



How to harness AI to streamline your IT operations

Simplify operations, boost uptime, and
secure IT with AI: A practical guide from
ManageEngine

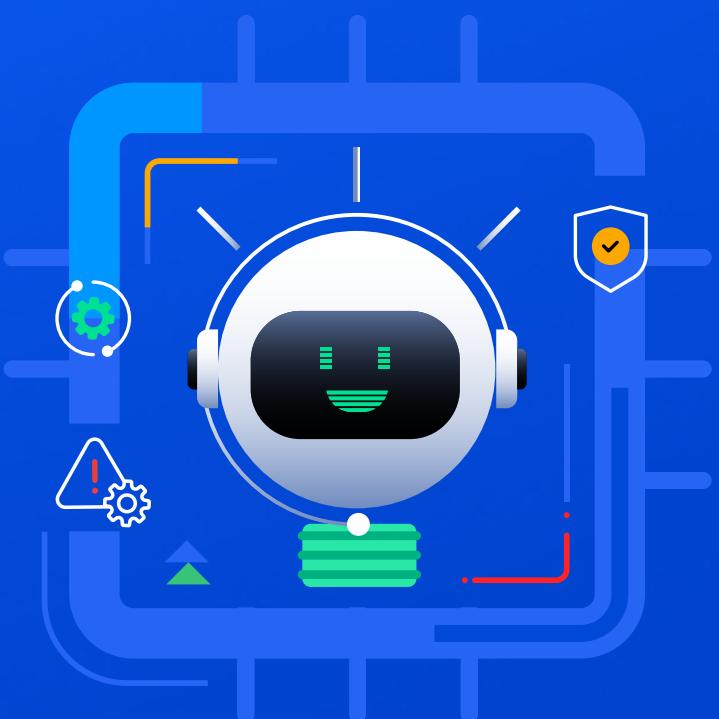
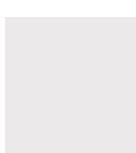


Table of Contents

AI in IT: From buzzword to business value	03
ManageEngine AI: Smarter, simpler, more secure	04
Zia, our AI powerhouse	07
How AI powers our solutions	09
AI in action	10
AI in USM	11
AI in SIEM	24
AI in IAM	29
AI in ITOM and observability	36
AI in UEMS	48
AI in IT analytics	56
AI in low-code application development	63
Secure, explainable, yours: ManageEngine's approach to AI	68
The ManageEngine AI advantage	71
More about ManageEngine	73



AI in IT: From buzzword to business value

Today, everyone seems eager to jump on the AI bandwagon, which is fueled by a mix of hype and genuine potential. From an IT management perspective, it's crucial for organizations to look beyond the buzz and truly understand the transformative value of AI.

Making IT operations smarter with AI

AI has transcended its experimental origins to become a strategic tool for IT organizations worldwide. Its integration is no longer a mere technological enhancement but a fundamental shift in how IT departments operate and deliver value.

By harnessing these capabilities, AI is transforming how IT teams operate, empowering them to optimize infrastructure, align operations with business goals, and move from reactive management to proactive innovation. By automating repetitive tasks, AI reduces operational costs and accelerates service delivery. Predictive analytics enhance incident detection, maintenance scheduling, and resource optimization, while AI-driven monitoring enables IT teams to efficiently manage growing volumes of traffic and security threats. Combined with data-driven insights and advanced analytics, AI helps organizations make smarter decisions, optimize infrastructure usage, and drive measurable business outcomes.



ManageEngine AI: Smarter, simpler, more secure

At ManageEngine, we see AI as a catalyst for meaningful business transformation. For more than 13 years, we've been advancing AI and ML to deliver real-world value. We've refined and embedded these technologies seamlessly across our portfolio, from service management and cybersecurity to endpoint management. By integrating AI deeply into our IT management solutions not as an add-on, but as a core capability, we empower organizations to harness its full potential.

Our vision is to make IT smarter, operations simpler, and business environments more secure, enabling enterprises to achieve scalability, resilience, and success in today's complex digital landscape.



“

ManageEngine's emphasis on owning its AI stack and maintaining control over data reflects a broader trend in enterprise technology that prioritizes transparency, privacy, and explainability.

For enterprises, this is not just a matter of innovation but of accountability, as controlling data flows and model behavior enables the development of AI systems that are explainable, privacy-conscious, and aligned with governance and compliance needs.



Alejandro Leal

Senior Analyst, KuppingerCole



“

Privacy isn't an afterthought at ManageEngine; it is integral to how we design and deploy AI.

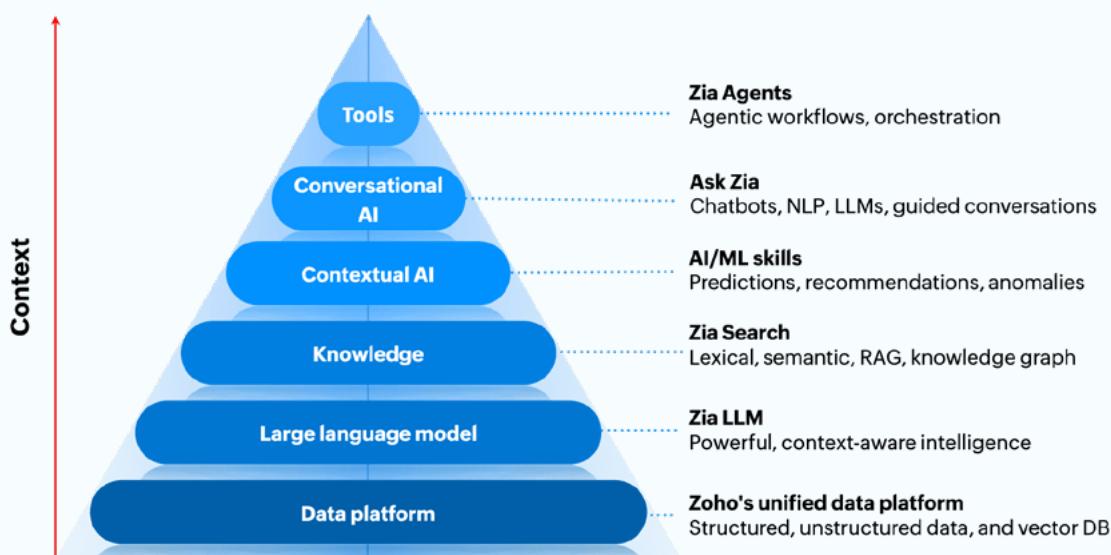
Your data and models remain exclusively yours, while privacy-bound AI is seamlessly integrated into contextual features that enable secure, intelligent innovation.



Sujatha S Iyer
Head of AI Security, ManageEngine

Zia, our AI powerhouse

Zia is ManageEngine's AI powerhouse, designed to transform IT management from reactive to proactive. By harnessing ML, natural language processing (NLP), semantic search, and large language models (LLMs), Zia empowers IT leaders to anticipate issues, automate operations, and strengthen resilience. Acting as a unified layer of intelligence across ManageEngine's platform, Zia helps organizations reduce risk, boost efficiency, and deliver seamless digital experiences at scale.



Zia Agents are self-sufficient, AI-powered bots designed to think, learn, and act smartly. Using semantic search, retrieval-augmented generation (RAG), and knowledge graphs, they deliver precise, human-like experiences resolving queries, uncovering insights, and guiding users with intelligence and ease.

Ask Zia combines the capabilities of chatbots, NLP, and LLMs to deliver natural, human-like conversations that make data and insights instantly accessible. With guided dialogues and contextual intelligence, it simplifies complex queries, enabling teams to decide faster, resolve smarter, and engage customers better.

Zia Skills empower IT with a comprehensive suite of AI and ML capabilities designed to predict, analyze, and act intelligently. From forecasting trends and detecting anomalies to NLP, sentiment analysis, and workflow automation, Zia seamlessly blends data-driven insights with contextual intelligence.

Zia Search combines lexical, semantic, RAG, and knowledge graph approaches to deliver enterprise-grade search. By uniting keyword precision, semantic understanding, AI-powered contextual answers, and relationship-driven insights, it ensures users can find not just exact matches but also the most relevant, connected knowledge across the organization.

Zia LLM is Zoho's proprietary LLM, engineered from the ground up to deliver powerful, context-aware intelligence across our entire suite of applications. It runs securely on Nvidia GPUs within our private data centers.

Zoho's vision for a unified data platform is to bring enterprise data from all applications, sources, and formats into a single governed, AI-ready environment, breaking down silos across operational, analytical, and AI workloads to enable seamless integration and governance.

How AI powers our solutions

Our AI capabilities have been purposefully developed in-house to address specific IT needs.

Grammar correction	Translation	Parsers	Language detection	Voice assistant	Keyword extraction
Sentiment analysis	Handwriting recognition	Product recommendation	Icon recommendation	NLP report generation	Data cleaning
Domain name recommendation	Chatbots	Zia search	Ask Zia	Report narration	Conversational analytics
Language prediction	Image parsing	Bin packing analysis	Phishing detection	Malicious file detection	Bot detection
Captcha	Anomalous behavior	Forecasting	Root cause analysis	Log analysis	Outage prediction
Trend detection	Seasonality detection	Classifiers	OCR	Facial recognition	Object detection
Scanning itemized receipts	Few-shot recognition	Lead enrichment	Macro suggestion	KB article recommendation	Adaptive MFA

Here's the breadth of AI capabilities across our solutions.



Note: Some capabilities are a work in progress.

AI
in action

AI in USM

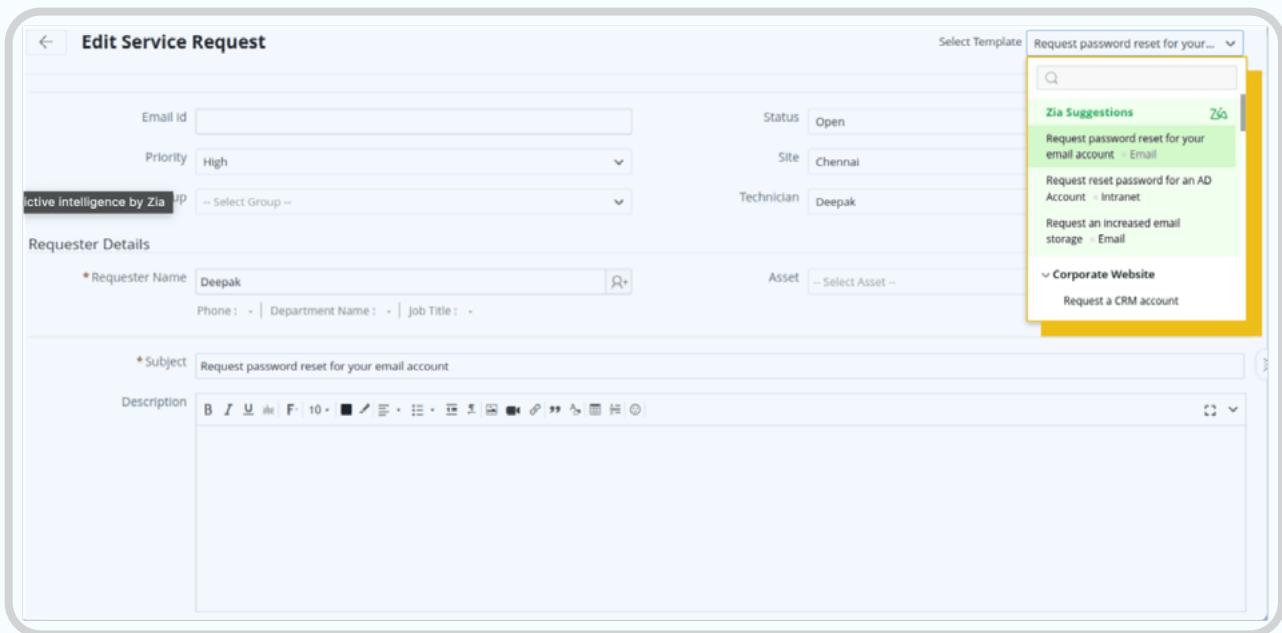
AI is transforming IT operations by intelligently connecting people, processes, and data. In unified service management (USM), AI acts as an ever-present assistant, providing users instant support, enabling technicians to resolve incidents efficiently, and empowering process owners to make proactive, data-driven decisions.



Deliver faster support and intelligent self-service

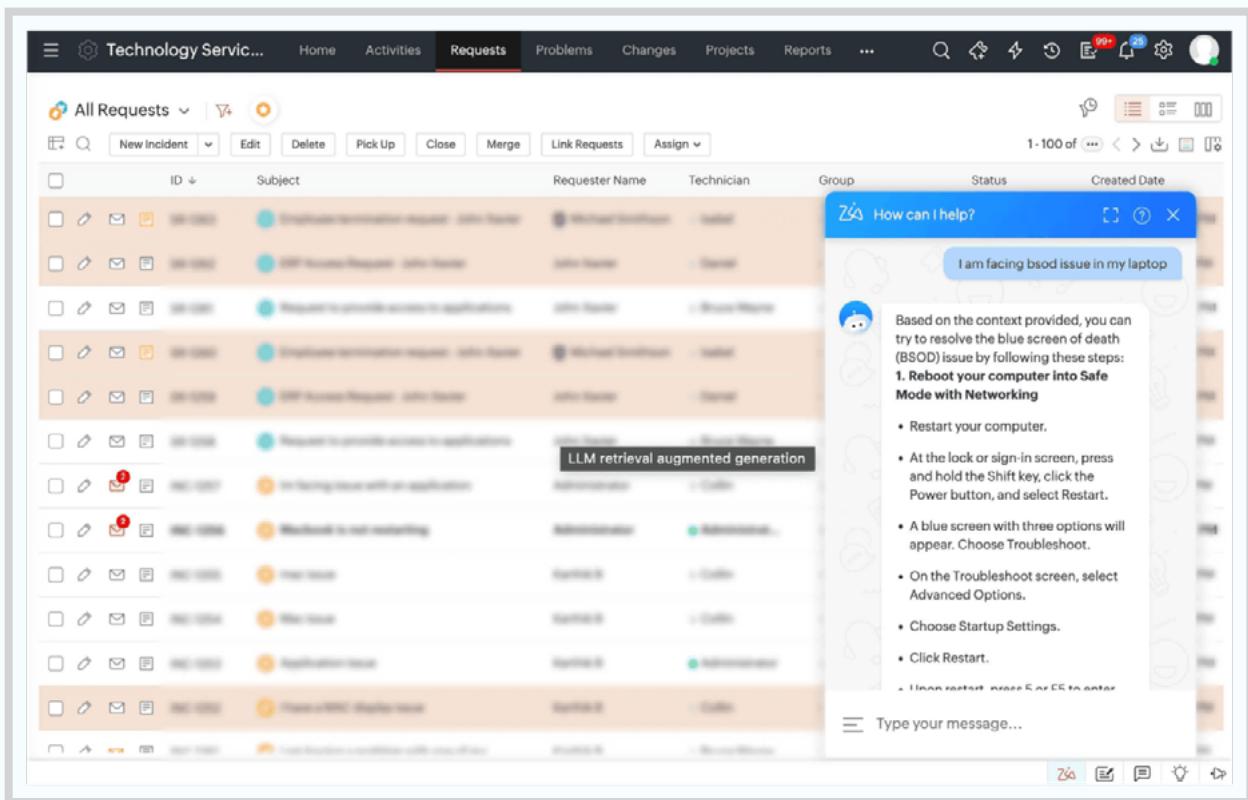
AI is making IT support frictionless and intuitive by providing instant, intelligent help.

Employees no longer need to search across multiple systems or submit long forms to get what they need. With **intelligent public and private knowledge search powered by GenAI**, employees can find accurate, contextual solutions drawn from both internal documentation and trusted external sources. Whether they're seeking how-to guides, configuration steps, or policy clarifications, AI retrieves the most relevant answer in seconds.



The screenshot shows a 'Edit Service Request' interface. On the right, a sidebar titled 'Request password reset for your...' displays 'Zia Suggestions' with several options: 'Request password reset for your email account' (Email), 'Request reset password for an AD Account' (Intranet), and 'Request an increased email storage' (Email). Below this is a section for 'Corporate Website' with the option 'Request a CRM account'. The main form includes fields for 'Email Id', 'Priority' (High), 'Status' (Open), 'Site' (Chennai), 'Technician' (Deepak), and 'Asset' (dropdown). Under 'Requester Details', there is a 'Requester Name' field with 'Deepak' entered, and dropdowns for 'Phone', 'Department Name', and 'Job Title'. The 'Subject' field contains 'Request password reset for your email account'. The 'Description' field is a rich text editor with a toolbar. The overall interface is clean and modern, with a light blue header and a white background.

