calls, cross-functional investigations, and navigating a multitude of monitoring dashboards.

With stakeholders demanding answers and resolution, teams often resort to quick temporary patches that plug the gap but fail to address the underlying problem, leaving the door wide open for downtime recurrence.

Sustained IT downtime management requires an accelerated RCA approach that moves beyond manually sifting through logs, frantic tool-hopping, and educated guesswork.

Conversational analytics: An AI-driven revolution to traditional RCA

GenAI-powered conversational analytics offers a vital lifeline for IT teams. It helps them analyze, triage, and act on downtime swiftly without complex or time-consuming data investigations.

An AI-driven conversational assistant, like Analytics Plus' Ask Zia, helps teams detect downtime incidents, diagnose their root causes, and recommend targeted resolutions within minutes—all in a single, interactive window through simple, natural language queries.

By correlating real-time key metrics, historical events, and performance baselines across multiple resources, applications, and dashboards, these assistants highlight abnormal metrics that are indicative of downtime.

But they do much more than just surface key indicators. Conversational assistants can backtrack events, identify dependent metrics, correlate anomalies, and uncover other related incidents and configuration changes across the system that contributed to the downtime. They provide tailored, actionable corrective and preventive strategies based on these insights—bringing true end-to-end clarity.

Imagine a critical payment gateway for an e-commerce marketplace suddenly fails on a busy day. Users are unable to complete purchases or proceed with payments, and tickets citing payment gateway issues pile in from both internal and external sources. This is no ordinary glitch; it's a business-critical outage that requires a quick, foolproof solution and a preventive mechanism to avoid future recurrences.

The first step is to identify the volume of outages that have occurred over the past 24 hours. But instead of manually checking logs or combing through tickets, IT technicians can simply say: ***Show me the trend of payment gateway outages in the past 24 hours.***

Within seconds, the conversational analytics assistant pulls data from system logs and service desk tickets, presenting the clear, ready-to-consume hourly trend line analysis shown below.



The next step is to discover and fix the root cause. The analysis above reveals a spike in payment gateway outages between hour 18 and hour 22.

IT teams can now follow-up on this conversational investigation with:

Why did payment failures spike from hour 18 to 22 today?

The AI-powered assistant instantly correlates event streams and influencing factors from servers, databases, middleware, and service desk tickets. It analyzes an eclectic list of events, such as traffic surges, latency spikes, and configuration changes, that occurred during the period, surfacing the exact combination of events that triggered the outage. This all-encompassing analysis surfaces a quick snapshot of the three key drivers or factors that led to the outage.

The screenshot shows a web interface for 'Ask Zia', an AI assistant. At the top, there's a header with the 'Ask Zia' logo, a 'Conversation mode' toggle, and settings icons. Below the header, a user query is displayed in a blue bubble: 'Why did payment failures spike from hour 18 to 22 today?'. The assistant's response is contained in a white box with a light blue border. It starts with a title: 'Reason for increase in payment gateway downtime (from hour 18 to hour 22)'. This is followed by a paragraph: 'The key drivers that might have influenced the increase in No. of downtime incidents are:'. Then, there is a numbered list of four items: 1. CPU saturation from Application resource health, 2. Concurrent request volume from Application performance, 3. New patch deployment from Asset lifecycle, and 4. Database pool from Application resource health. Below the list is a table with three columns: 'Potential drivers', 'Contribution to increase in downtime incidents', and 'Impact on downtime incidents'. The table contains four rows of data corresponding to the items in the list. A small chat icon is visible in the bottom left corner of the response box.

Potential drivers	Contribution to increase in downtime incidents	Impact on downtime incidents
CPU saturation	194	45%
Concurrent requests	192	44%
New patch deployment	122	38%
Database pool	60	20%

