ManageEngine
Log360 Cloud

DATASHEET

Zia for Log360

AI-powered security operations

Zia is the AI layer inside Log360. It brings contextual insights, autonomous investigation, conversational search, prebuilt and custom security agents, and open AI interoperability through the MCP into a single platform. Analysts move from manual log parsing and console-hopping to natural-language workflows, with full control over models, data residency, and agent boundaries.

Built for the realities of the SOC

Modern security operations live with rising alert volume, fragmented tooling, query syntax that locks data behind specialists, and investigations that span multiple products. Zia AI in Log360 Cloud is built around these realities, returning analyst time back so teams can focus to what really matters.

Zia delivers this through progressive layers of AI capability, each one addressing a distinct bottleneck in the modern SOC.

Augment

The first stage adds context to every alert so triage starts from an analyst-ready picture instead of raw data.

Assist

The second replaces query syntax with natural language, so analysts get answers from the data without manual queries.

Accelerate

The third lets agents run bounded tasks across the stack and opens Log360 to external AI clients, so investigations don't have to live in one tool.

Each layer builds on the last, laying the path to autonomous security operations, where AI-driven workflows perform triage, make verdicts, and initiate response actions with minimal human intervention.

Ask Zia: talk to your SIEM in plain language

A built-in conversational AI assistant accessible from anywhere in the Log360 Cloud console. Analysts query logs, alerts, and audit data in natural language, and invoke agents directly from chat. No search syntax. No module switching.

Key capabilities

Conversational log and alert search

Ask questions and get results instantly.

Examples:

"Show top 5 users with failed logons", "Show critical alerts in the past 1 hour", "Who modified group policies recently?"

Audit retrieval in natural language

Surface technician activity with prompts such as

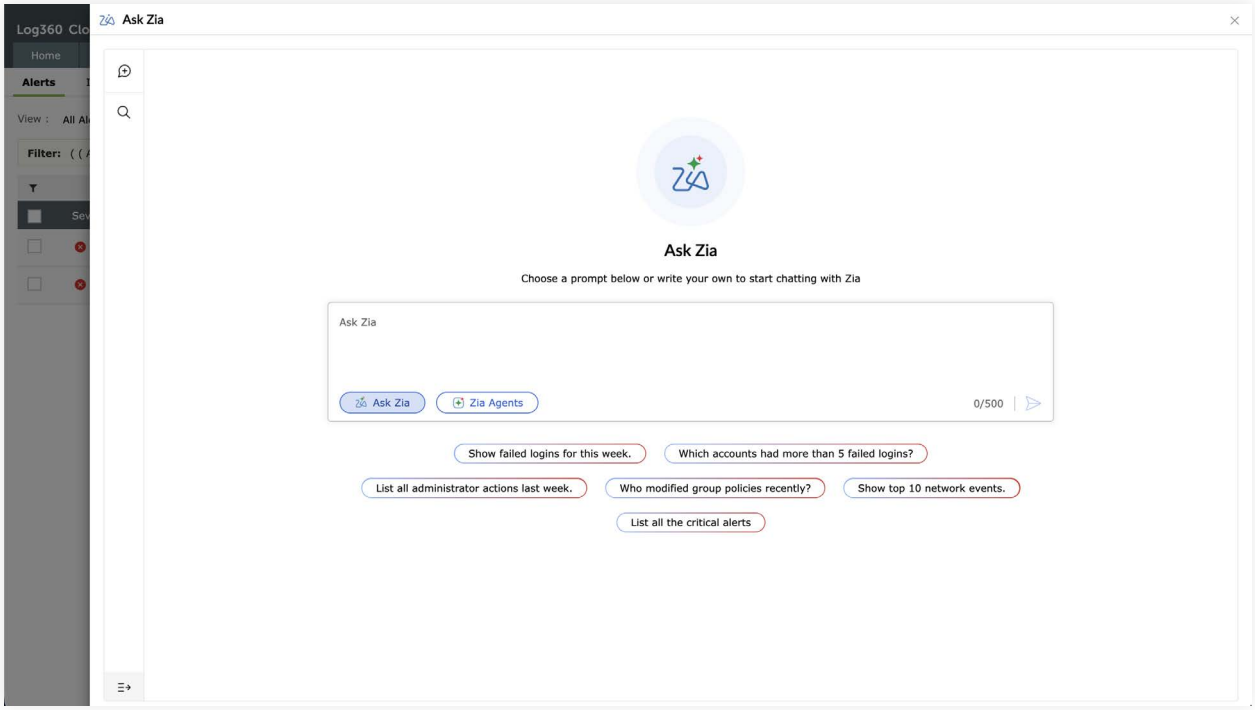
"Show me recent storage tier actions by my technicians."

