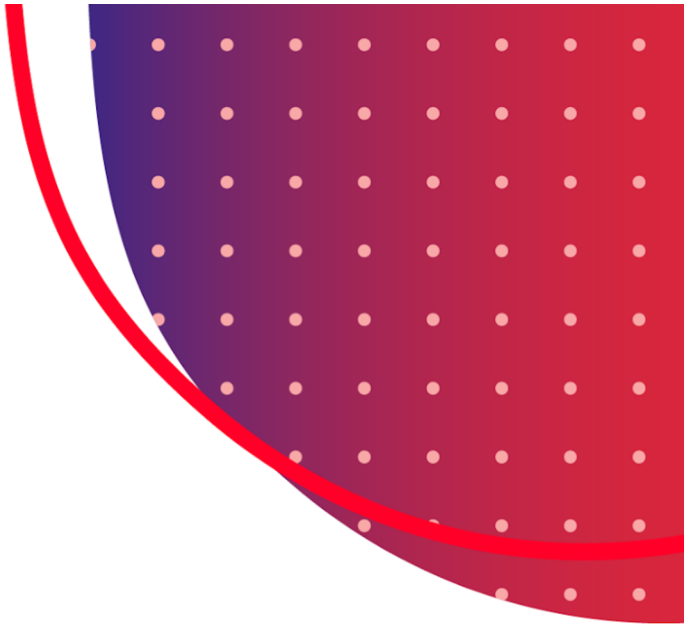


Cisco Secure AI Factory Accelera l'AI in Azienda

Stefano Gioia

EMEA Solution Architect
Cloud & AI Infrastructure,
Cisco

Cisco connects and protects the AI era

AI infrastructure

Security for AI

Data

