



Cisco AI

Security for AI and AI for Security

Pavel Smolík, Cisco



Agenda

- 1 AI – nedílná součást bezpečnostních řešení
- 2 Bezpečnostní řešení pro využívání AI modelů

AI @ Cisco

Cisco and NVIDIA to Help Enterprises Quickly and Easily Deploy and Manage Secure AI Infrastructure

Reimagining Communication with Webex's Pervasive AI

News Summary:

- New Real-Time Media Models (RMMs) in Webex harnesses audio and video in powerful new ways.
- Customers benefit from crystal-clear audio and video regardless of bandwidth with the new Webex AI Codec.
- New Webex AI Assistant brings together RMM and Large Language Models (LLMs) to help hybrid workers and contact center agents do their jobs better.

Cisco, Splunk CEOs Say Future of Cybersecurity Turns on AI

Cisco Unleashes AI Assistant for Security

Cisco unveils 'Identity Intelligence' to enhance cloud security with AI and networking integration

Cisco launches Motific hub to streamline generative AI deployment

Cisco launches new AI networking chips to compete with Broadcom, Marvell

Cisco Eyes \$1 Billion in Artificial Intelligence (AI) Orders

Cisco Acquisitions of Splunk, Isovalent Underscore Focus on Cybersecurity and AI

Využití AI v Cisco Secure portfoliu

Injecting AI Across The Portfolio

Assist

AI Assistant Experience

Give your admins superpowers.
Simplify management, improve outcomes.

Augment

AI Powered Detection

Correlate 550B security events at
machine-speed.

Automate

Autonomous Actions

Learn from human-to-machine
interactions to automate complex
playbooks.

Cisco Security Cloud

Breach Protection

User Protection

Cloud Protection

Firewall Foundation

Cisco Security Assistants

Assist

AI Assistant Experience

Give your admins superpowers.
Simplify management, improve outcomes.

Augment

AI Powered Detection

Correlate 550B security events at
machine-speed.

Automate

Autonomous Actions

Learn from human-to-machine
interactions to automate complex
playbooks.

Cisco Security Cloud

Breach Protection

User Protection

Cloud Protection

Firewall Foundation



AI Assistant in Firewall

- Improve visibility
- Speed up troubleshooting
- Act faster


What do you want to ask today?
Choose from a suggestion below or use the text field to ask a question. I have limitations and won't always get it right, but your feedback will help me improve.

Access Control Rule Summary
Provide a summary of all access control policies.

Schedule Recurring Backups: A How-To Guide
How do I schedule a recurring backup?

Initial Setup Guide: Common best practices
What are the best practices you can walk me through?

Access Control Rule Count
How many access control rules are there?

Ask the AI Assistant a question 

[View our FAQs to learn more.](#)

AI Assistant in Secure Access

- Simplify and speed up policy administration by 70%
- Reduce human error with automatic error handling prompts.

The screenshot displays the Cisco Secure Access dashboard. The main content area is titled 'Access Policy' and contains a table of 894 rules. Below the table is a section for 'Default Access Rules'. A 'Cisco Assistant' overlay window is open on the right side of the dashboard, featuring a large blue circular logo and a text prompt: 'Let's create some access rules today, shall we?'. The assistant provides instructions on how to create rules and offers two buttons: 'Create a single rule' and 'Create multiple rules'. A text input field is also present for creating rules.

Rule name	Access	Action	Sources
889 Any employee access to any application	Private	Allow	Any User Groups +3
890 US-Canada Employees	Private	Block	North American Employees
891 Product Management Resources	Internet	Warn	PM User Group +1
892 Europe Content Block List	Internet	Isolate	Europe Employees +1
893 Contractors access to Lab App	Private	Allow	Contractors User Group
894 Workday resources	Internet	Block	Any User Groups +7

Rule name	Action	Sources
For all private destinations	Block	Any
For all internet destinations	Allow	Any

