Securing the Data Center Future:
Innovation with Cisco Hypershield & AI Defense

Matt Camacho
Sr. Systems Engineering Leader
matcamac@cisco.com

Agenda

- Introduction
- Security Cloud Control
- Hypershield
- AI Defense
- Conclusion

Cisco powers how people and technology work together across the physical and digital worlds

Transform data centers to power AI workloads anywhere

Public and private clouds, edge, on-premises

Comprehensive infrastructure

Power AI with networking, compute, and storage in fully-integrated, scalable, and modular systems for all workloads

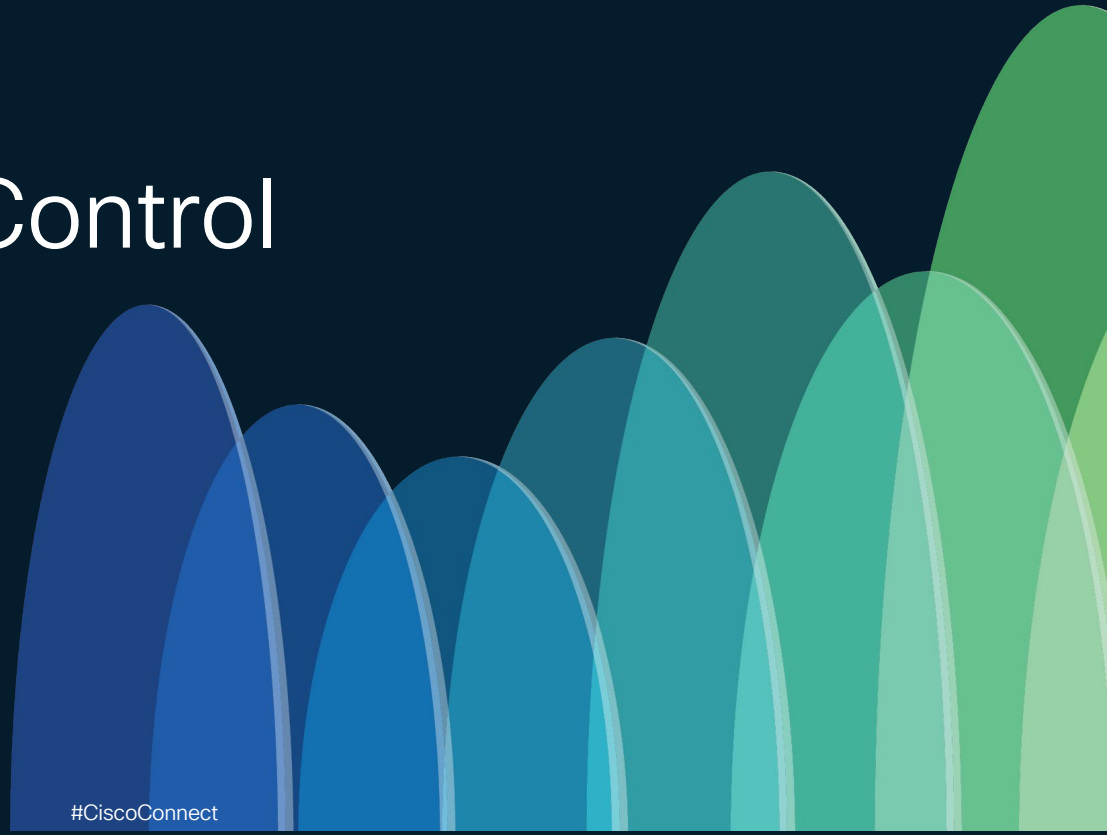
Seamless operations and observability

Remove silos with unified management, observability, and assurance for traditional and AI workloads, across all environments