Agent invocation from chat

Trigger and interact with prebuilt or custom agents.

Example:

"/Device_Risk: Analyze risk for [Server-01]".



Zia Agents: prebuilt and custom agents for your SOC

Zia Agents lets security teams hire prebuilt agents from the Zia Agent Store and build custom AI agents for tasks specific to their environment. No code required. Every agent is callable from Ask Zia.

Prebuilt agents, ready to deploy

User Activity Review Agent

Compiles a complete record of any user's logon, authentication, file access, and alert activity over a specified time period into a single defensible summary. Built for pre-termination reviews, compliance audits, and active investigations.

Alert Correlation Agent

Reviews alerts in a chosen time window, identifies shared entities (hosts, users, IPs) across them, and sequences them into a probable attack chain with MITRE ATT&CK stage labels, a confidence rating, and remediation steps.

Build your own custom agents, no code

Security teams describe what the agent should do in plain language. From there, the builder walks through five steps:

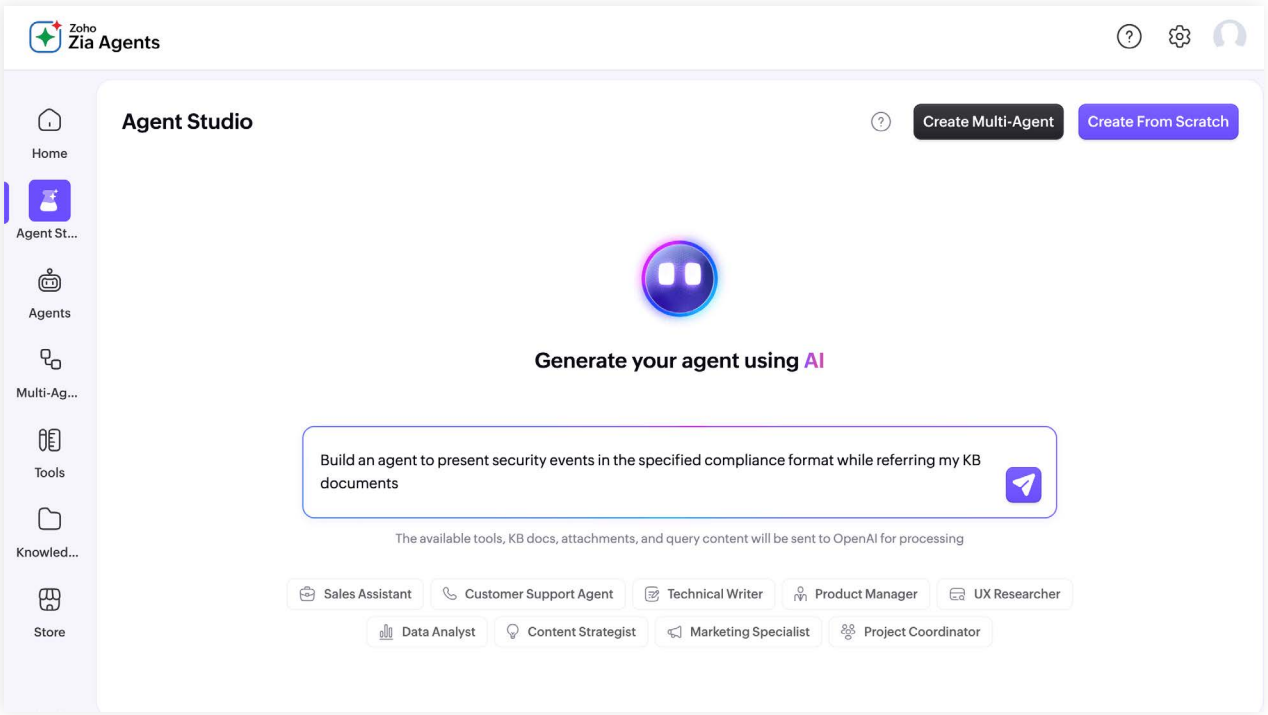
01 Describe:
Type the agent's purpose in plain language. Zia generates the structure and initial configuration.

