Cisco AI

Security for AI and AI for Security

Milan Habrcetl, Cisco

Agenda

1 AI – nedílná součást bezpečnostních řešení

2 Bezpečnostní řešení pro využívání AI modelů

Využití AI v Cisco Secure portfoliu

Využití AI napříč celým Cisco portfoliem

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

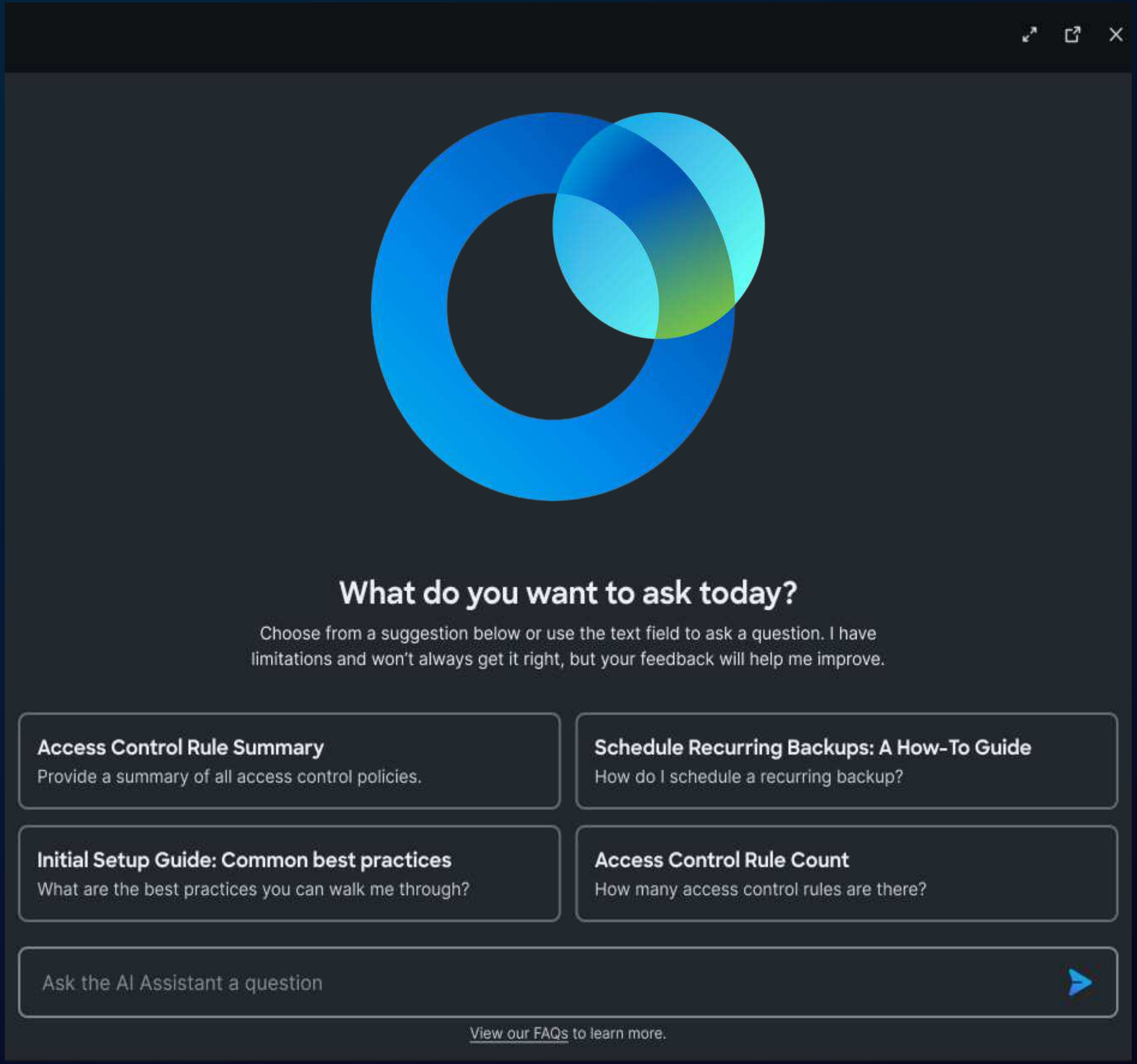
Cloud Protection

Firewall Foundation

Use-Cases Driven by Customer Feedback

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?