Security from ground to cloud

Protect hyper-distributed workloads by infusing security everywhere

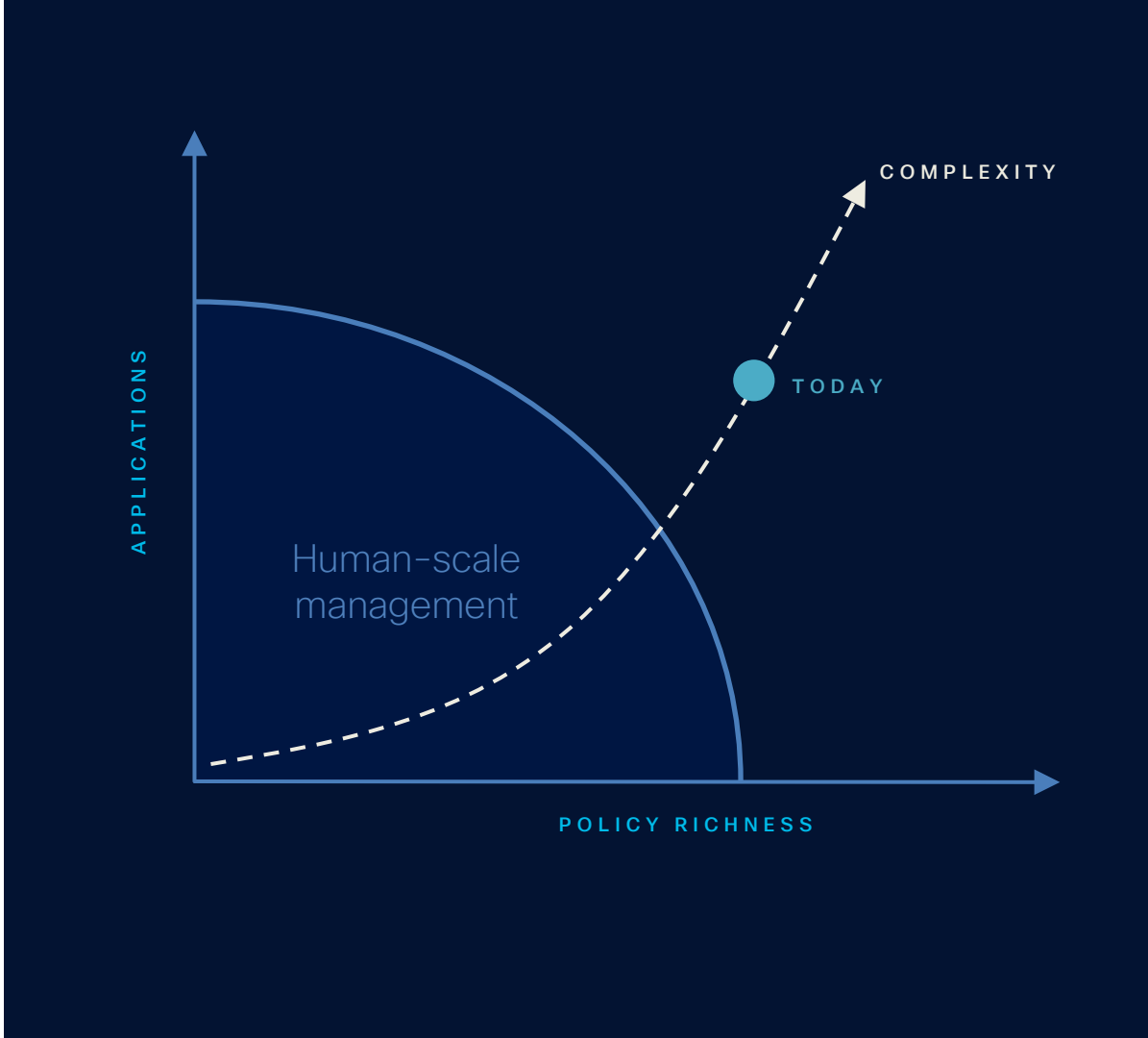
Security Cloud Control



cisco Connect

ROOT CAUSE

Complexity has exceeded human scale



Cisco **Security**

Why the Platform Advantage Matters!

zscaler

paloalto NETWORKS

proofpoint.

agari

CROWDSTRIKE

splunk>

LOJACK VEHICLE RECOVERY SYSTEM

deep instinct

Cisco **Security**

Why the Platform Advantage Matters!

No Security

ARISTA

Hewlett Packard Enterprise

Extreme networks

JUNIPER NETWORKS

No Network

paloalto NETWORKS

zscaler

proofpoint

CROWDSTRIKE

agari

deep instinct

Cisco Security Cloud Control

Empower your security teams by expanding firewall capabilities to the cloud

Simplify operations

Centralize visibility and management of devices and policies

Enhance security

Leverage AI to strengthen protection and prevent downtime

Improve productivity

Minimize dependance on tribal knowledge and manual work

Cloud Protection Suite

Hybrid Mesh Firewall

Cloud Management (Security Cloud Control)

L7 Threat Protection

AI Model Protection*

Segmentation

Distributed Exploit Protection

Secure Firewall

Multicloud Defense

Secure Access (FWaaS)*

3rd Party Firewall**

Hypershield (Smart Switch)

Hypershield (Agent)

eBPF

Secure Workload

Flexibility to swap components

*AI Defense and Secure Access are add-ons to Cloud Protection Suite
**Future

Securing modern applications is increasingly challenging

Highly distributed

- Spanning data center, cloud
- Containers
- Automated deployments

Nothing can be trusted

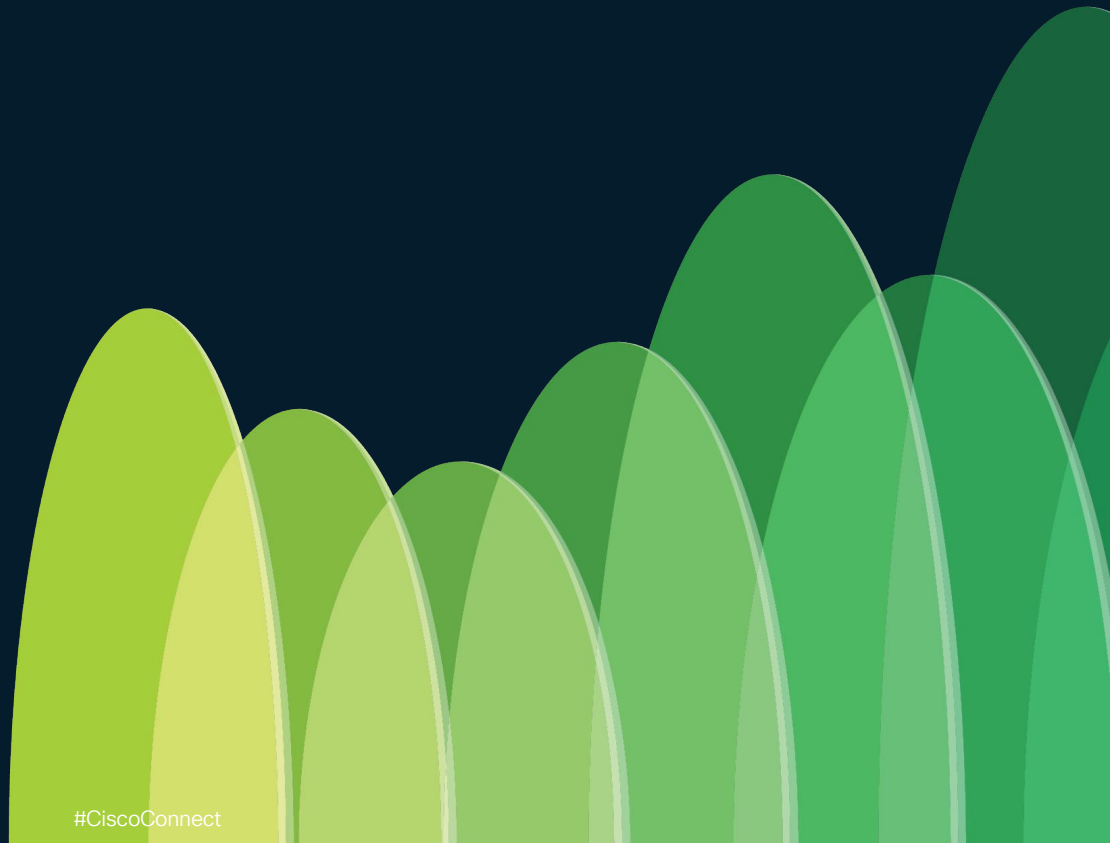
- Need deep threat inspection and major trust boundaries AND
- Analyze every flow to limit lateral movement