02 Choose the LLM:
Zoho-hosted models or BYOK with leading third-party LLMs. Different agents can run on different models.

03 Connect tools:
Authorize prebuilt API tools from Log360 Cloud, other ManageEngine apps, and Zoho apps. Add external APIs if needed. Agents only use what you authorize.

04 Add a knowledge base:
Upload SOC SOPs, internal runbooks, compliance policies, or reference material. The agent reasons against this context.

05 Set guardrails and deploy:
Define do's and don'ts, restrict actions, and control scope. Once deployed, the agent is callable from Ask Zia.



Cross-product reach

Agents can pull context from Log360 Cloud, Endpoint Central, ServiceDesk Plus, and Site24x7 in a single investigation. A custom agent for device risk analysis can return a consolidated risk summary built from asset ownership, known vulnerabilities, detections, UEBA signals, and network anomalies across the four products.

Run agents with confidence

- **Scoped access:**
  Agents only access the API tools you explicitly authorize.
- **Full audit trail:**
  Every session records queries made, tool calls, and actions taken.
- **Guardrails always on:**
  Bias checks, toxicity filters, and custom rules hold regardless of how a session unfolds.

Zoho MCP Server: connect Log360 to your preferred AI client

Log360 Cloud supports the Model Context Protocol (MCP) through the Zoho MCP Server. Connect Log360 Cloud to AI clients such as Claude, Copilot, and Cursor, and let your team interact with Log360 capabilities from the tools they already work in.

What it enables

Query, hunt, and act from any AI client

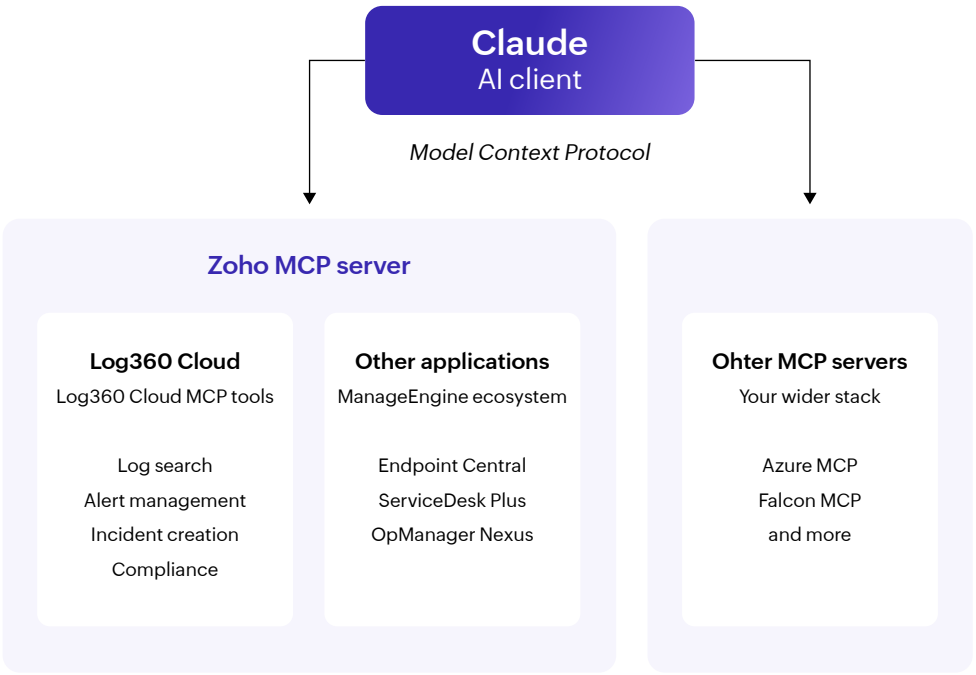
Query log and alert data, hunt for threats, manage configurations, and act on incidents from Claude, Copilot, Cursor, or any MCP-compatible client. Log360 Cloud becomes the data and action layer beneath the conversation.