AI Assistant in XDR

- Recommend actions
- Investigate IOCs
- Get incident summaries

The screenshot displays the Cisco XDR AI Assistant interface. At the top, the navigation bar includes the Cisco logo, 'XDR', a search bar, and user information for 'Alexander Business Corp, Inc'. The main content area is titled 'AI Assistant' and contains a chat window. The chat history shows a user asking 'Who are the owners associated with these endpoints?' and the AI Assistant responding with a list of four endpoints: E2E-DataLake-Internet1, DESKTOP-2ER967Q, E2E-Win10-x64-G, and Desktop-Win53. Below the list, the user asks 'How do you want to address this incident?' and the AI Assistant suggests 'Quarantine the compromised systems.' To the right of the chat is a network diagram showing relationships between various assets. A 'Malicious URL' (mta3.mixamail...) is linked to a 'Malicious SHA' (263efd9cd6...) via a 'Behavioral relationship'. Another 'Malicious SHA' (bfd9cd626...) is also linked to the same 'Malicious SHA' (263efd9cd6...). An 'Asset (Endpoint)group' is also linked to the 'Malicious SHA' (263efd9cd6...). The diagram uses red dashed circles to highlight the malicious IOCs and blue solid circles for the assets.

Bezpečnostní řešení pro používání AI

Proč? Nový rizikový vektor

AI Applications can be non-deterministic



Cisco AI Defense

Cisco Secure Access and Umbrella AI app detection

AI Security Journey

Safely enable generative AI across your organization



Discovery

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



Detection

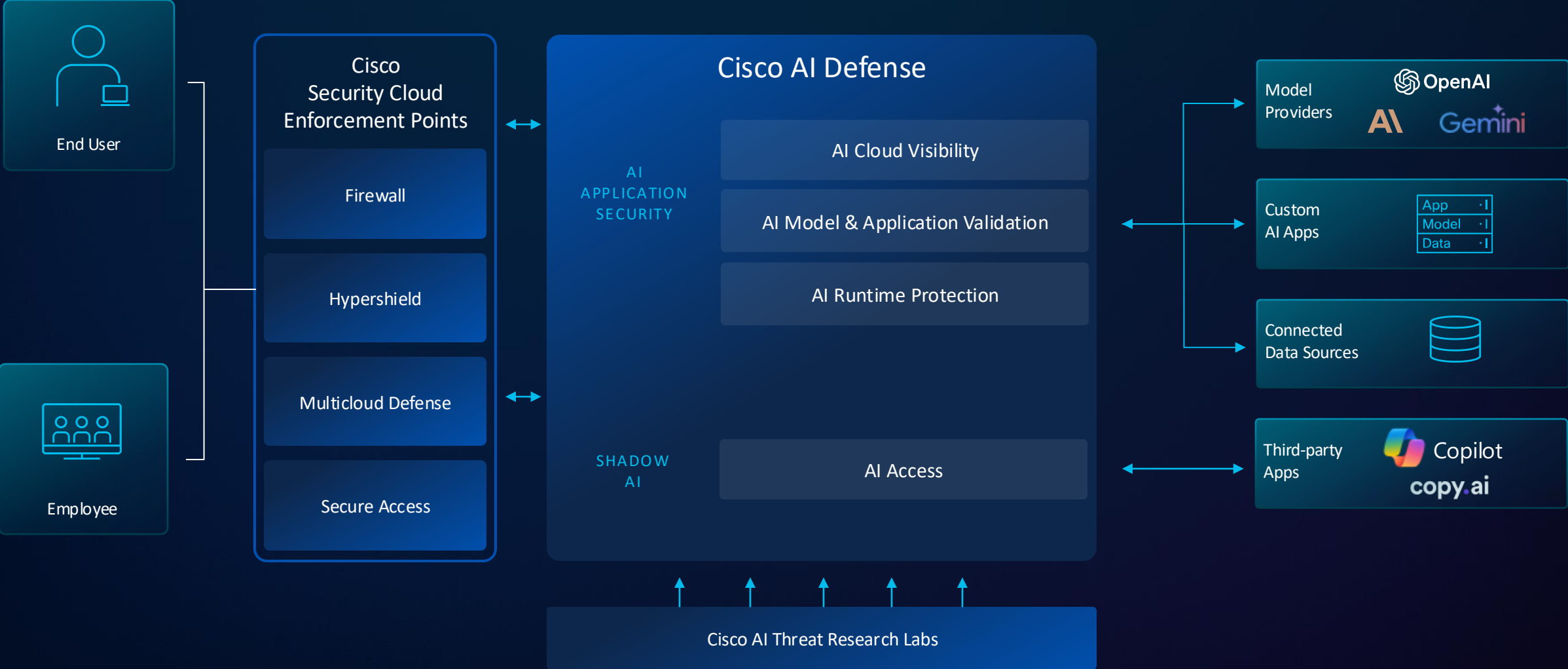
Test for AI risk, vulnerabilities, and adversarial attacks



