



Redefining data centers for the agentic organization

The AI-ready data center



Engineered for the AI era, not just an AI cycle

AI is moving faster than any technology shift in history, and organizations are struggling to keep pace. AI network traffic is set to triple within three years¹, accelerated by physical AI and robotics workloads.

Today's data centers weren't built for this scale, speed or complexity, and trying to re-architect environments is only widening the gaps in performance, observability and security. The operating model itself must change.

Cisco's AI-Ready Data Center is designed with intelligent networking at its heart, security built-in not bolted on, and agentic operations founded on decades of enterprise expertise.

It's a full-stack solution within a single, coherent system, optimized for complex environments and engineered to help you keep pace with AI innovation without a constant rebuild. All of Cisco, all-in for this in-between moment – and beyond.

Watch >

Tom Gillis (CTO, Cisco) leads a conversation on future-proofing infrastructure

Three forces are straining infrastructure built for the previous era

39%



job completion time lost to
inefficient network usage²

As east-west traffic grows, poor path selection slows training, leaves GPUs waiting and raises operating costs as teams pay for compute the network can't fully feed.

Full-stack AI infrastructure

A coherent, optimized system with Cisco and NVIDIA validated designs. Eliminates the performance bottleneck rather than shifting it elsewhere.

10,000+



high / critical vulnerabilities found
in first month of Project Glasswing³

AI models now exploit infrastructure via black-box testing without needing access to source-code. Static defenses designed for human-speed attacks were never built for this threat vector.

Distributed security

Security fused into every layer from silicon to runtime, operating at machine-speed. Reduces AI-speed risk in the agentic and post-quantum era.

100x



more telemetry than fragmented
tools were built to handle⁴

AI systems generate exponentially more signals across infrastructure, workloads, and agents. Fragmented tools weren't designed for this and create blind spots and operational drag.

Agentic operations

A unified operations platform to absorb AI-scale telemetry across every infrastructure layer. Turns signal overload into operational clarity.

THE SYSTEM

A data center solution built for the agentic era – not the last one

01

Full-stack AI infrastructure, engineered as one system for predictable outcomes

AI rewards the best-integrated system, not the best individual components.

Optimize any layer in isolation and the constraint just moves. Most vendors stop at compute and storage but that's where Cisco begins.

Co-designed programmable silicon, networking, security and operations, validated end-to-end and proven at scale. A single system designed for coherence.

02

Distributed security, fused into every layer for resilient infrastructure and apps

AI brings new vulnerabilities and demands a change to the architecture of trust itself.

Security starts with trusted devices, verified software, and encrypted communications that evolve with cryptography.

Controls then move closer to risk: temporary protection ahead of patches/upgrades, segmentation to contain blast radius, and runtime guardrails to stop unsafe AI interactions before impact.

03

Agentic operations aligning speed, precision and simplicity

You can't manage what you can't see. At AI scale, chances are you can't see enough.

For teams working in separate toolchains, a stalled training run becomes a guessing game when AI apps create 10 to 100 times more logging data.

Cisco Cloud Control draws on Cisco's data flywheel of 39M managed devices and 1B+ connected clients, for pattern recognition no point solution can replicate.

This is the platform effect: fabric, compute, security, observability and operations working as one system.

System building blocks

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

More >

Find out how AI leaders are architecting infrastructure differently

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

Validated AI-ready systems, deployed in weeks

Pre-validated

AI Pods deliver co-designed silicon, compute, and networking as a single, pre-validated rack-scale solution. Proven before deployment and automated into repeatable production-ready builds.

Deep technology partnership

Cisco and NVIDIA-validated reference architectures give enterprise AI deployments a proven, repeatable starting point. Custom design work is reduced, accelerating the path from planning to production.

Programmable silicon

Programmable silicon evolves with every AI workload generation, and new load-balancing algorithms arrive as software updates. Fixed-function alternatives ship locked to what they launched with.

CISCO CAPABILITIES AI Pods · Silicon One G300 · Nexus 9300 / 8100 Systems · Cisco Hyperfabric · Cisco UCS · Cisco Unified Edge · Stack Automation by Quali