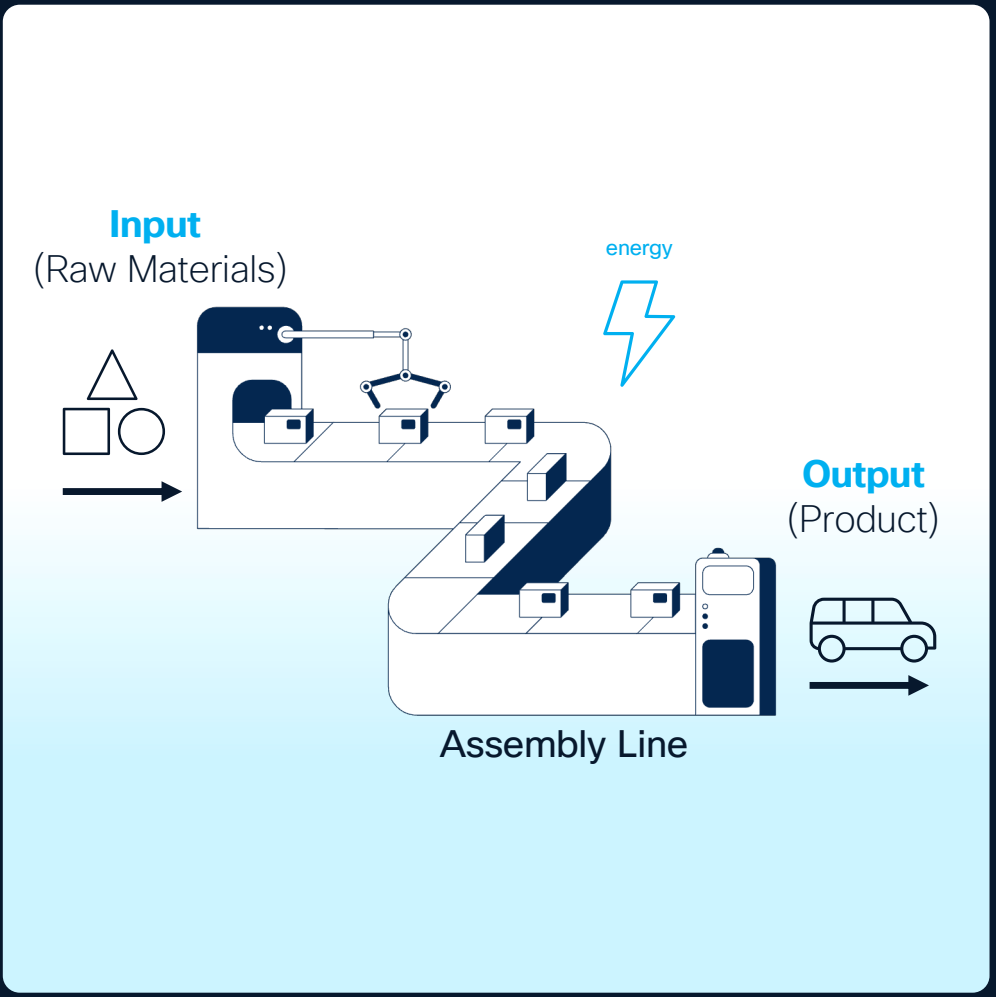
AI-native products

Services

The Factory

Repeatable, scalable business capability

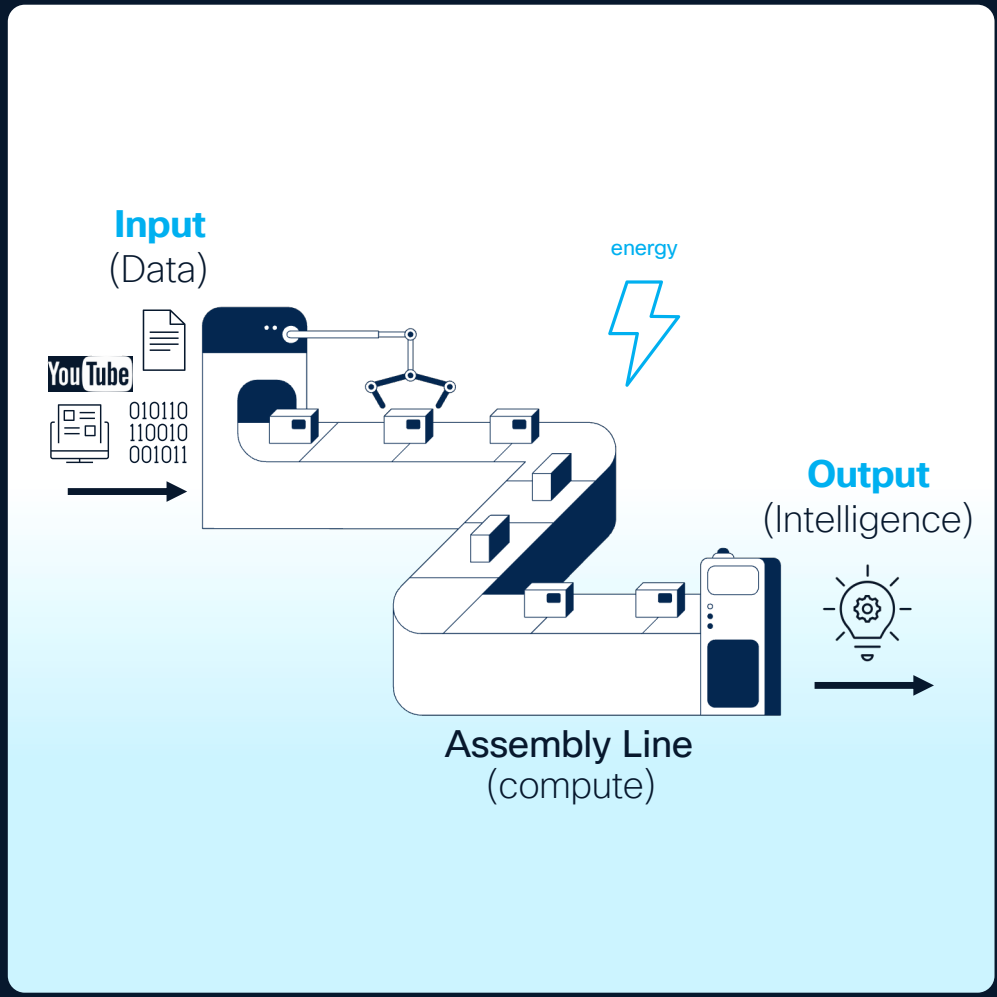
- Mass Production Efficiency
- Quality Control
- Supply Chain Integration