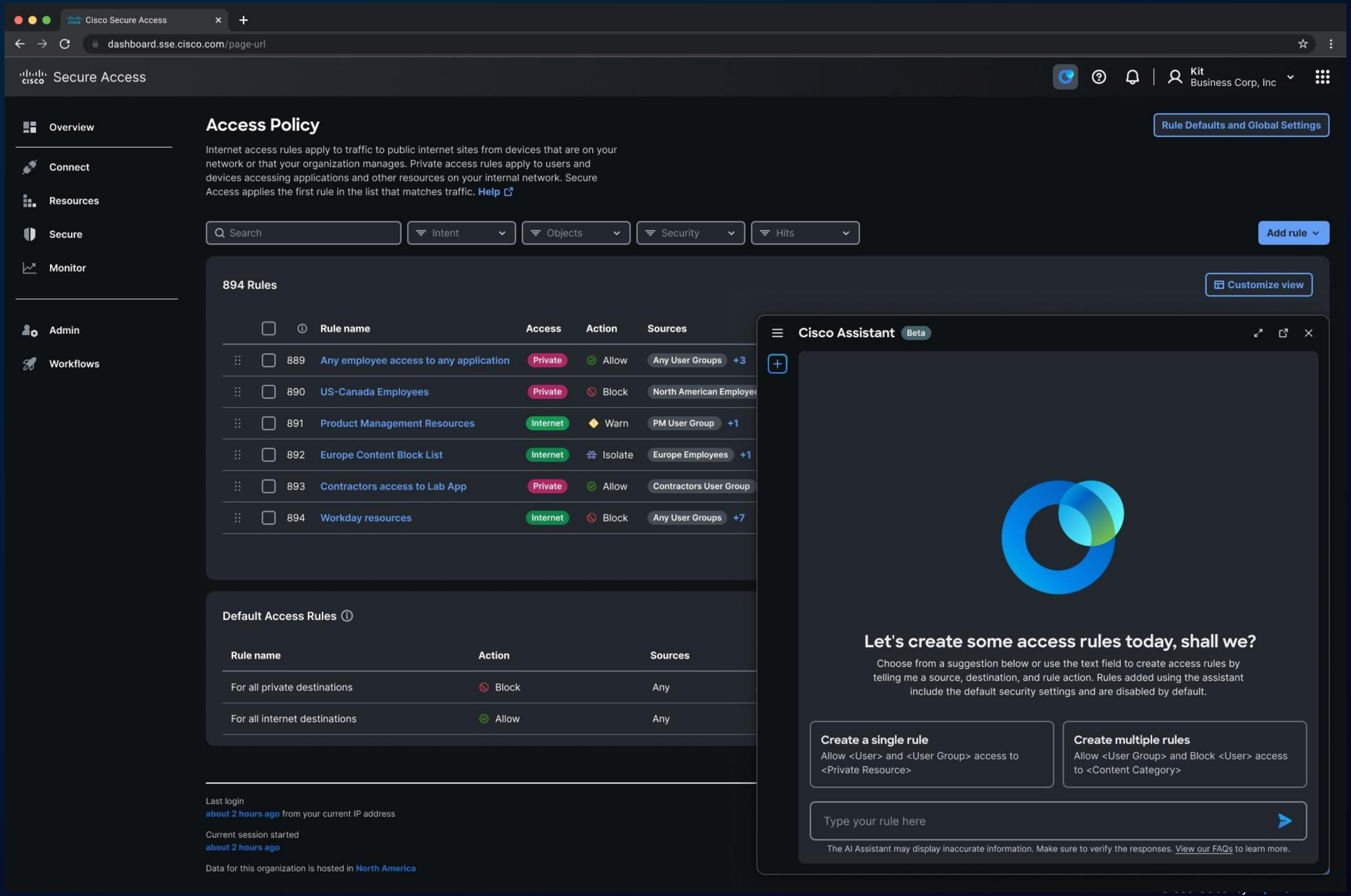
Access Control Rule Count
How many access control rules are there?

View our FAQs to learn more.

Use-Cases Driven by Customer Feedback

AI Assistant in Secure Access

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



Access Policy

Internet access rules apply to traffic to public internet sites from devices that are on your network or that your organization manages. Private access rules apply to users and devices accessing applications and other resources on your internal network. Secure Access applies the first rule in the list that matches traffic. Help

894 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 Employe
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

Default Access Rules

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

Last login
about 2 hours ago from your current IP address

Current session started
about 2 hours ago

Data for this organization is hosted in North America

Cisco Assistant Beta

Let's create some access rules today, shall we?