Watch >

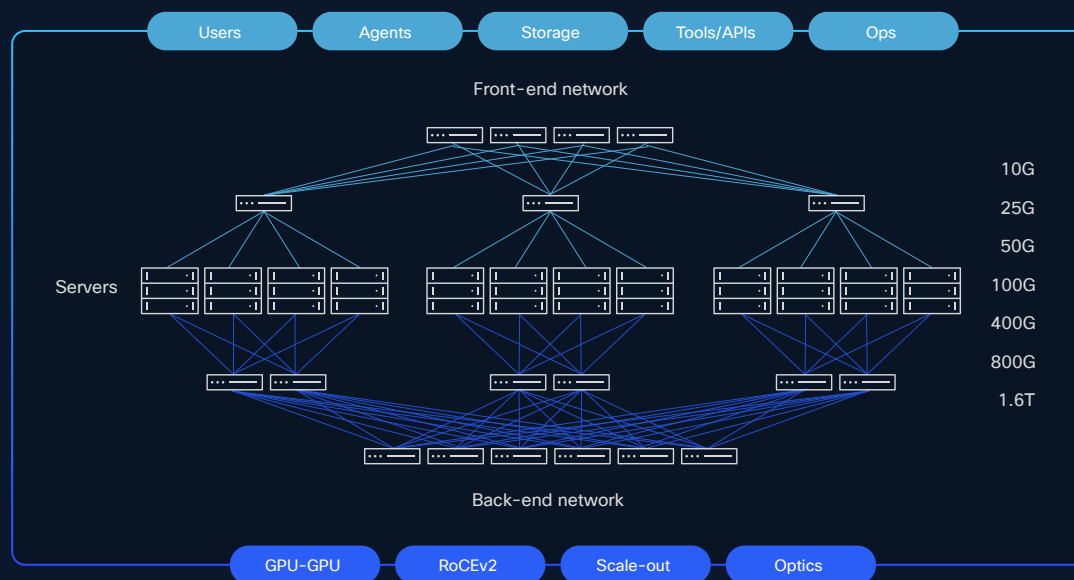
Tom Gillis (CTO, Cisco) and Kevin Deierling (SVP, NVIDIA Networking)
on the Cisco-NVIDIA technology partnership | Watch Clip (0:25)

Validated design

AI networking

Kubernetes-native
intelligenceWorkload exploit
protectionAI model
protectionObservability
with Splunk

The AI spinal cord for performance at scale



AI is a networking revolution. Engineered for performance, resilience and security across critical AI traffic patterns, from training and inference to the fabric flows that keep workloads running.

01: Front-end and back-end networking

Cisco transforms Ethernet into a deterministic, high performance AI-ready fabric, unifying front-end and back-end traffic in a single programmable and orchestrated system.

02: Network intelligence

East-west congestion and poor path selection leave GPUs waiting. Cisco's intelligent load sharing delivers up to 33% higher network utilization⁵ and 28% lower job completion time⁶. Programmable silicon keeps pace with AI standards.

03: Resilient optics

When one degraded optic can cost a multi-day training run, optics must meet all the stress, interoperability and longevity requirements. In tests against 20+ third-party optics, only Cisco met the required standard⁷. Trusted at hyperscale.

CISCO CAPABILITIES · Silicon One G300 · Nexus 9300 / 8100 Systems · N9000 Switches · Cisco Optics · Cisco Hyperfabric

Watch >

Watch Cisco leaders discuss production-ready AI networking outcomes

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

Infrastructure intelligence operating inside the workload

AI workloads increasingly run in Kubernetes environments where traditional infrastructure visibility stops at the cluster boundary.

eBPF-based intelligence extends networking, security and observability directly into containerized workloads, down to the pod and process level, without excessive overhead or application changes.

Process is the new form of identity.

Every container-to-container flow is visible down to the initiating process, beyond just the IP address. This is the foundation for zero-trust segmentation that works at Kubernetes scale.

One operating model extending Nexus One EVPN fabrics to Kubernetes

With Cisco Nexus switches and Isovalent CNI, teams extend their existing network operating model into Kubernetes – so workload context, segmentation and enforcement stay connected across the environment.

- ✓ Use Kubernetes labels, namespaces and workload identity as network context
- ✓ Carry EVPN and VRF context to Kubernetes workloads
- ✓ Align segmentation, visibility and enforcement across VMs, bare metal and pods
- ✓ Trace a flow from the fabric to the pod, and the process behind it

CISCO CAPABILITIES Isovalent Enterprise Platform

Watch >

See how Cisco and Isovalent extend the network fabric into Kubernetes

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

From post-quantum foundations to machine-speed shielding

AI-speed threats can move faster than patch windows, software upgrades and operational change controls. Live Protect shields vulnerable infrastructure during remediation.



Trust, built in

Data captured today can be decrypted tomorrow. Post-quantum cryptography helps establish integrity from first power-on, shielding training sets and model IP across the fabric.



Thousands of enforcement points

Smart Switch brings security enforcement closer to the workload path, using dedicated DPU silicon so protection can update without disrupting network behavior. Stateful protection at the port scales with the fabric.



