

Edwin AI Agent

Built to understand IT context and orchestrate incident response across systems

When incidents strike, IT operations teams need AI that turns alerts into action.

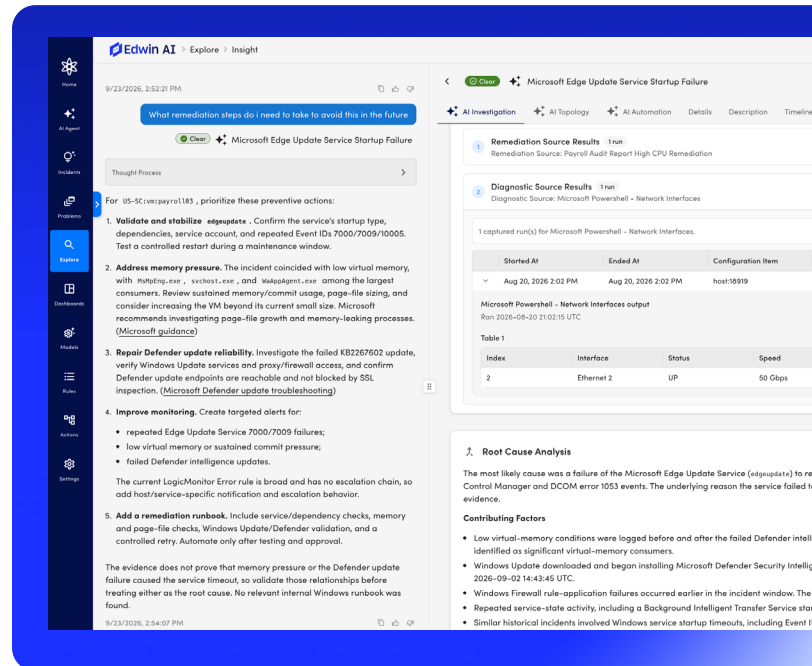
Incident response breaks down across fragmented tools: alerts in one place, logs in another, tickets somewhere else, and runbooks scattered across teams. Engineers lose critical time switching between systems, manually correlating signals, and coordinating response while services remain degraded.

Edwin AI: **AI Agent** brings investigation, service context, and response orchestration into a single system. Built on top of **Event Intelligence**, it enables teams to move from fragmented analysis to coordinated response, accelerating resolution and reducing operational overhead.

With AI Investigation, Edwin AI correlates logs, metrics, incident data, knowledge sources, and change data to accelerate root cause analysis. AI Topology Intelligence adds dependency-aware context to help you understand the blast radius and prioritize incidents by business impact, while the Orchestrator coordinates investigation and response across LogicMonitor and connected tools, speeding up insights, triage, and remediation. Expanded MCP integrations extend this intelligence across your existing toolchain, unifying data and actions in a single workflow. This results in a single system that helps teams understand, prioritize, and orchestrate response, without manual coordination.

"AI Agents like Edwin AI will be 10x or 100x faster than a human...able to manage complex problems."

Gaël Grootaert, Group Director, Devoteam Managed Services



Proven AI Customer Success in Production

CUSTOMER

IMPACT

syngenta

1 hour time to value



88% noise reduction

nexon

67% incident reduction



58% operational efficiency



68% deduplication

What AI Agent Delivers

AGENT CATEGORY	AGENTS & CAPABILITIES
ITOps Agents	Accelerate investigation and decision-making • ITOps Agent: Provides guided investigation, triage, and remediation recommendations through a natural language interface—enabling teams to query incidents, request RCA, and access system context instantly. • Charts Agent: Generates real-time visualizations to help teams understand trends and system behavior.
ITSM Agents	Integrate service management and speed resolution • Similar Incidents Agent: Identifies past incidents and surfaces proven resolutions automatically. • Change Requests Agent: Highlights recent configuration changes and deployments to accelerate root cause identification.
Observability Agents	Analyze operational signals across infrastructure, networks, logs, metrics, and digital experience • Log Intelligence Agent: Detects anomalies and patterns in logs (from LogicMonitor and third party sources) to accelerate root cause analysis. • Metrics Agent: Analyzes performance metrics to identify issues before they escalate. • Network Agent: Applies domain-specific intelligence to analyze network issues, expedite troubleshooting, and identify likely causes and next steps. • Alert Threshold Recommendations Agent: Analyzes alert behavior and recommends threshold adjustments to reduce noise and improve alert effectiveness. • Digital Experience Agent: Surfaces high-confidence insights across alerting and non-alerting conditions—including anomalies, SSL certificate expirations, script drift, and coverage gaps—with supporting evidence and recommended next steps, so teams know where to investigate or act without digging through dashboards.
Knowledge Agents	Makes operational knowledge instantly accessible • Public Knowledge Agent: Surfaces relevant vendor documentation and external knowledge sources. • Private Knowledge Agent: Retrieves answers from internal documentation, runbooks, and standard operating procedures without context switching.
Automation Agents	Coordinate response and reduce manual effort • Generate Automation Agent: Creates remediation workflows based on incident context and best practices. • Discover & Execute Automation Agent: Identifies and coordinates execution of existing automation across tools to resolve incidents quickly.