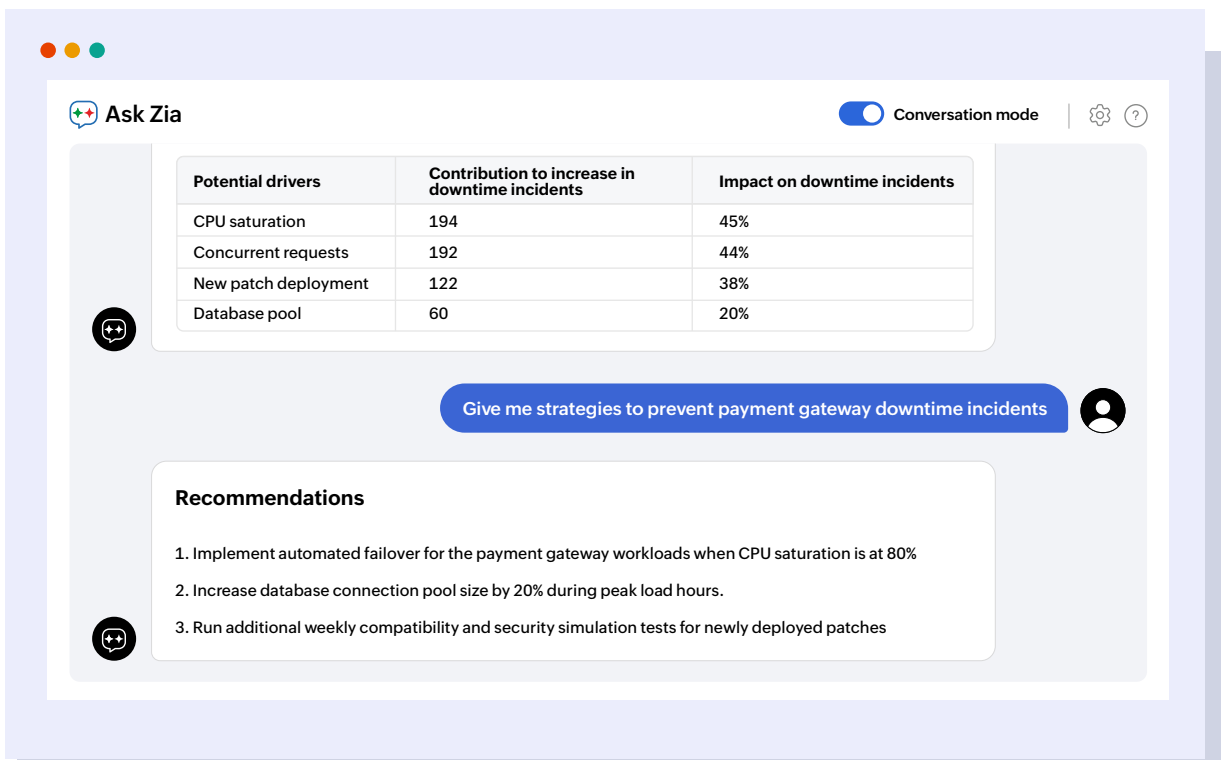
What once took hours of manual log-diving and cross-team coordination is now transformed into a simple, conversational data-backed investigation in minutes.

What's next: Moving from insights to resolution

Even the most advanced AI solutions stop once they've identified the root cause. IT teams then spend valuable time manually translating these insights into timely decisions to address and avoid downtime.

This is where the GenAI-powered conversational IT analytics truly stands out and delivers a powerful edge over manual processes.

Beyond identifying why the outage happened, Zia uses its data-driven reasoning engine to offer real-time, actionable remediation strategies. In the Ask Zia interface, teams receive tailored recommendations to address the specific key drivers that caused the payment gateway failure.



The screenshot displays the 'Ask Zia' interface. At the top, there's a header with the 'Ask Zia' logo, a 'Conversation mode' toggle switch, and settings/help icons. Below the header, a table lists 'Potential drivers' and their impact on downtime incidents. A blue button prompts the user to 'Give me strategies to prevent payment gateway downtime incidents'. Below this, a 'Recommendations' section lists three actionable items.

Potential drivers	Contribution to increase in downtime incidents	Impact on downtime incidents
CPU saturation	194	45%
Concurrent requests	192	44%
New patch deployment	122	38%
Database pool	60	20%

Recommendations

1. Implement automated failover for the payment gateway workloads when CPU saturation is at 80%
2. Increase database connection pool size by 20% during peak load hours.
3. Run additional weekly compatibility and security simulation tests for newly deployed patches

The outcome? Application downtime that once took hours to identify and resolve is now fixed in minutes. And more importantly, IT teams can proactively monitor the identified risk factors to prevent future recurrences of events that could lead to an outage.

