Security Summit

Milano 11-12-13 marzo 2025

AI for Security, Security for AI

Andrea Verri | Solution Engineer, *Cisco*
Luciano Pomelli | Solution Engineer Leader, *Cisco*

Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit Associazione Italiana per la Sicurezza Informatica

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection del Politecnico di Milano osservatori.net digital innovation

Andrea Verri
Solution Engineer Cisco

Andrea è entrato a far parte di Cisco nel 2000 e ha sempre lavorato su tecnologie emergenti nel settore della sicurezza e dei data center, ricoprendo da allora diversi ruoli in azienda. Ora lavora nel team EMEA Security come Cyber Security Solution Engineer, Cloud and Workload Security con alcuni dei più grandi account aziendali di Cisco per progettare e mettere in atto strategie di protezione dei carichi di lavoro attuali ed emergenti (cloud native) in un ambiente multicloud.

La sua area di competenza abbraccia diversi domini tecnologici (sistemi, networking, data center, sicurezza, cloud, containers, programmabilità) per adattarsi perfettamente alle tecnologie di protezione cloud di Cisco come Cisco Secure Workload, Cisco Multicloud Defense, Isovalent Cilium e Cisco Hypershield.

Prima di entrare a far parte di Cisco, Andrea ha lavorato in altre aziende multinazionali dove ha ricoperto ruoli di consulenza e management sempre legati alle nuove ed emergenti tecnologie sia nel settore delle telecomunicazioni che in quello del software.

Luciano Pomelli

Solution Engineer Leader Cisco

Luciano ha iniziato la carriera professionale lavorando sui sistemi IBM Mainframe, per poi ampliare la sua esperienza nel campo delle reti e delle tecnologie emergenti, con particolare focus sulla sicurezza, i data center e il cloud.

Entrato in Cisco nel 1996, ha ricoperto diversi ruoli nell'ambito dell’organizzazione tecnica di vendita, maturando una solida esperienza nell'implementazione di soluzioni tecnologiche avanzate.

Attualmente, ricopre il ruolo di responsabile tecnico per l’offerta di cybersecurity, dove guida l’innovazione e la protezione delle infrastrutture aziendali.

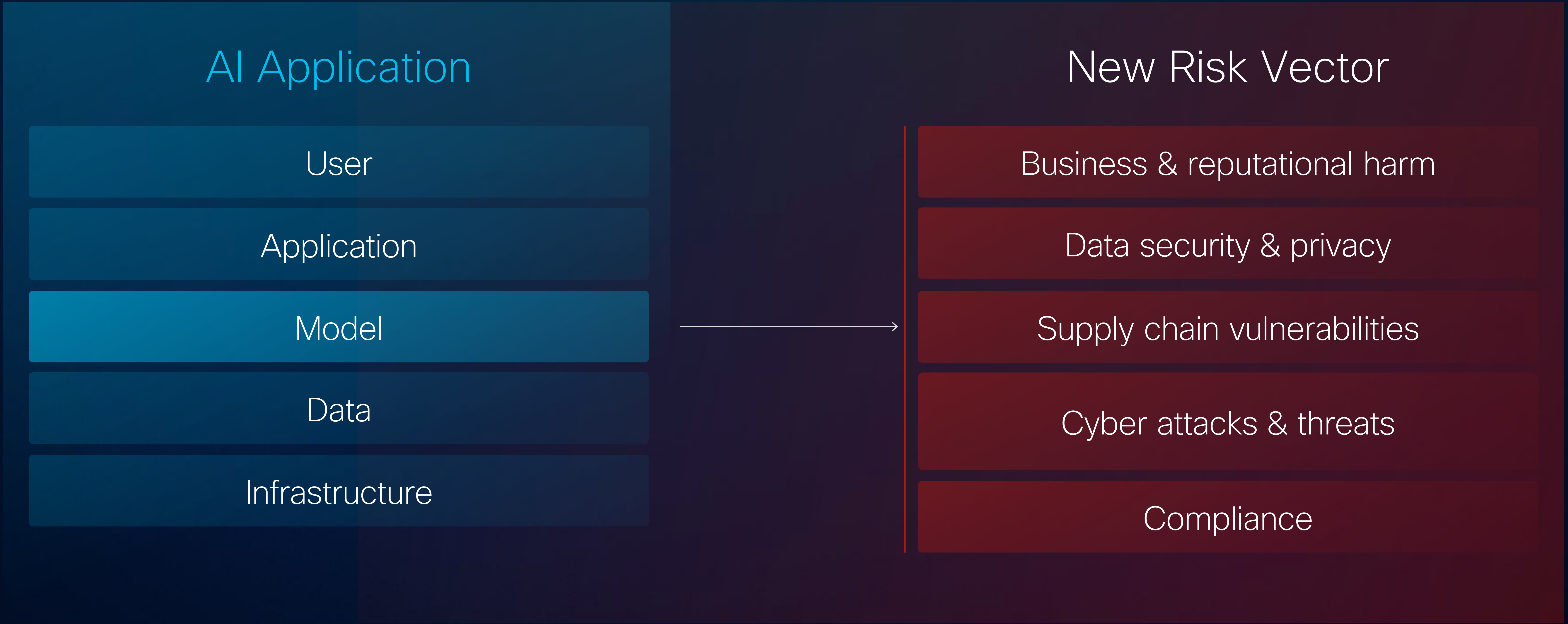
Security for AI

Using AI Apps

Developing AI Apps

What’s the risk?