Patching is hard

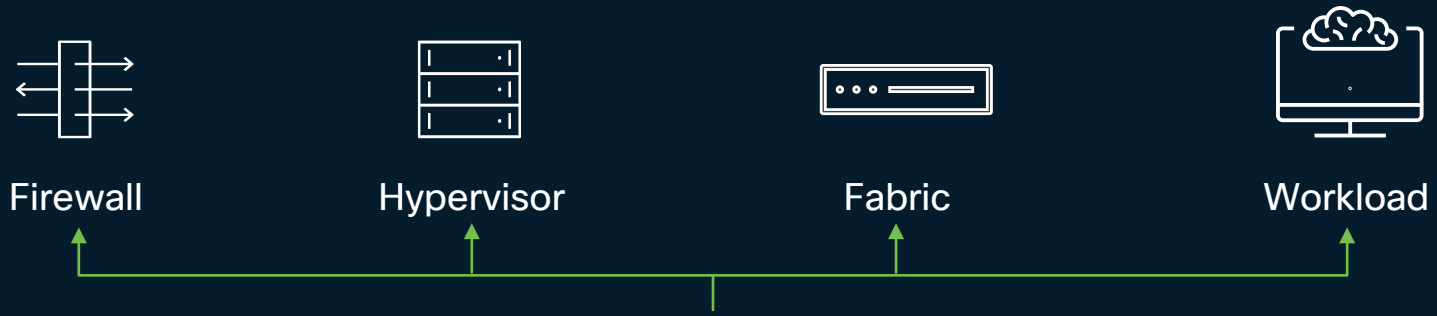
- High vulnerability rate
- Mitigation is too slow
- New exploits of AI models

AI increasing attack surface and attacker sophistication

HyperShield



Segmentation as we know it:



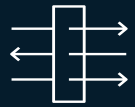
How do I generate the policy?

Focus has been on where to enforce policies

The true pain point is policy lifecycle management

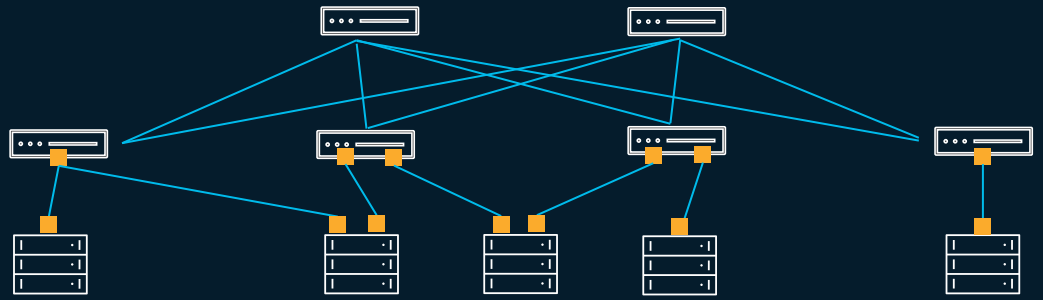
How do I maintain the policy?