The AI Factory

Repeatable, scalable business capability

- Mass model/token production
- Model performance control
- Data and workflow integration



cisco

The pace of AI innovation is staggering

Inference Demand

Power | Compute | Networking

1990s

Machine learning

ChatGPT

Assistants

Agentic AI

Physical AI

Robust, flexible infrastructure to meet your needs

Infrastructure

Data center building blocks

- Nexus
- Silicon One
- Nexus Hyperfabric
- Unified Computing System

Full stack systems

- AI Pods
- Nexus Hyperfabric AI

Secure AI Factory

Cisco Validated Designs

Cisco AI POD Full Stack System

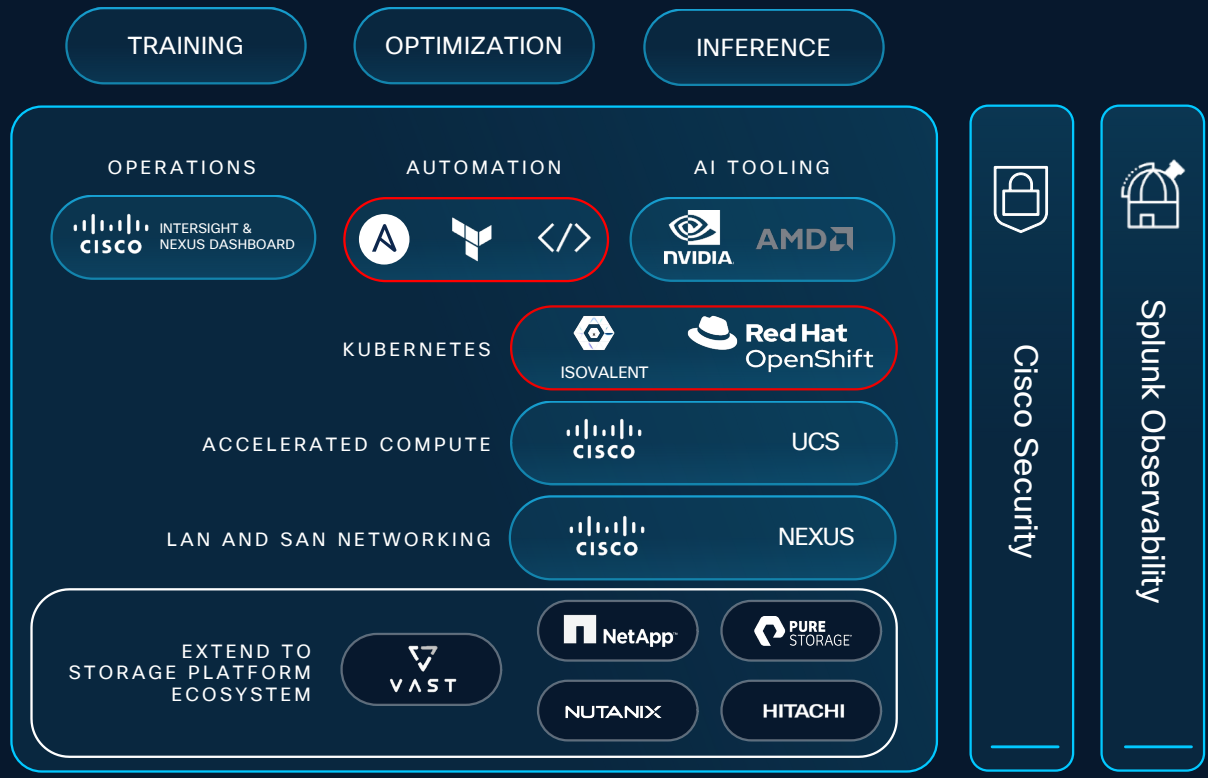
What is an AI POD?