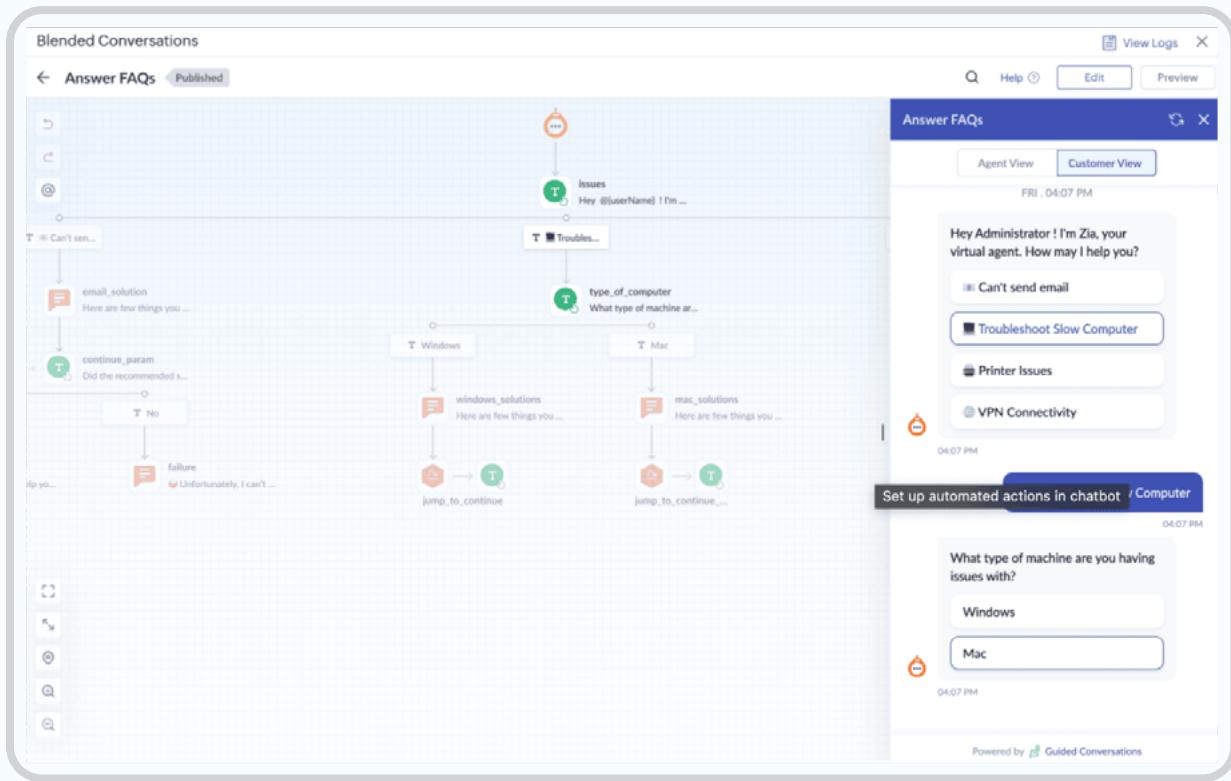
Recommend appropriate templates to your requesters.



Provide users contextual recommendations by extracting key information from solution articles in the knowledge base using Zia's RAG.

Through **automated yet human-like conversation flows**, Zia provides personalized assistance via text or voice, handling everything from password resets to complex multi-step service requests by understanding context, intent, and sentiment. These conversational experiences extend across web, mobile, and voice interfaces, ensuring consistent support no matter where employees engage.





Build intuitively flowing conversations that guide employees with predefined questions, replies, and automated actions.

What makes Zia's ecosystem truly powerful is its flexibility of intelligence sources. Organizations can choose between Zia's enterprise-tuned LLM, ManageEngine's native private model, or public LLMs such as ChatGPT or Azure OpenAI, depending on compliance needs and data preferences.



The screenshot shows the Zia Solution Generator interface. At the top, it says "Zia Solution Generator" and "Powered by ChatGPT" with a close button. The "Prompt" section contains the text "Facing printer issues." Below it is a "Generated Solution" section. The solution is titled "Troubleshooting Common Printer Issues" and includes a "Content" block with a detailed list of troubleshooting steps for printer issues. The "Content" block ends with a note that the text is generated by "AI solution generator". Below the content is a "Keywords" section listing terms like "printer", "troubleshooting", "issues", "paper jams", "print quality", "connectivity problems", "slow printing", and "error messages". At the bottom of the solution section are two buttons: "Change Length" and "Change Type". At the very bottom of the interface are "Add Generated Solution" and "Cancel" buttons.

Generate structured, ready-to-use solutions with simple natural language prompts.

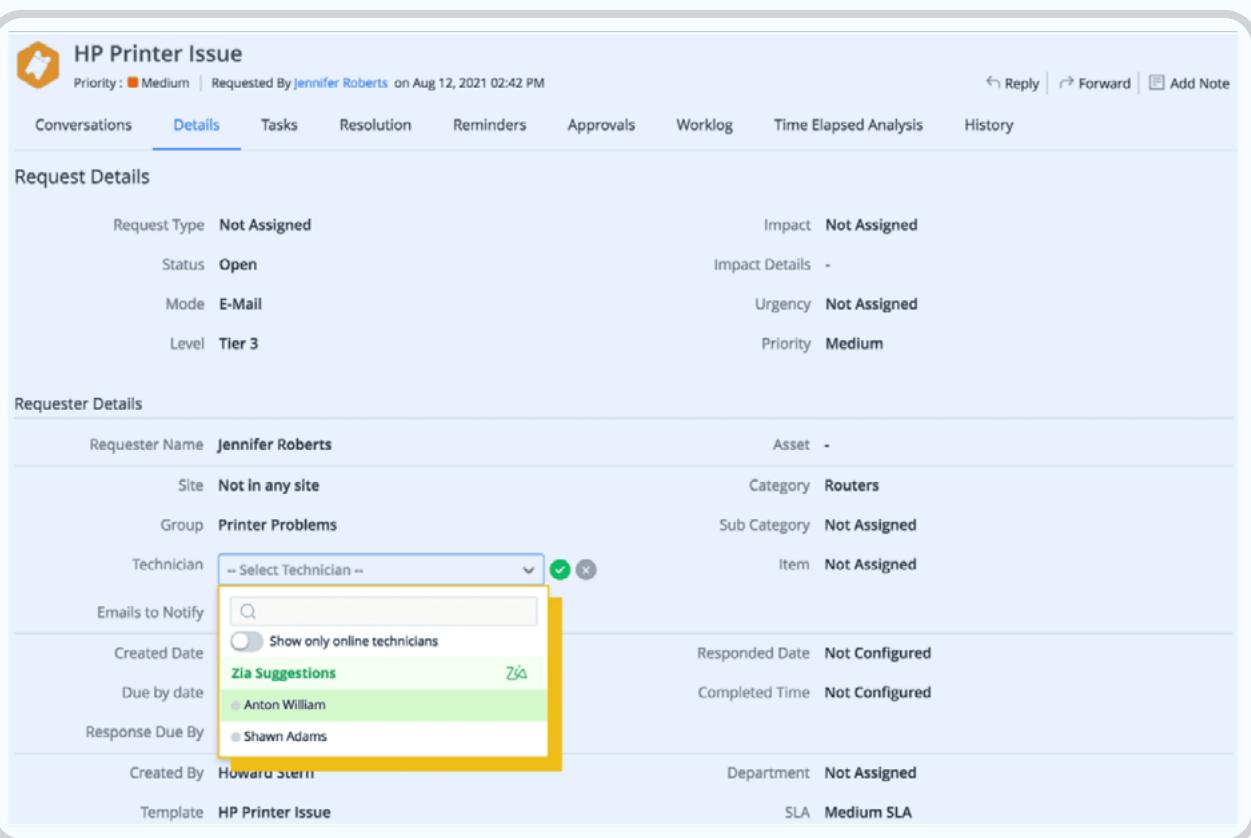
Additionally, Zia can perform ticketing actions directly within the chat, enabling employees to create, update, or close requests without leaving the conversation. Even quick report generation is possible through contextual search, allowing employees or managers to view status updates or service metrics instantly.

The result? Higher satisfaction, reduced ticket volume, and a culture of self-service empowerment that scales effortlessly.

Drive faster resolutions with intelligent insights

For IT technicians, AI becomes an intelligent partner that streamlines operations, surfaces insights, and automates time-consuming tasks.

Through intelligent triage and routing, incoming tickets are automatically categorized, prioritized, and assigned to the right technician, cutting down response times dramatically.



The screenshot shows a ticket detail page for an 'HP Printer Issue'. The top navigation bar includes 'HP Printer Issue', 'Priority: Medium', 'Requested By Jennifer Roberts on Aug 12, 2021 02:42 PM', and buttons for 'Reply', 'Forward', and 'Add Note'. Below the navigation is a tabs section with 'Conversations', 'Details' (which is selected and underlined), 'Tasks', 'Resolution', 'Reminders', 'Approvals', 'Worklog', 'Time Elapsed Analysis', and 'History'. The main content area is divided into 'Request Details' and 'Requester Details'. In the 'Requester Details' section, there is a 'Technician' field with a dropdown menu titled 'Select Technician'. A modal window titled 'Zia Suggestions' is displayed, showing two options: 'Anton William' and 'Shawn Adams', with 'Anton William' highlighted. Other fields in the 'Requester Details' section include 'Requester Name: Jennifer Roberts', 'Site: Not in any site', 'Group: Printer Problems', 'Emails to Notify' (empty), 'Created Date' (empty), 'Due by date' (empty), 'Response Due By' (empty), 'Created By: Howard Stern', 'Template: HP Printer Issue', 'Asset' (empty), 'Category: Routers', 'Sub Category: Not Assigned', 'Item: Not Assigned', 'Item' (empty), 'Responded Date: Not Configured', 'Completed Time: Not Configured', 'Department: Not Assigned', and 'SLA: Medium 5LA'.

Put the right technician to work with intelligent routing predictions.

Anticipate priorities based on relevant ticket attributes.

With **instant ticket conversation summaries**, Zia ensures that technicians have a concise understanding of context before diving into long email chains or chat transcripts.

Reopen tickets and greenlight requests by letting Zia interpret email replies.



The screenshot shows a ticket detail page for an 'Incident Request'. The ticket has a 'Major lifecycle' and is 'Not Assigned'. It includes sections for Conversations, Details, Tasks, Checklists, Resolution, Reminders, Approvals, Worklog, and Actions. A 'Sentiment analysis using Zia' card is displayed, showing a positive sentiment with a smiley face icon. The card also displays a summary of the last conversation and overall sentiment (50% neutral).

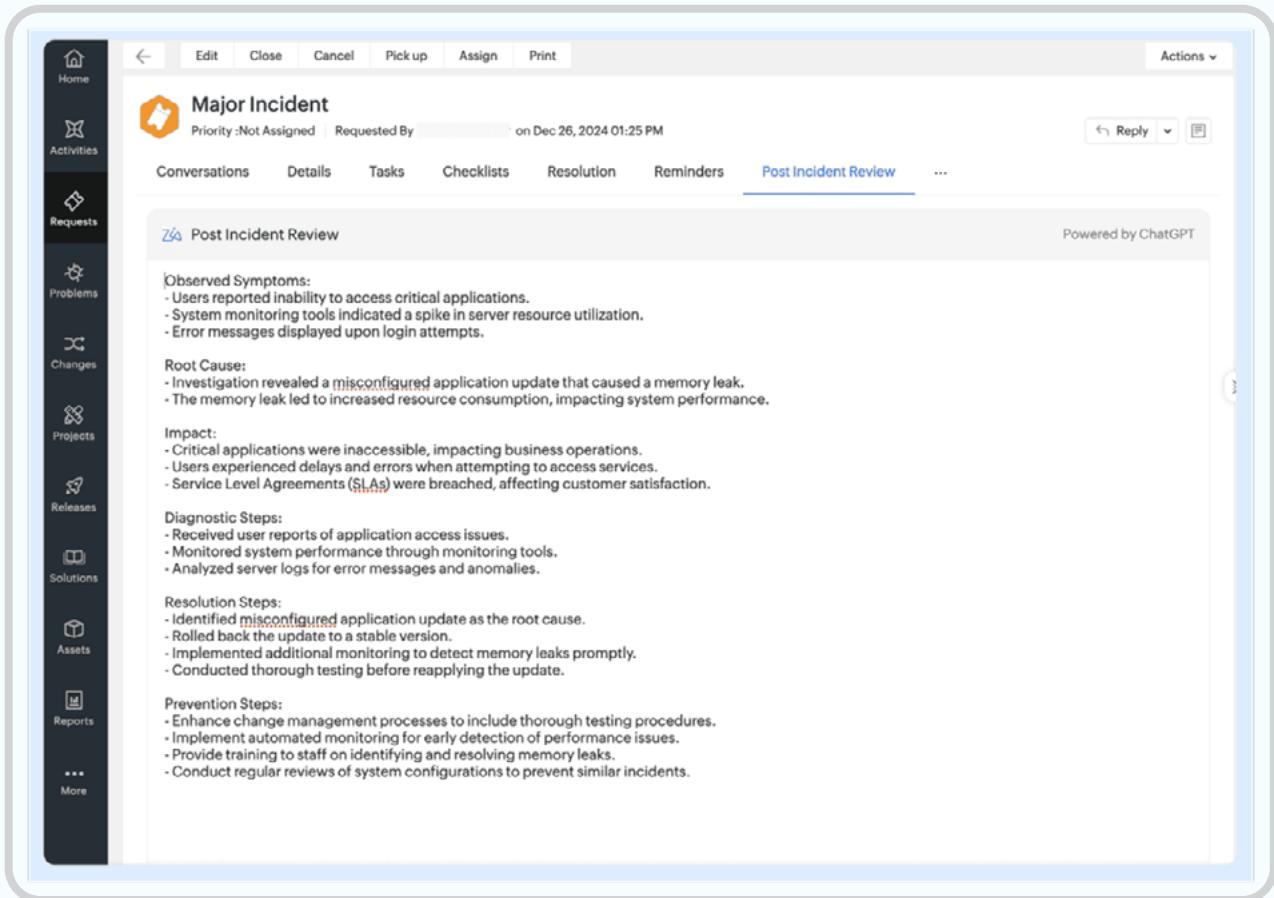
Take appropriate ticketing actions by understanding end-user emotions with sentiment

The screenshot shows the Zia AI interface with a chart titled 'Insights from Zia chatbot'. The chart displays the trend of incoming and escalated requests from January 2021 to October 2022. The Y-axis represents the number of requests, and the X-axis represents the months and years. The chart includes a trend line and two data series: 'Total Incoming requests' (blue line) and 'Total Escalated requests' (green line). A 'Chart Information' box provides details about the data and formulas used. The interface also includes a sidebar with various options like Create, Ask Zia, and Data Sources.

Get to insights faster by letting Zia extract meaningful data from tickets.



Once an incident is resolved, AI can draft comprehensive post-incident reviews, documenting the resolution path, root cause, and lessons learned automatically.



The screenshot shows a software interface for managing incidents. On the left is a vertical sidebar with icons and labels for Home, Activities, Requests, Problems, Changes, Projects, Releases, Solutions, Assets, Reports, and More. The main content area is titled 'Major Incident' and shows a 'Post Incident Review' section. The review details include:

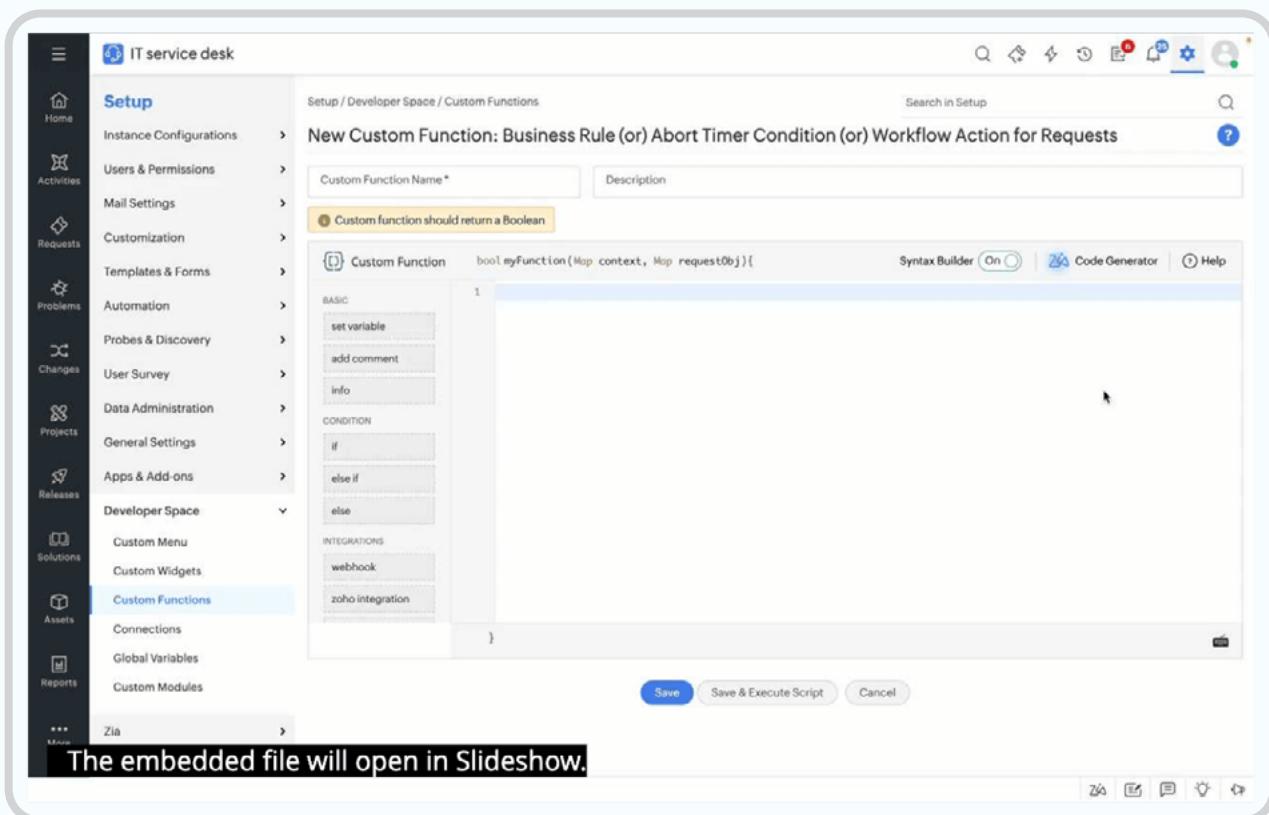
- Observed Symptoms:**
 - Users reported inability to access critical applications.
 - System monitoring tools indicated a spike in server resource utilization.
 - Error messages displayed upon login attempts.
- Root Cause:**
 - Investigation revealed a misconfigured application update that caused a memory leak.
 - The memory leak led to increased resource consumption, impacting system performance.
- Impact:**
 - Critical applications were inaccessible, impacting business operations.
 - Users experienced delays and errors when attempting to access services.
 - Service Level Agreements (SLAs) were breached, affecting customer satisfaction.
- Diagnostic Steps:**
 - Received user reports of application access issues.
 - Monitored system performance through monitoring tools.
 - Analyzed server logs for error messages and anomalies.
- Resolution Steps:**
 - Identified misconfigured application update as the root cause.
 - Rolled back the update to a stable version.
 - Implemented additional monitoring to detect memory leaks promptly.
 - Conducted thorough testing before reapplying the update.
- Prevention Steps:**
 - Enhance change management processes to include thorough testing procedures.
 - Implement automated monitoring for early detection of performance issues.
 - Provide training to staff on identifying and resolving memory leaks.
 - Conduct regular reviews of system configurations to prevent similar incidents.