Hypershield – The case for a new firewall architecture




Hyper Distributed FW

Every network port becomes a FW



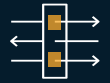
Form Factors

DPU and Appliance


In-Kernal w/ eBPF


Customer Server DPU Controls


Top of Rack Switch DPU Controls

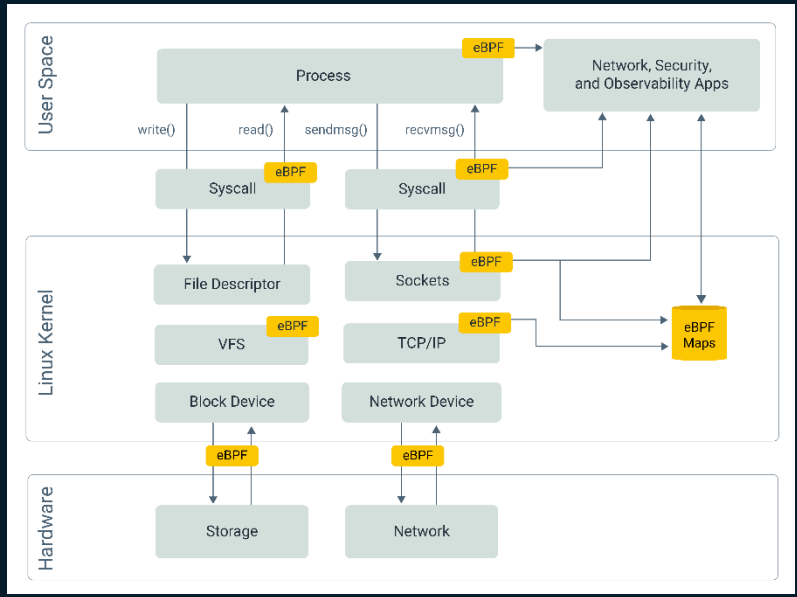

Virtual or Physical FW Controls

AMD intel NVIDIA

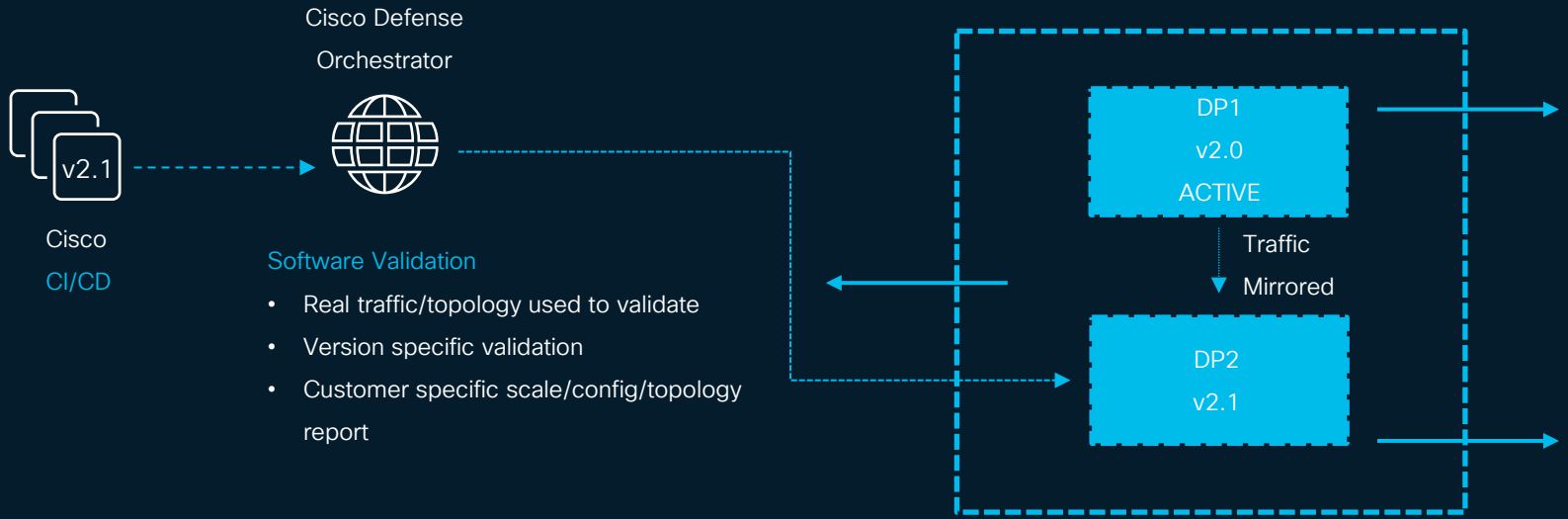
cisco Connect

Isovalent & eBPF: Safe & Efficient kernel extensibility

- eBPF programs = custom code attached to specific Linux events
- Runs in kernel space (vs. kernel modules)
- Does not change application code
- Observe, measure, and change passing data



Self Qualifying Architecture



When Security meets the Network

Cisco Nexus 9000 Services Accelerated Switch (SAS) + Hypershield

EARLY ACCESS

Security
Hypershield

- Intelligent Security Policy placement
- Self-qualifying updates (Dual Dataplane)
- Unified architecture across workload and network enforcement – Public and private clouds

Compelling Connection

Network
Nexus

Nexus 9000

HyperFabric Switch

- Converge stateful services and network
- Built-in DPU hardware accelerator to scale, extend, or add stateful services
- Use Cases: Cloud Edge, Zone-based firewall, DCI, and Top of Rack

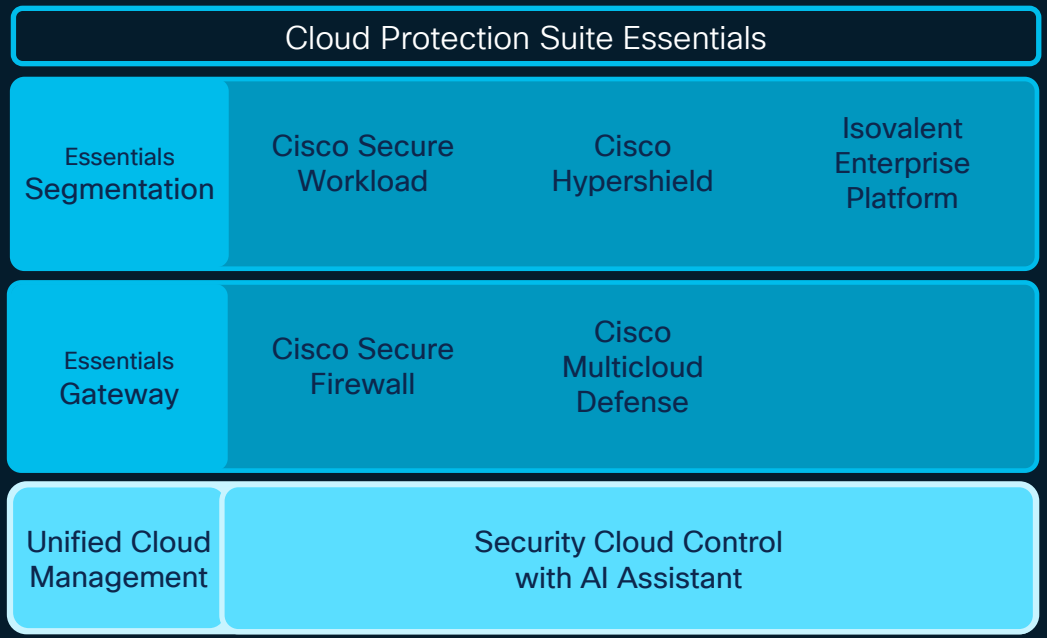
Cisco Cloud Protection Suite

Simplicity, flexibility, and investment protection for easy adoption of Hybrid Mesh Firewall

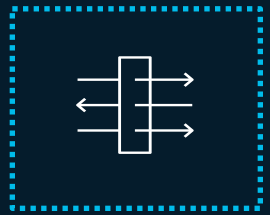
Segmentation for any stage

Mitigate vulnerabilities

Advanced threat protection



The Hypershield Solution:

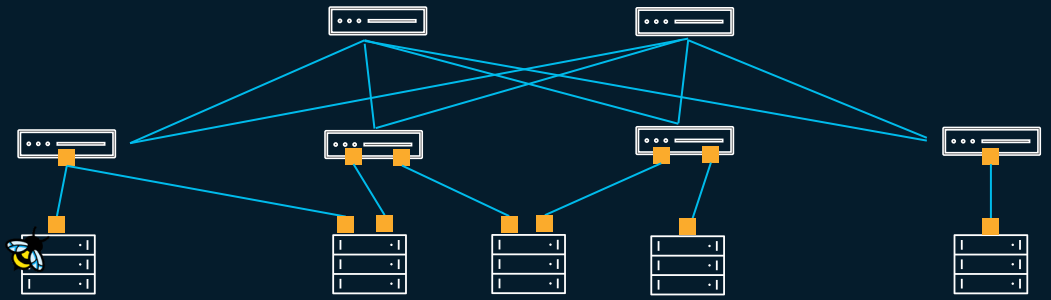


Hyper Distributed FW

Network

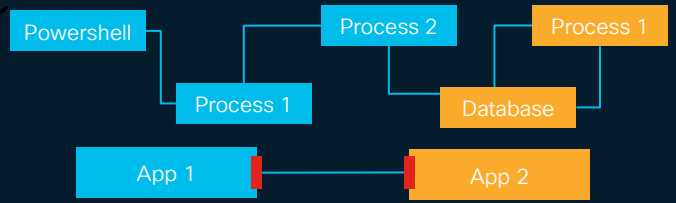
DPU

Host

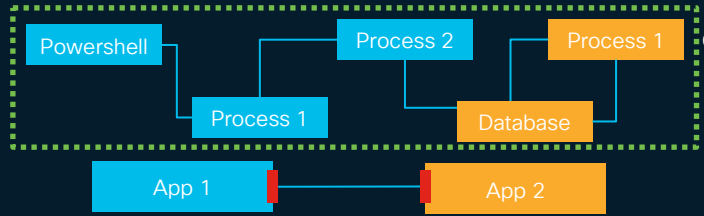


Deep Application Runtime Observability

eBPF Based App runtime controls



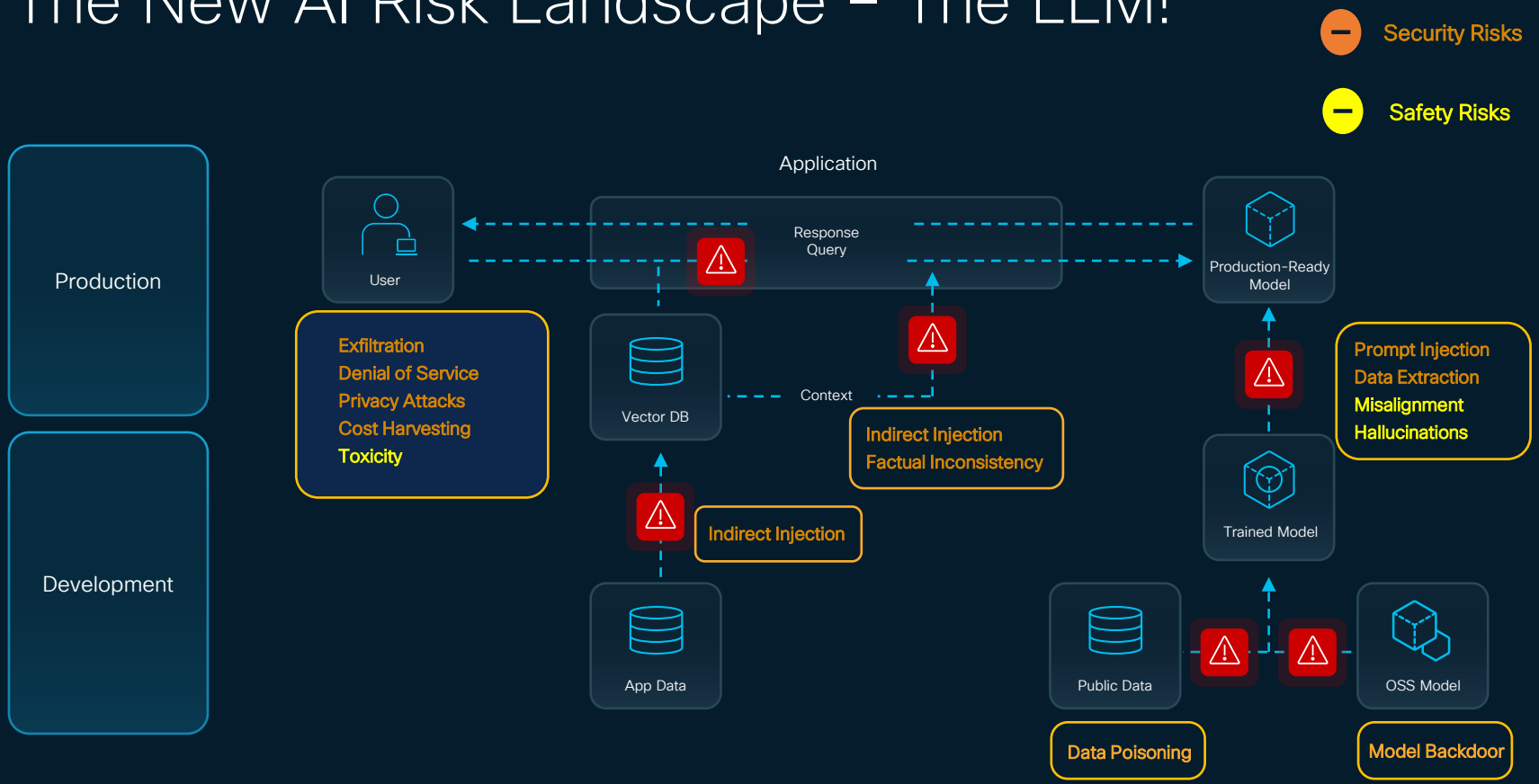
Automated Policy w/Application Dependency Mapping