Choose from a suggestion below or use the text field to create access rules by telling me a source, destination, and rule action. Rules added using the assistant include the default security settings and are disabled by default.

Create a single rule
Allow <User> and <User Group> access to <Private Resource>

Create multiple rules
Allow <User Group> and Block <User> access to <Content Category>

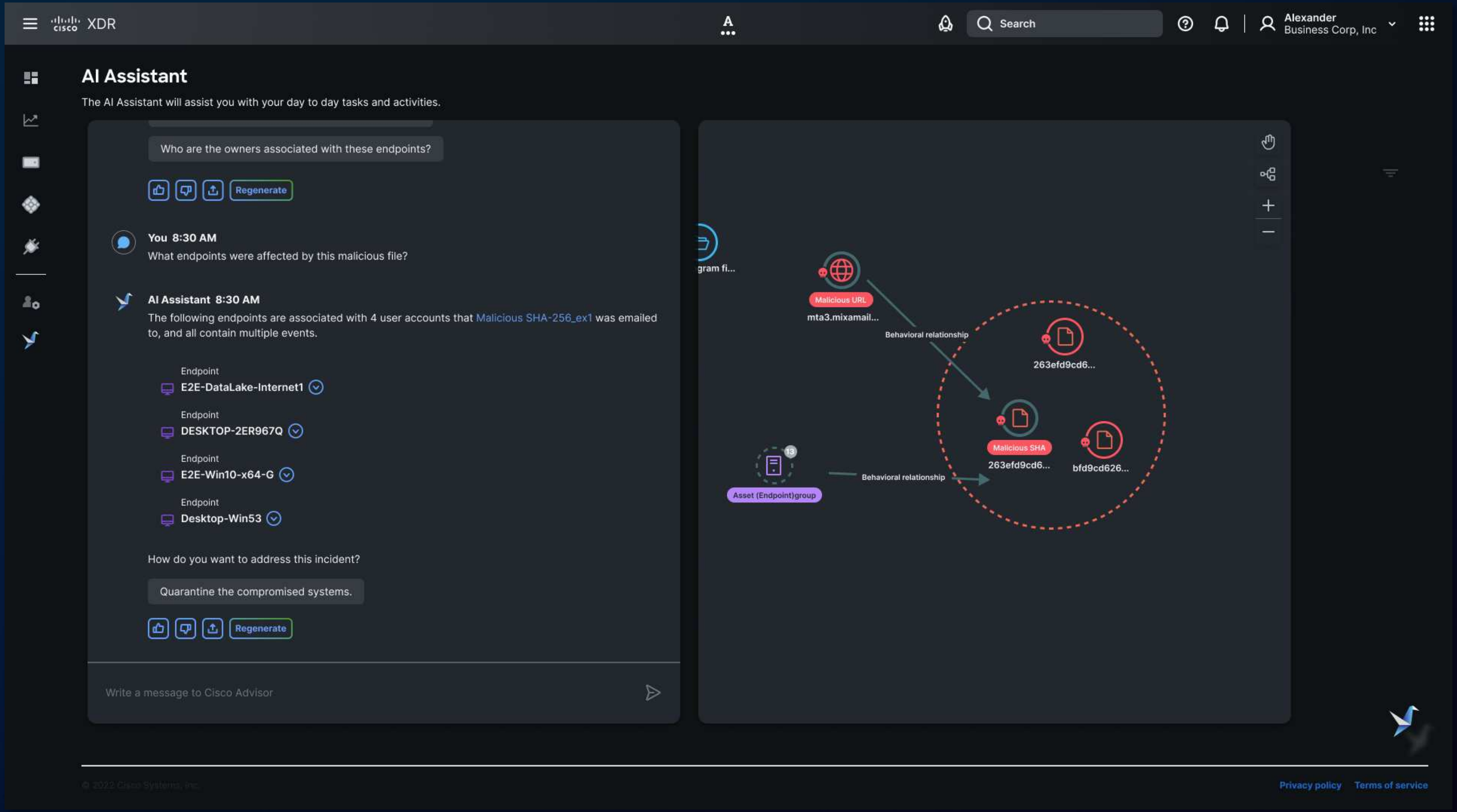
Type your rule here

The AI Assistant may display inaccurate information. Make sure to verify the responses. View our FAQs to learn more.

