

Cisco **Cloud Control** unifies networking, security, compute, observability, and collaboration into a single management plane with one login, unified inventory, and real-time topology. It provides a centralized operational layer to help IT teams by consolidating visibility, insights, workflows, and AI-assisted operations across domains.

Benefits:

Unified Management: Centralized management across multiple Cisco product domains with shared identity and topology, providing a single login and unified inventory.

Support for large-scale environments with multiple tenants, regions, and teams.

AI-Driven Automation and Collaboration: Through AI Canvas, it enables operators and AI agents to collaborate on cross-domain investigations and issue resolutions.

Consistent Security: Define security policies once and enforce them uniformly across both Cisco and third-party systems from a single location.

Cross-Domain Alert Correlation: It correlates alerts and recommends next steps to reduce mean time to resolution.

Proactive Issue Resolution: Predict and resolve performance or security issues before they impact users through advanced telemetry and automated workflows.

Integration: Beyond the Cisco ecosystem, the platform connects to major third-party services and tools with Cisco Cloud Control Studio for building custom AI agents and apps. Connect your data with external platforms like *AWS, Microsoft, Google Cloud, ServiceNow, PagerDuty, Wiz, and Slack*.

Operational Efficiency: It reduces fragmentation, improves operational efficiency, and enables governed agentic IT operations with AI assistance.

Cloud-based SaaS delivery with plans for expanded geographic availability and on-premises connectivity.

AgenticOps: AI agents that can safely monitor, configure, and remediate across domains, with human guardrails.

No Additional Licensing Cost: The platform is included at no extra charge for existing customers who have active subscription licenses for eligible Cisco products.

Conversation Starters:

- What is your typical mean-time-to-resolution on cross-domain incidents, and where does most of the delay occur?
- How many operational tools and consoles does your team navigate across networking, security, and observability today?
- Is your organization evaluating or piloting AI agents in IT operations today? What has held you back from production adoption?
- Are you aware that Cloud Control and AI Canvas are included with your existing Cisco subscriptions?

Capabilities:

AgenticOps Foundation: It serves as an operating model designed to let AI agents and humans work together, sharing the exact same context, system of action, and data.

AI Canvas: A multiplayer digital workspace where operators and AI agents can investigate issues, correlate data across domains, and resolve complex problems together in real time.

Cloud Control Studio: A governed design space where teams can build, customize, and manage their own AI applications and security agents.

Unified Policy & Control: It eliminates passive dashboards by building identity, policy, and Zero Trust directly into the control path, allowing for active execution and automated remediation.

Cisco Integrations:

 AI Defense	 Hypershield	 Nexus Hyperfabric
 Catalyst Center	 Intersight	 Secure Access
 Cisco IQ	 ISE	 Secure Firewall
 Crossworks	 Meraki	 Splunk
 Duo	 Nexus Dashboard	 ThousandEyes
		 Webex Control Hub

3rd Party Integrations:

Anthropic	Flexera	MS Entra ID	OpenAI	ServiceNow
Atlassian	Google	MS Teams	PagerDuty	Slack
Bluecat	Infoblox	Nvidia	Panduit	Vertiv
BMC	Jamf	Okta	PingIdentity	<i>More to come...</i>

Resources:

SalesResources	FAQ's	Cisco IQ (Blog)	C3 Interface
C3 Overview	C3 Studio	AI Assistant	C3 Beta Guide
C3 for DC AAG	AI Canvas	dCloud Demo	Public page