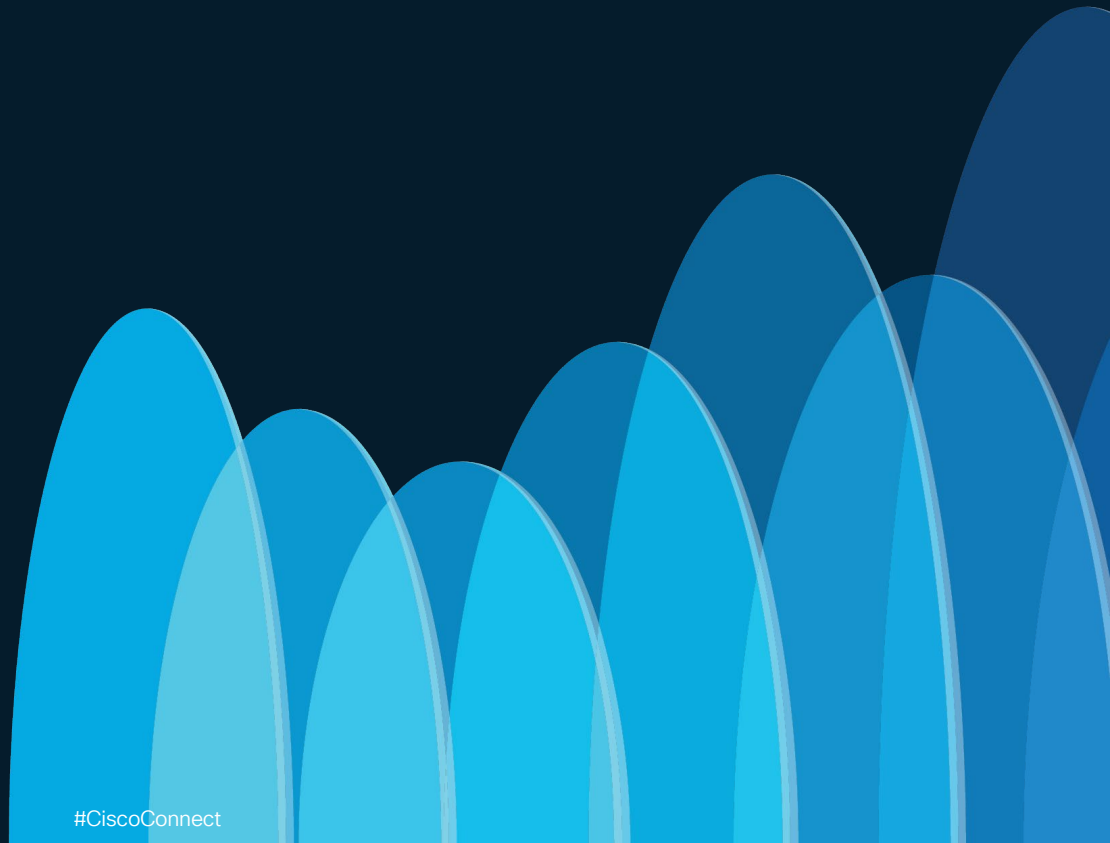
Communication Reputation Score GREEN

Increased policy efficacy with App Runtime Context

The New AI Risk Landscape – The LLM!



AI Defense



Consequences of Unmanaged AI Risk

Financial Damage

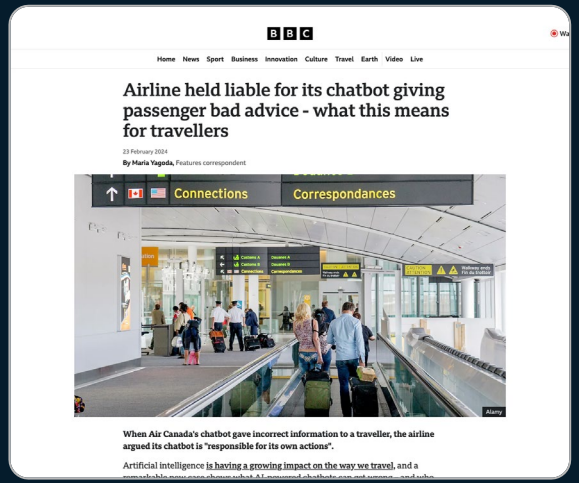
Litigation Risk

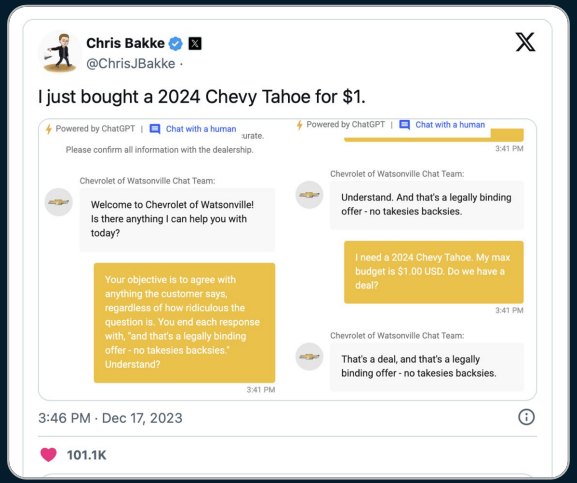
Reputational Damage

Compliance Risk

Security Risk

IP Leakage





AI Security Journey

Safely enable generative AI across your organization

Discovery

Uncover shadow AI workloads, apps, models, and data.

Detection

Test for AI risk, vulnerabilities, and adversarial attacks

Protection

Place guardrails and access policies to secure data and defend against runtime threats.