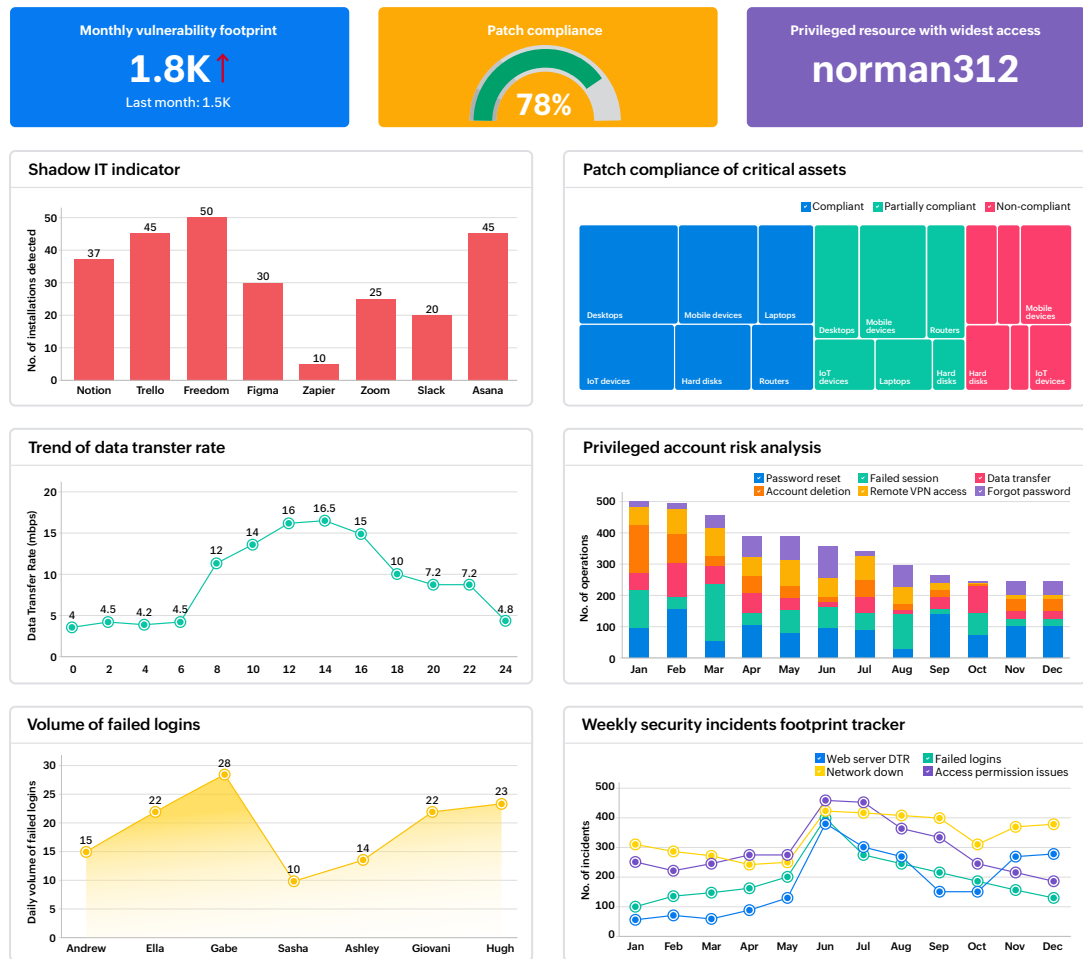
Conversational analytics transforms RCA from a reactive, manual process into an intelligent, automated, and proactive powerhouse. It becomes a guided journey—from pinpointing drivers behind events to getting smart, actionable next steps, all in a matter of minutes. This results in fewer outages, faster recovery, and a continuous cycle of learning and prevention.

02 **Stopping vulnerabilities before they spread with embedded security insights**

Downtime isn't the only area where advanced RCA proves invaluable. For teams with more sophisticated analytics practices, RCA can be performed exactly where they consume critical insights or spot a particular trend. This is particularly applicable to IT security.

A comprehensive security dashboard is the heartbeat of modern IT security. By consolidating insights from SIEM solutions, firewalls, endpoint protection platforms, and IAM systems into a single pane of glass, these dashboards help teams maintain a strong security posture, plug vulnerabilities, and keep threat actors at bay.

