ManageEngine Log360 Cloud

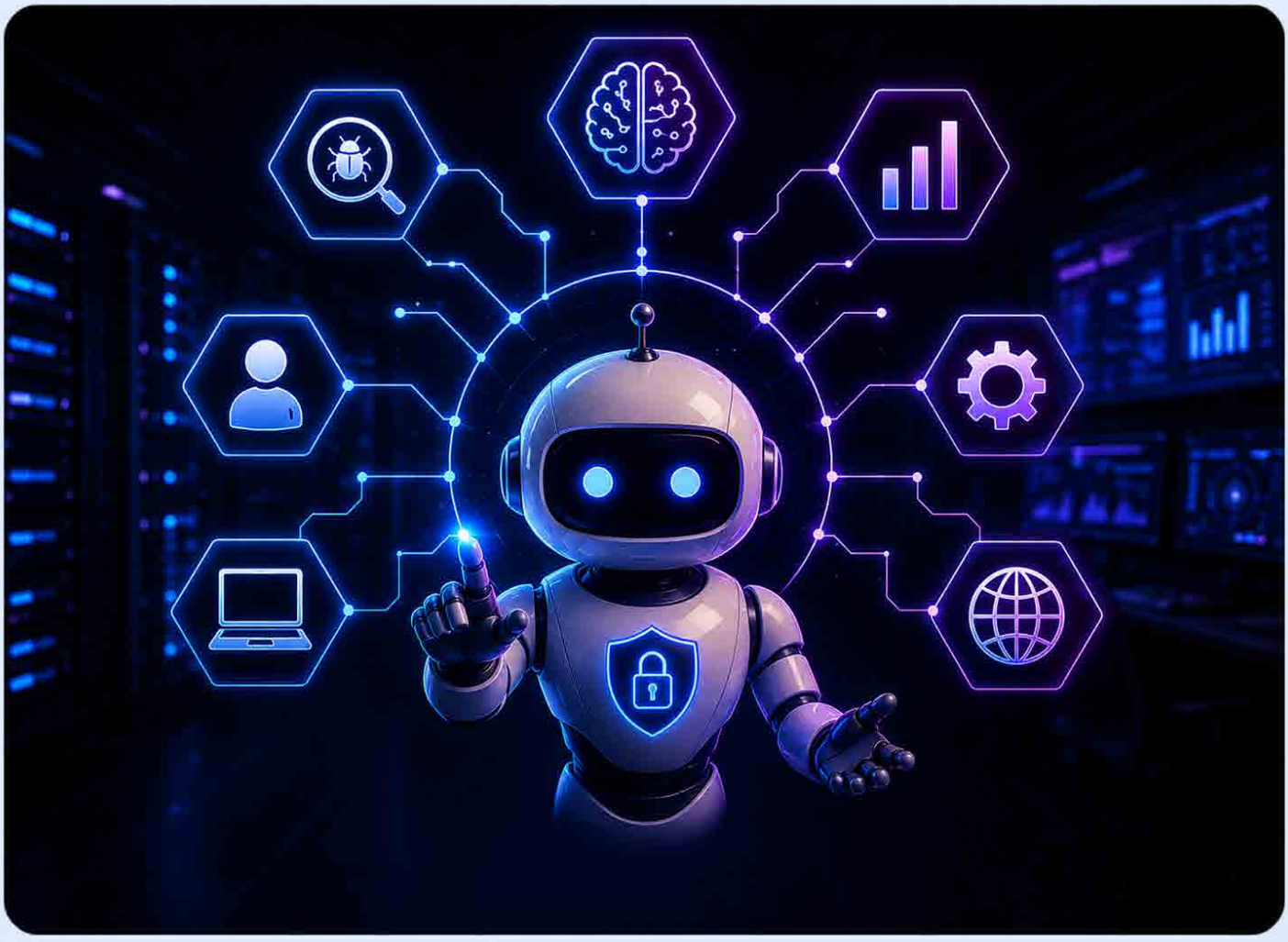
Zoho Zia Agents

DATASHEET

AI Agents for your SOC

Zia Agents in Log360 Cloud

A native platform to deploy prebuilt AI agents from the Agent Store, and build custom agents using no-code to automate investigations, risk assessments, and other parts of your SOC workflows.



www.manageengine.com/cloud-siem

Zoho Zia Agents allows Log360 Cloud users to build, deploy, and manage AI agents that work inside Log360 Cloud. It combines a store of prebuilt agents with a no-code builder for creating custom ones. Every agent runs on the model you select, uses only the APIs you authorize, follows the instructions you provide, and operates within the guardrails you define. Deployed agents are invoked from Ask Zia, the conversational AI assistant inside Log360

How to get started

1. Sign in to Zia Agents at agents.zoho.com with your Log360 Cloud account.
2. Browse the Agent Store and hire prebuilt agents that fit your workflows
3. Open Agent Studio to build custom agents from scratch using natural language.
4. Manage agents from the Agents page, including tools, instructions, and knowledge bases.
5. Invoke deployed agents from Ask Zia inside the Log360 Cloud console.