Modular components for flexible adoption

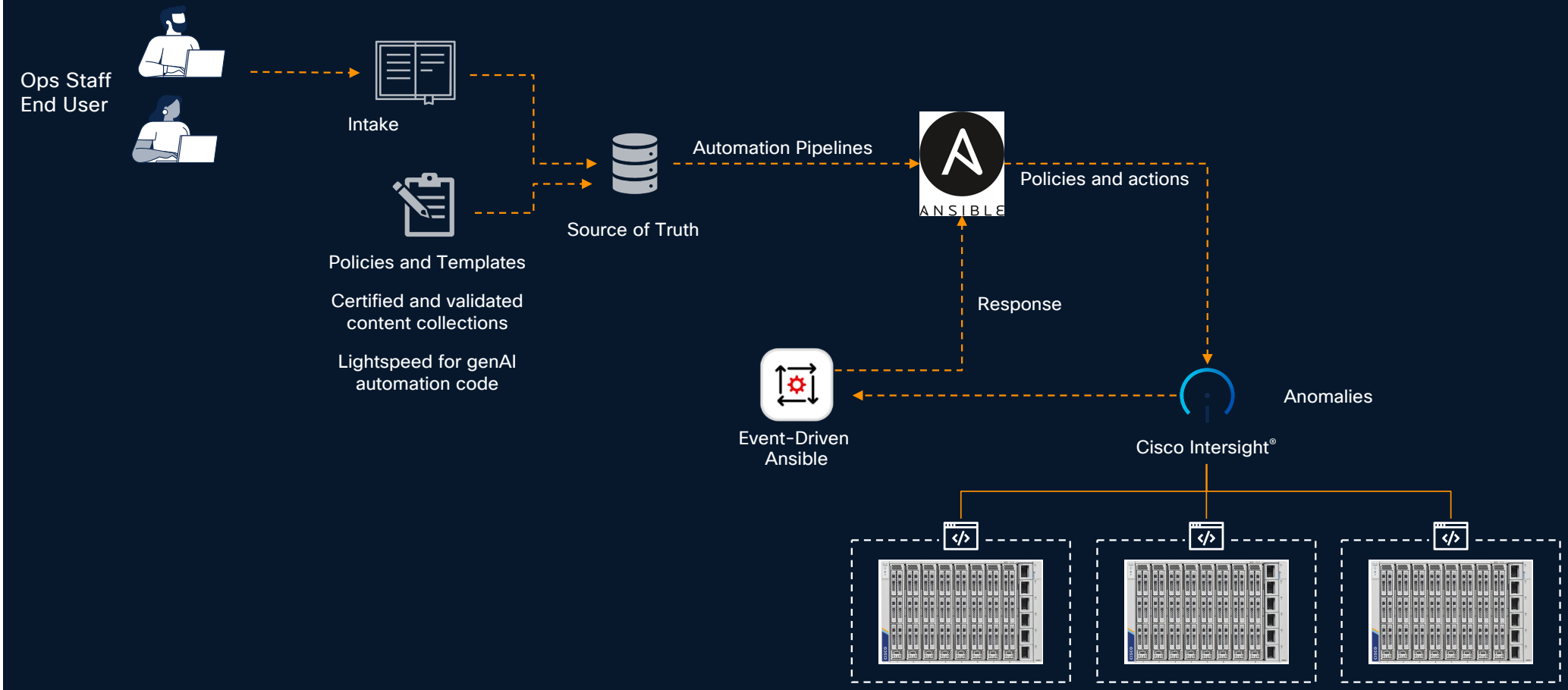
Deploy AI with confidence: CVD

Sizing tools for predictability

Fully stack by Cisco, including 3rd Party



Operations as Code for the DC Compute

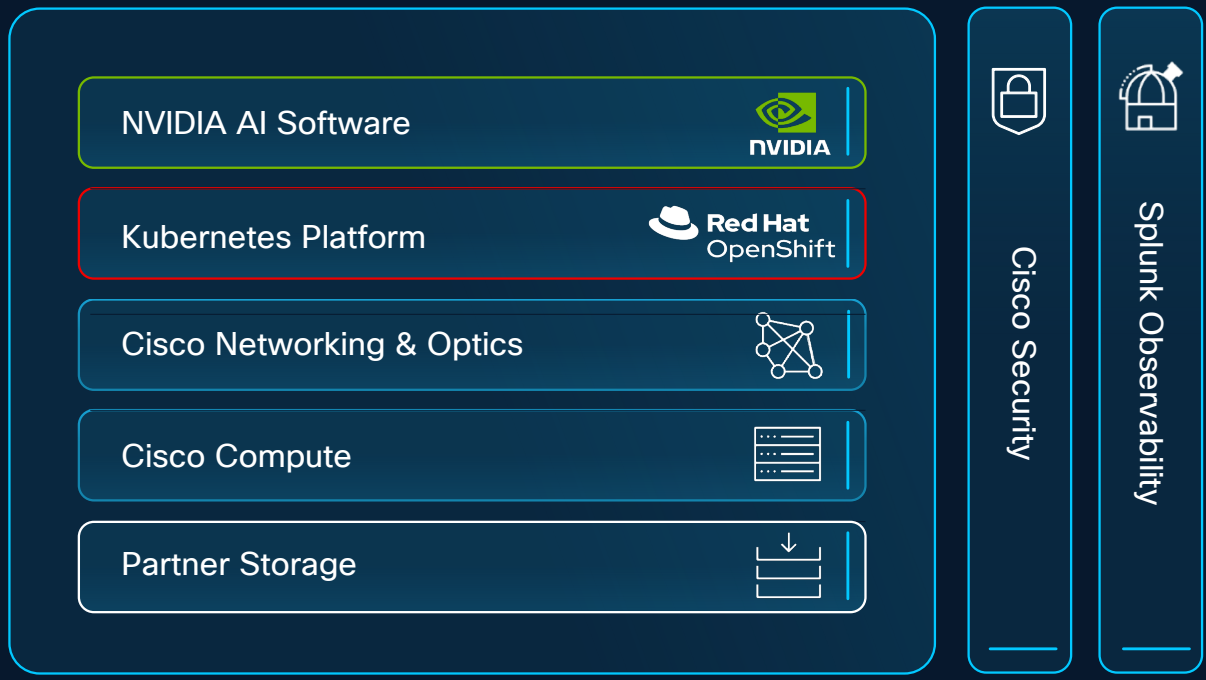


Cisco Secure AI Factory with NVIDIA

Bringing hyperscaler innovation to enterprises

What is it?

- Reference architecture
- Validated solutions and turnkey offerings
- Differentiated with Security and Observability
- Securing the Application, workloads & infrastructure