At the bottom right of the review section, it says 'Powered by ChatGPT'.

Draft comprehensive post-incident reviews.

As knowledge builds, **Zia instantly generates reusable artifacts** including how-to documents, known error records, and solution templates that feed back into the knowledge base to improve future efficiency.

When automation is needed, Zia provides a **low-code console for custom actions**, where technicians can generate code for bespoke automations in seconds. This allows teams to rapidly build or modify workflows, like automatically reassigning tickets, restarting services, or updating assets, without writing extensive code.



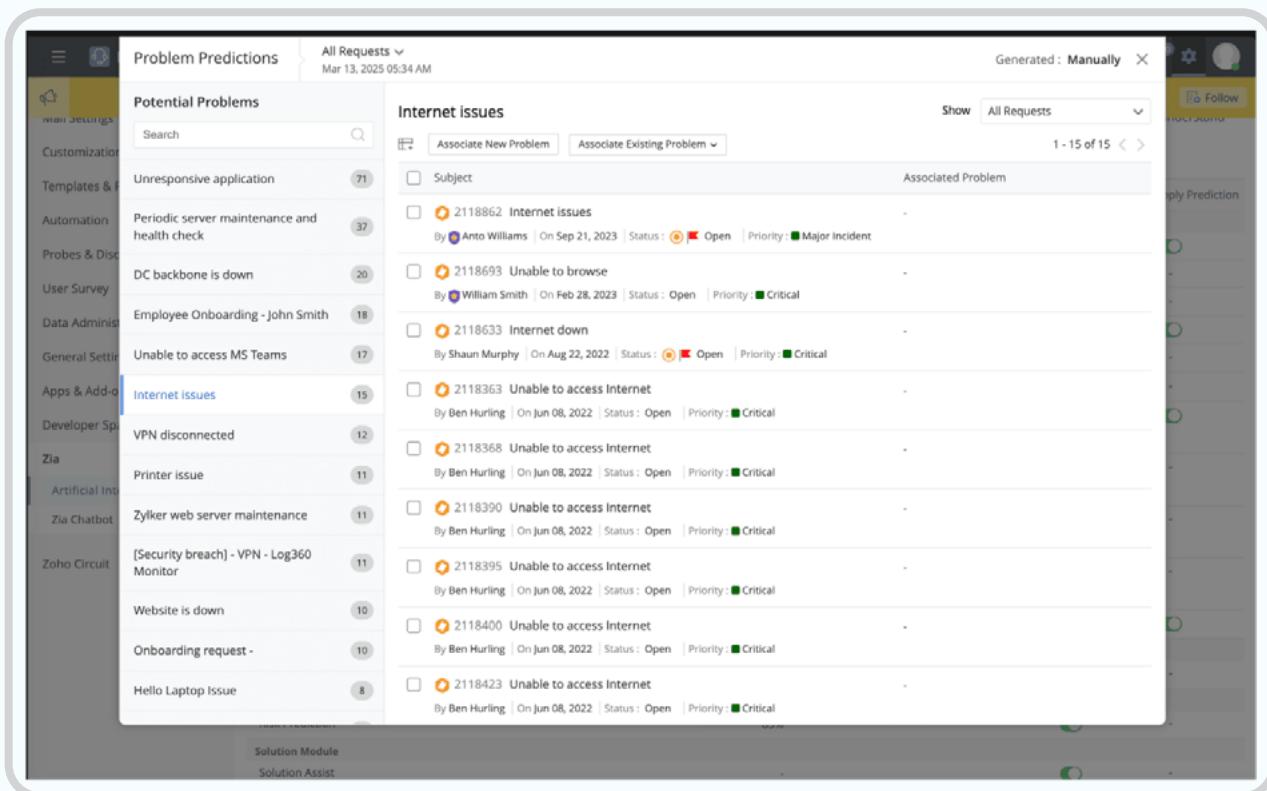
Prompt and generate low-code custom functions in Deluge.

Moreover, because AI is now integrated across channels, technicians can trigger ticketing actions, asset updates, or service approvals directly through chat, blending human oversight with intelligent automation.

With these features, AI transforms IT teams from reactive troubleshooters into **data-driven problem solvers**.

Strengthen IT operations with proactive intelligence and predictive control

For IT leaders, AI delivers a new level of predictive visibility and strategic control. By applying incident clustering, AI uncovers hidden correlations across tickets, revealing recurring issues before they snowball into major outages.



The screenshot shows a software interface for managing IT operations. The main window is titled 'Problem Predictions' and 'All Requests' (Mar 13, 2025 05:34 AM). The interface is generated manually. On the left, there's a sidebar with various settings and customization options. The main panel shows a list of 'Potential Problems' under 'Internet issues'. The list includes:

- Unresponsive application (71)
- Periodic server maintenance and health check (37)
- DC backbone is down (20)
- Employee Onboarding - John Smith (18)
- Unable to access MS Teams (17)
- Internet issues (15)
- VPN disconnected (12)
- Printer issue (11)
- Zylker web server maintenance (11)
- [Security breach] - VPN - Log360 Monitor (11)
- Website is down (10)
- Onboarding request - (10)
- Hello Laptop Issue (8)

For each item in the list, there's a checkbox labeled 'Subject' and a link to the ticket details. The ticket details include the subject, created by, creation date, status (Open), priority (Major Incident, Critical), and a brief description. The interface also includes a 'Follow' button and a 'Reply Prediction' button.

Identify potential problems by having Zia analyze incident trends.

Change risk prediction enables data-backed decision-making by flagging potentially risky changes before they impact business systems.



The screenshot shows the 'New Change' form in the Zia AI platform. The 'Change Risk' field is currently selected, displaying a dropdown menu with 'Zia Suggestions' for 'High' and 'Medium' risk levels. A yellow box highlights this dropdown. The form also includes fields for Change Requester, Change Type, Retrospective, Impact, Urgency, Priority, Change Risk, Site, Group, Change Owner, Change Manager, Stage, Status, Status Comment, CSI Section, Category, Item, Scheduled Start, Services Affected, Assets Involved, and Reason for Change.

Drive successful changes with intelligent change risk predictions.

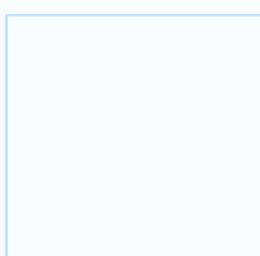
AI also detects and automates asset receipts from emails, eliminating a common manual cost while improving accuracy in inventory and asset management.

When customization is needed, **Zia's low-code console** provides flexibility to integrate new automations or monitoring workflows that are supported by AI-generated code snippets that accelerate rollout.

Process owners also benefit from **AI-driven insight generation**, where Zia extracts key metrics and generates **quick reports through contextual prompts**, allowing leaders to understand ticket trends, SLA compliance, and change success rates in natural language.

In parallel, **Zia's multi-model intelligence** (integrated with Zia LLM, ManageEngine LLM, or trusted public models) ensures that organizations can tailor their AI strategy according to data sensitivity and performance needs without compromising compliance or control.

The outcome is **reduced risk, smarter planning**, and a stronger, more resilient IT ecosystem.



AI in SIEM

AI is revolutionizing cybersecurity by transforming how organizations detect, investigate, and respond to threats. ManageEngine Log360, our unified security information and event management (SIEM) platform, empowers security teams to move faster and smarter by streamlining analysis, enriching context, and accelerating response to evolving attacks.



Log360 goes beyond static correlation rules by using ML and behavioral analytics to identify subtle patterns that signal emerging threats. These systems continuously learn what normal activity looks like across the environment, enabling them to detect anomalies such as insider threats, credential misuse, or zero-day exploits. This adaptive, behavior-based approach enhances detection accuracy and minimizes false positives, allowing analysts to focus on what truly matters.

For specialized log management and compliance monitoring, EventLog Analyzer applies AI to automate the collection, parsing, and analysis of log data from diverse sources. It uses ML to baseline normal log patterns, automatically identify anomalies that indicate security or compliance risks, and generate intelligent audit reports for regulations like the PCI DSS, HIPAA, and the GDPR.

By correlating events, AI turns data overload into actionable insights. It automatically maps security alerts to frameworks like MITRE ATT&CK®, giving analysts clear visibility into the tactics and techniques behind attacks for richer, contextual understanding.

AI further accelerates investigations by summarizing complex incidents in natural language, visualizing attack timelines and offering data-driven remediation guidance. Through automation and GenAI-powered insights, the SIEM can triage alerts, prioritize high-risk events, and guide security teams toward faster, more effective resolutions.



AI transforms SIEM from a reactive monitoring tool into an intelligent, proactive defense system—one that empowers organizations to stay ahead of threats with clarity, speed, and confidence.

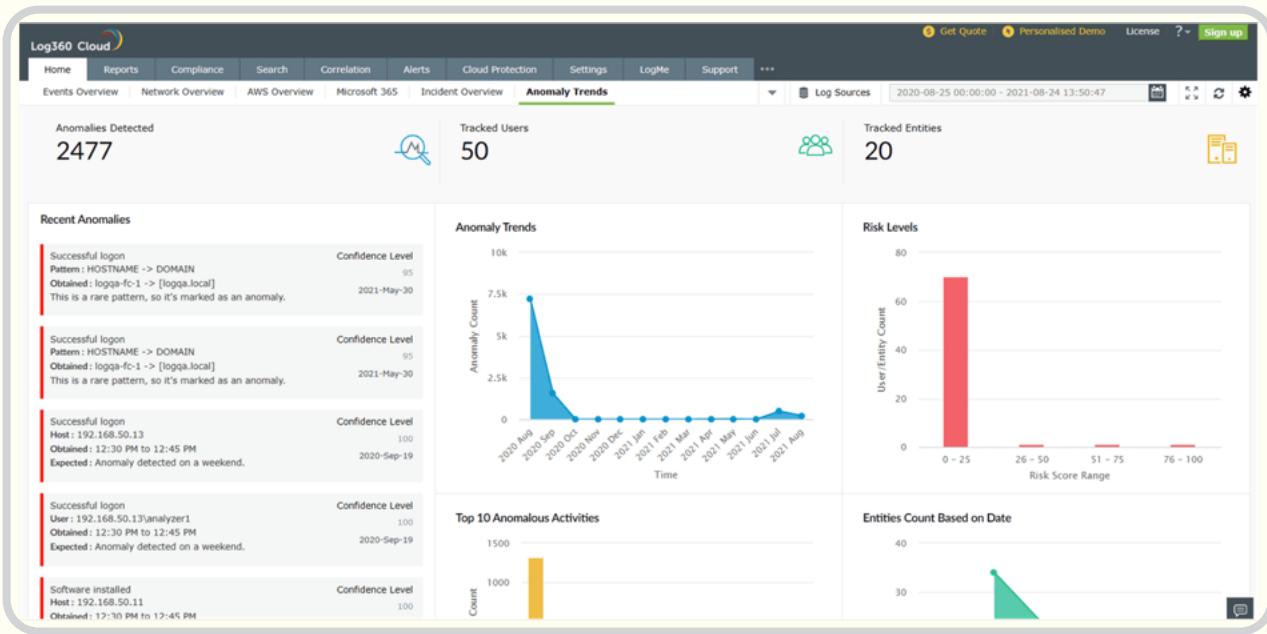
Stay ahead with smarter detection and proactive defense

With Log360's **UEBA engine**, AI becomes a vigilant analyst that continuously learns normal behavior and identifies anomalies in real time.

By profiling users and entities across login patterns, access behavior, and location trends, it establishes **dynamic baselines** to detect threats such as **lateral movement, privilege abuse, and impossible travel**.

Each user and entity is assigned a **risk score**, enabling teams to instantly spot high-risk behavior in context. By **grouping related anomalies** and **prioritizing alerts** based on severity, our SIEM solution reduces alert fatigue and helps analysts **investigate faster and respond smarter**.





Anomaly trends

Make better decisions with contextual intelligence

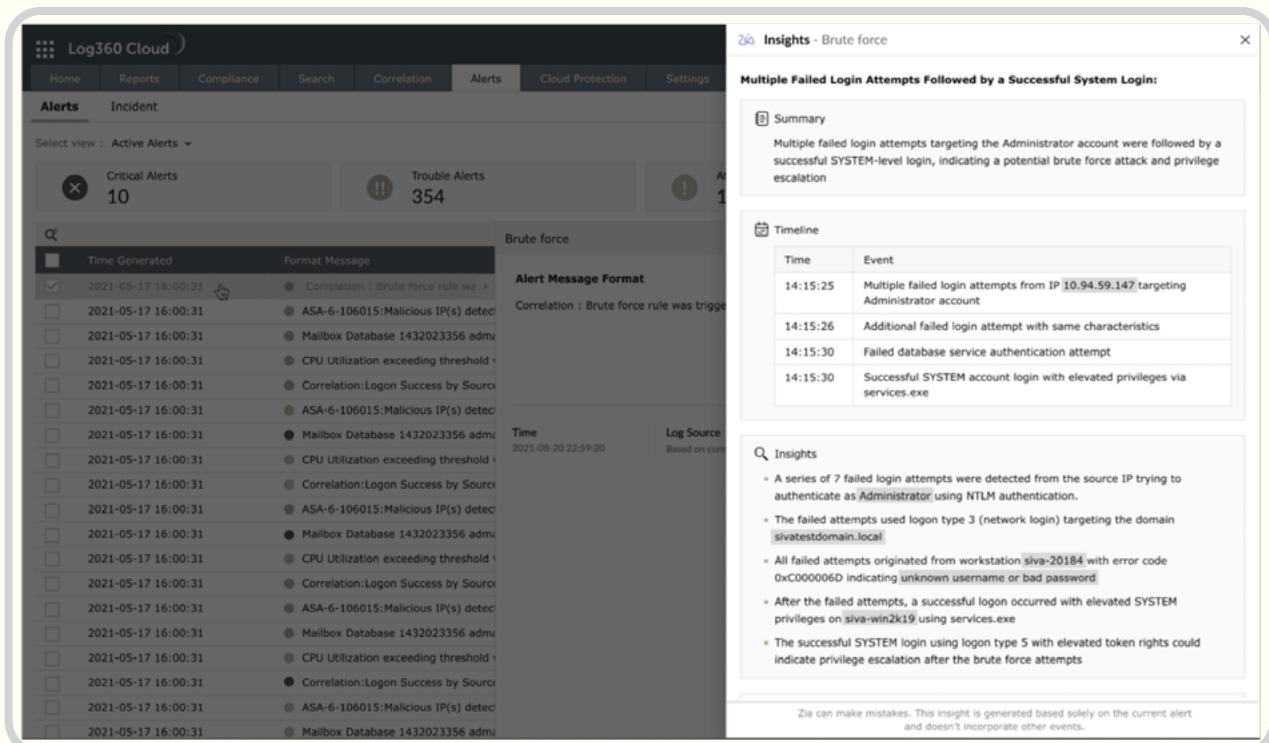
AI helps security teams cut through data noise by **automatically correlating events**. Through GenAI-driven Zia Insights, our SIEM solutions **converts complex logs and alerts into natural-language summaries** that simplify investigation and speed decision-making.

It also **maps security alerts to the MITRE ATT&CK® framework**, giving analysts clear visibility into the tactics and techniques behind each incident. This contextual understanding empowers teams to see not only what happened, but also the why and how behind every attack.

Speed up investigations with guided, intelligent response

Zia Insights goes beyond detection and acts as an intelligent assistant during investigations. It visualizes attack timelines, helping analysts reconstruct threat sequences and understand the full scope of an incident.

AI-generated remediation tips in plain language guide analysts through the next steps and by automating correlation and surfacing key insights, our SIEM solutions ensures that high-priority threats are resolved swiftly and confidently.



The screenshot displays the Log360 Cloud interface. On the left, the 'Alerts' tab is selected, showing a list of critical alerts. One alert is highlighted with a red box, labeled 'Brute force'. The alert details show a correlation rule triggered by CPU utilization exceeding a threshold. The timeline on the right shows a series of failed login attempts followed by a successful system login. The 'Insights' section provides a summary of the attack, a timeline of events, and a detailed list of findings, including the source IP, logon type, and target account. It also includes a note that Zia can make mistakes and that the insight is generated based solely on the current alert.

Visualize attack progression through entity-specific insights.

AI in IAM

AI is redefining identity security by continuously learning user behavior and strengthening access governance.

AI-powered identity and access management (IAM) solutions analyze user activity patterns to establish baselines for normal behavior, helping to spot anomalies and surface potential insider threats before they escalate. By applying ML-driven recommendations, they streamline provisioning and access reviews, suggesting the most appropriate group memberships and highlighting which access rights to retain or revoke.



With AI guiding access decisions, organizations can maintain consistent, compliant controls while minimizing manual effort. This intelligent automation not only enhances operational efficiency but also reinforces a Zero Trust security posture.

Transform complex Active Directory operations with AI

Zia, the AI assistant, transforms complex Active Directory operations into simple conversations.

Using natural language, administrators can instantly perform tasks like unlocking accounts, resetting passwords, and generating reports without navigating menus.

Zia Insights delivers AI-driven group membership analysis, including anomaly detection, peer comparison scores, and actionable recommendations to enforce least privilege access.

The screenshot shows the ADManager Plus interface. At the top, there's a navigation bar with Home, Management, Reports, Microsoft 365, Governance, Delegation, Workflow, Automation, Admin, Backup, and Support. Below the navigation bar, a sub-menu for 'User Reports' is open. The main content area is titled 'All Users' and shows a list of users with columns for Display Name, SAM Account Name, and Email Address. A user named 'John' is selected, and a modal window titled 'Zia AI Assistant' appears, asking 'Would you like to proceed with unlocking the user account for John?'. The modal shows the user's details: OU Name: Users, SAM Account Name: John, Domain Name: admptest.com, and Full Name: John. A note at the bottom says 'Please confirm to execute the action.' At the bottom of the interface, there's a message: 'Zia can make mistakes. Please verify the responses.'