Continuous machine-speed protection

Exploits don't wait for maintenance windows. Live Protect helps shield affected Cisco infrastructure while teams plan the required reboot or software upgrade, and Workload Exploit Protection extends the same distributed model to customer workloads.

Controlling the agentic era exposure window

Security for AI

Security risks

AI Apps, Models and Agents



New AI attack surface

Workloads & Kubernetes



Runtime behavior, lateral movement, container risk

Networking Infrastructure



Exposed systems, unpatched CVEs, trust boundaries

CISCO CAPABILITIES Cisco Hybrid Mesh Firewall · Live Protect · Secure Firewall 6100 · Isovalent Enterprise Platform

Watch >

Watch Cisco's Glasswing Moment on
AI-speed infrastructure security

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

AI risk controlled from testing to runtime

AI risk does not stop at the network. AI Defense helps teams discover AI applications, models and agents, assess risk before go-live, and apply runtime guardrails in production.

01: Discover AI assets

Identify the AI workloads, applications, models, data and users across your distributed on-premises and cloud environments.

29% of firms feel able to secure agents today⁸

02: Assess risk before go-live

Test for prompt injection, data leakage, unsafe model behavior, misconfiguration, and vulnerable AI components.

92.8% attack success rate for multi-turn jailbreak attacks⁹

03: Protect in real time

Safeguard AI apps and agents against rapidly evolving threats, including prompt injections, denial of service and data leakage.

32% of firms hit by an exploit attack on the AI app prompt¹⁰

At runtime, inline guardrails help block prompt injection, data extraction and misuse, with consistent enforcement across every app. Multi-turn extraction attacks are detected and blocked without app changes.

CISCO CAPABILITIES Cisco AI Defense

More >

See how Cisco AI Defense protects AI apps, models and agents from real-world attacks

Validated design

AI networking

Kubernetes-native
intelligence

Workload exploit
protection

AI model
protection

Observability
with Splunk

Observability across AI, infrastructure, and agentic operations

When AI jobs stall, every minute burns expensive compute and confidence. These systems are too distributed and fast-changing for monitoring alone. Teams need analysis and guidance that pulls the full picture together.

See the signal. Find the cause. Sort the incident

Splunk brings the Kubernetes “IP blob” to life; Isovalent adds eBPF service maps, L3-L7 flows and local telemetry analysis where the work runs. AI Job Observability links GPU and scheduler data so teams move from symptoms to cause, constraint and next best action.

Incident path



The observability advantage is structural.

Cisco Cloud Control turns those signals into shared context, recommended action and governed workflows. It shows what’s running, where, what changed and what to do next.

UNIFIED SIGNALS

Network Fabric

Security Enforcement

Kubernetes / CNI

AI Jobs and GPU Health

CISCO CAPABILITIES · Nexus Dashboard · Splunk AI Infrastructure Monitoring · Isovalent Enterprise Platform · Cisco Cloud Control · Cisco AI Canvas · Deep Network Model

More >

Learn how to turn data into intelligence in the agentic era

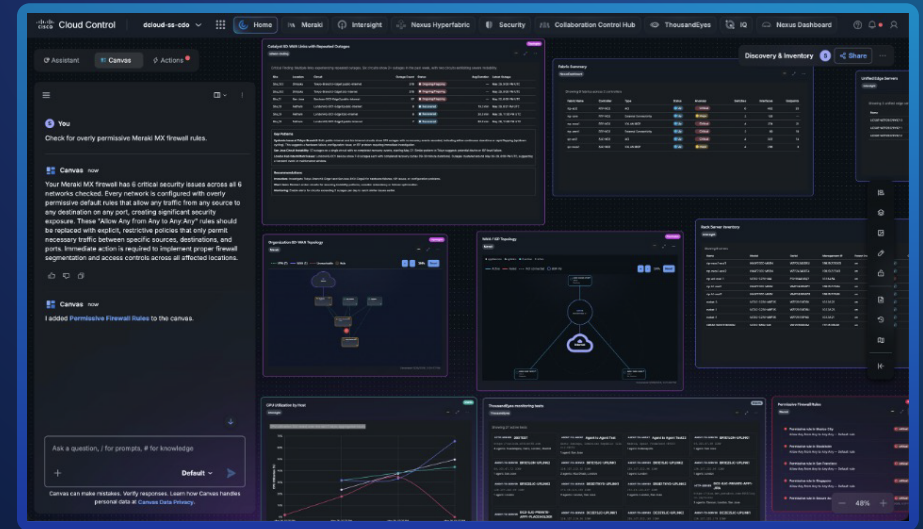
An AgenticOps platform to see and control everything

A single pane of glass was never enough. It unified the view but the data underneath remained fragmented. That's just changed with Cisco Cloud Control, a command center for the agentic enterprise.