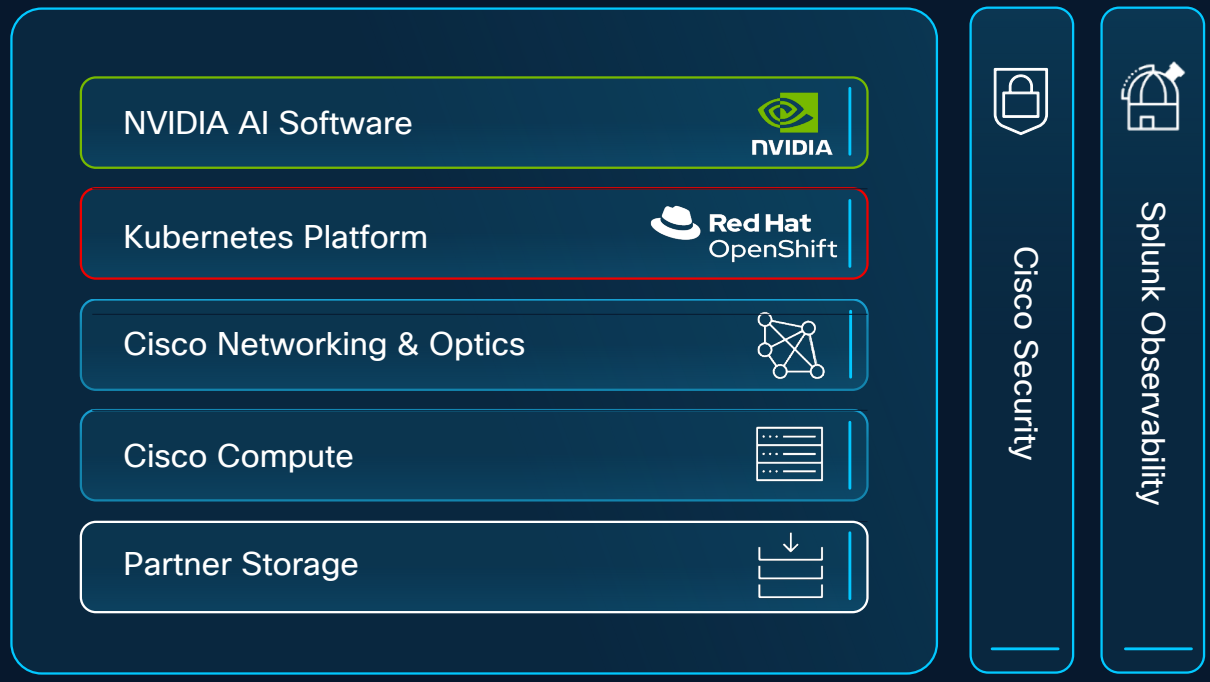


Cisco Secure AI Factory with NVIDIA

Who is it for?