360-degree security tracker



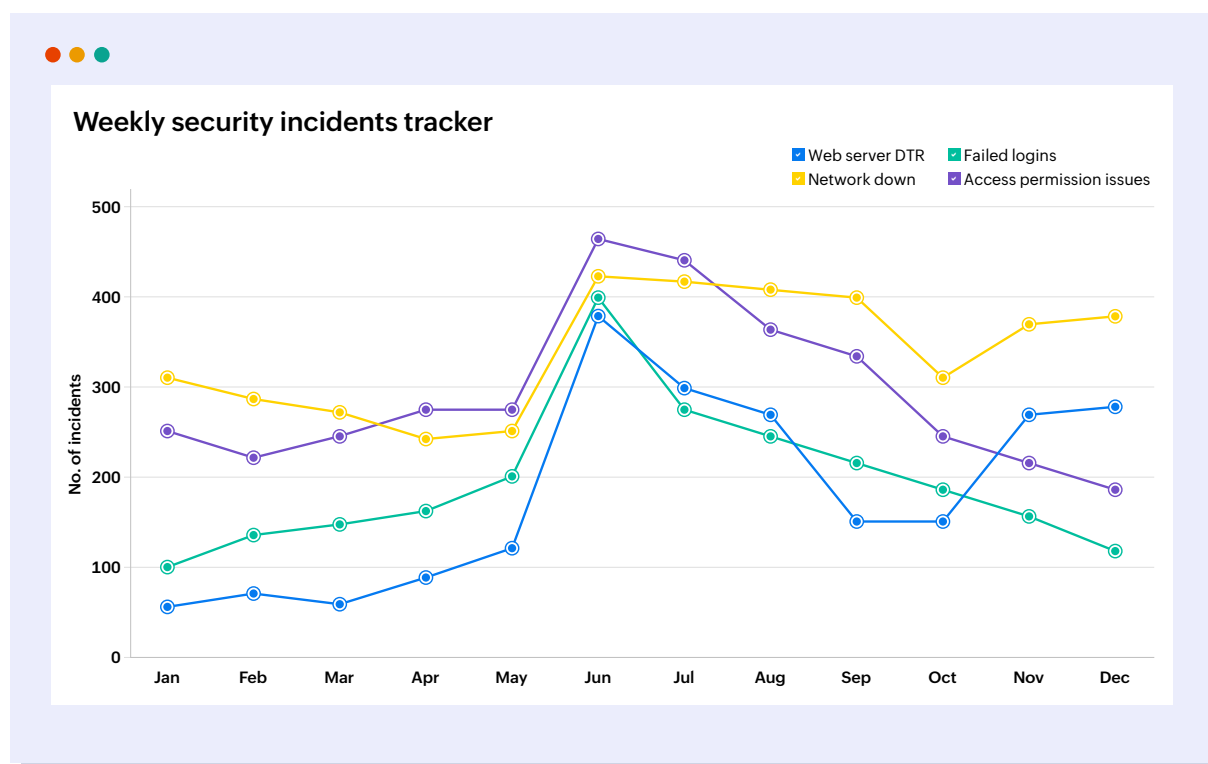
However, during a breach, traditional security dashboards fall short. Yes, they show clear indicators of a compromise—such as spikes in failed logins, unusual traffic surges, or abnormal data exfiltration. But when it comes to connecting the dots across hundreds of reports and isolating the true root cause, traditional RCA is slow, tedious, and often ineffective. In a moment when attackers are moving fast, the last thing security teams can afford is to waste time staring at reports, sifting through alerts, and manually stitching together patterns.

With embedded GenAI-powered summarization from Zia insights, security analysts and IT teams can change the game. Instead of manually sifting through a plethora of reports, this summarization layer provides instant, simplified visual and narrative insights into the key drivers that led to multiple breach indicators. This enables intuitive and actionable RCA directly within the dashboard.

Acting as a real-time investigation partner, Zia's powerful summarization layer accelerates security RCA by running real-time analyses over live security dashboards. They cut through the noise of metrics overload to surface evidence-backed insights and critical vulnerability indicators that matter most, without the analyst having to toggle between multiple systems.