Cisco Cloud Control converges identity, assets, topology and telemetry beneath the interface – the operating layer of AgenticOps – so teams work together from the same source of truth. Agentic actions stay directed by human judgment.

Cross-domain operations.

A stalled training run or a creeping vulnerability surfaces as one causal chain, not four dashboards telling four partial stories. Cisco Cloud Control connects Cisco products and lets teams build their own apps and agents in natural language across 50+ third-party tools. Cloud Control Studio gives teams visibility and control without adding complexity.



Where you work
AI Canvas
Cloud Control Studio

Humans + AI agents
working together

Deep Network Model
+ Frontier AI

One login. One inventory. One topology.

Hours of triage collapse to seconds
Agents run multi-step investigations

Bridge calls replaced by one causal chain
A multi-player workspace with full context

A brand-new operating model
Designed for the agentic era

CISCO CAPABILITIES AI Canvas · Cloud Control Studio · Deep Network Model · Nexus Dashboard · Live Protect · Cisco IQ

Watch >

See how Cisco is reimagining operations across the agentic enterprise with Cloud Control

THE UNFAIR ADVANTAGE

Building every layer creates a unique advantage

Cisco AI-ready Data Center

Cisco connects the critical enterprise control points:
networking, security, observability, and operations.

This platform effect brings unprecedented control, security and simplicity at enterprise scale. It's a distinction that won't be measured in terabits per second, it'll be measured in cost per token, resilience under failure, and speed of policy change.



Protects your AI investment

A capital-efficient growth platform that adapts as AI models, workloads and deployment patterns evolve. Program-mable silicon and upgradable software to outlast the refresh cycle.



Protects your enterprise

Security from silicon to model runtime across on-premises, cloud and sovereign deployments so AI innovation isn't a liability. Because switches in some enterprise networks could be old enough to vote.



Protects your operations

AgenticOps built on decades of enterprise expertise. 39M managed devices. 1B+ connected clients. 15B+ API calls per month. A data flywheel no point solution can replicate¹¹.

Watch >

See how McLaren creates an advantage
with Cisco AI-Ready Data Center

A NEW INFRASTRUCTURE ERA STARTS TODAY

Engineered for the AI era – not an AI cycle

The Cisco AI-ready data center is a complete enterprise system with validated architecture, built on silicon and software tested at NeoCloud scale. Designed to carry your critical workloads and maintain control as your AI scales.



**Full-stack AI infrastructure,
engineered as one system**



**Distributed security, fused
into every layer**



**Agentic operations aligning
speed with precision**

CISCO CLOUD CONTROL

One platform. Every domain. The foundation everything else is built on.

ThousandEyes · Security Cloud Control · Stack Automation · Nexus Dashboard · Nexus Hyperfabric · Catalyst SD-WAN · Intersight · & more

Silicon One G300

Programmable silicon that
adapts as AI standards
evolve

Cisco Hyperfabric

NVIDIA-validated fabric
automation for repeatable
AI deployment

Live Protect

Vulnerability shielding at
machine speed for Cisco
infrastructure

Secure Firewall 6100

AI-scale threat protection
that grows with the
data center

Splunk AI Monitoring

Federated full-stack
observability for AI
infrastructure

Deep Network Model

Network AI: 20% more
accurate than general LLMs¹²

Nexus 9300 / 8100

Intelligent AI-scale
networking with predictable
performance

UCS / Unified Edge

Compute from edge to core:
traditional to AI

Hybrid Mesh Firewall

Unified distributed firewalling,
exploit protection and
segmentation

Cisco AI Defense

Model protection, prompt
injection defense, runtime
guardrails

AI Canvas

Multiplayer, role-aware
agentic operations

Cisco 400G / 800G Optics

Validated optics for
AI-scale fabric reliability

Isovalent CNI

Kubernetes-native
networking, policy and
fabric connectivity

Isovalent Runtime Security

Process, file and network
enforcement at the kernel

More ➔

Learn more about Cisco AI-ready Data Center



Learn more at cisco.com/whycisco

Sources: 1. Cisco & Foundry, 'No time to wait' report, 2026 · 2. Cisco Silicon One and G300 data, 2026 · 3. Anthropic, Project Glasswing data, 2026 · 4. Apica, telemetry growth data, 2026
5. Cisco Silicon One and G300 data, 2026 · 6. Cisco Silicon One and G300 data, 2026 · 7. Cisco optics reliability data, 2025 · 8. Cisco, State of AI Security report, 2026
9. Cisco, State of AI Security report, 2026 · 10. Gartner, Generative AI attack survey, 2025 · 11. Cisco operational data, 2026 · 12. Cisco Deep Network Model benchmark data, 2025