AI Practitioners

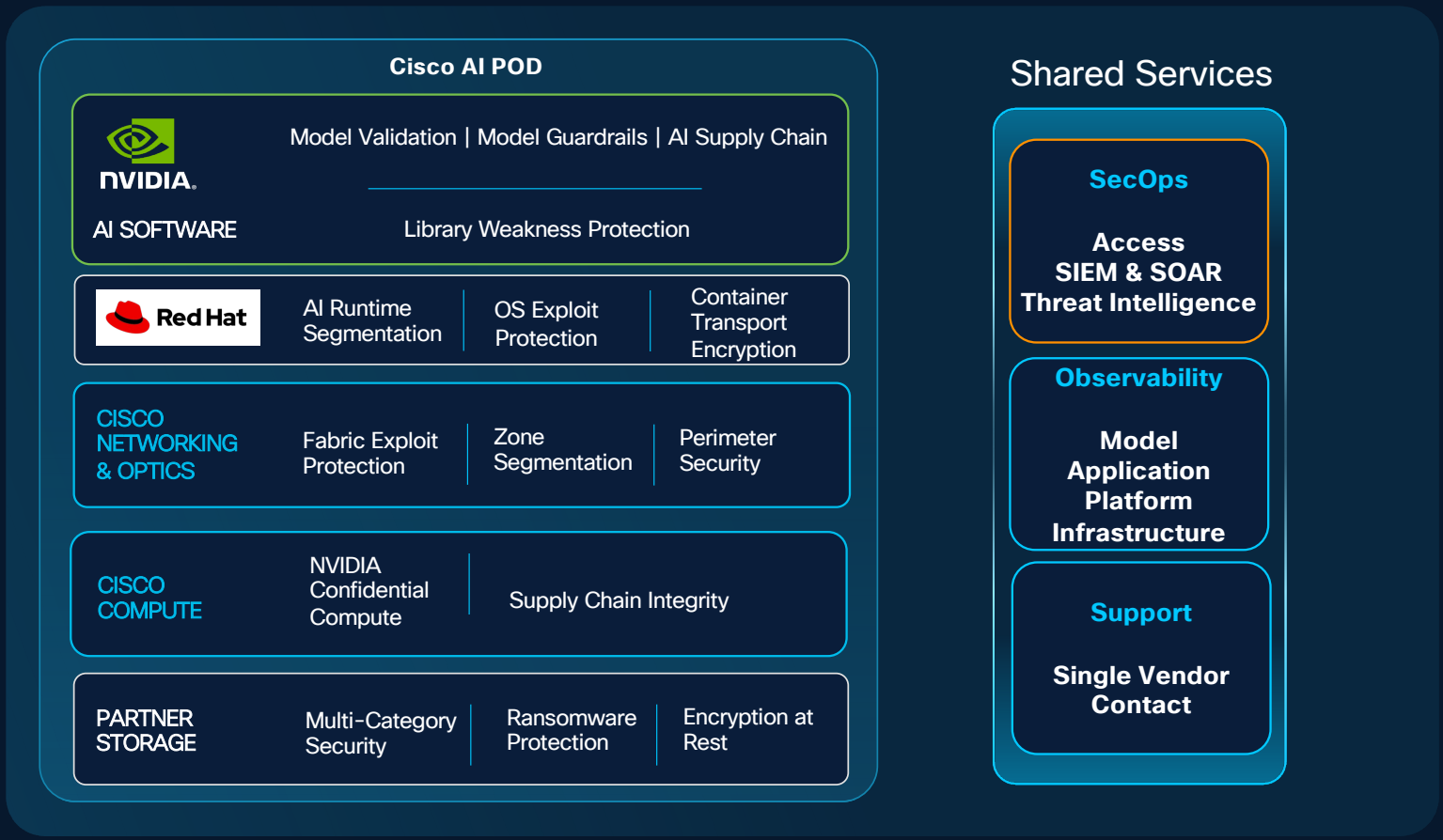
IT Infrastructure & Operations



SecOps and Site Reliability Engineering

Security capabilities in Cisco Secure AI Factory with NVIDIA

Delivering Trusted AI Outcomes



Securing the AI stack

Secure Use of AI

Protect both the development and use of AI applications

AI Defense

AI-native Security

Ensure secure networks and systems with AI-powered capabilities

Cisco Live Protect, Hybrid Mesh Firewall, Universal Zero Trust Network Access, Isovalent