Use-Cases Driven by Customer Feedback

AI Assistant in XDR

- Recommend actions
- Investigate IOCs
- Get incident summaries



AI Assistant

The AI Assistant will assist you with your day to day tasks and activities.

Who are the owners associated with these endpoints?

Regenerate

You 8:30 AM
What endpoints were affected by this malicious file?

AI Assistant 8:30 AM
The following endpoints are associated with 4 user accounts that Malicious SHA-256_ex1 was emailed to, and all contain multiple events.

Endpoint
E2E-DataLake-Internet1

Endpoint
DESKTOP-2ER967Q

Endpoint
E2E-Win10-x64-G

Endpoint
Desktop-Win53

How do you want to address this incident?

Quarantine the compromised systems.

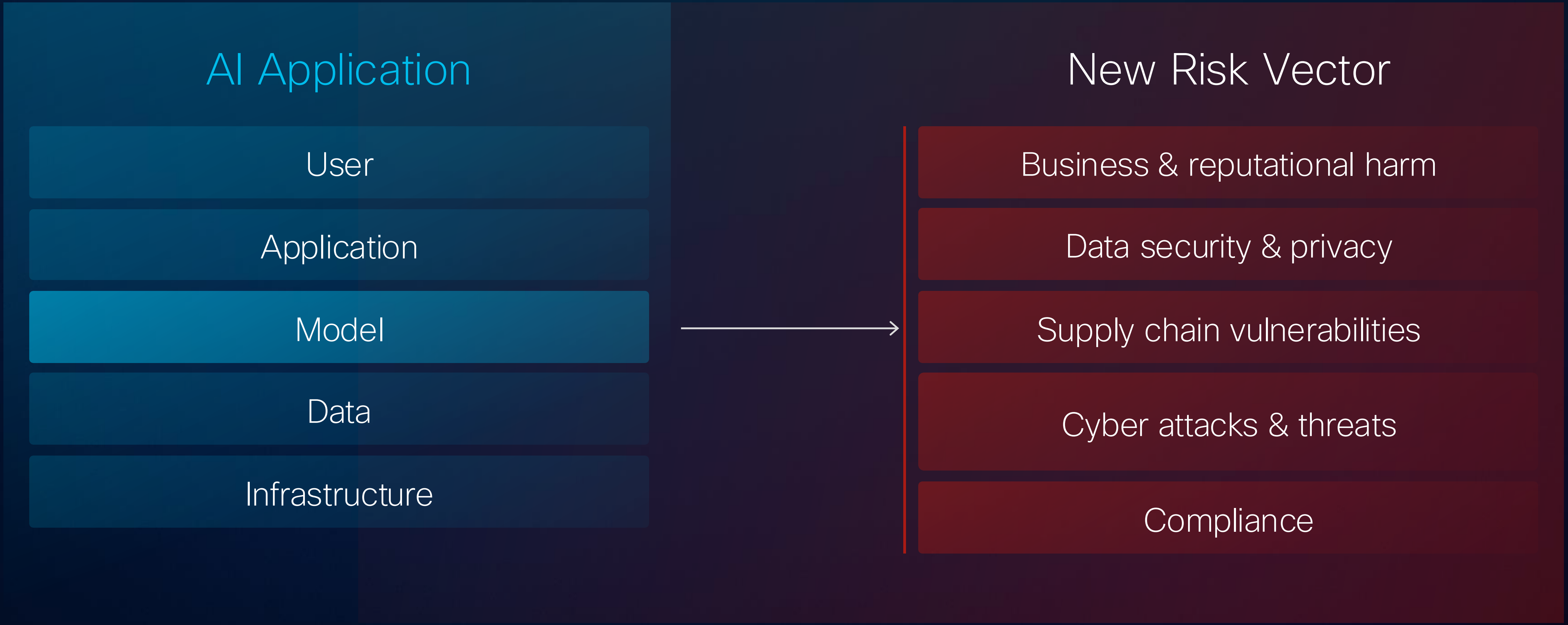
Regenerate

Write a message to Cisco Advisor

Bezpečnostní řešení pro používání AI

Proč? Nový rizikový vektor

AI Applications can be non-deterministic



Cisco AI Defense

Cisco AI Defense

AI Security Journey

Safely enable generative AI across your organization

Discovery

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

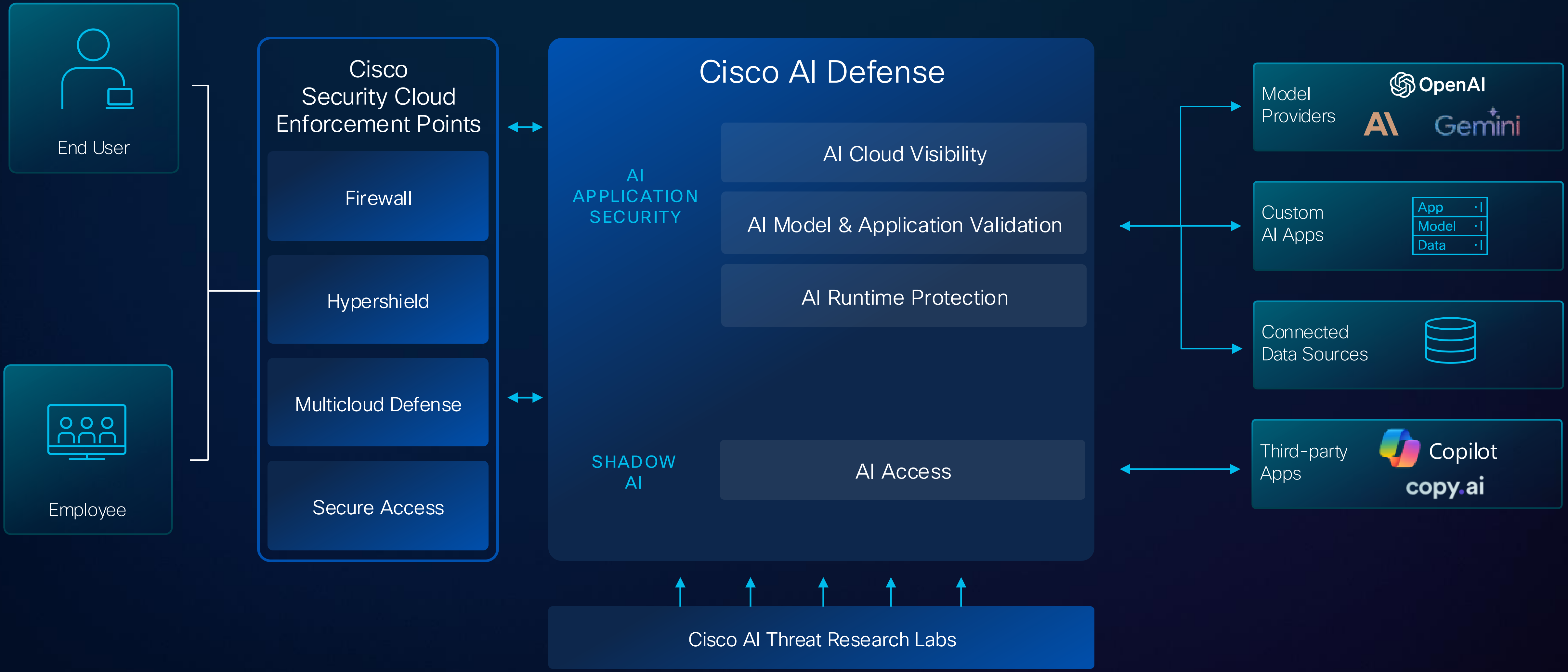
Detection

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!



