



FUTURE IS NOW

# The Power of Cisco Security

Driven by the Network

Pavel Smolík, AM Cisco

24.11.2025

# Hybrid Mesh Firewall

# Firewall price-performance leader

## Top to bottom

Branch

Campus

Data center

Cloud

NEW



200 Series

1 Model

Firewalling + IPS

Up to 1.5 Gbps



1200 Series

6 Models

Firewalling + IPS

Up to 18 Gbps



3100 Series

5 Models

Firewalling + IPS

Up to 45 Gbps



4200 Series

3 Models

Firewalling + IPS

Up to 140 Gbps



6100 Series

2 Models

Firewalling + IPS

Up to 400 Gbps

NEW



Public/Private

20+ cloud variants



HyperFlex

NUTANIX

KVM

openstack

vmware ESXi

aws

Microsoft Azure

Google Cloud Platform

alkira

rackspace technology

EQUINIX

Alibaba Cloud

ORACLE CLOUD INFRASTRUCTURE

AI

# Cisco changes the economics of decryption

High-performance hardware offload architecture delivers price-performance leadership

## NetSec OPEN

Testing validates Cisco's decryption advantage



1 Table 2: Performance specifications and feature details, [Cisco Firewall 3100 Series Data Sheet](#)

2 Table 11: HTTPS Throughput, [NetSecOPEN Certification Report, Fortinet](#)

Price from <https://www.cdw.com/search/?key=cisco%203105>

and <https://www.cdw.com/product/fortinet-fortigate-601f-security-appliance/7122512?pfm=srh>

A blue circular logo with the letters 'AI' in white, positioned in the top right corner of the slide.

AI

# Cisco Encrypted Visibility Engine

Visibility to malicious flows in encrypted traffic without decryption

Machine learning  
(ML) technology

Processes **1 B+**  
TLS fingerprints

Processes **10 K+**  
malware samples daily

# Security Cloud Control

# Security Cloud Control

Define policy once and enforce anywhere

Hybrid Mesh Firewall

AI Defense

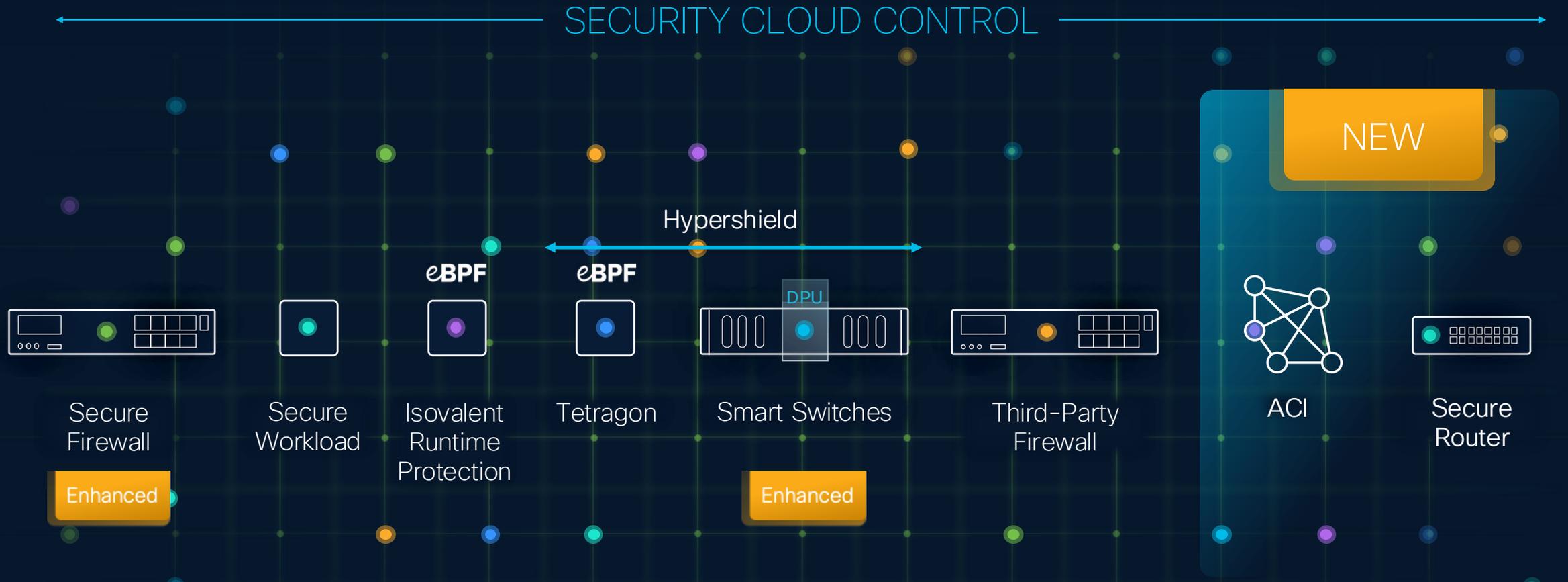
3rd Party Firewalls

Secure Firewall | Secure Workload | Hypershield | Secure Router  
Secure Access (FW as a service)