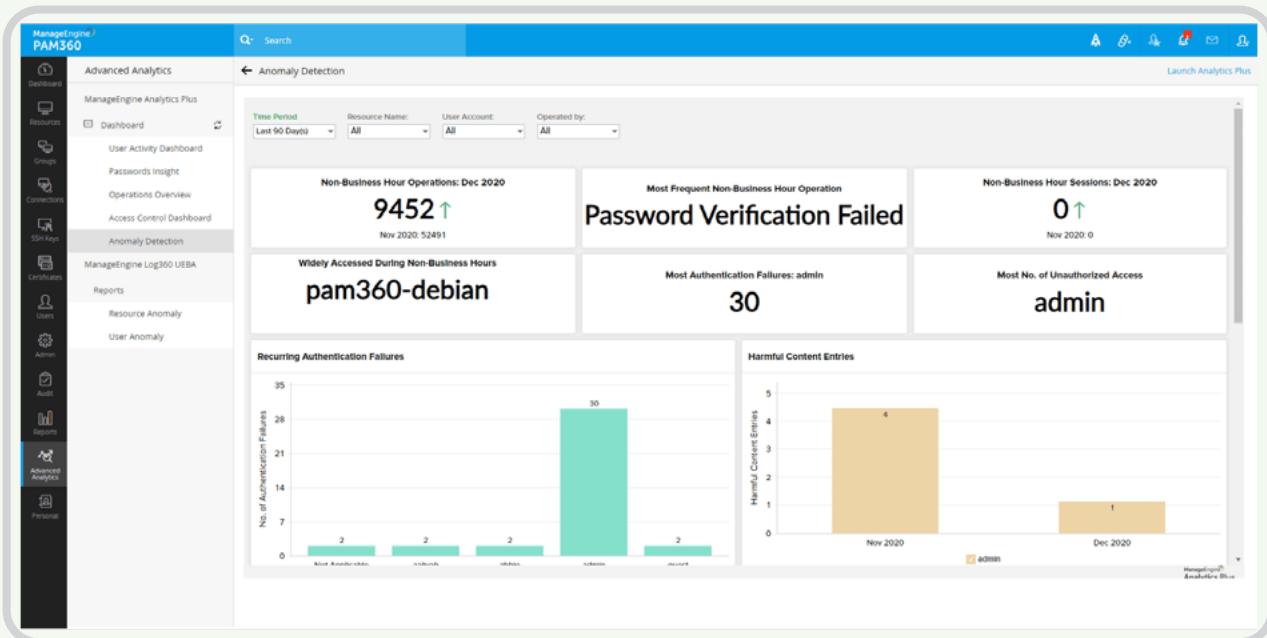
Translate complex Active Directory operations into simple conversations.

Detect anomalous behavior and enforce smarter protection

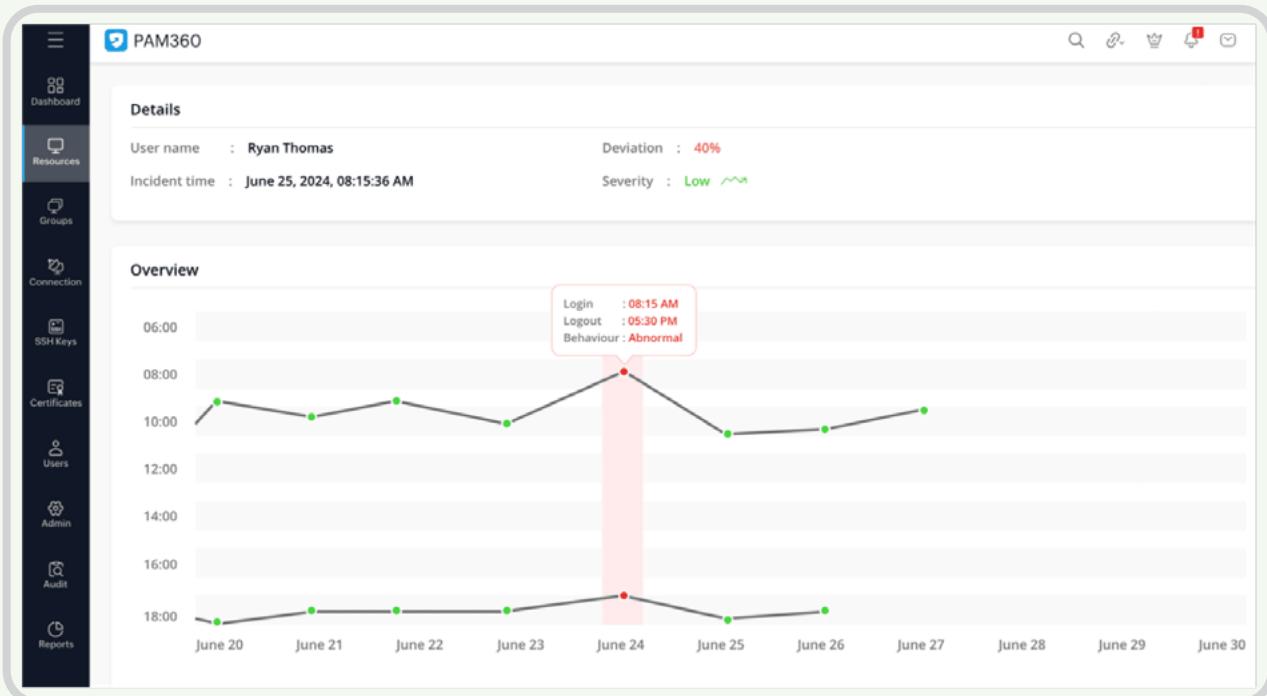
By **establishing dynamic baselines** of normal activity, such as login times, access frequency, and resource usage, the system detects deviations that indicate risk.

When anomalies occur, security teams receive real-time alerts with contextual insights, enabling swift, focused action before issues escalate.



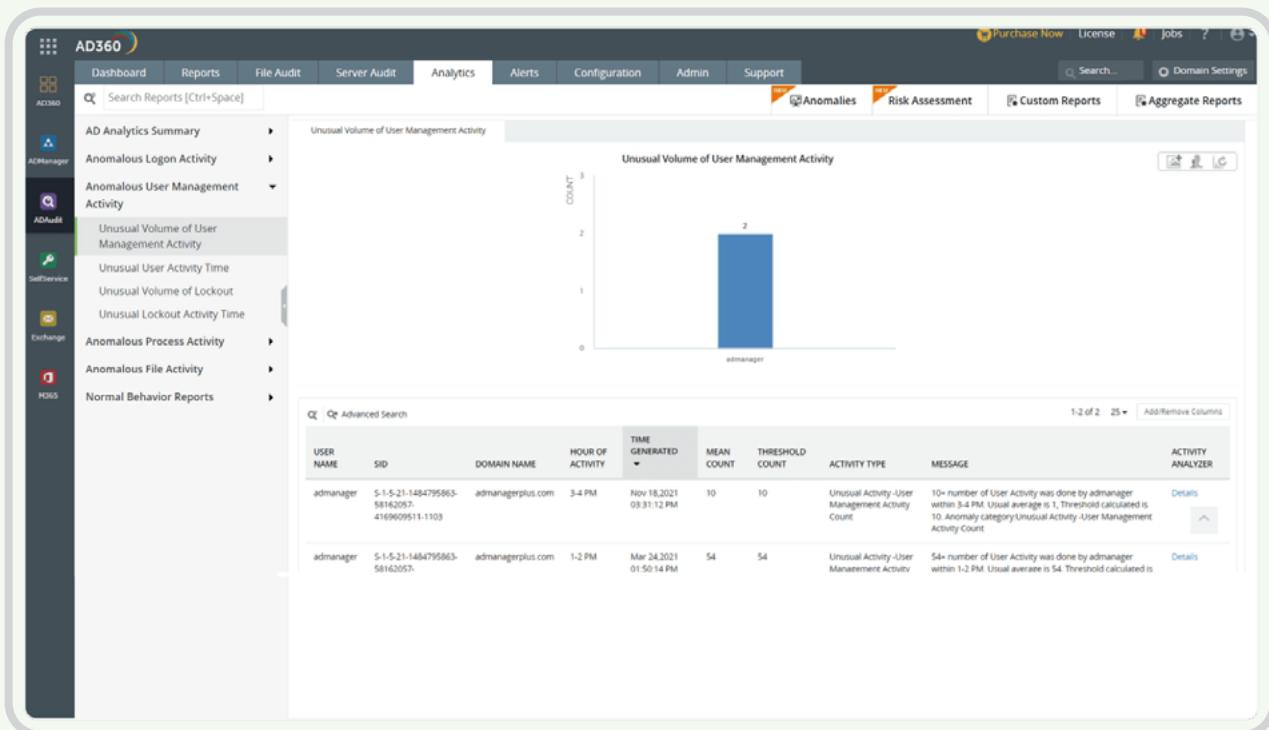


Anomaly detection.



Detect and predict anomalies with the help of a deep learning-based threat detection system.





Insider threat detection.

Authenticate smarter with context-aware access control

AI enhances authentication policies by factoring in user location, device type, and login history to validate access attempts.

This **context-aware intelligence** helps ensure that only legitimate users and trusted devices gain access to your network, strengthening defenses against credential theft and session hijacking. By continuously assessing behavior and risk, AI makes authentication more adaptive, intelligent, and secure without adding friction for users.



A screenshot of a terminal window titled 'pam360uc.manageengine.com/STATE_ID/1719408038344/ssh.ma'. The terminal shows a user session with the following commands and output:

```
last login: Tue Jun 25 21:09:52 2024 from 192.168.101.127
testuser@pmpdemo-cent7 ~]$ cd
testuser@pmpdemo-cent7 ~]$ pwd
/home/testuser
testuser@pmpdemo-cent7 ~]$ cd /home
testuser@pmpdemo-cent7 home]$ ls
ppserveradmin appserverguest enable firewalladmin firewallserveradmin firewallserverguest pmp priyanka ptuser sas sysadmin test1 testuser user
testuser@pmpdemo-cent7 home]$ cd appserveradmin
bash: cd: appserveradmin: Permission denied
testuser@pmpdemo-cent7 home]$ cd pmp
bash: cd: pmp: Permission denied
testuser@pmpdemo-cent7 home]$ :(){ :|:& };: fork() bomb code
```

A yellow box highlights the command ':(){ :|:& };: fork() bomb code'.

A yellow box at the bottom right contains the text: 'Warning! Dangerous command detected, contact administrator'.

Predict risk by learning user behavior using AI-based session monitoring and analysis.

Provision smarter and govern access more efficiently

AI simplifies identity management by providing **ML-driven recommendations for access provisioning and certification reviews.**

It analyzes usage patterns and role-based needs to suggest the most appropriate group memberships and access rights, while flagging excessive or outdated permissions. This ensures users have the right access at the right time, minimizing overexposure and maintaining a clean, compliant access environment.

ADManager Plus

Home Management Reports Microsoft 365 Delegation Workflow Automation Admin Backup Support

Search AD Objects

Directory/Application Settings

View, review, approve and execute workflow requests here. [Learn more...](#)

Task Details

Task Name	Input Details	Total Objects : 27						
Group Membership	Selected Groups	ADSM - DevSupport						
		Approved	Revoked	Pending				
Franks	Franks@child.xcross.com	ADSM VDDesigners, ADSM - DevSupport, WSMSecurity, Domain Users, ADSM - Git	Domain Users	CN=Franks,OU=WSM,OU=ML,DC=child,DC=xcross,DC=com	child.xcross.com	Franks	 	ADSM - DevSupport : Approve 65% of users sharing matching attributes are part of this group. More
Fsolo	Fsolo@child.xcross.com	ADSM VDDesigners, ADSM - DevSupport, WSMSecurity, Domain Users, ADSM - Git	Domain Users	CN=Fsolo,OU=WSM,OU=ML,DC=child,DC=xcross,DC=com	child.xcross.com	 	ADSM - DevSupport 65% of users sharing matching attributes are part of this group. 93% of group members are in the same OU as this user.	
Jaime	Jaime@child.xcross.com	ADSM VDDesigners, ADSM - DevSupport, Domain Users, ADSM - Git, ADSMProductFeatureList	Domain Users	CN=Jaime,OU=Leads,OU=ML,DC=child,DC=xcross,DC=com	child.xcross.com	Jaime	 	ADSM - DevSupport : Deny 7% of users sharing matching attributes are part of this group. More
Kesdlo	Kesdlo@child.xcross.com	ADSM - DevSupport, Domain Users, ADSMProductFeature	Domain Users	CN=Kesdlo,OU=WSM,OU=ML,DC=child,DC=xcross,DC=com	child.xcross.com	Kesdlo	 	-

Request Details

Workflow Status **Raised**

Request Status **Open**

Request ID 607

Priority Normal

Description: -

Created Time 2025-01-28 14:52:07

Expiration 23 Hour(s) left

[View Workflow Process](#)

Approve **Reject** **Execute** **Cancel**

Access recommendations.

AI in ITOM and observability

AI is transforming IT operations management (ITOM) and observability by turning vast streams of performance data into proactive intelligence. With AI at its core, IT operations move beyond reactive troubleshooting to achieve real-time awareness, predictive insights, and autonomous optimization.

By analyzing data from applications, devices, and network components, AI provides a comprehensive visualization of business-critical systems and their dependencies, giving administrators a wider, unified view of the entire IT ecosystem. It helps detect network congestion, latency issues, and resource bottlenecks, dynamically optimizing traffic flow and allocation to enhance both performance and user experience.



AI-driven analytics continuously learn from patterns in your IT environment, enabling predictive maintenance that identifies anomalies and anticipates outages before they affect performance. This reduces downtime, improves reliability, and ensures smoother service delivery.

Routine operational tasks like provisioning, configuration management, and fault resolution are automated through intelligent orchestration, cutting down manual effort while increasing accuracy and speed. At the same time, AI strengthens network security by analyzing traffic behavior, detecting threats early, and supporting rapid, proactive incident response.

Beyond operations, AI empowers IT teams to make strategic decisions backed by data. By analyzing historical performance and utilization data, it forecasts future demand, optimizes resource planning, and drives smarter investments that elevate overall business performance.

AI models can consolidate alerts from metrics, logs, anomaly detectors, and monitor states into a single intelligence layer. AI-driven correlation then connects related alerts into one incident instead of noisy fragments. Causal analysis maps the event chain to isolate the true trigger, not just surface symptoms.



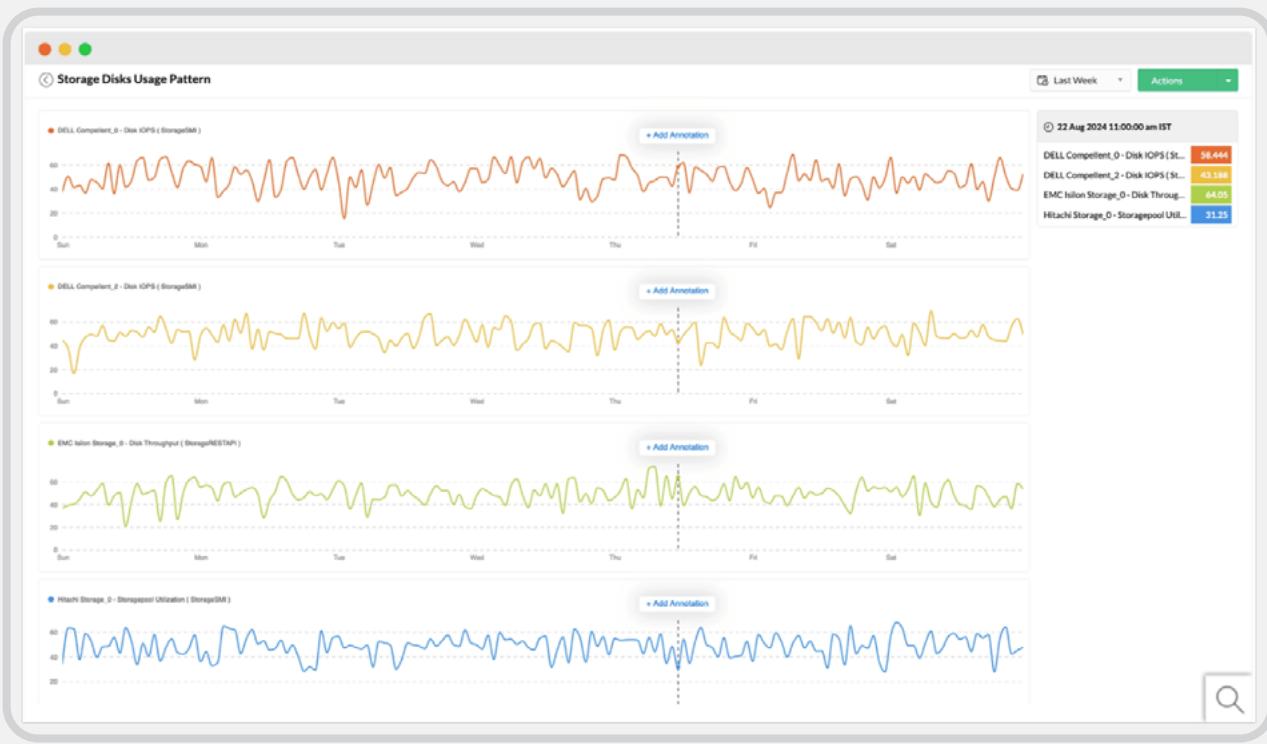
With GenAI (i.e., LLM) integrations, AI transforms raw monitoring data into concise, actionable summaries that accelerate decision-making. It detects trends and behavioral patterns across vast datasets to surface insights humans would miss. Through its NLP chatbot, users get instant, context-aware answers sourced from knowledge base.

AI brings clarity, efficiency, and foresight to IT operations and observability by enabling organizations to operate with agility, ensure resilience, and deliver exceptional digital experiences.