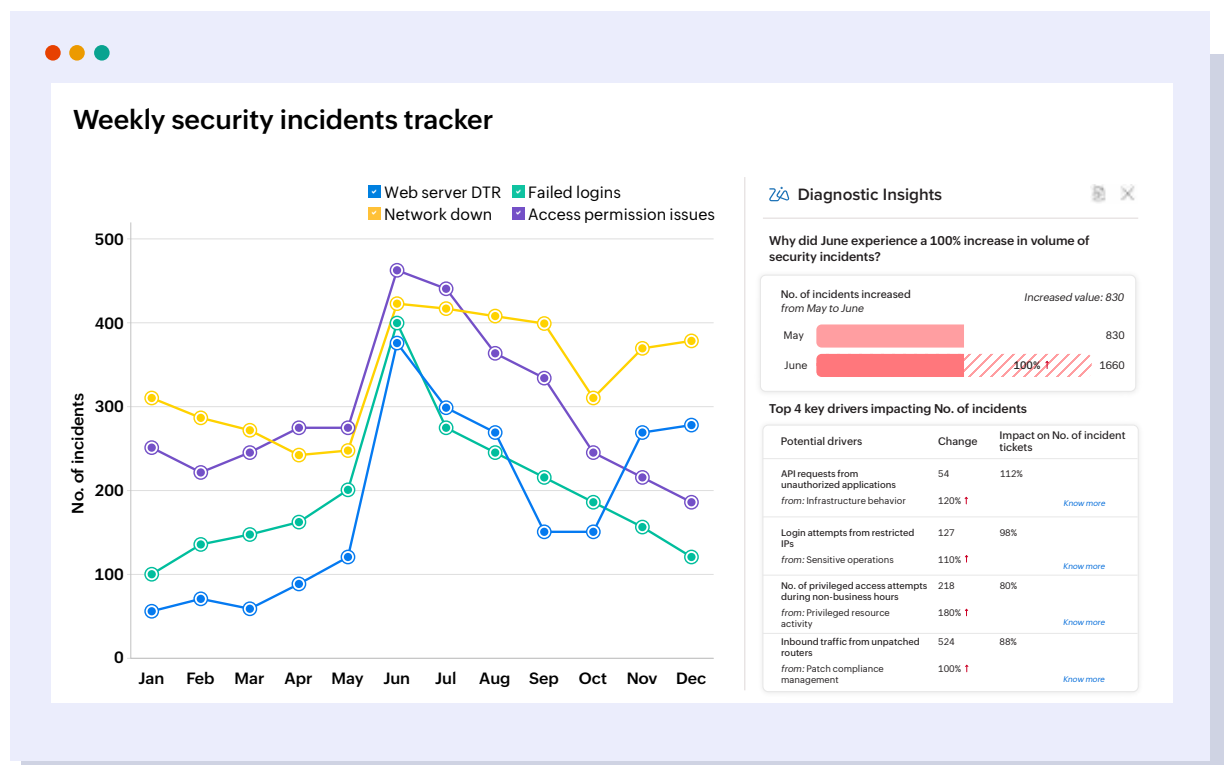
Consider the case of a multinational enterprise where a monthly trend analysis of service desk tickets revealed an alarming spike in:

- Web server data transfer rate (DTR)
- Failed logins
- Network down alerts
- Access permission issues



This points to a potential sophisticated attack, like a brute-force attack or credential stuffing, aimed at sensitive data exfiltration.

While the enterprise's security dashboard shows spikes in indicators like traffic volume, patch non-compliance, and login failures, it's impossible to filter out the driving factors for the vulnerabilities buried under a mountain of alerts and visualizations. In such scenarios, security teams can use key driver analysis in Zia insights to sift through the complex, crowded dashboard to uncover the underlying vulnerabilities responsible for the spike.



The visualization above uncovers the four key vulnerabilities driving the anomalous increase in volume security incidents during the month of June:

- **API requests from unauthorized applications:** Shadow IT or other unauthorized applications can be used by attackers to integrate with sensitive business resources through unapproved API calls. Such calls can result in an unusually high volume of inbound and outbound data, which causes the web server DTR to spike.
- **Login attempts from restricted IPs:** Attackers often try to access enterprise systems from IP addresses outside approved geographies or networks. These login attempts—whether credential stuffing, brute force, or probing attempts—are automatically rejected by authentication controls, leading to a sudden increase in failed login counts.
- **Privileged account misuse:** When access attempts from privileged accounts spike during non-business hours, the IAM policies often block these requests by design, resulting in access permission issues recorded in the service desk.
- **Unpatched network devices:** An unpatched router can become an entry point for malicious inbound traffic. Exploits targeting outdated firmware can flood the network with malicious packets or alter routing behavior, leading to network downtime.

Once vulnerabilities are identified through key driver analysis, teams can implement targeted defense strategies, such as:

- **Improved patch management:** Update security patches on all network devices. Up-to-date patches and regular patch cycles are a direct defense against routers being exploited as gateways for malicious traffic.
- **Better access controls:** Implement more stringent access protocols, and if necessary, restrict access to privileged accounts to minimize risk. Meticulously monitor all non-business hour operations across privileged accounts to stop potential breaches at their onset.

- **Shadow IT regulation:** Track the volume of unauthorized software installations per device. Evaluate their impact on the organization's security posture and impose stricter controls over subsequent installations while providing safer, approved alternatives.
- **Geo-blocking and multi-factor authentication:** Correlate login anomalies with user activity to spot both insider misuse and external attacks. Enforce IP allow and deny lists and pair this with adaptive multi-factor authentication that triggers extra authentication challenges for logins from suspicious regions or outside normal patterns.

What once required hours of manual analysis can be accomplished in a fraction of the time with the power of GenAI-driven analytics.