End User

Employee

Cisco Security Cloud Enforcement Points

Firewall

Hypershield

Multicloud Defense

Secure Access

Cisco AI Defense

AI APPLICATION SECURITY

AI Cloud Visibility

AI Model & Application Validation

AI Runtime Protection

SHADOW AI

AI Access

Cisco AI Threat Research Labs

Model Providers

Custom AI Apps

Connected Data Sources

Third-party Apps

AI Access: Third–Party AI App Security

Discovery

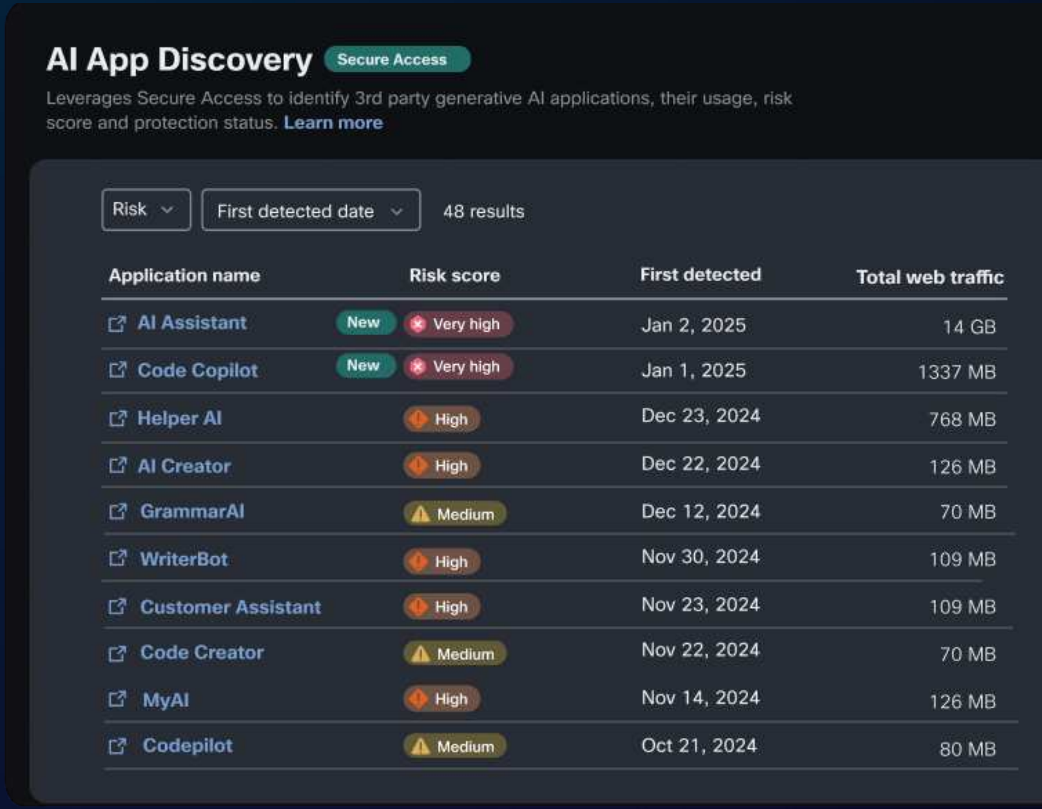
Find use of shadow AI apps across organization

Detection

Assess risk of third-party apps and get context around devices, location, network, and more

Protection

Control access and protect prompts and answers from exposing sensitive data and propagating threats, using best-in-class ML models



AI App Discovery Secure Access

Leverages Secure Access to identify 3rd party generative AI applications, their usage, risk score and protection status. Learn more

Risk ⌄ | First detected date ⌄ | 48 results

Application name		Risk score	First detected	Total web traffic
AI Assistant	New	Very high	Jan 2, 2025	14 GB
Code Copilot	New	Very high	Jan 1, 2025	1337 MB
Helper AI		High	Dec 23, 2024	768 MB
AI Creator		High	Dec 22, 2024	126 MB
GrammarAI		Medium	Dec 12, 2024	70 MB
WriterBot		High	Nov 30, 2024	109 MB
Customer Assistant		High	Nov 23, 2024	109 MB
Code Creator		Medium	Nov 22, 2024	70 MB
MyAI		High	Nov 14, 2024	126 MB
Codepilot		Medium	Oct 21, 2024	80 MB