Eliminate noise for smarter decision making

Cut through the noise with **AI-powered data filtering and correlation** that intelligently eliminates irrelevant alerts, consolidates information across devices, and highlights what truly matters. By leveraging advanced algorithms to dynamically **set and adjust performance thresholds based on historical trends**, AI helps ITOps teams drastically reduce false positives and missed alerts thereby enabling faster, more accurate responses and more confident decision-making.





Aggregated performance data for faster and precise fault identification.

Attention	Trouble	Critical
10%	15%	20%

Attention	Trouble	Critical
5	8	15

Setting an adaptive threshold using AI and ML for proactive monitoring.

Gain complete visibility with automated insights

Get a unified view of your IT landscape with **AI-powered, in-depth reports** that track performance, availability, and configurations across your entire infrastructure. These automated insights help teams **make smarter decisions**, identify optimization opportunities, and maintain a consistently healthy network environment.

Automate fault resolution with intelligent workflows

Leverage **AIOps-driven automation and real-time topology mapping** to detect, diagnose, and resolve faults faster. By orchestrating workflows and streamlining responses, AI reduces mean time to resolve, enhances visibility, and ensures reliable, agile network operations.

Plan smarter with AI-powered capacity forecasting

Proactively plan and optimize resource usage with **AI-driven capacity forecasting**. By analyzing workload patterns, performance data, and usage trends, AI helps IT teams anticipate demand, prevent bottlenecks, and reduce unnecessary costs, ensuring optimal performance before issues arise.

⌚ RAID Forecast By Utilization ☆

Filter | Export | More Actions

Storage	Monitor Name	Used (%)	80 %	90 %	100 %
HPE Storage Device(WSAPI)_0	Capacity Utilization	87.0	Already Reached	No Growth	No Growth
INFINIBOX Storage_0	Capacity Utilization	76%	7 days	30 days	50 days
HPE StoreOnce_0	Capacity Utilization	74%	2 days	5 days	9 days
NetApp E2X00/E5X00/EF5X0_0	Capacity Utilization	71%	5 days	18 days	27 days
IBM DS Series_0	Capacity Utilization	68%	23 days	52 days	78 days
Huawei Storage_0	Capacity Utilization	63%	No Growth	No Growth	No Growth
Fujitsu Storage_0	Capacity Utilization	51%	17 days	29 days	49 days
Synology DSM_0	Capacity Utilization	47%	11 days	23 days	34 days
EMC Isilon Storage_0	Capacity Utilization	44%	No Growth	No Growth	No Growth
Netapp ONTAP(Cluster)_0	Capacity Utilization	38%	16 days	33 days	45 days
DELL Compellent_2	Capacity Utilization	33%	No Growth	No Growth	No Growth
DELL Compellent_0	Capacity Utilization	31%	No Growth	No Growth	No Growth
HPE Nimble_0	Capacity Utilization	30%	44 days	59 days	68 days
Huawei 18800 series_0	Capacity Utilization	25%	No Growth	No Growth	No Growth
Pure Storage(API)_0	Capacity Utilization	21%	36 days	57 days	72 days
Hitachi Storage_0	Capacity Utilization	19%	23 days	46 days	61 days
HPE Storage Device(WSAPI)_2	Capacity Utilization	18%	No Growth	No Growth	No Growth

Storage capacity forecasting.

Forecast Recommendations ?

Alarm Message	Possible Impact	Recommendations	Actions
⌚ Capacity Utilization [RAID] is currently at 84.11 % and is expected to reach 100 % in 12 days. OPM-RAID9 RAID 13 Aug 2025 06:47:32 AM IST	Consider deleting a few large files or increase the storage capacity to address this issue.	Consider deleting a few large files or increase the storage capacity by 292.33 TB to address this issue.	  
⌚ Capacity Utilization [RAID] is currently at 90.74 % and is expected to reach 100 % in 11 days. OPM-RAID17 RAID 13 Aug 2025 12:47:32 AM IST	Consider deleting a few large files or increase the storage capacity to address this issue.	Delete or backup Snapshot_7, Snapshot_3 and 11 other snapshots to free up 62.192 TB of space. Click here to view the complete list of snapshots.	  
⌚ Capacity Utilization [RAID] is currently at 81.81% and is expected to reach 100 % in 24 days. OPM-RAID19 RAID 13 Aug 2025 12:47:32 AM IST	Consider deleting a few large files or increase the storage capacity to address this issue.	Delete or backup Snapshot_8, Snapshot_0 and 12 other snapshots to free up 103.8 TB of space. Click here to view the complete list of snapshots.	  
⌚ MSSQL Instance [DEFAULT] - Log Files Used Percentage [WMI] is currently at 99.16 % and is expected to reach 100 % in 16 days. OPM-HYPERV-DomainController... DomainController 12 Aug 2025 09:47:32 AM IST	This might impact the transactions occurring on the database(s) present in this SQL Server.	Consider backing up the log files to a different location and deleting them, or increase the current log file size.	  
⌚ Capacity Utilization [RAID] is currently at 83.31 % and is expected to reach 100 % in 24 days. OPM-RAID13 RAID 12 Aug 2025 09:47:32 AM IST	Consider deleting a few large files or increase the storage capacity to address this issue.	Consider deleting a few large files or increase the storage capacity by 110.783 TB to address this issue.	  
⌚ Capacity Utilization [RAID] is currently at 93.84 % and is expected to reach 100 % in 12 days. OPM-RAID18 RAID 11 Aug 2025 06:47:32 PM IST	Consider deleting a few large files or increase the storage capacity to address this issue.	Consider deleting a few large files or increase the storage capacity by 636.333 TB to address this issue.	  

Forecast recommendations.

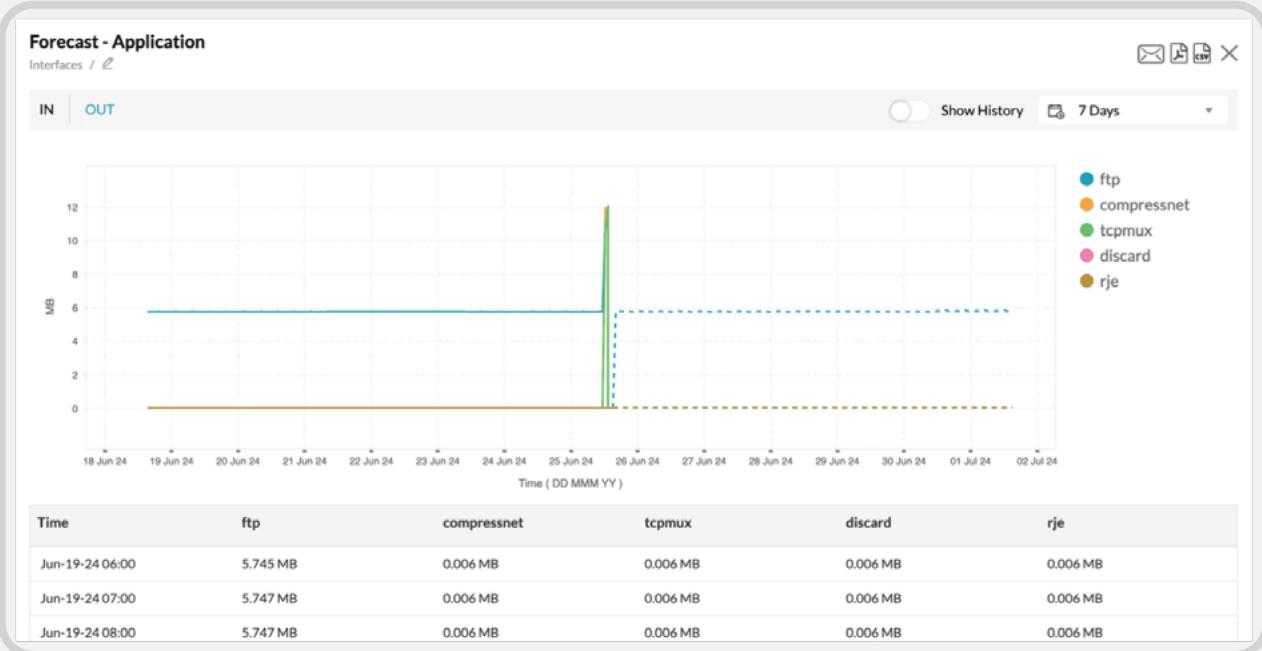


Disk Forecast By Usage

Filter | Export | More Actions

Device Name	Partition	Currently Used(%)	Prediction(80%)	Prediction(90%)	Prediction(100%)
OPM-Server3	/snap/wine-platform-6-stable/19	78	53 Days	76 Days	107 Days
OPM-DomainController1	E:	11	64 Days	93 Days	122 Days
OPM-Server1	/dev/shm	47	74 Days	113 Days	144 Days
OPM-DomainController1	C:	8	90 Days	137 Days	176 Days
OPM-Desktop1	E:	42	101 Days	140 Days	179 Days
OPM-Server3	/snap/wine-platform-3-stable/14	20	95 Days	134 Days	181 Days
OPM-Server3	/snap/notepad-plus-plus/386	64	98 Days	137 Days	184 Days
OPM-DomainController2	C:	68	No Growth	No Growth	No Growth
OPM-Server2	C:	79	No Growth	No Growth	No Growth
OPM-Server1	/run/user/125	76	No Growth	No Growth	No Growth
OPM-Server1	/snap/gnome-3-38-2004/137	59	No Growth	No Growth	No Growth
OPM-Server1	/dev	20	No Growth	No Growth	No Growth
OPM-Server1	/snap/snap-store/638	46	No Growth	No Growth	No Growth
OPM-Server1	/snap/core20/1891	26	No Growth	No Growth	No Growth
OPM-Server1	/snap/gnome-42-2204/111	41	132 Days	191 Days	No Growth

Disk forecasting.

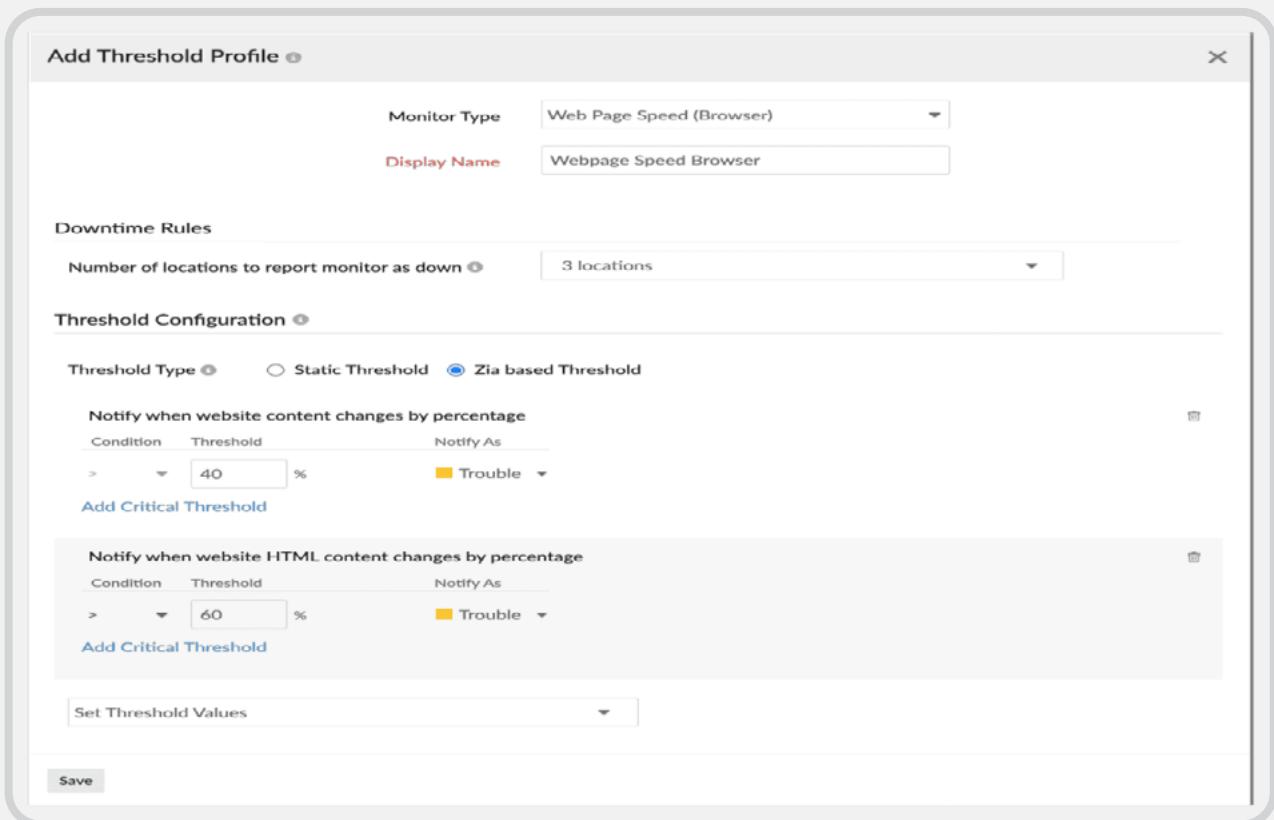


Application traffic forecasting.



Detect anomalies before they impact performance

Use AI-powered anomaly detection to identify deviations from normal behavior and uncover hidden trends in real time. This enables IT teams to detect performance issues before they escalate, prevent outages, and maintain seamless operations across applications and infrastructure.



Add Threshold Profile

Monitor Type: Web Page Speed (Browser)

Display Name: Webpage Speed Browser

Downtime Rules: Number of locations to report monitor as down: 3 locations

Threshold Configuration:

Threshold Type: Zia based Threshold

Notify when website content changes by percentage:

Condition	Threshold	Notify As
>	40 %	Trouble

Add Critical Threshold

Notify when website HTML content changes by percentage:

Condition	Threshold	Notify As
>	60 %	Trouble

Add Critical Threshold

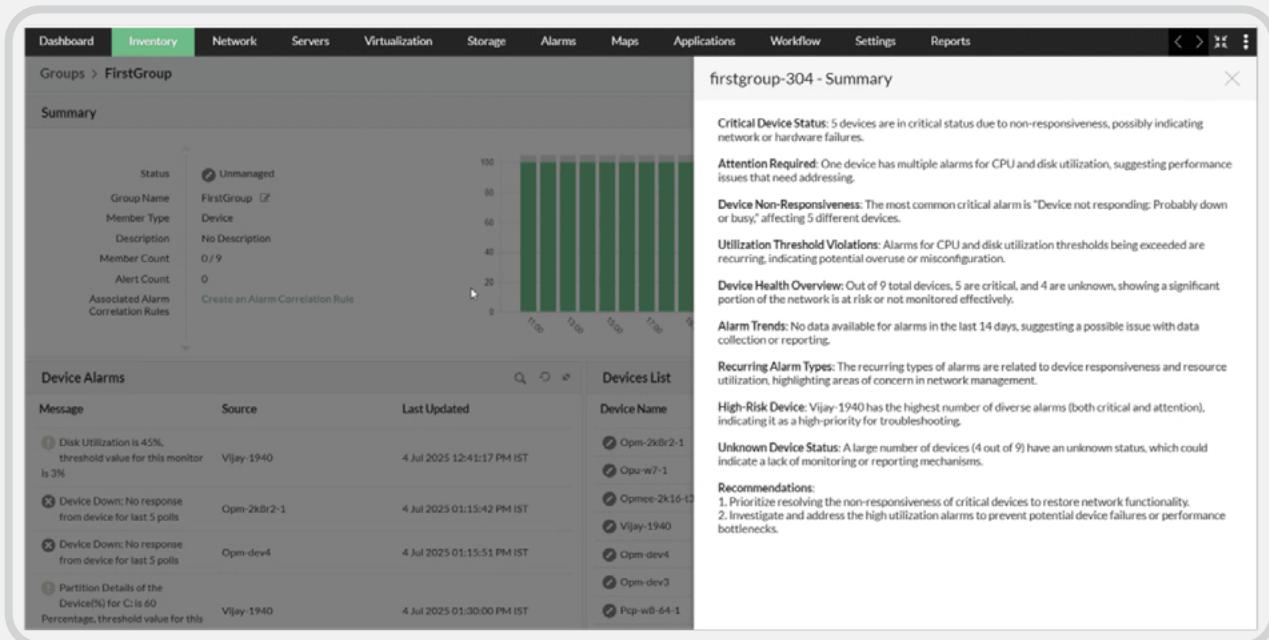
Set Threshold Values

Save

Anomaly detection with Zia-based threshold.

Accelerate root-cause analysis with GenAI integration

Zia, our native AI platform, integrates with various GenAI tools and **converts raw monitoring data into clear, actionable intelligence** that speeds up operational decision-making. It continuously analyzes large volumes of telemetry to uncover trends and behavioral patterns that would otherwise go unnoticed. Through its NLP-driven assistant, users receive instant, context-aware responses powered by our platform's native knowledge base and documentation. With prompt-based automation and intelligent log pattern generation, it significantly reduces manual effort while improving the speed and accuracy of incident response.



Summarization via OpenAI integration.

The screenshot shows the Site24x7 dashboard with the Zia AI chatbot integrated. The Zia Bot window is open, displaying information about monitors and logs, and a query input field.

Plan Details

Enterprise Plan

Plan Summary

Plan	Enterprise Plan
Total Monitors	525
Basic Monitors	500
Advanced Monitors	25
RUM Page views	10M
Network Interfaces	3100
Netflow Analyzer Interfaces	1020
NCM Devices	5
AppLogs	1.00 GB
Alert Credits	500

Addon

Temporary	Additional
Additional	Additional
Additional	Additional
Additional	Additional
Mobile AP	Mobile AP
APM Ingest	1000 Intel
1000 Intel	100 GB Local
250K Basic	10K Advanced
10K Advanced	1000 Network
1000 Network	1000 NCA

Zia Bot

Gain instant assistance and AI-driven insights to assess health, monitor performance, and identify patterns across your resources. Learn more.

What are Basic and Advanced Monitors?

How to send an alert to my mobile phone?

How to retrieve logs from different Site24x7 monitors?