ManageEngine and Zoho product orchestration

Take real actions across Endpoint Central, ServiceDesk Plus, Site24x7, and Zoho business applications from a single prompt. Investigation and response no longer require switching between product consoles.

Cross-stack threat investigation

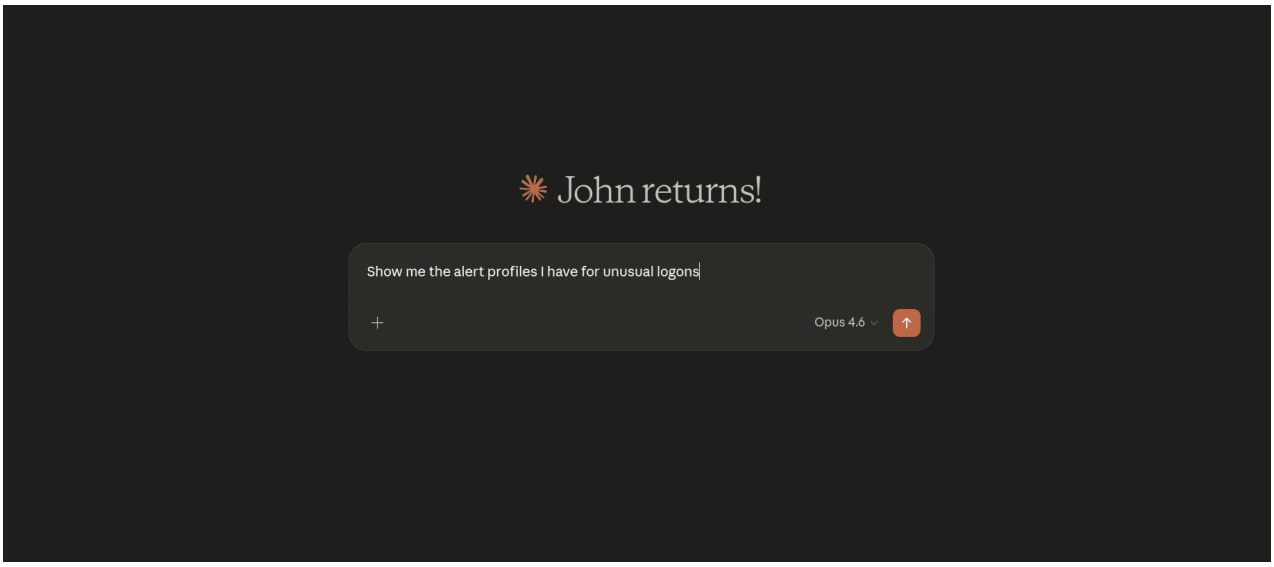
Chain the Log360 Cloud MCP server with other MCP servers in your environment, including Azure MCP, Falcon MCP, and others. Investigations span EDR, cloud security, identity, and SIEM in a single workflow.



Also compatible with Copilot, Cursor, and any MCP-compatible AI client

Try these from Claude, Copilot

- *"Show me alert profiles I have for unusual logons"*
- *"Enable or disable profiles"*
- *"Show me recent alerts from profile 'dropbox brute force logon'"*
- *"Investigate the alert 'brute force attack'"*



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