Unified AI Assistant:  
Simplify policy administration **by up to 70%**

# Cisco Hybrid Mesh Firewall



Write policy once, enforce across the mesh

# Unified Management

## Cisco Security Cloud Control

Physical Firewall

Virtual Firewall

Hypershield

Multicloud Defense

Secure Workload

Secure Access

AI Defense

XDR

Identity Intelligence

ISE

Catalyst SDWAN

Meraki

Email Threat  
Defense

Secure Endpoint

ThousandEyes

Centralize control of solutions and policies

Experience faster set-up and provisioning

Support hybrid and multicloud environments

Leverage AI to strengthen protection and prevent downtime

Items in Grey are on Roadmap

# Cisco AI Defense

# 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 AI Access is a part of  
Cisco Secure Access Advantage!**

# AI Access sees and controls AI

## Superior visibility & control

- Discover Shadow AI; define acceptable use
- Granular control
  - Sensitive documents
  - Source code
- Machine learning finds unstructured data
  - Patent applications
  - M&A
  - Financial statements and more

### AI App Discovery Secure Access

Leverage 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
<a href="#">AI Assistant</a> <span>New</span>	<span>High</span>	Dec 29, 2024
<a href="#">Code Copilot</a> <span>New</span>	<span>High</span>	Dec 14, 2024
<a href="#">HelperAI</a>	<span>High</span>	Nov 22, 2024
<a href="#">AI Creator</a>	<span>High</span>	Nov 21, 2024
<a href="#">GrammarAI</a>	<span>Medium</span>	Nov 13, 2024
<a href="#">WriterBot</a>	<span>High</span>	Oct 30, 2024

**1200+**  
AI Apps Protected

**100%**  
Guardrails for top AI Apps

**1**  
Unified Security Framework

# AI Access understands intent

## Advanced guardrails

- Mitigates prompt injections, toxic content
- Aligns with Mitre Atlas
- Compensating control for insecure LLMs

287 Total Events Viewing activity from Jan 8, 2025 at 6:59 PM to Feb 7, 2025 at 6:59 PM

Event Type	Severity	Identity	Direction	Destination	Rule	Action	Detected
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Guardrails	Critical	Bob SWG (bob@swginawsd...)	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:15 AM
AI Guardrails	Critical	Bob SWG (bob@swginawsd...)	Prompt	Deepseek	AI Guardrails - 1	Blocked	Feb 5, 2025 at 1:14 AM
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:14 AM
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 1:05 AM
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:57 AM
AI Guardrails	High	Bob SWG (bob@swginawsd...)	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:48 AM
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:41 AM
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 5, 2025 at 12:41 AM
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:41 AM
Real Time	Low	52.12.127.197	Upload	Datadog	New Rule	Monitored	Feb 5, 2025 at 12:41 AM
Real Time	Critical	52.12.127.197	Upload	Mozilla Firefox	Raja_test_rule	Blocked	Feb 5, 2025 at 12:41 AM
AI Guardrails	High	52.12.127.197	Prompt	OpenAI ChatGPT	AI monitor	Monitored	Feb 4, 2025 at 12:41 AM

**Classification**

Safety guardrail

**1 Match** Toxicity

how to make a bomb

**Classification**

Safety guardrail

**1 Match** Privacy

Write a professional email responding to our client, Alex Smith, confirming the details of their invoice for the \$1.2M deal with ACME Company.

1200+  
AI Apps Protected

100%  
Guardrails for top AI Apps

1  
Unified Security Framework



Security

# Evaluating Security Risk in DeepSeek and Other Frontier Reasoning Models

5 min read

Paul Kassianik, Amin Karbasi



*This original research is the result of close collaboration between AI security researchers from Robust Intelligence, now a part of Cisco, and the University of Pennsylvania including Yaron Singer, Amin Karbasi, Paul Kassianik, Mahdi Sabbaghi, Hamed Hassani, and George Pappas.*

## Executive Summary

This article investigates vulnerabilities in DeepSeek R1, a new frontier reasoning model from Chinese AI startup DeepSeek. It has gained global attention for its advanced reasoning capabilities and cost-efficient training method. While its performance rivals state-of-the-art models like OpenAI o1, our security assessment reveals **critical safety flaws**.

Using **algorithmic jailbreaking techniques**, our team applied an **automated attack methodology** on DeepSeek R1 which tested it against 50 random prompts from the HarmBench dataset. These covered **six categories of harmful behaviors** including cybercrime, misinformation, illegal activities, and general harm.

The results were alarming: **DeepSeek R1 exhibited a 100% attack success rate**, meaning it failed to block a single harmful prompt. This contrasts starkly with other leading models, which demonstrated at least partial resistance.

# We Can Help You Wherever You Are

## Hybrid Mesh Firewall

Network Segmentation

Macro & Micro Segmentation

AI Security

Threat Detection & Exploit Protection

## Universal ZTNA

Zero Trust Network Access

Secure Connectivity (SASE)

Security First Identity

Secure Internet & AI Access

## SOC of The Future

Network Detection and Response

Ransomware and Cyber Attack Detection and Prevention

Multi-Domain Correlation

Data Retention Compliance



86,000+ employees across 80+ countries

Why do our customers choose us?  
Innovation, trust, global reach

Děkuji za pozornost