The Zia chatbot is still learning, so it might occasionally make mistakes or show inaccurate information.

Type your query here... Use '@' to mention a monitor or monitor group.

The screenshot shows the Site24x7 interface with the 'Add Automation Templates' dialog box open. A modal window titled 'Zia Assistant' is open, displaying a command to truncate Docker logs and its result.

Add Automation Templates

Type: Server Command

Display Name: Docker Logs Clearing

Enter Command to be Executed: Eg. mv /local/dad/app/logs/backup/logs

Filter by: 06f6c538-e600e868

Select Hosts for Server Script Execution

Max Allowed Action Execution Time

Send the Automation Result via Email

Save

Zia Assistant

command to truncate all docker logs

Result

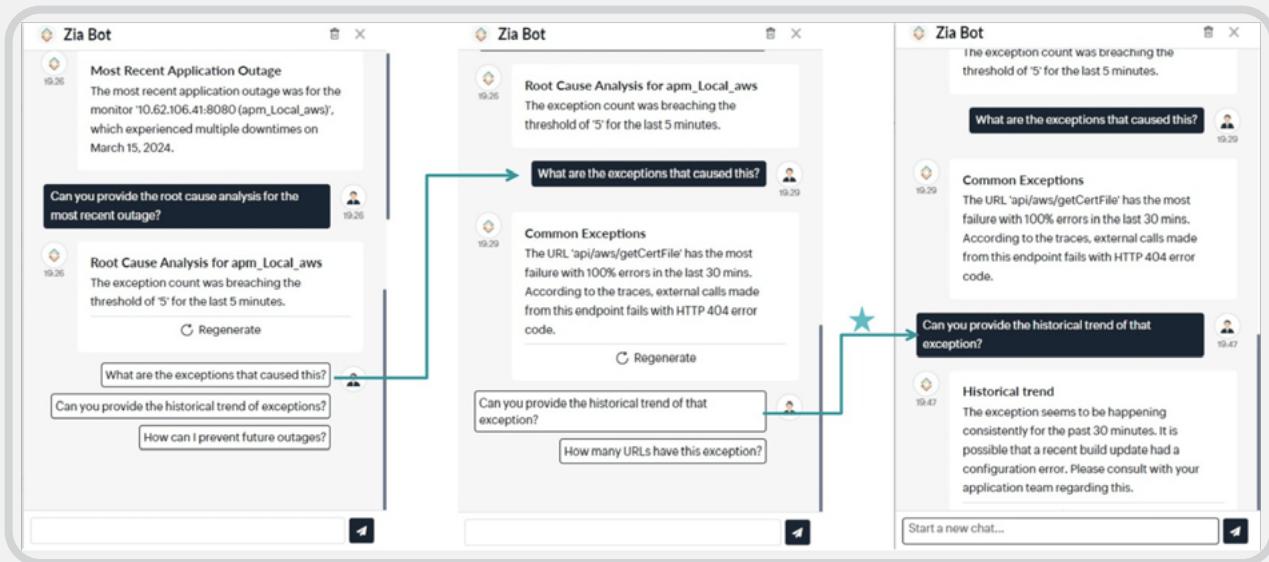
```
truncate -s 0 $(docker inspect --format='{{.LogPath}}' $(docker ps -aq))
```

Move to Editor Regenerate

The Zia chatbot is still learning, so it might occasionally make mistakes or show inaccurate information.

Generate Docker Scripts using Zia's GenAI capabilities for IT automation.





Zia chatbot with GenAI capabilities.

Correlate events to analyze the root cause of issues

ManageEngine solutions collect alerts from performance metrics, logs, anomaly detection systems, and monitor statuses to create a consolidated event pipeline.

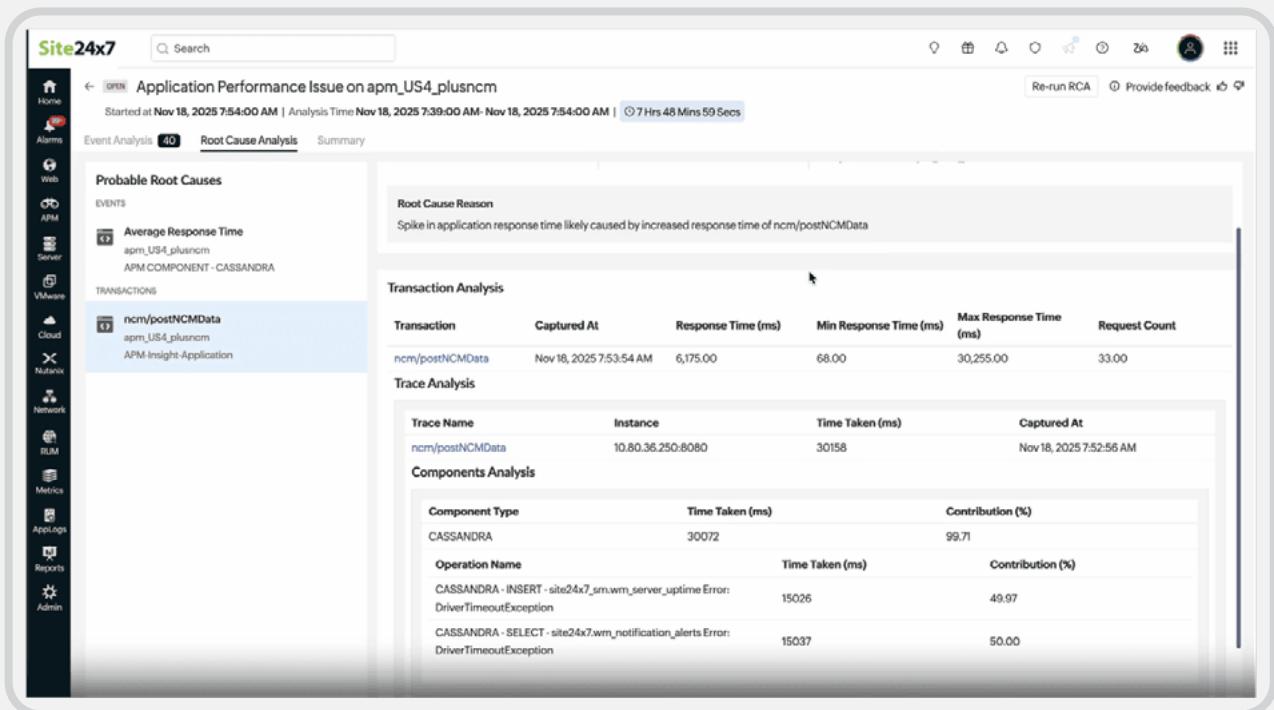
Smart Groups dynamically organize interconnected resources based on topology (i.e., Layer 2 topology mapping) and dependency mappings.

Rules-based and AI-powered correlation merges related alerts into a single incident, eliminating fragmented and distracting noise.



Causal analysis traces the sequence of events to identify the actual source of the issue, rather than the most visible symptom.

Root cause is determined with **deep trace-level accuracy**, pinpointing the precise application component or method responsible.



The screenshot shows the Site24x7 APM interface with the following details:

- Page Title:** Application Performance Issue on apm_US4_plusncm
- Start Date:** Nov 18, 2025 7:54:00 AM
- Analysis Time:** Nov 18, 2025 7:39:00 AM - Nov 18, 2025 7:54:00 AM
- Duration:** 7 Hrs 48 Mins 59 Secs
- Event Analysis:** 40
- Root Cause Analysis:** (selected)
- Summary:**

Probable Root Causes:

- EVENTS:**
 - Average Response Time: apm_US4_plusncm APM COMPONENT - CASSANDRA
- TRANSACTIONS:**
 - ncm/postNCMData: apm_US4_plusncm APM Insight Application

Root Cause Reason: Spike in application response time likely caused by increased response time of ncm/postNCMData

Transaction Analysis:

Transaction	Captured At	Response Time (ms)	Min Response Time (ms)	Max Response Time (ms)	Request Count
ncm/postNCMData	Nov 18, 2025 7:53:54 AM	6,175.00	68.00	30,255.00	33.00

Trace Analysis:

Trace Name	Instance	Time Taken (ms)	Captured At
ncm/postNCMData	10.80.36.250:8080	30158	Nov 18, 2025 7:52:56 AM

Components Analysis:

Component Type	Time Taken (ms)	Contribution (%)
CASSANDRA	30072	99.71

Operation Name	Time Taken (ms)	Contribution (%)
CASSANDRA - INSERT - site24x7_jrm.wm_server_uptime Error: DriverTimeoutException	15026	49.97
CASSANDRA - SELECT - site24x7.wm_notification_alerts Error: DriverTimeoutException	15037	50.00

Event correlation and causal analysis.

AI in UEMS

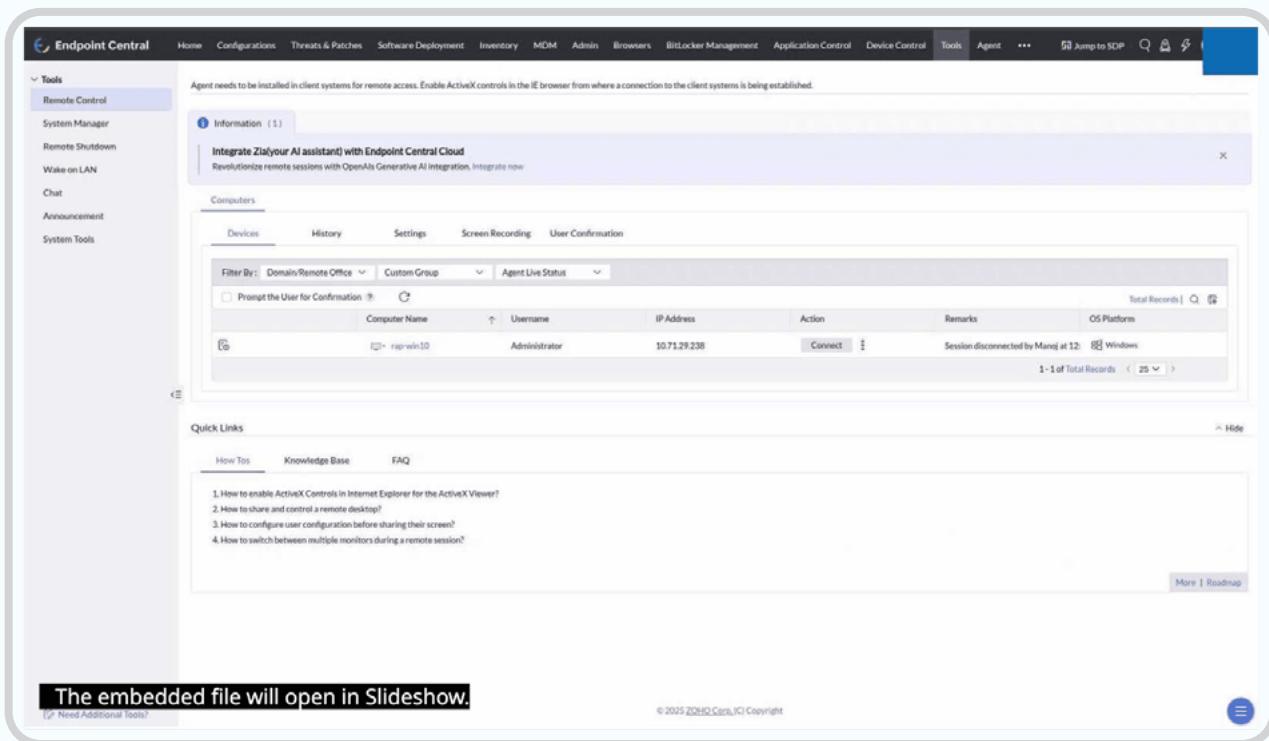
AI is redefining unified endpoint management and security by combining intelligence, automation, and predictive capabilities to create a more resilient IT environment. In unified endpoint management and security (UEMS), AI empowers administrators to detect and neutralize threats faster, automate repetitive tasks, and gain deeper visibility into endpoint performance.

From identifying unknown malware and zero-day ransomware through behavioral detection and ML-driven analysis to intelligent remote troubleshooting and providing a secure browsing experience, AI enables proactive protection at scale. It also enables you to collect endpoint telemetry at a granular level, helping IT teams anticipate issues, optimize device health, and ensure uninterrupted productivity across every endpoint.



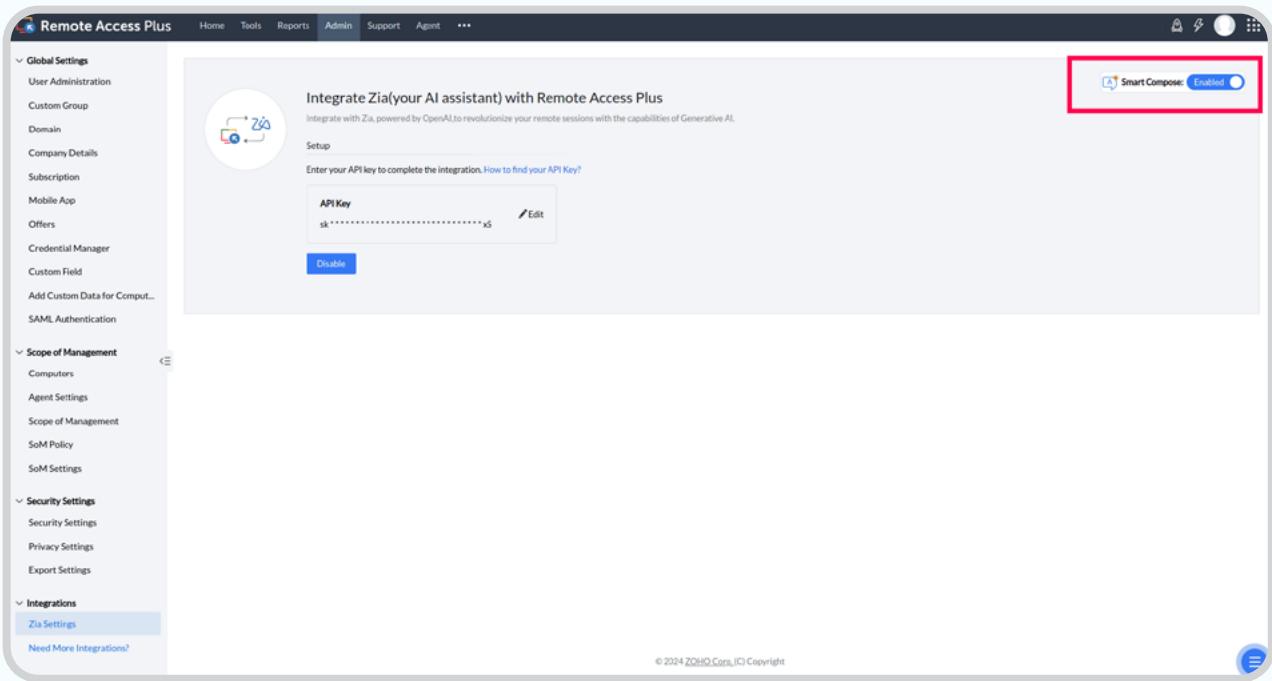
Resolve issues faster with intelligent assistance

Enhance remote troubleshooting with **AI-driven assistance** that understands context and accelerates response. From intelligent chat suggestions and real-time sentence completion to automated responses, AI helps technicians resolve issues quickly and efficiently.



The embedded file will open in Slideshow.

© 2025 ZOHO Corp. All Rights Reserved.

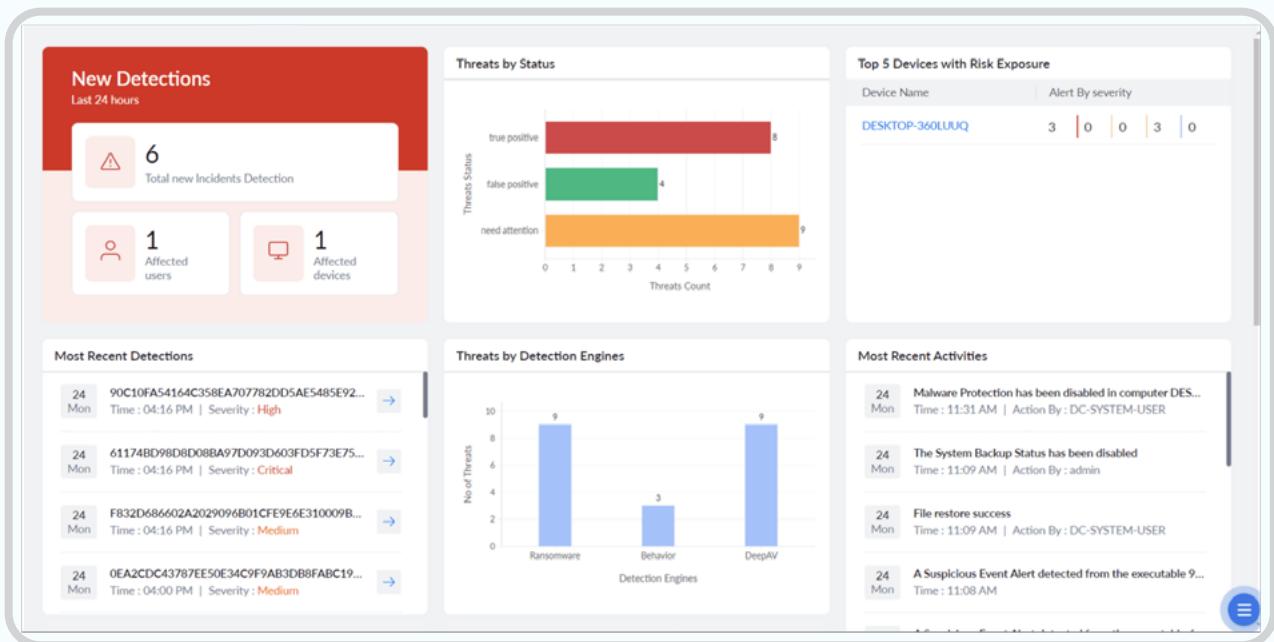


The screenshot shows the 'Remote Access Plus' software interface. The left sidebar contains a navigation menu with sections like 'Global Settings', 'Scope of Management', 'Security Settings', 'Integrations' (which is currently selected), and 'Zia Settings'. The main content area is titled 'Integrate Zia(your AI assistant) with Remote Access Plus' and includes a 'Setup' section for entering an API key. A red box highlights the 'Smart Compose' status indicator in the top right corner, which shows 'Enabled' with a blue button. The bottom right corner of the main window has a blue circular icon with a white 'M'.