Secure Use of AI: Cisco AI Defense

A three-step framework for developing secure AI applications

Discovery

Uncover AI assets including models, agents, and datasets

Detection

Test for AI risk, vulnerabilities, and susceptibility to attack

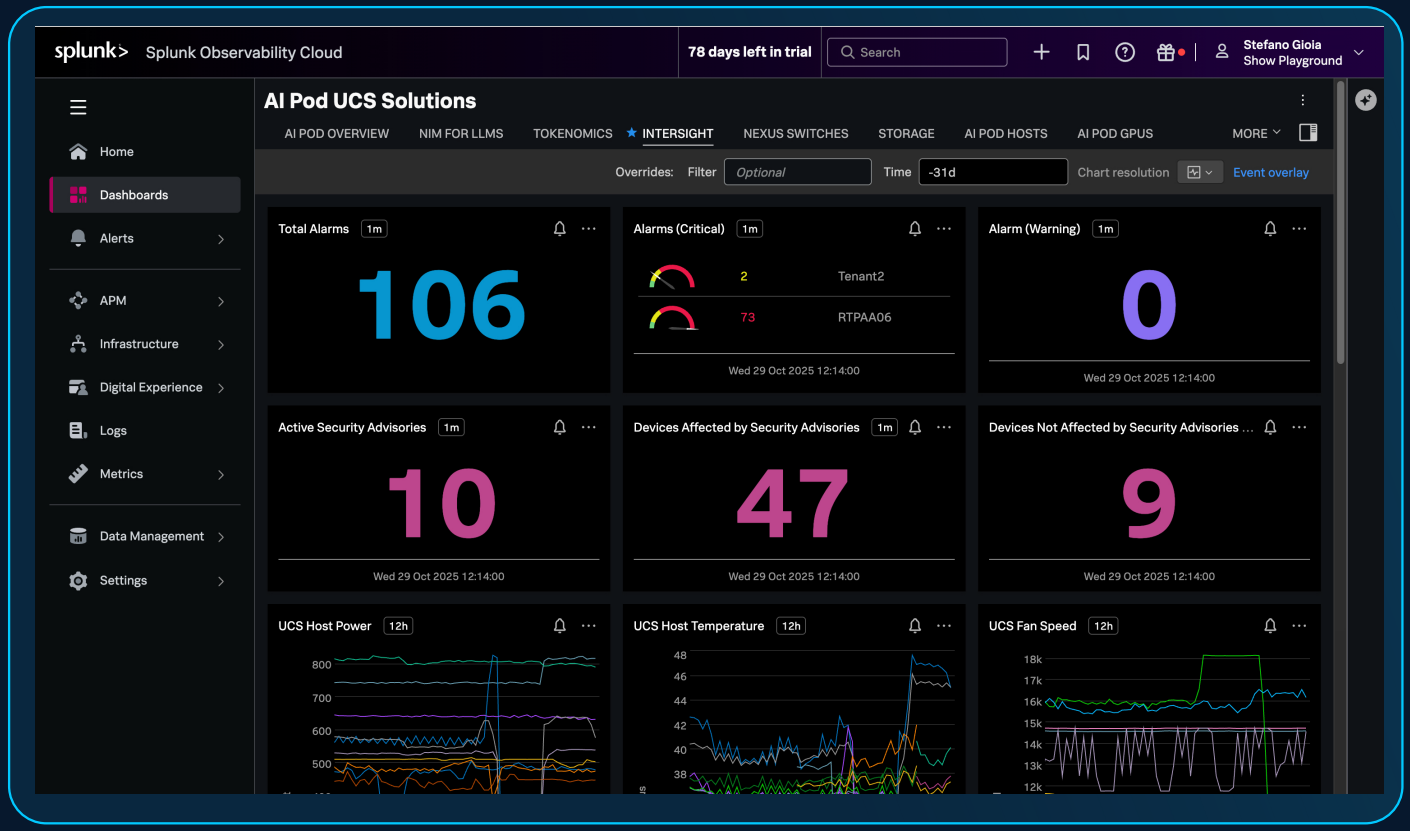
Protection

Define guardrails that secure data and defend against runtime threats

Unified management with Cisco Security Cloud Control

Cisco AI Observability

Real time Monitor & Troubleshooting



Secure Factory at the edge with Cisco Unified Edge

Red Hat Enterprise Linux

Red Hat Enterprise Linux (RHEL) on Cisco Unified Edge

Secure operating system:
Stable, enterprise-grade foundation for all edge workloads, ensuring reliability and security for critical operations.

Consistent foundation:
Deployed using Cisco Validated Designs and Cisco Intersight® blueprints, thereby ensuring a standardized and manageable OS layer across all edge sites.

Optimized for performance:
Leverages Cisco Unified Edge's high-performance hardware, including CPU, memory, and storage, for efficient execution of applications.

Cisco Secure AI Factory

Cisco Differentiation

The Security

Security-first architecture enables safe enterprise AI

The Network

High-performance integrated AI networking enables efficient model training and inferencing

The Assurance

Pre-validated AI infrastructure stack with flexible deployment options improves data scientists and developer productivity


CISCO