With Model Context Protocol (MCP) server support, available in advanced IT analytics applications like Analytics Plus, IT and security teams can transform data-backed insights into intelligent, actionable triggers. This automatically initiates corrective workflows—such as secure patch deployment, auditing, implementing regulated privileged access controls, and identifying and removing shadow IT—by connecting IT insights with targeted actions in relevant applications in a single, context-aware, closed-loop automation.

In short, AI-powered visual and textual insights in security dashboards and key driver analysis unravel the why behind any critical vulnerability. In the event of a breach, the MCP server expedites the restoration process and prevents further threat progression. Together, they transform security RCA into a closed-loop cycle of AI-driven detection, triaging, automated correction, and prevention, all with minimal to zero manual involvement.

Cracking the cause of service desk SLA violations with AI-driven contextual recommendations

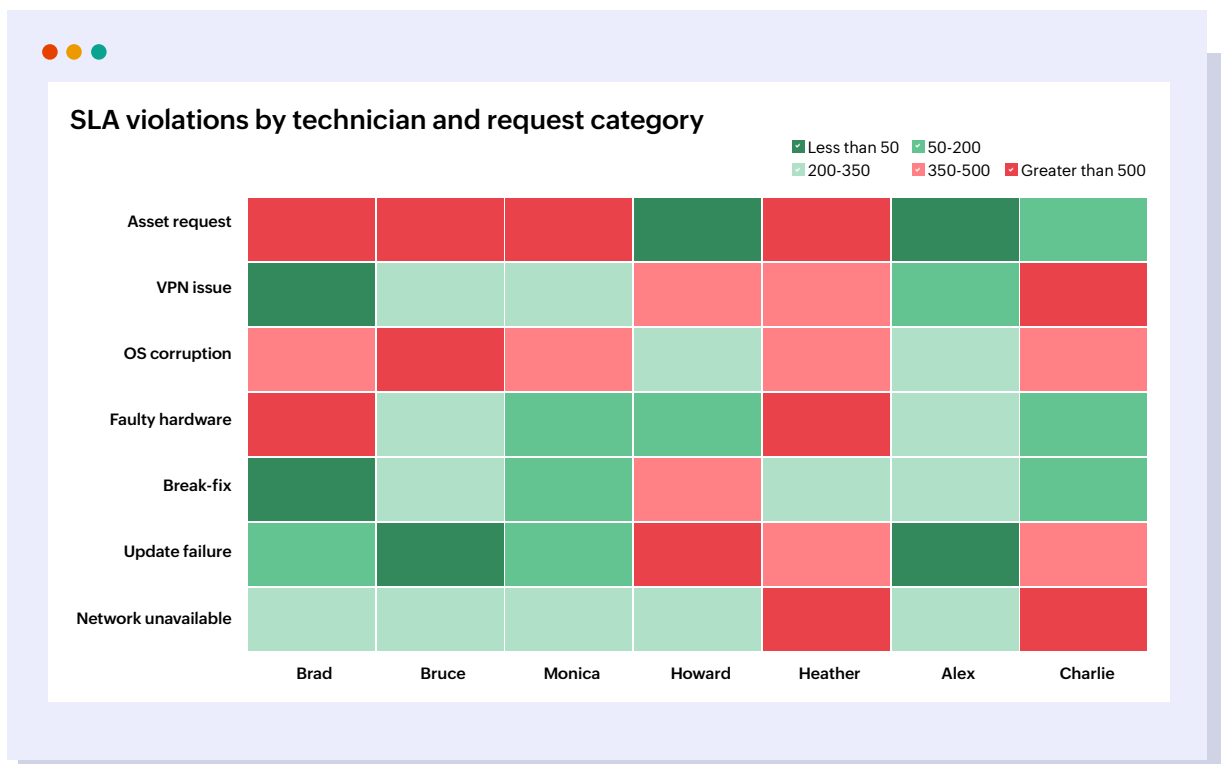
Evolving user needs have transformed IT service desks from simple issue resolution hubs into a frontline for fostering employee productivity and ensuring business continuity. In this context, a missed SLA or delayed resolution is more than an inconvenience—it creates ripple effects across departments, disrupts operations, and erodes trust in IT service management.

With thousands of tickets logged every week across categories, service desks face a daunting challenge: proactively identifying bottlenecks and systemic issues that lead to recurring SLA violations.

Traditional, manual RCA simply cannot keep pace. By the time trends are uncovered, ticket volumes may have multiplied, resulting in inefficient resolutions, technician burnout, and rising support costs. Worse still, manual analysis is often influenced by human bias, leading to inconsistent and incomplete insights.