AI-based remote support and chat.

Stay ahead of threats with AI-driven protection

Defend endpoints against evolving cyber threats with AI-powered behavioral analysis that identifies unknown malware strains even offline.



AI-based behavior detection for malware protection.

Our AI-powered Next-gen DeepAV Engine uses advanced ML to spot subtle, zero-day ransomware behaviors and encryption patterns with high accuracy. By combining deep-learning-driven ransomware detection with anomaly-based data exfiltration prevention, the platform stops emerging threats before they spread or steal data, keeping every endpoint protected, even from attacks never seen before.



The screenshot shows a software configuration interface with the following sections:

- General Settings**:
 - System Backup Creation: Enabled (radio button)
 - Allocated Backup storage: 10 %
 - Backup Interval: 180 Min
- Anti-Ransomware**:
 - Ransomware Detection Engine: Instantly identifies ransomware through AI-powered behavioral analysis, offering single-click rollback and secure incremental backups using Microsoft VSS. Learn more
 - Detection Policy: Audit Only (radio button)
 - Detection Sensitivity: Standard (radio button)
 - Decoy File deployment: Enabled (radio button)
- Next-Gen Antivirus**:
 - DeepAV - Deep Learning based Antivirus: Deep learning-based static analysis enhances threat detection by scrutinizing code structures and characteristics, increasing accuracy in identifying known and unknown malware. Learn more
 - Detection Trigger: On Execute (checkbox), On DLL Load (checkbox), On Write (checkbox)
 - Detection Policy: Audit Only (radio button)

DeepAV, the deep learning-based antivirus.

Behavioral detection engine for threat hunting

Our behavioral detection engine continuously monitors endpoint activities including process executions, file modifications, and flags deviations from normal patterns. When an attacker deploys a fileless payload or leverages legitimate tools like PowerShell or WMI, the engine detects the abnormal behavior sequence and alerts security teams. This enables proactive threat hunting, early-stage containment, and rapid incident response before the attack spreads.



Deep learning–based malicious script detection engine

Our deep-learning model trained on massive datasets of benign and malicious scripts can identify harmful intent even when content is hidden, encoded, or transformed. If a seemingly harmless JavaScript, PowerShell, or Python script attempts to execute encrypted code, initiate unauthorized downloads, or trigger silent persistence, the deep-learning engine identifies the malicious pattern and blocks execution instantly, stopping zero-day and script-based attacks at the endpoint.

Anticipate issues before they impact performance

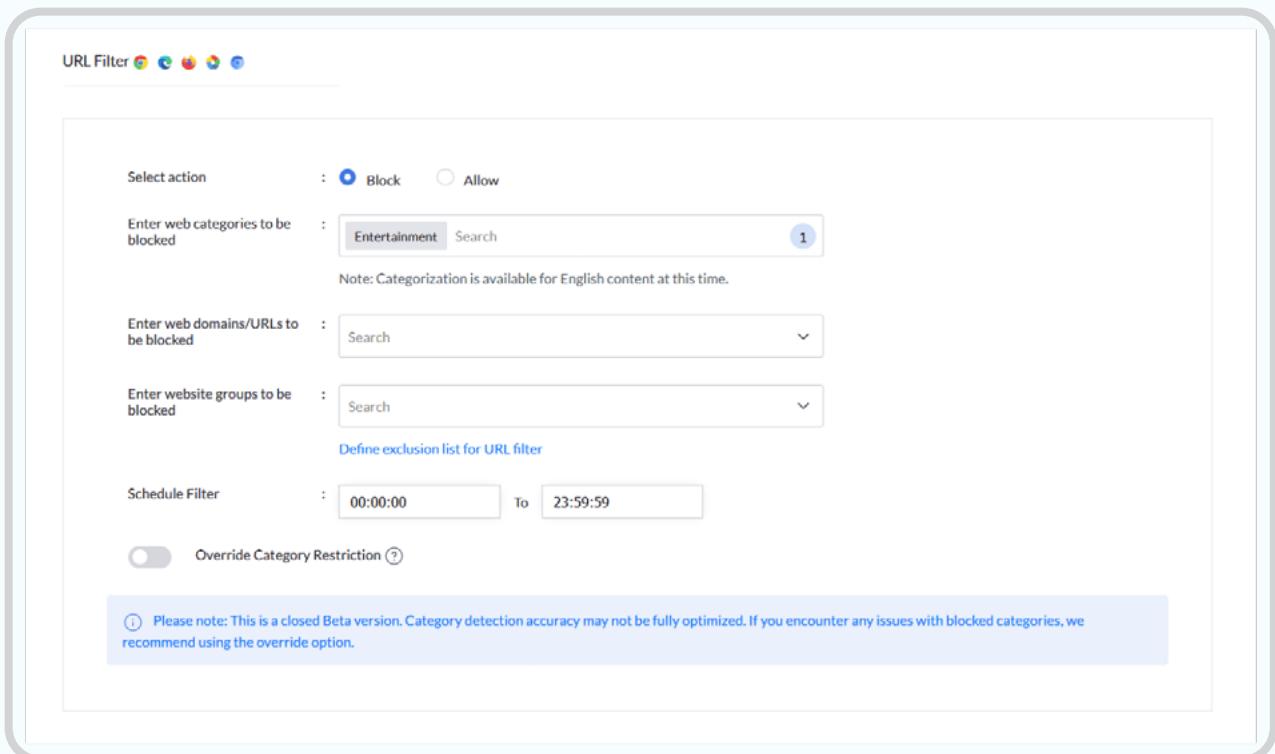
AI transforms endpoint visibility by turning data into actionable intelligence. Through **custom sensors and automated analysis**, IT teams can forecast issues such as degraded battery health, storage bottlenecks, or system slowdowns and act before they disrupt productivity.

When **forecasts cross defined thresholds**, AI triggers **proactive alerts**, giving teams time to respond before downtime, slowdowns, or data loss affect operations. **ML-based monitoring** ensures continuous performance optimization and minimizes disruption across all devices.

Secure browsing and boost productivity

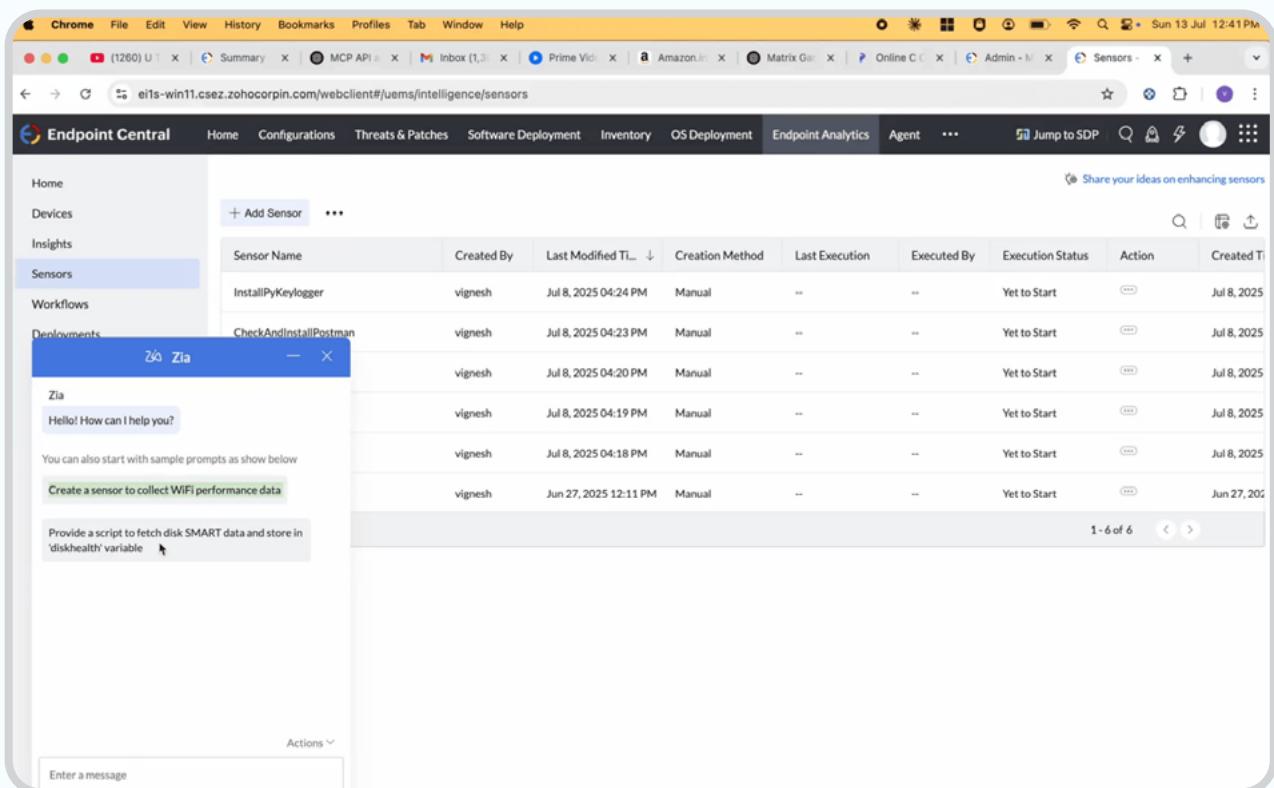
AI strengthens endpoint protection beyond device-level security by using **smart content filters** to block malicious or restricted websites.

Instead of relying on manual blocklists, AI dynamically detects unsafe or unproductive browsing patterns and restricts access automatically reducing exposure to cyber risks and improving employee focus during work hours.



AI-based web filters.

AI supercharges endpoint visibility by transforming insights into action. With **custom data sensors**, IT teams can automatically generate scripts, trigger workflows, and streamline remediation processes. This intelligent automation accelerates response times, improves operational efficiency, and ensures faster, data-driven outcomes across all managed endpoints.



The screenshot shows a web-based interface for managing custom sensors. The top navigation bar includes links for Home, Configurations, Threats & Patches, Software Deployment, Inventory, OS Deployment, Endpoint Analytics, Agent, and Sensors. The Sensors menu item is currently selected. The main content area displays a table of sensors with columns for Sensor Name, Created By, Last Modified Time, Creation Method, Last Execution, Executed By, Execution Status, Action, and Created Time. The table lists two sensors: 'InstallPyKeylogger' and 'CheckAndInstallPostman', both created by 'vignesh' on July 8, 2025. The interface also features a sidebar with a 'Zia' AI chatbot, a message input field, and a 'Actions' dropdown.

Sensor Name	Created By	Last Modified Time	Creation Method	Last Execution	Executed By	Execution Status	Action	Created Time
InstallPyKeylogger	vignesh	Jul 8, 2025 04:24 PM	Manual	--	--	Yet to Start	...	Jul 8, 2025
CheckAndInstallPostman	vignesh	Jul 8, 2025 04:23 PM	Manual	--	--	Yet to Start	...	Jul 8, 2025
	vignesh	Jul 8, 2025 04:20 PM	Manual	--	--	Yet to Start	...	Jul 8, 2025
	vignesh	Jul 8, 2025 04:19 PM	Manual	--	--	Yet to Start	...	Jul 8, 2025
	vignesh	Jul 8, 2025 04:18 PM	Manual	--	--	Yet to Start	...	Jul 8, 2025
	vignesh	Jun 27, 2025 12:11 PM	Manual	--	--	Yet to Start	...	Jun 27, 2025

AI-based custom sensors and script generation for digital employee experience.

AI in IT analytics

AI is redefining IT analytics by turning complex operational data into real-time intelligence that drives faster, smarter decisions. It elevates this further by unifying data across systems and delivering contextual, predictive insights tailored for modern IT environments.

By combining ML, decision intelligence, and GenAI, IT teams can uncover hidden IT dependencies, detect inefficiencies, implement corrective strategies, and optimize performance across the entire IT stack. With contextual intelligence embedded across every IT application, it provides actionable insights, expedited root cause analysis, and outcome predictions through no-code interactions. And with LLM-driven analytics and AI orchestration, real-time IT metrics seamlessly evolve into intelligent automated actions that strengthen agility, reliability, and performance across the IT ecosystem.



Supercharge IT intelligence

Empower your IT ecosystem with LLM-powered intelligence to **import data, perform complex analyses, and extract actionable insights and recommendations**. Integrate your preferred LLM for automated analysis, real-time insight interpretation, and intelligent workflow automation, turning IT data into a dynamic, strategic asset that enables faster, smarter operations.

Orchestrate agentic AI workflows

Transform real-time IT metrics into intelligent, actionable triggers powered by AI orchestration. AI automatically initiates workflows such as scaling infrastructure, reallocating resources, or adjusting configurations when dynamic thresholds are met, enabling next-generation IT automation that adapts instantly to changing conditions and enhances speed, efficiency, and reliability across operations.

Accelerate decision-making with decision intelligence

Leverage contextual, AI-driven strategies to **tackle operational bottlenecks and prioritize high-impact fixes**. The AI-powered decision intelligence platform streamlines decision-making, minimizes monitoring effort, prevents service disruptions, boosts operational efficiency, and ensures optimal IT performance.



Contextual recommendations with Spotlight.

Get instant, code-free insights with GenAI-powered Zia

Ask questions and get instant insights with Zia, the GenAI-powered analytics assistant. Use simple voice or text commands to build complex reports and dashboards, decode analyses, uncover root causes, predict outcomes, turn insights into action, and gain contextual intelligence across your IT environment.

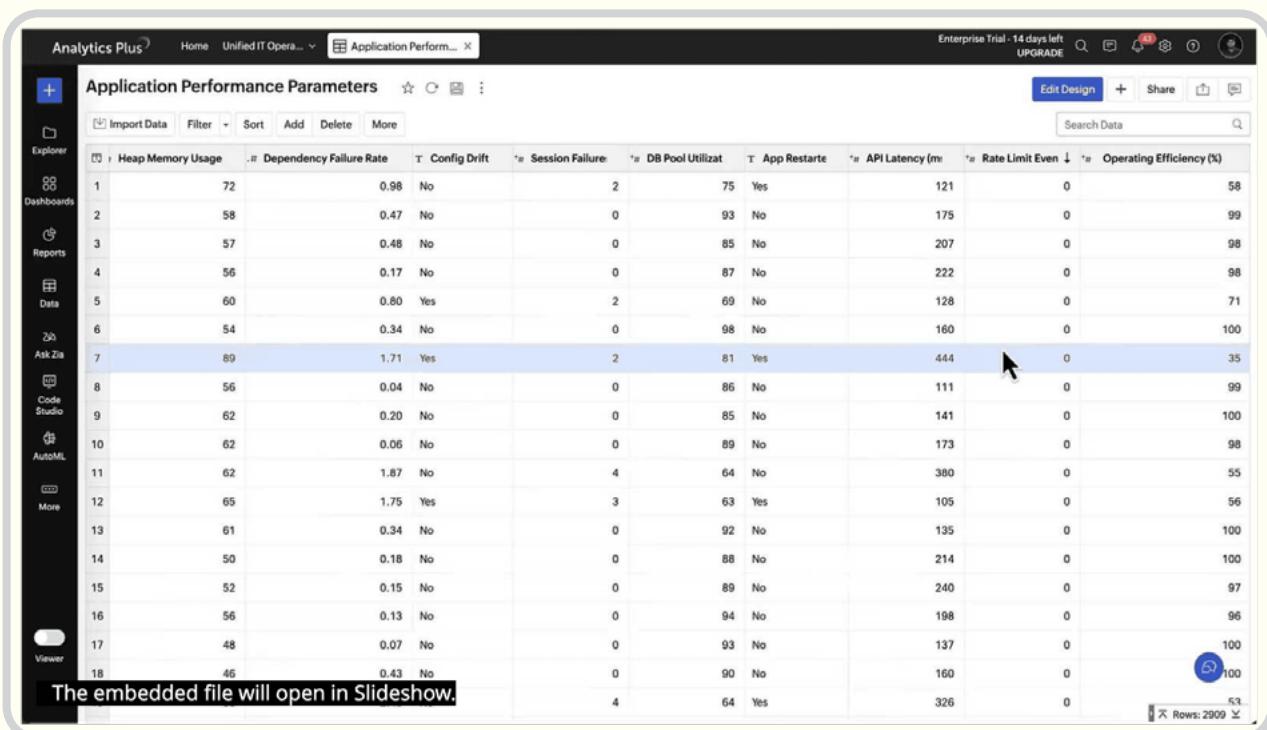


Experience contextual intelligence

Zia adapts seamlessly across IT applications, **providing context-aware** insights that unify data and drive AI-powered decision-making across your IT stack. This enables smarter, connected ITOps by offering a holistic view of system health, performance, and improvement opportunities.

Run complex, tailored computations with no-code ML

Create custom IT analyses effortlessly with a no-code ML builder. Tailor models to your environment to run complex computations such as outage prediction and escalation probability, generating precise, actionable insights.



The screenshot shows a data grid titled 'Application Performance Parameters' within the 'Analytics Plus' application. The grid displays 18 rows of data with the following columns: Row, Heap Memory Usage, Dependency Failure Rate, Config Drift, Session Failure, DB Pool Utilizat, App Restart, API Latency (m), Rate Limit Even, and Operating Efficiency (%). The data includes various numerical values and boolean entries (Yes/No). A cursor is hovering over the data in the 7th row. The application interface includes a sidebar with 'Explorer', 'Dashboards', 'Reports', 'Data', 'Ask Zia', 'Code Studio', 'AutoML', and 'More' sections. A message at the bottom states: 'The embedded file will open in Slideshow.'