Protection

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

The AI Defense Solution – Březen 2025!



Secure Access: protecting the usage of AI

Protect intellectual property as it flows in and out of AI systems

Threat Visibility

Discover and Assess Activities

Leakage Prevention

DLP Inspection of Prompts/Uploads

Threat Prevention

Block Apps and Control Downloads

Discovers and controls more than **70** Gen AI apps (including APIs)



DeepSeek

Block



Secure Access: New DLP Policy

- Adds to the traditional DLP capabilities.
- Uses predictive classifier model to detect “intent” in prompts vs regex type patterns
- Example: “please generate a table with all emails from the attached database”

Data Loss Prevention Policy
When enabled through its rules, the Data Loss Prevention policy can monitor or block the data being uploaded to the web. As well, it can discover and protect the sensitive data stored and shared in your cloud sanctioned applications. [Help](#)

DISCOVERY SCAN ADD RULE

12 DLP Rules

Rule Type	Name	Severity	Action	Identities or File Owners	Destinations	Data Classifications File Labels	Last Modified
AI Defense	AI Defense traffic direction	Medium	Monitor	Inclusion 1 Identity	Inclusion 2 Applications	Data Classifications Privacy guardrail	Dec 17, 2024

Data Classifications
Select data classifications to add them to this rule.

Search Classifications

- Privacy guardrail [PREVIEW](#)
- Copy of Privacy guardrail [PREVIEW](#)
- Custom Privacy guardrail [PREVIEW](#)
- Example AI Classification [PREVIEW](#)
- Safety guardrail [PREVIEW](#)
- Security guardrail [PREVIEW](#)

Security guardrail
Protect your generative AI applications from threats and unauthorized access and prevent these applications from being used to carry out such activities.

Included Data Identifiers (OR Boolean)

- Code detection
- Prompt injection

DATA CLASSIFICATION

Umbrella: AI apps blocking

Cisco Umbrella

Overview

Deployments >

Policies >

Management

- DNS Policies
- Firewall Policy
- Web Policy
- Data Loss Prevention Policy

Policy Components

- IPS Signature Lists
- Destination Lists
- Content Categories
- Application Settings**
- Tenant Controls
- Schedule Settings
- Security Settings
- Block Page Appearance
- Integrations Settings
- Selective Decryption Lists
- Data Classification

Policies / Policy Components

Application Settings i

Application Settings enable you to enforce special permissions on supported applications.

Add New Application Setting

Give Your Setting a Name

This Application List Applies To

Applications To Control

<input type="checkbox"/>	DeepfakesWeb	
<input type="checkbox"/>	Deepgram	
<input type="checkbox"/>	DeepImage	
<input type="checkbox"/>	DeepL Translate	
<input type="checkbox"/>	DeepL Write	
<input type="checkbox"/>	DeepMotion	
<input checked="" type="checkbox"/>	DeepSeek	Block ⚙️
<input type="checkbox"/>	Deepswap	
<input type="checkbox"/>	SenseDeep	