Without rapid and effective RCA, recurring violations quickly escalate into operational disruptions that erode trust, reduce employee productivity, increase service costs, and negatively impact the bottom line.

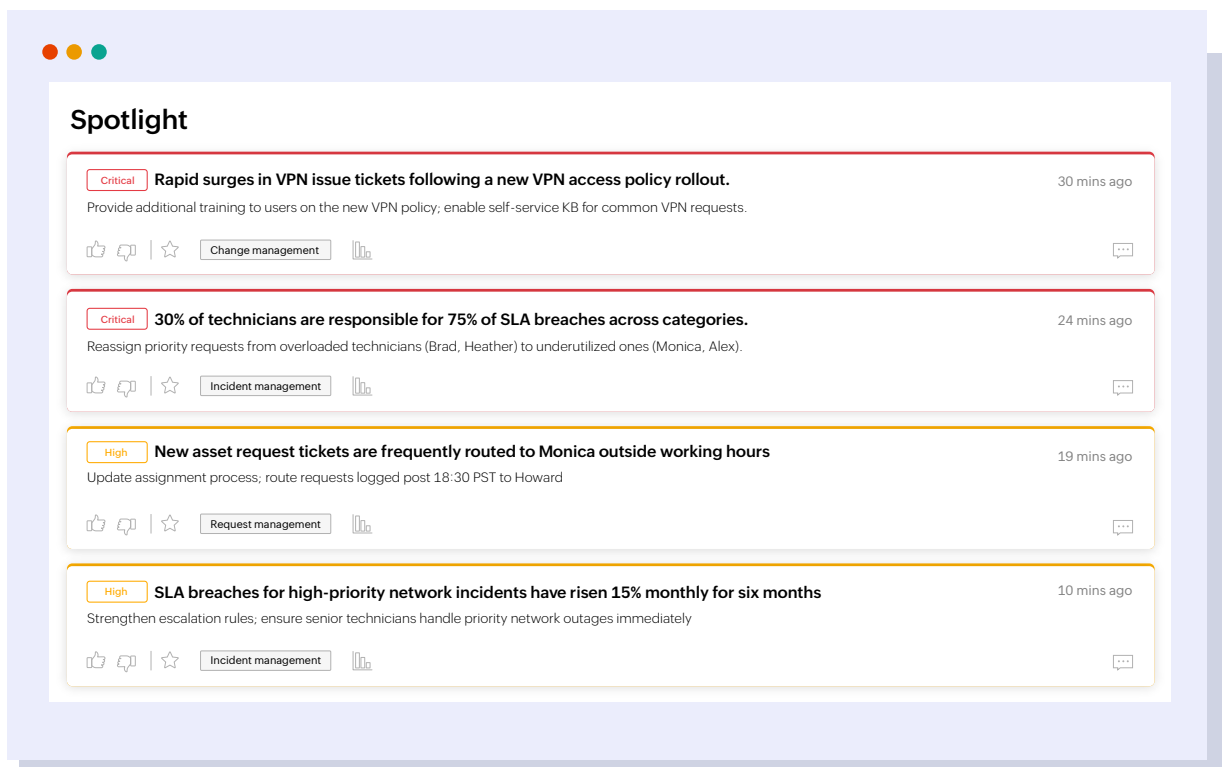
Consider the example of an enterprise service desk that processes over 10,000 tickets per month. A comprehensive analysis of monthly SLA violations by technician and request category over a six month period reveals worrying trends.



The visualization quickly highlights zones where certain technicians have contributed to an unacceptably high volume of SLA violations. For example, Bruce has consistently had high violations for OS corruption requests, while Monica has consistently violated SLAs for asset requests.

Manually dissecting technician workloads, ticket assignment policies, and ticket complexities of each request to uncover the underlying reasons for these violations would be impractical, if not impossible. This is where Spotlight, a contextual decision intelligence engine in ManageEngine Analytics Plus, makes all the difference.

Spotlight automatically monitors and analyzes the service desk's data over a period of time, identifying hidden bottlenecks and inefficiencies at both the technician and request category levels. It then presents data-driven recommendations to address them. Spotlight also categorizes these factors and dynamically assigns priorities based on their impact and criticality, seamlessly transforming data into actionable decisions in real time.



This snippet of Spotlight's recommendations highlights overall technician performance gaps, request categorization, and assignment inefficiencies identified from service desk data, pinpointing exactly where attention is needed. Spotlight then goes a step further by offering specific remediation suggestions, shortening the RCA cycle from weeks to minutes.