Row	Heap Memory Usage	Dependency Failure Rate	Config Drift	Session Failure	DB Pool Utilizat	App Restart	API Latency (m)	Rate Limit Even	Operating Efficiency (%)
1	72	0.98	No	2	75	Yes	121	0	58
2	58	0.47	No	0	93	No	175	0	99
3	57	0.48	No	0	85	No	207	0	98
4	56	0.17	No	0	87	No	222	0	98
5	60	0.80	Yes	2	69	No	128	0	71
6	54	0.34	No	0	98	No	160	0	100
7	89	1.71	Yes	2	81	Yes	444	0	35
8	56	0.04	No	0	86	No	111	0	99
9	62	0.20	No	0	85	No	141	0	100
10	62	0.06	No	0	89	No	173	0	98
11	62	1.87	No	4	64	No	380	0	55
12	65	1.75	Yes	3	63	Yes	105	0	56
13	61	0.34	No	0	92	No	135	0	100
14	50	0.18	No	0	88	No	214	0	100
15	52	0.15	No	0	89	No	240	0	97
16	56	0.13	No	0	94	No	198	0	96
17	48	0.07	No	0	93	No	137	0	100
18	46	0.43	No	0	90	No	160	0	100

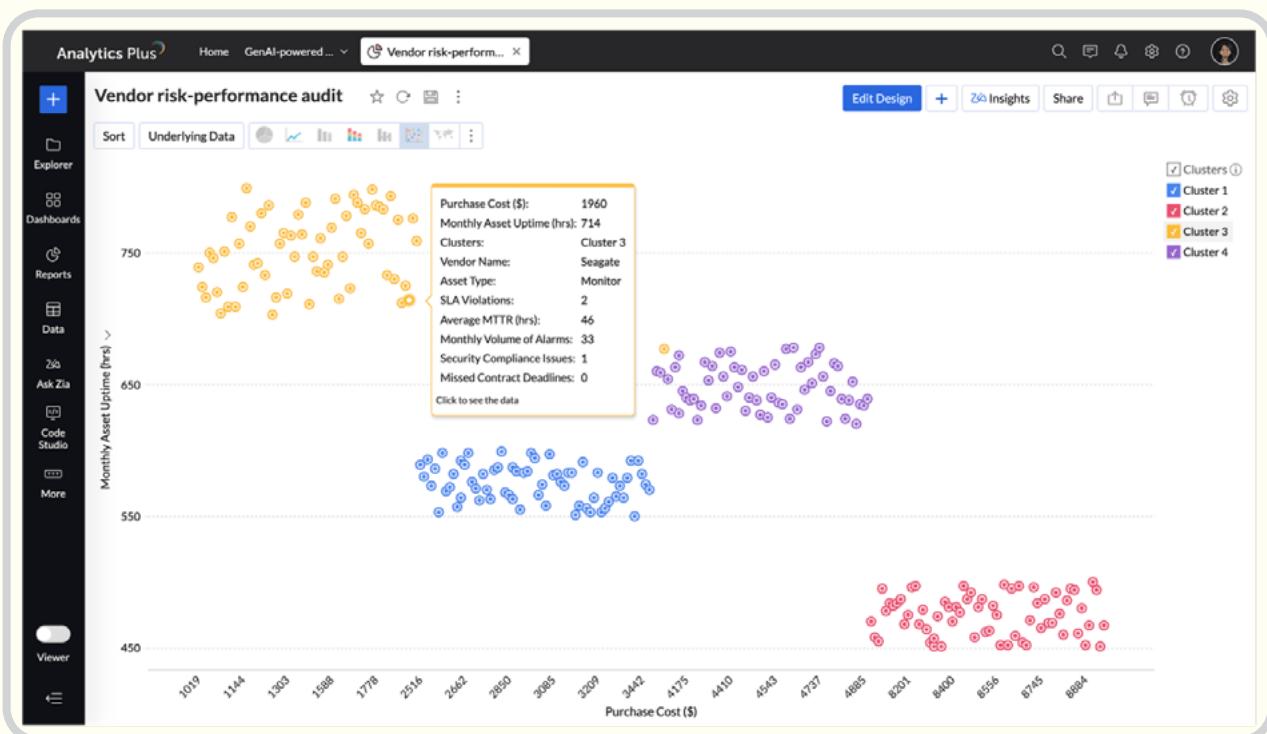
No-code ML models for tailored IT analysis.

Expedite root cause analysis

Pinpoint key trends driving inefficiencies such as SLA violations, unexpected costs, and resource constraints, and get real-time data-driven remediation strategies that accelerate remediation and restore optimal performance in seconds.

Uncover inefficiencies faster with ML-based clustering

Leverage ML algorithms to automatically segment IT resources by shared characteristics, such as frequent downtime or high resolution times, to quickly spot recurring issues and accelerate resolution. Turn these insights into targeted actions that address each segment's unique challenges.



Cluster analysis for faster resolution

Predict trends with precisio

Go beyond historical trend forecasting by incorporating real-time factors such as traffic variations, application load, and incident volume to **elevate prediction accuracy, optimize resource allocation, and prevent bottlenecks** before they impact performance.

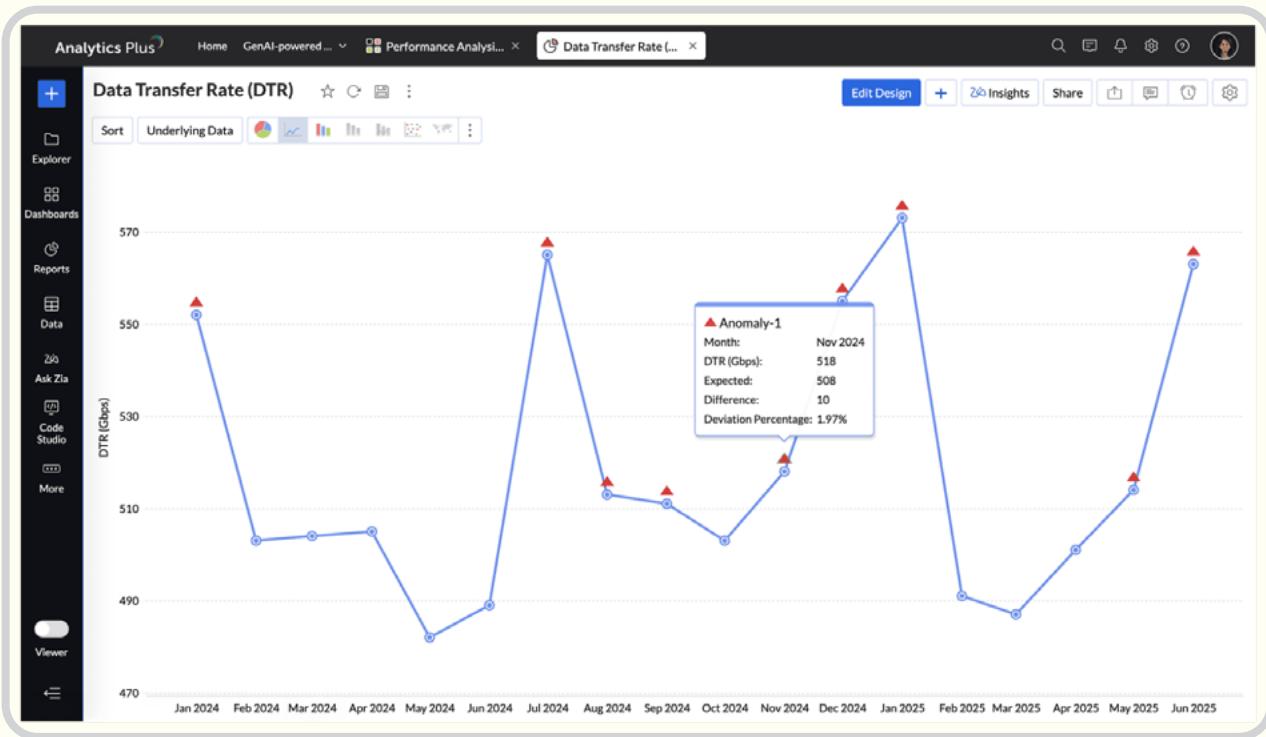


Predict IT trends with multivariate forecasting.

Detect anomalies early

Identify early warning signs with **AI-powered anomaly** detection that triggers alerts only when real risk thresholds are crossed. This precision-driven monitoring minimizes false positives, enabling IT teams to **focus on true threats and maintain seamless operations.**





Anomaly detection to catch deviations early.

AI in low-code application development

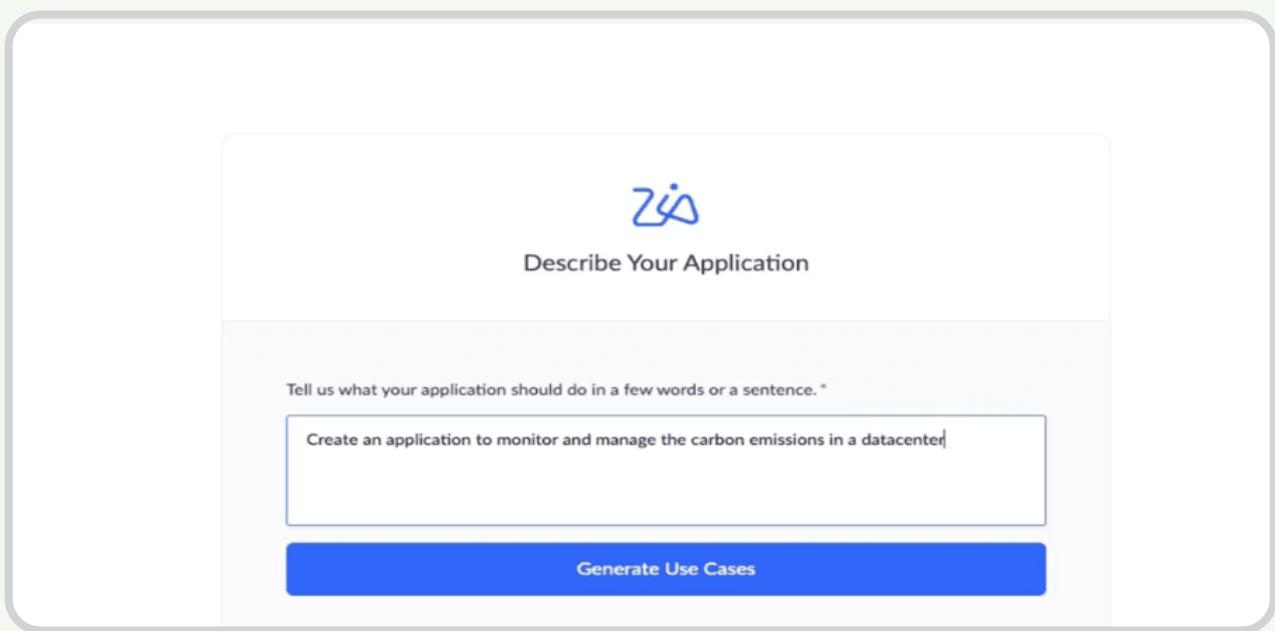
AI is revolutionizing low-code development by transforming how applications are built, automated, and optimized. With Zia, AI becomes a creative and analytical partner empowering users to build applications instantly from ideas, automate workflows intelligently, and uncover insights effortlessly.

Developers and business users alike can leverage no-code AI models to predict outcomes, detect anomalies, and personalize experiences without complex coding. From agentic AI assistants that execute tasks autonomously to chatbots and smart forms that enhance engagement and accuracy, AI infuses every layer of application creation with intelligence. The result is a new era of faster development, smarter automation, and adaptive, insight-driven applications that evolve alongside your business.



Build smart applications with ease

Turn ideas into reality instantly with Zia's AI-powered application builder. Simply provide a text prompt, sketch, or diagram, and Zia automatically generates complete applications, including forms, reports, dashboards, workflows, and blueprints helping teams accelerate development and innovation with minimal effort.



Zia's AI-powered application builder.

Predict, classify, and detect with no-code AI

Empower your applications with no-code AI models trained on your own data. Predict outcomes, forecast trends, categorize information, and detect anomalies effortlessly, bringing intelligence and adaptability to every business workflow—no data science expertise required.

The screenshot shows the AI Modeler interface. At the top, there are navigation links: 'AI Modeler' (with a back arrow), 'Help', 'What's New', 'Post Your Requirement', and a close button. The main content is divided into two sections: 'Build - Custom Models' and 'Deploy - Ready to Use Models'.
Build - Custom Models
This section is titled 'Train and publish your own models with a relevant dataset and address specific tasks'. It contains three cards:

- Prediction**: Predict future outcomes based on historical data.
- OCR**: Extract specific field-value pairs from text-based images or PDFs.
- Object Detection**: Identify custom objects and streamline your business process.

Deploy - Ready to Use Models
This section is titled 'Deploy models straight into your applications for enhanced productivity'. It contains four cards:

- Keyword Extraction**: Extract most relevant keywords from a text.
- Sentiment Analysis**: Analyse sentiment from a text and categorise feedback.
- OCR (Pre-Built)**: Detect and extract text present in any image or PDF.
- Object Detection (Pre-Built)**: Identify and detect common objects present in an image.

On the right side, there is a 'FAQ's' panel with expandable questions:

- What are custom models?
- What are ready to use models?
- What are the tasks or processes that I can automate using AI Modeler?
- How can my organization benefit from using AI Modeler?

AI modeler.

Automate workflows intelligently

Streamline operations with AI-driven automation that triggers actions based on user behavior, historical patterns, or predictive inputs. By intelligently orchestrating workflows, Zia helps you eliminate manual effort, reduce response time, and improve business agility.

Create autonomous AI agents

Design agentic AI-powered assistants that can analyze data, make decisions, and perform complex tasks autonomously, all driven by natural language instructions. These AI agents act as proactive problem-solvers, enhancing productivity and accelerating outcomes across your organization.

Understand emotions with sentiment analysis

Use AI-powered sentiment analysis to interpret text from reviews, surveys, or feedback forms. Detect positive, neutral, or negative sentiments automatically, helping you gauge customer satisfaction and drive smarter, insight-backed decisions.

Extract data instantly with AI vision

Leverage optical character recognition and AI vision to automatically extract critical information from documents and images such as invoices, receipts, or ID cards. Reduce manual data entry and increase accuracy with instant, intelligent data capture.

Enable multilingual and context-aware applications

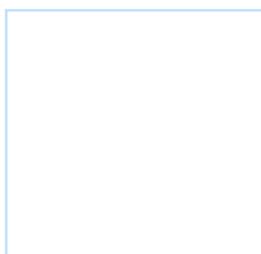
Classify and translate text seamlessly to support multilingual, content-sensitive, and region-specific use cases. With AI language models integrated into your applications, you can deliver localized experiences that resonate with users everywhere.

Deliver conversational application experiences

Enhance user engagement with AI-powered chatbots built on Zia's natural language understanding. These conversational interfaces guide users, answer queries, and automate routine actions turning static applications into interactive, intuitive experiences.

Simplify data entry with smart suggestions

Boost data accuracy and speed with AI-driven auto-suggestions and field-level predictions. Zia anticipates user inputs, recommends relevant values, and reduces human error making form filling faster, smarter, and more reliable.



Secure, explainable, yours: ManageEngine's approach to AI

For more than 13 years, ManageEngine's R&D team has been dedicated to building transformative AI capabilities that are seamlessly integrated into our solutions.

Developed from the ground up and powered by our independent stack, our AI not only delivers intelligent, explainable features but also ensures the highest standards of privacy. By keeping every operation in house, we ensure your data remains protected always. Moreover, we design our AI capabilities as integral features that enhance our product capabilities, never as an add-on that users pay extra for.

Our strength lies in a foundation of reliable infrastructure and purpose-built AI models engineered to deliver scale, speed, and trust without compromise.

The infrastructure

- 18 data centers across the globe, with more on the way.
- GPU-accelerated databases that enable high-speed data access.
- Investment in ASICs in addition to GPUs.
- Designed for scale: Strategically positioned network PoPs.
- Strategic alliances with NVIDIA, Intel, and AMD/Xilinx to fuel performance.

The models

- 80 AI algorithms deployed.
- Right-sized models that optimize compute and data usage.
- Our search platform doubles as a RAG database.
- Designed with data boundaries in mind.
- Built on top of self-hosted Llama and Mistral models.

For us, AI isn't just a buzzword—it represents a long-term commitment to building solutions that make a real impact for our customers. Our focus is on delivering technology that drives lasting value, respects your data, and integrates seamlessly into your system.



The ManageEngine AI advantage

With ManageEngine, your AI is truly yours. Built entirely in-house with no external dependencies, our AI gives you explainability, reliability, and full control over your data. It's a powerful yet privacy-first solution that seamlessly integrates across our IT management suite to help IT leaders secure operations, simplify complexity, and stay ahead with confidence.

Explanation-ready

As explainable AI becomes increasingly vital, we have prioritized clarity by implementing an explanation-first approach wherever feasible.

Optimized for low data environments

Recognizing the importance of data efficiency, our AI models are fine-tuned using transfer learning techniques to excel even with minimal data inputs.

Built to separate signals from noise

Data preparation and cleansing are needed for AI to deliver insights from noise, and we've added this approach to our models to help with predictions and actions.

Proactive by nature

Our AI models anticipate and respond to IT incidents by taking proactive actions, ensuring smoother operations.

Not resistant to change

Adaptability is key, and our AI systems continuously learn and adapt to changes, ensuring relevance and effectiveness.

Privacy comes first

We've built our AI to be privacy-first, ensuring that your information remains fully protected and independent of any external dependencies. All data and models are exclusive to each organization or user, with no cross-organization data sharing.

More about ManageEngine

ManageEngine crafts the industry's broadest suite of IT management software. We have everything you need—over 60 products—to manage all of your IT operations, from networks and servers to applications, service desk, Active Directory, security, desktops, and mobile devices.

Since 2002, IT teams like yours have turned to us for affordable, feature-rich software that's easy to use. As you prepare for the IT management challenges ahead, we'll lead the way with new solutions, contextual integrations, and other advances that can only come from a company singularly dedicated to its customers. And as a division of Zoho Corporation, we'll continue pushing for the tight business-IT alignment you'll need to seize opportunities in the future.



Trusted by



Recognized by leading
analyst firms



