



Product Brief

Uptycs Juno AI Assistant

The verifiable AI assistant built for modern security teams

The Challenges Security Teams Face



Noise and false positives

High alert volume and irrelevant signals slow down investigations.



Fragmented context

Critical data lives across separate tools, making it harder to see the full picture.



Opaque AI output

Many AI tools summarize findings without showing how they reached their conclusions.

How Juno Solves These Challenges



A real AI assistant

Juno focused on understanding daily workings of SOC analysts and was designed to add value to the hard working team in the SOC, understand how they work, what they need and provide them with a tool that drives real value



Evidence-backed findings

Transforms complex signals into plain-language conclusions supported by data, queries, and visible reasoning.



Immediate impact clarity

Shows what is affected, what is safe, and what requires action.



Faster triage and reduced noise

Improves investigation flow by removing uncertainty and minimizing distractions.

Juno is a fully embedded AI assistant inside the Uptycs platform. It works on the same unified telemetry and data lake that power Uptycs visibility, investigation, and detection. By interpreting signals across clouds, containers, endpoints, and identities, it delivers clear answers supported by real evidence that analysts can trust.

The Value Juno Delivers

With Juno, analysts gain the insight and confidence needed to resolve investigations faster and with greater accuracy.

- Clear, trusted insights rooted in unified telemetry
- Faster investigations with consistent context
- Reduced noise across cloud, containers, endpoints, and identities
- Analysts stay focused on meaningful risks
- Confident decision-making supported by transparent reasoning

I'm **Juno**, your verifiable AI assistant

Ask me a question

Agent: Auto-Select

Suggestions:

Find EC2 instances with outbound traffic spikes in the last 6 hours
Show suspicious IAM activity involving cross-account role assumption
Check for large S3 downloads by unusual users

The screenshot displays the Uptycs Juno AI Assistant interface. On the left, a 'Finding 1: Active Cryptocurrency Mining Operations' is highlighted with a 'CRITICAL' status. The finding text states: 'Critical cryptocurrency mining compromise detected across multiple Linux systems. Cudo Miner software actively running on demo-u20-1 and demo-az-atk-1 with persistent connections to Cloudflare-hosted mining pools, consuming unauthorized compute resources.' Below this, 'Recommended Actions' are listed with corresponding bash commands: 'Immediately terminate mining processes' (sudo pkill -f cudo-miner && sudo systemctl stop cudo-miner), 'Remove mining software' (sudo rm -rf /usr/local/cudo-miner/ && sudo find /etc -name "cudo" -delete), and 'Block mining pool IPs' (sudo iptables -A OUTPUT -d 104.26.10.102 -j DROP && sudo iptables -A OUTPUT -d 104.26.11.102 -j DROP). A final note says 'Investigate how mining software was installed and patch entry vector'. On the right, a search bar shows 'Show any evidence of Unusual transfers'. Below it, a 'Unusual Transfer Activity Investigation' summary is shown with tabs for Summary, Execution Plan, Findings, and Raw Data. The status is 'Completed', time taken is '2 minutes, 13 seconds', and the agent is 'Security Analyst'. A list of investigation steps is provided: 'Initialize investigation', 'Discover network and file transfer data sources', 'Analyze network traffic patterns for unusual volumes' (with an 'Expand' link), 'Investigate file transfer activities' (with an 'Expand' link), and 'Examine CloudTrail for data movement events' (with an 'Expand' link).

Why Juno Is the Best Choice

How Juno Compares to a Leading AI Security Platform

Capability	Juno AI Assistant	Other AI Security Platforms
Beyond the CNAPP Platform	Juno can look at websites, logs or any external source of information and provide an analysis of your company's position	CNAPP vendors use AI to provide access to the data set they have, it improved usage but do not add additional value
Data foundation	Unified data model backed by Uptycs telemetry across cloud, workloads, containers, endpoints, and identities	Strong visibility, but data often segmented by product area (endpoint-first, cloud-first, or identity-first)
Insight transparency	Provides evidence, queries, and reasoning for every conclusion	Uses advanced AI, but findings are typically summarized without showing underlying logic
Analyst workflow fit	Designed specifically for triage and investigation workflows	Often delivered via chatbot or general-purpose AI not optimized for SOC tasks
Security and trust	Powered by Claude on AWS Bedrock with enterprise-grade protections	AI hosting and data handling vary, with less transparency across vendors
Coverage consistency	Consistent insight across the entire attack surface within one platform	Coverage depends on deployed modules or agents, leading to varied depth

Uptycs provides a SaaS and on-prem SQL-powered security analytics platform for security analysts, site reliability engineers, incident response teams, and IT professionals to observe and secure their productivity endpoints (macOS, Windows), server endpoints (Linux, containers), and cloud providers. Enterprises are using Uptycs for comprehensive security visibility at scale. Common use cases include fleet visibility, intrusion detection, vulnerability management, audit, and compliance for their laptops, servers, and cloud workloads.



Secure Everything from
Dev to Runtime

See Uptycs in action