These agents are powered by a set of core AI capabilities that bring context, precision, and coordination to every interaction.

Core Capabilities Powering Edwin AI Agents

The intelligence layer behind every agent interaction

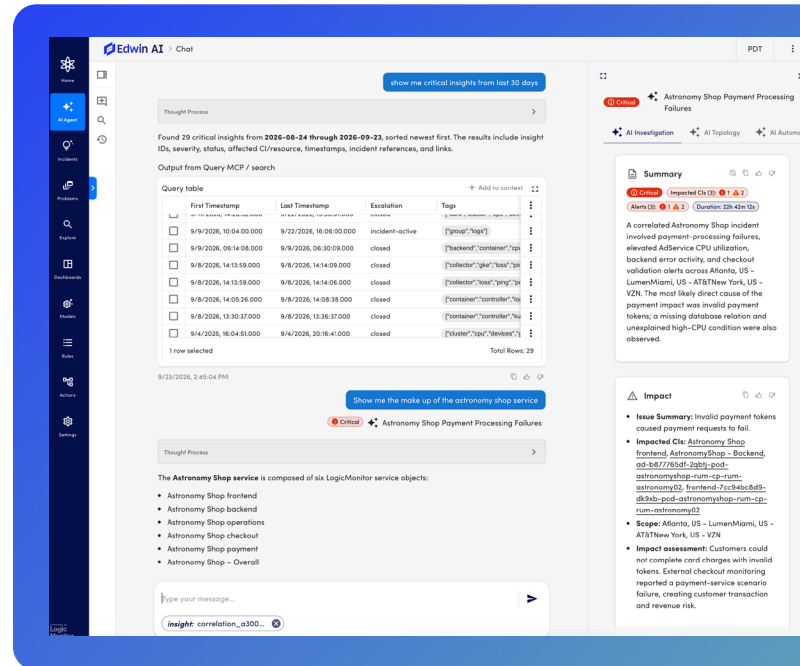
- **AI Investigation:** Multi-source reasoning across logs, metrics, ITSM, knowledge, collaboration tools, and change data, which accelerates root cause analysis and reduces escalations.
- **AI Topology Intelligence:** Dependency-aware context that maps relationships across infrastructure and services that enables teams to understand service impact, reduce false positives, and prioritize incidents effectively.
- **Orchestrator Agent:** Coordinates investigation and response across LogicMonitor and connected systems, reducing handoffs and accelerating resolution across your environment.
- **Expanded Model Context Protocol (MCP) Ecosystem:** Native integrations with ServiceNow, Dynatrace, Splunk, Elastic, GitHub, and Confluence to unify observability and workflow intelligence across your existing toolchain.

ITOps detects incidents. Edwin AI understands, prioritizes, and orchestrates response.

Edwin AI closes the execution gap between detection and action, bringing context, prioritization, and coordinated response into a single system. Teams resolve incidents faster, reduce escalations, and eliminate the manual effort required to manage complex environments.

By combining topology-aware context with change-aware investigation, Edwin AI agents help teams pinpoint root causes faster and act with confidence.

Edwin AI represents a critical step toward Autonomous IT, where operations become more proactive, more intelligent, and increasingly coordinated without human bottlenecks.



Book a demo today and see how Edwin AI moves your IT operations from detection to coordinated response.

BOOK A DEMO TODAY

logicmonitor.com/edwin-ai-demo