splunk> a cisco company

Cisco Security AI Innovation

IDEME 2026

Bratislava

May 21st, 2026

Securing the Agentic Workforce

Milan Habrcetl

Account Executive Security

Securing the Agentic Workforce

Protect the agents from the world

Protect the world from the agents

Detect & respond at machine speed & scale

Protecting the World from the Agents

Zero Trust for Agents

KNOW
EVERY AGENT

AUTHORIZE
EVERY ACTION

ADAPT TO RISK
IN REAL TIME

Visibility, identity, and ownership for every AI agent interacting with your environment

Agentic IAM by Duo

- Agent & Tool Discovery
- Agent Directory
- Agent Access Policy
- Human Accountability
- Lifecycle Management

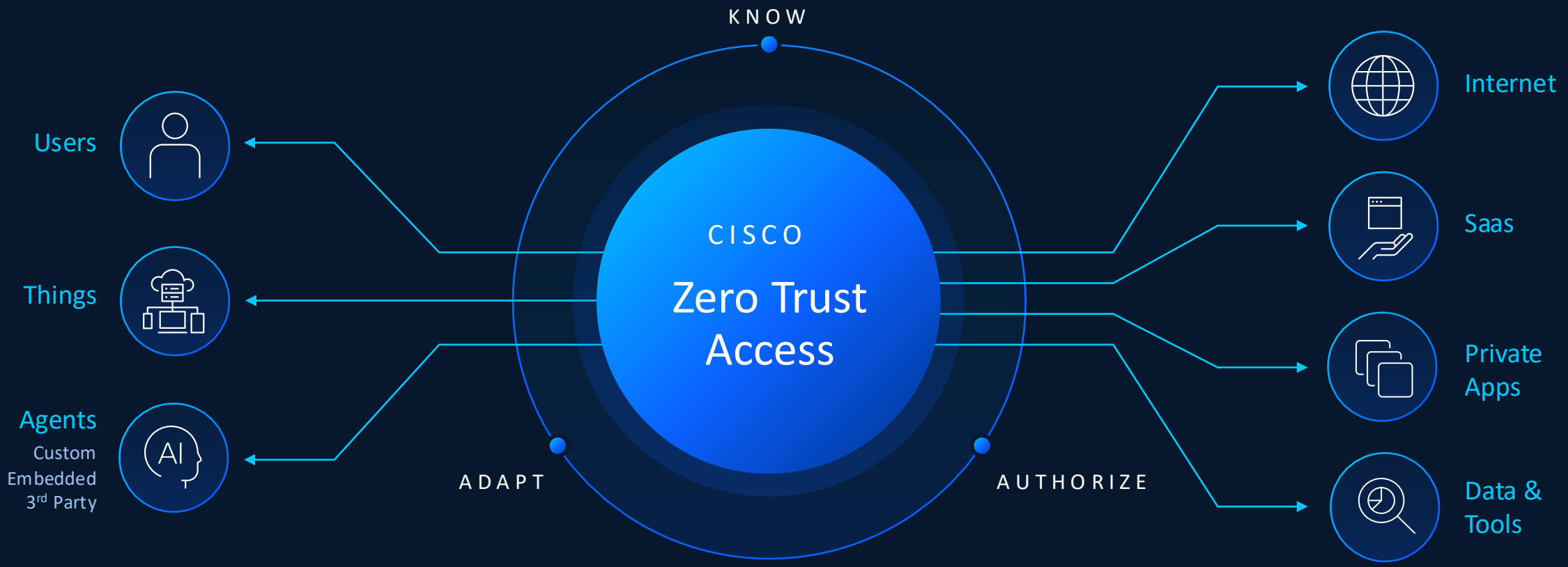
KNOW EVERY AGENT | AUTHORIZE EVERY ACTION | ADAPT TO RISK IN REAL TIME

Consistently enforced where agents access enterprise data & tools

Agentic Workforce

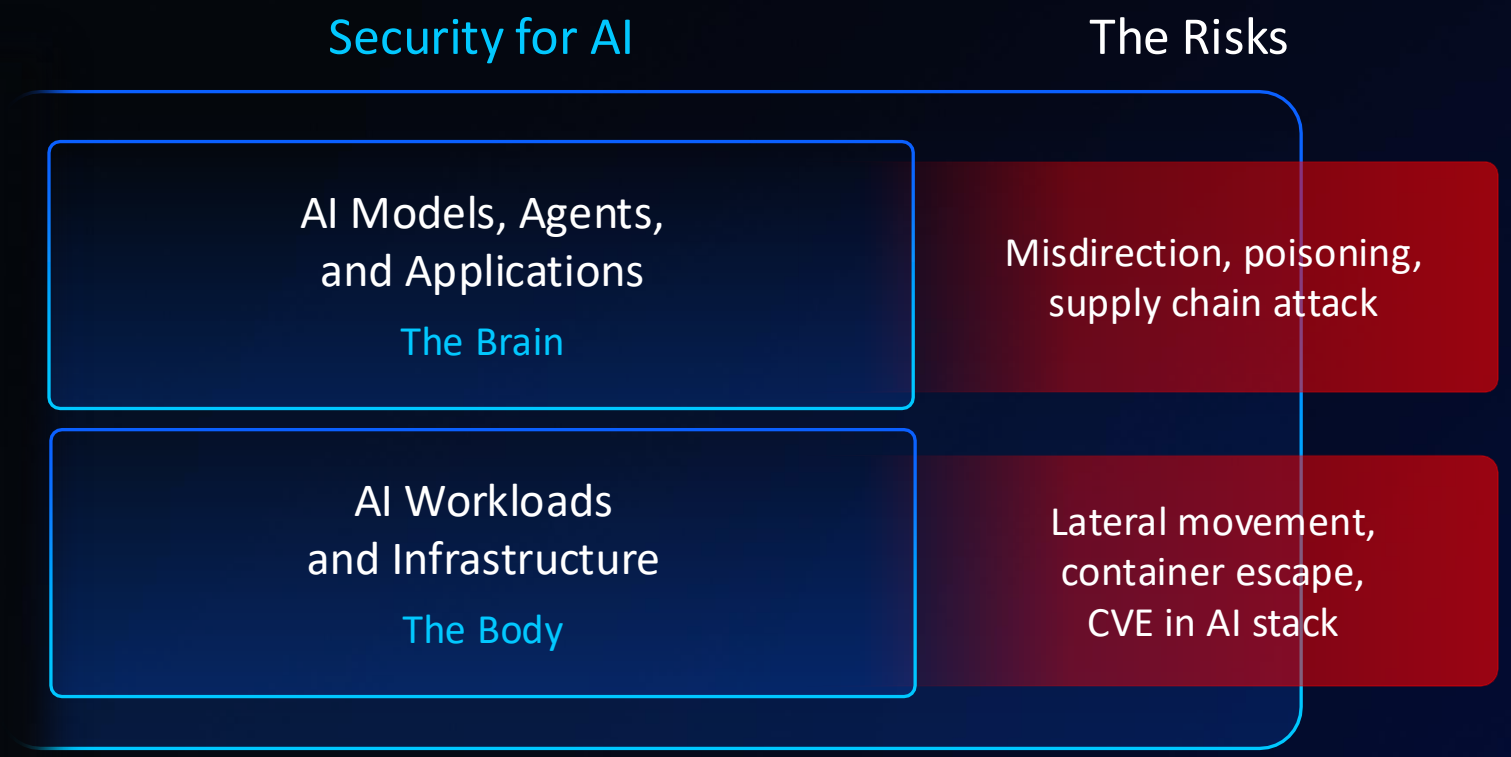
Tools, resources and data

Extending Zero Trust Access to the Agentic Workforce

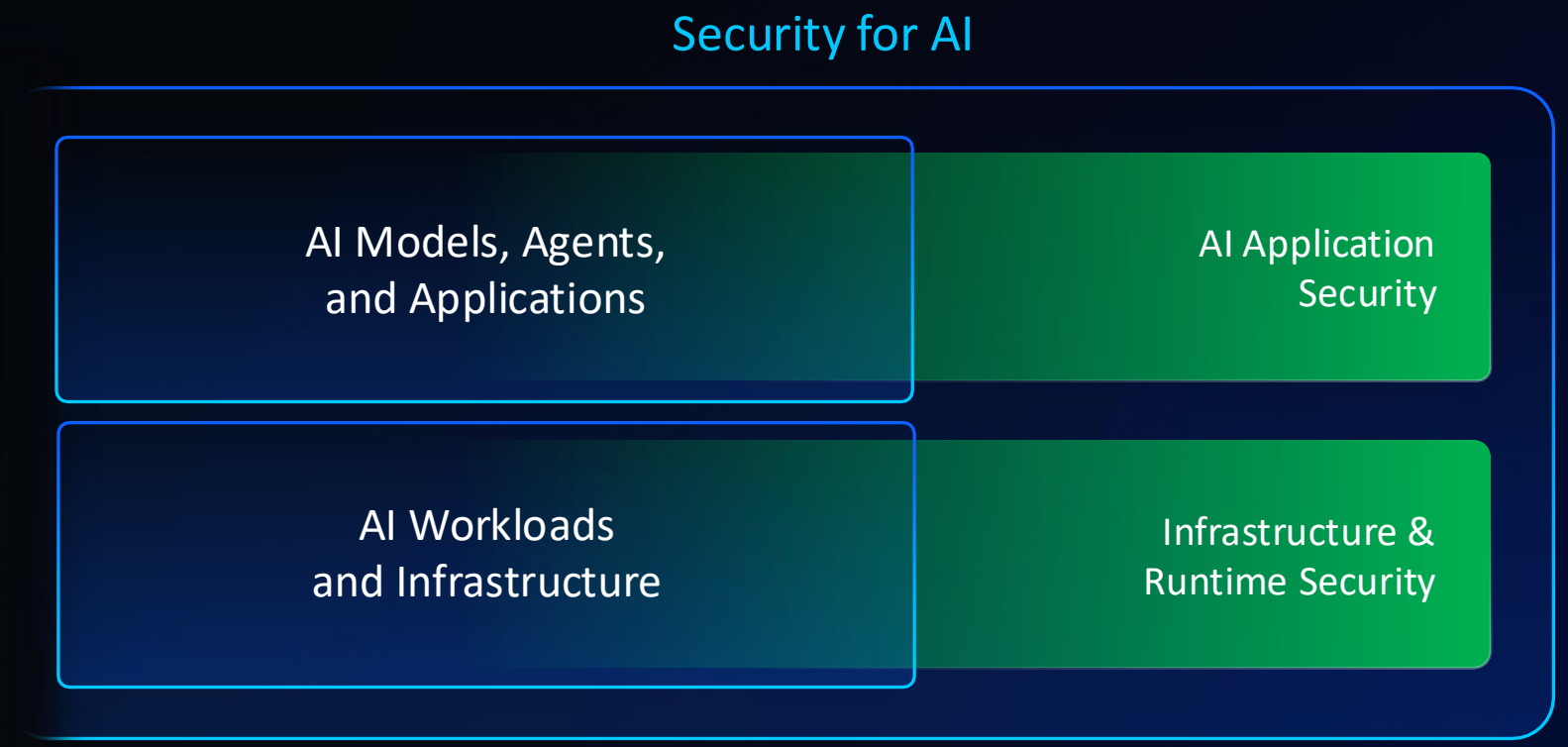


Protecting the Agents from the World

Security for AI



Securing the agentic stack



Securing the Model, Agent, and Application Layer

Cisco AI Defense

A three-step framework for developing secure AI agents

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

Powering the Agentic SOC

A new operating model for security

Anthropic announcing Project Glasswing, a new initiative that brings together Amazon Web Services, Anthropic, Apple, Broadcom, Cisco, CrowdStrike, Google, JPMorganChase, the Linux Foundation, Microsoft, NVIDIA, and Palo Alto Networks in an effort to secure the world's most critical software.

Cisco is delivering the visibility, control, and speed for security in the agentic era.