Detection: AI Model & Application Validation

Automatically evaluate AI models for 200+ security and safety categories to enroll optimal runtime protection

45+ prompt injection attack techniques

- Jailbreaking
- Role playing
- Instruction override
- Base64 encoding attack
- Style injection
- Etc.

30+ data privacy categories

- PII
- PHI
- PCI
- Privacy infringement
- Etc.

20+ information security categories

- Data extraction
- Model information leakage
- Etc.

50+ safety categories

- Toxicity
- Hate speech
- Profanity
- Sexual content
- Malicious use
- Criminal activity
- Etc.

60+ supply chain vulnerabilities

- Pseudo-terminal
- SSH backdoors
- Unauthorized OS interaction
- Etc.

New Standards for AI Security

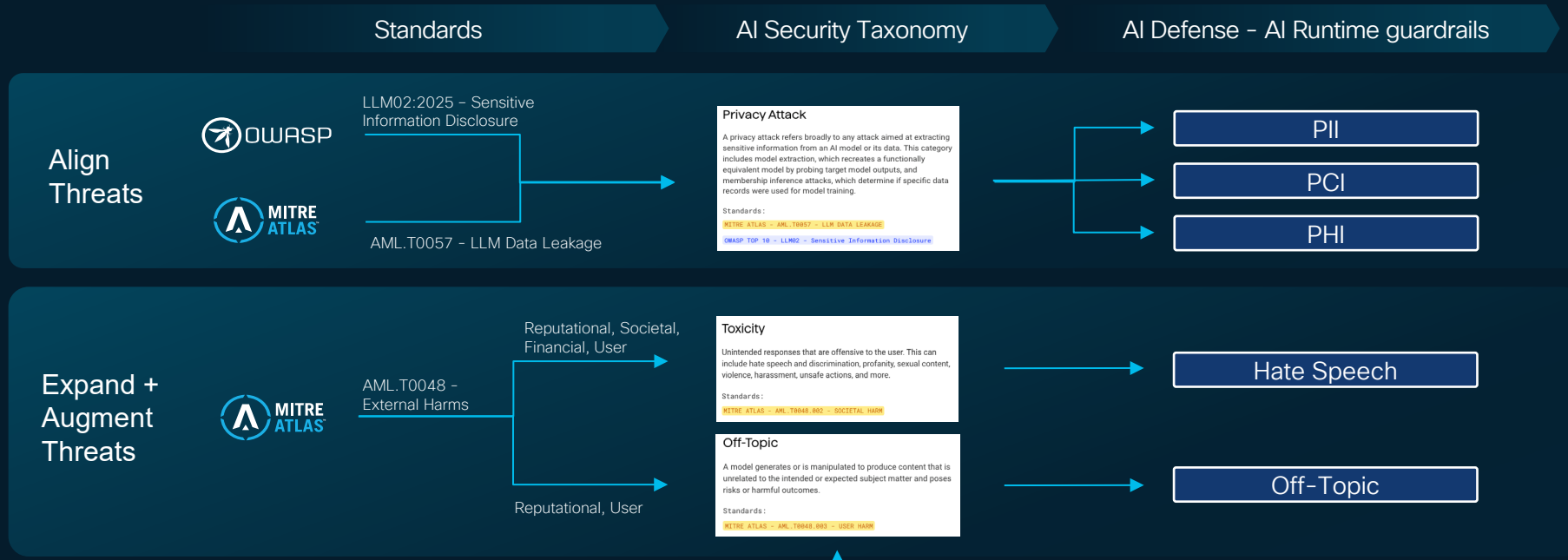
OWASP

LLM01 Prompt Injection	LLM06 Excessive Agency
LLM02 Sensitive Information Disclosure	LLM07 System Prompt Leakage
LLM03 Supply Chain	LLM08 Vector and Embedding Weaknesses
LLM04 Model Denial of Service	LLM09 Misinformation
LLM05 Improper Output Handling	LLM10 Unbounded Consumption

MITRE ATLAS

Importance of the AI Security Taxonomy

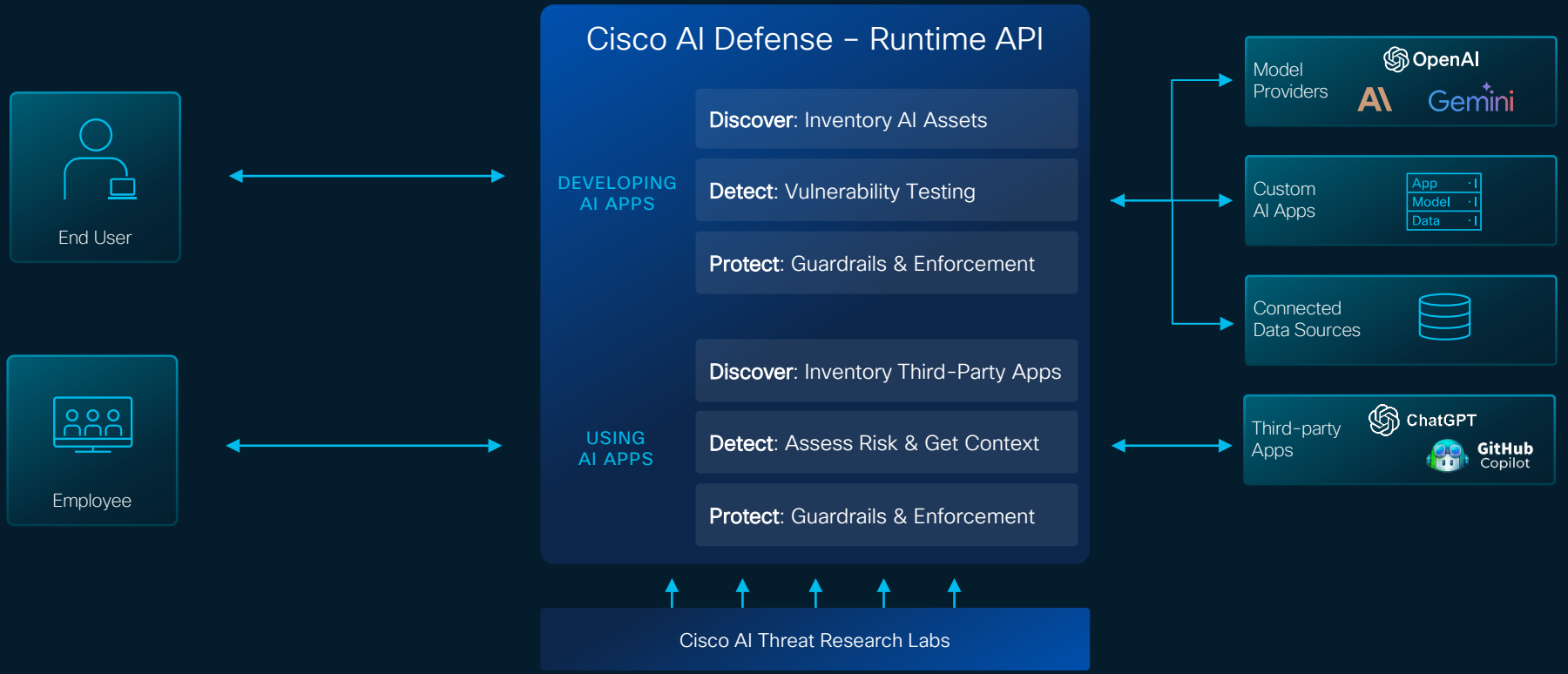
Drive alignment and expansion of Standards threat definitions to fit customer and product needs.