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

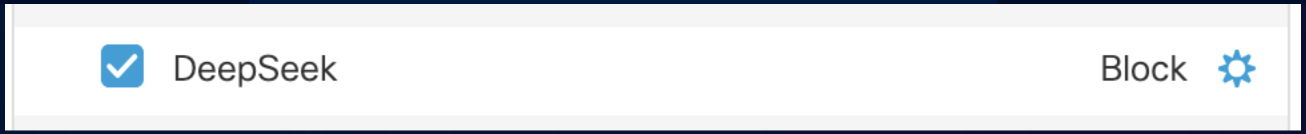
Leakage Prevention

DLP Inspection of Prompts/Uploads

Threat Prevention

Block Apps and Control Downloads

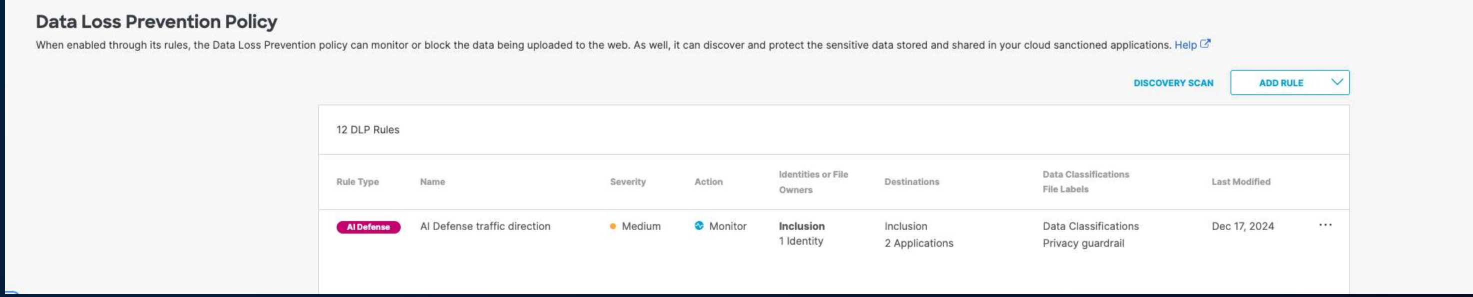
Discovers and controls more than **70** Gen AI apps (including APIs)



☑ 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”

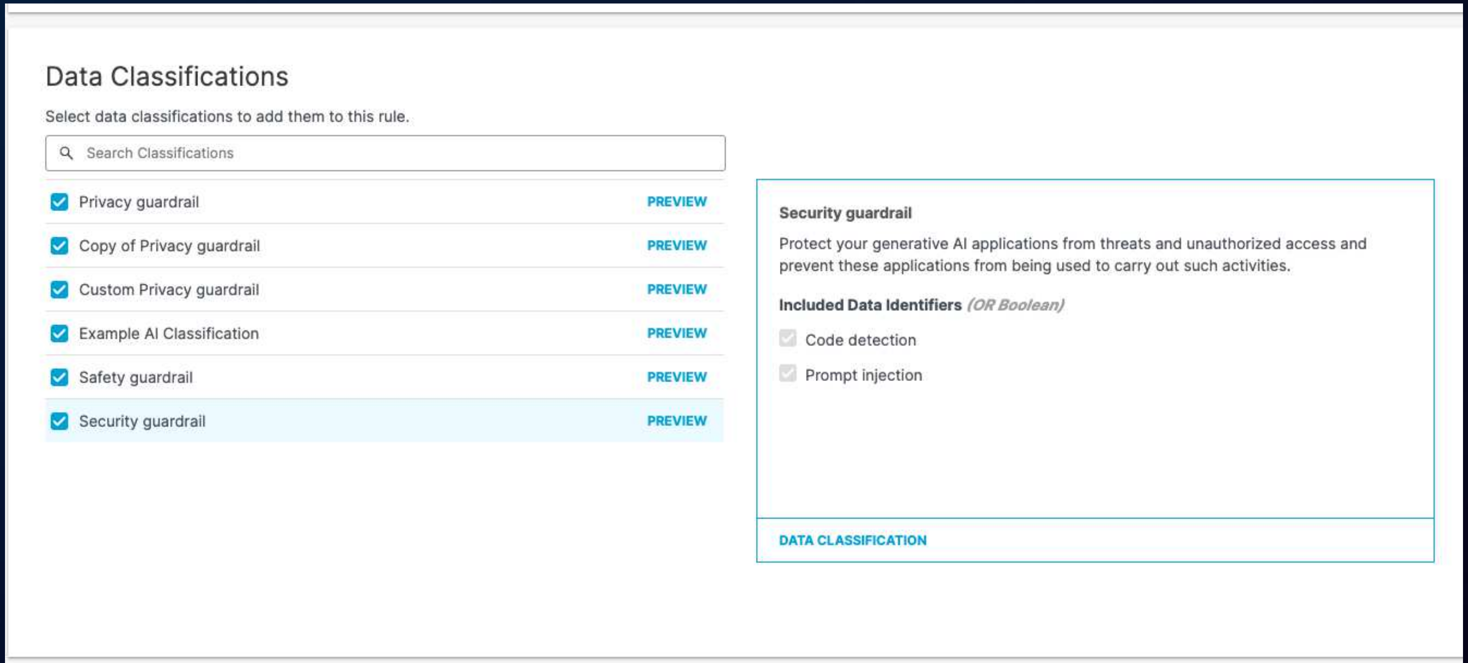


Data Loss Prevention Policy

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

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.

- ☑ 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

CISCO