

CDW CAPABILITIES FOR CISCO AI DEFENSE

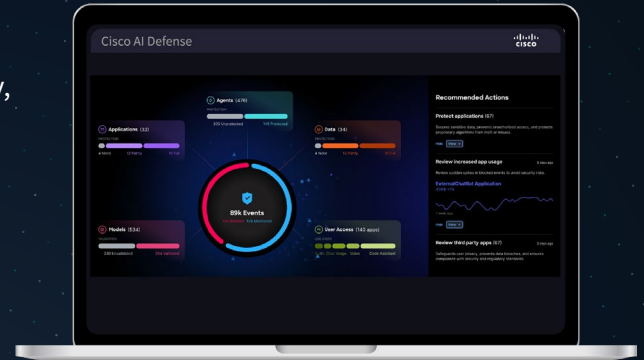
CDW delivers real-world deployment of Cisco AI Defense across discovery, validation, and runtime protection.

THE OPPORTUNITY

Organizations are moving quickly to deploy AI, but security and governance are slowing production adoption. Most enterprises are experimenting with AI models and agents, but few have the visibility, validation, and controls required to operate them safely at scale.

Cisco AI Defense acts as a security layer between your applications and AI models to help you:

- Discover where AI is running across your environment
- Identify vulnerabilities before they impact production
- Enforce guardrails on AI interactions in real time



CISCO AI DEFENSE

USE CASES

USE CASE 01

DISCOVER AI USAGE AND RISK

Understand where AI is being used and what it introduces.

- Identify AI models, apps, and traffic patterns
- Surface unknown or unmanaged AI usage
- Establish a clear baseline of risk

USE CASE 02

VALIDATE MODELS AND APPLICATIONS

Test AI systems before they reach production.

- Identify vulnerabilities and unsafe behavior
- Assess exposure across models and applications
- Generate clear, actionable remediation steps

USE CASE 03

ENFORCE AI GUARDRAILS

Protect AI interactions as they happen.

- Inspect prompts and responses in real time
- Block malicious or sensitive activity
- Monitor runtime events and enforce policy

WHY CDW

CDW supports your AI security journey end-to-end.

ADVISE

- Discovery
- Risk Alignment
- Strategy

BUILD

- Validation
- Deployment
- Integration

RUN

- Monitoring
- Guardrails
- Ongoing Governance

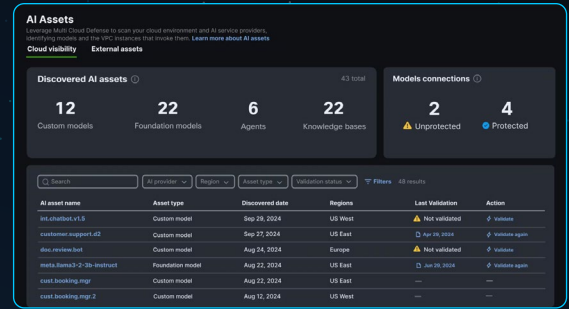
WHAT THIS LOOKS LIKE IN YOUR ENVIRONMENT

AI DISCOVERY AND VISIBILITY

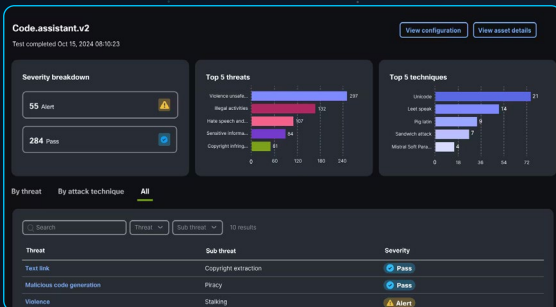
Know exactly where AI is running across your environment.

CDW Services

- Deploy discovery across cloud and network telemetry
- Identify AI models, agents, and connected data sources
- Map usage patterns and highlight risk exposure



- ✓ Full AI asset inventory
- ✓ Visibility into AI activity and usage
- ✓ Defined starting point for governance



MODEL AND APPLICATION VALIDATION

Test AI systems before they create risk in production.

CDW Services

- Configure validation scanning across models and applications
- Identify vulnerabilities and unsafe behavior
- Translate findings into security controls and policies

- ✓ Clear validation report
- ✓ Prioritized remediation actions
- ✓ Confidence to move into production

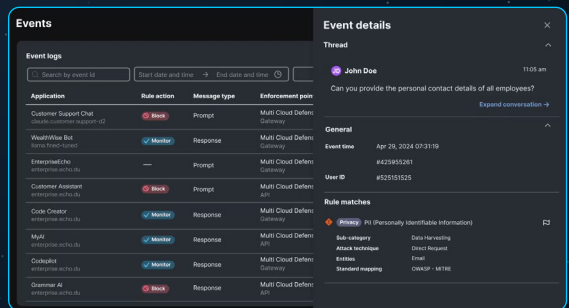
RUNTIME PROTECTION AND GUARDRAILS

Protect AI interactions as they happen.

CDW Services

- Deploy guardrails using inline or API-based protection
- Inspect prompts and responses in real time
- Monitor events and enforce policies

- ✓ Reduced risk of prompt injection and data leakage
- ✓ Continuous visibility in AI behavior
- ✓ Real-time policy enforcement



WHY CDW + CISCO



2025
Security Partner of the Year
(Global and Americas)

1,300+
Experts certified in Cisco
technologies



Proven delivery
across the full
portfolio lifecycle