Prebuilt agents store

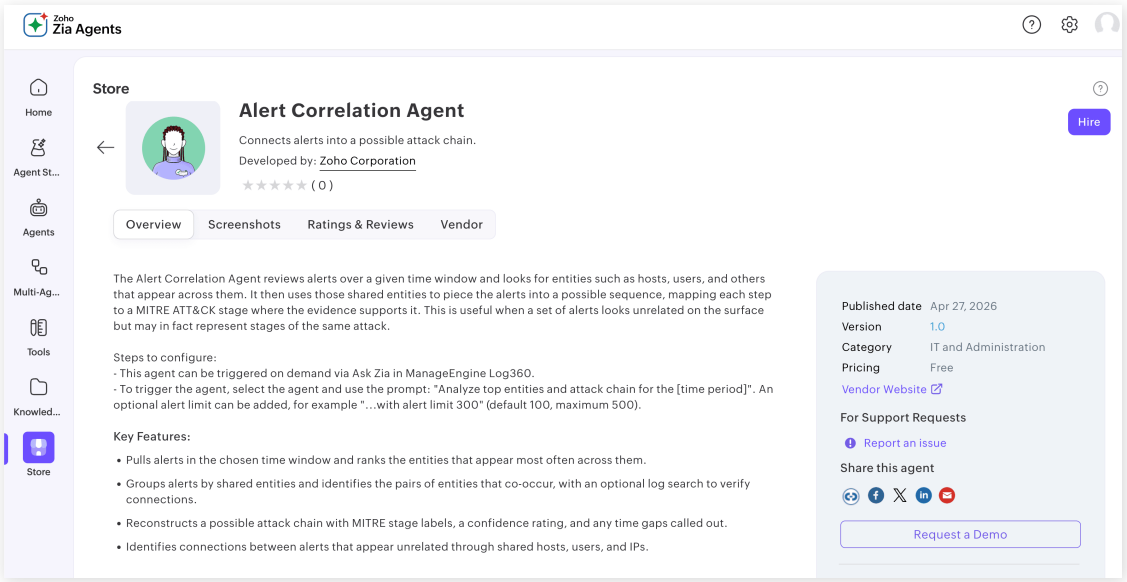
A growing library of purpose-built agents for common security workflows. Each one comes preconfigured with the tools, instructions, and guardrails needed for its task, and can be deployed in a single action.

- **User Activity Review Agent**

  Pulls together a user's logons, authentication events, file access, and alert history over a chosen time window into a single record. Useful for compliance audits, and any investigation where a user's activity needs to be assembled quickly.

- **Alert Correlation Agent**

  Takes a set of alerts from a chosen time window, extracts shared entities and sequences them into a probable attack chain with a confidence rating. Cuts down the manual work of spotting whether separate alerts are actually one incident.



How to build a custom AI agent

Every custom agent is built the same way: describe what it does, connect its tools, ground it in knowledge, and set the boundaries. The builder walks through six steps.

1. Name and role:

- Give the agent a name and one sentence describing what it does.

2. Choose a model:

- Pick a Zoho-hosted model or bring your own key for OpenAI or Anthropic. Different agents can run on different models.

3. Instructions:

- Write plain-language instructions for how the agent should approach its task, what to prioritize, and what to return.

4. Knowledge base:

- Upload SOC SOPs, runbooks, policies, or any reference material the agent should reason against.

5. Tools:

- Authorize the specific Log360 APIs, and if needed, tools from other ManageEngine or Zoho products. The agent can only use what you authorize

6. Guardrails:

- Set do's and don'ts, enable bias and toxicity checks, and restrict scope. Once deployed, the agent can be invoked from Ask Zia.

Example: GDPR Risk Analyzer

Field	Value
Name	GDPR Risk Analyzer
Role	Analyzes events for potential GDPR compliance risks and reports findings against organizational policy.
Model	Zoho Hosted (Qwen 3.5 122B MoE)
Instructions	Identify patterns that may indicate GDPR risk. Cross-reference findings against the organization's data-handling policy. Surface specific policy gaps rather than listing events. When policy interpretation is ambiguous, flag the gap instead of guessing.
Knowledge base	Organization data-handling policy · List of users with elevated privileges · Inventory of critical devices and repositories holding personal data
Tools	logs360_simpleSearch, logs360_aggregatedSearch. logs360_getAlerts, ogs360_getReportData, logs360_getEntityRiskProfile
Guardrails: Do's	Cite specific log evidence for critical finding. Reference relevant policy sections. Flag missing or ambiguous information rather than infer.
Guardrails: Don'ts	Do not fabricate compliance status. Do not expose PII in output; use user identifiers instead. Do not make legal determinations; findings are advisory.

More agents you can build

Alert Briefing Agent

Pulls open critical alerts and their profiles for the day based on risk and defined instructions so the incoming analyst starts with a prioritized list instead of scrolling the alert queue.

Detection Coverage Analyzer

Compares installed detection rules against the MITRE ATT&CK catalog and flags tactics or techniques with no corresponding rule, giving a detection engineer a gap list to speed up their work.

Rule Tuning Advisor

Reviews rules generating high alert volume and surfaces the suggested exclusions or tuning changes for each, so a rule doesn't get disabled outright just because it's noisy.

Cross-product agents

Agents aren't limited to Log360 tools. Authorize APIs from Endpoint Central to pull patch and vulnerability data for a host, ServiceDesk Plus to raise or update tickets, or Site24x7 to check network anomalies. A single agent can span multiple ManageEngine products for workflows like device risk analysis, incident enrichment, or cross-product compliance reporting.

ManageEngine
Log360 Cloud

About Log360 Cloud

Log360 Cloud is a unified security platform designed to help organizations progress from log visibility to measurable security outcomes. The platform unifies log collection, correlation, behavioral analytics, and built-in SOAR to take security teams from detection through investigation to automated response in a single workflow. Zia, the AI layer inside Log360, turns raw alerts into analyst-ready context, replaces manual queries with natural language, puts prebuilt and custom AI agents to work on bounded SOC tasks, and connects the platform to external AI tools through MCP. Log360 Cloud helps security teams reduce dwell time, improve operational efficiency, and strengthen overall SOC maturity.

For more information about Log360 Cloud, visit www.manageengine.com/cloud-siem/ and follow the LinkedIn page for regular updates.

Sign-up for free

Get a personalized walk-through