Spotlight makes RCA for SLA violations immediate and actionable. By correlating real-time technician and ticket data and translating these insights into prioritized, practical steps, it saves hours of manual investigation. It empowers IT managers with clear answers and actionable next steps to improve SLA compliance immediately. For enterprise service desks, this translates to a lower mean time to resolution, better accountability, higher efficiency, and improved user satisfaction—all of which foster trust between IT and the business.

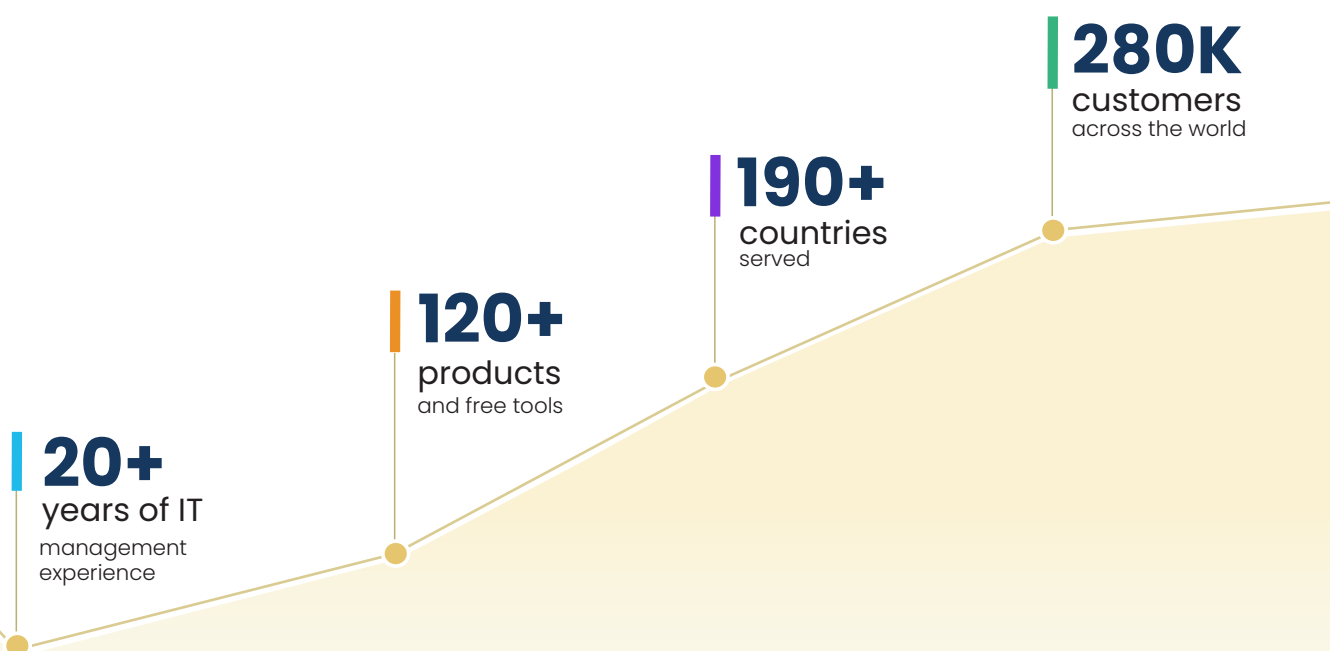
Conclusion

AI-powered analytics is transforming RCA, helping IT and security teams resolve incidents faster; prevent future breaches; and build a stronger, more resilient IT infrastructure. Embracing these GenAI-driven strategies empowers CIOs, IT managers, and SREs to move from firefighting to foresight and meet the scale and complexity demands of modern ITOps. By reducing downtime and eliminating vulnerabilities, GenAI-powered RCA turns every IT incident into an opportunity for proactive detection and continuous improvement.

About

ManageEngine Analytics Plus is an IT analytics and decision intelligence solution designed to provide organizations with a unified view of their IT operations, correlate interdependencies and derive meaningful insights. It breaks down data silos by consolidating both on-premises and cloud infrastructure KPIs. Analytics Plus measures the efficiency of network operations, tracks the responsiveness and availability of business applications, evaluates technician performance, assesses the progress of processes and flags security anomalies. This comprehensive analysis is achieved by connecting to all IT software that forms the backbone of an IT infrastructure. These consolidated insights enable organizations to make data-driven decisions that enhance operational efficiency and drive business success.

For more information about Analytics Plus,
visit: www.manageengine.com/analytics-plus/



Reference

1. https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf
2. <https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec>



© ManageEngine, a division of Zoho Corporation