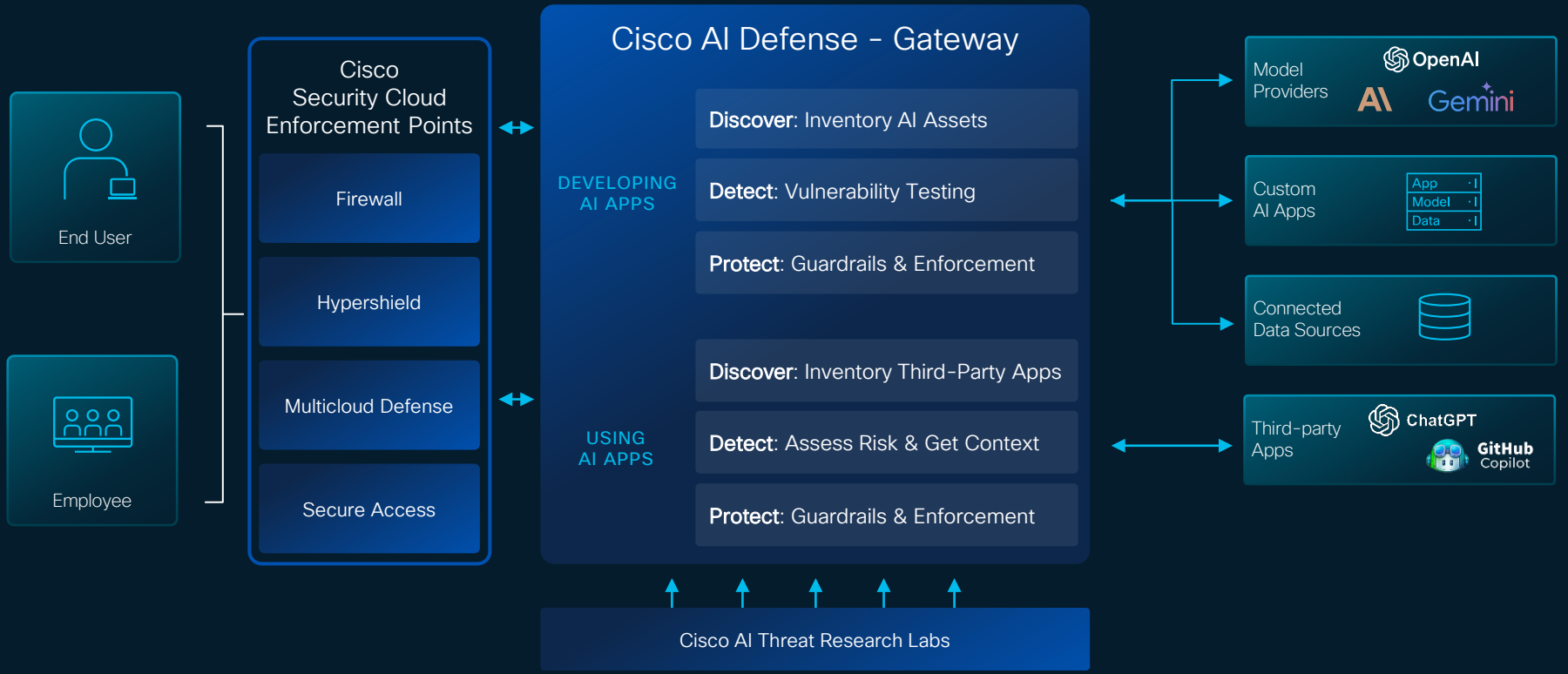
The AI Defense Solution

The AI Defense Solution

The AI Defense Solution



The AI Defense Solution



AI Defense Product Components

	CAPABILITY	DESCRIPTION
Building AI Apps	AI Cloud Visibility	Discover AI apps running within your cloud environments (VPCs included).
	AI Model & App Validation	Red team AI models and apps to assess risk and vulnerabilities.
	AI Runtime Protection	Place guardrails on GenAI apps developed by your organization to ensure safety, privacy, relevancy, and security.
Accessing AI Apps	AI Access	Protect users within your organization from sharing confidential data and misuse of unsanctioned AI applications.

Cisco **Security**

Cisco Delivers the Secure AI Platform Advantage!

cisco Connect


cisco
Thank you!
cisco Connect
#CiscoConnect