AI Applications can be non-deterministic



AI Application

- User
- Application
- Model
- Data
- Infrastructure

→

New Risk Vector

- Business & reputational harm
- Data security & privacy
- Supply chain vulnerabilities
- Cyber attacks & threats
- Compliance

Using AI Apps

Developing AI Apps

Using AI Apps

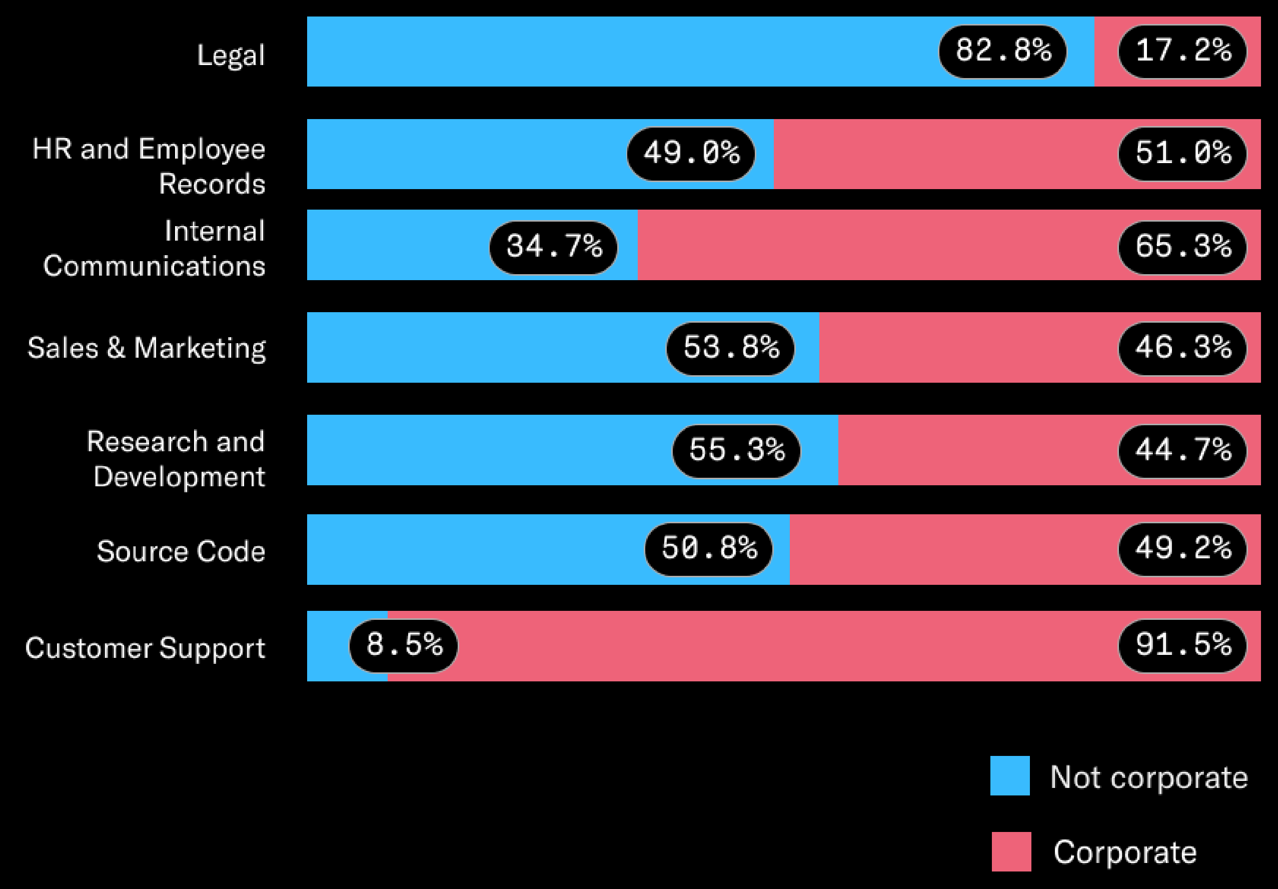
Unfettered use of Shadow AI poses risks

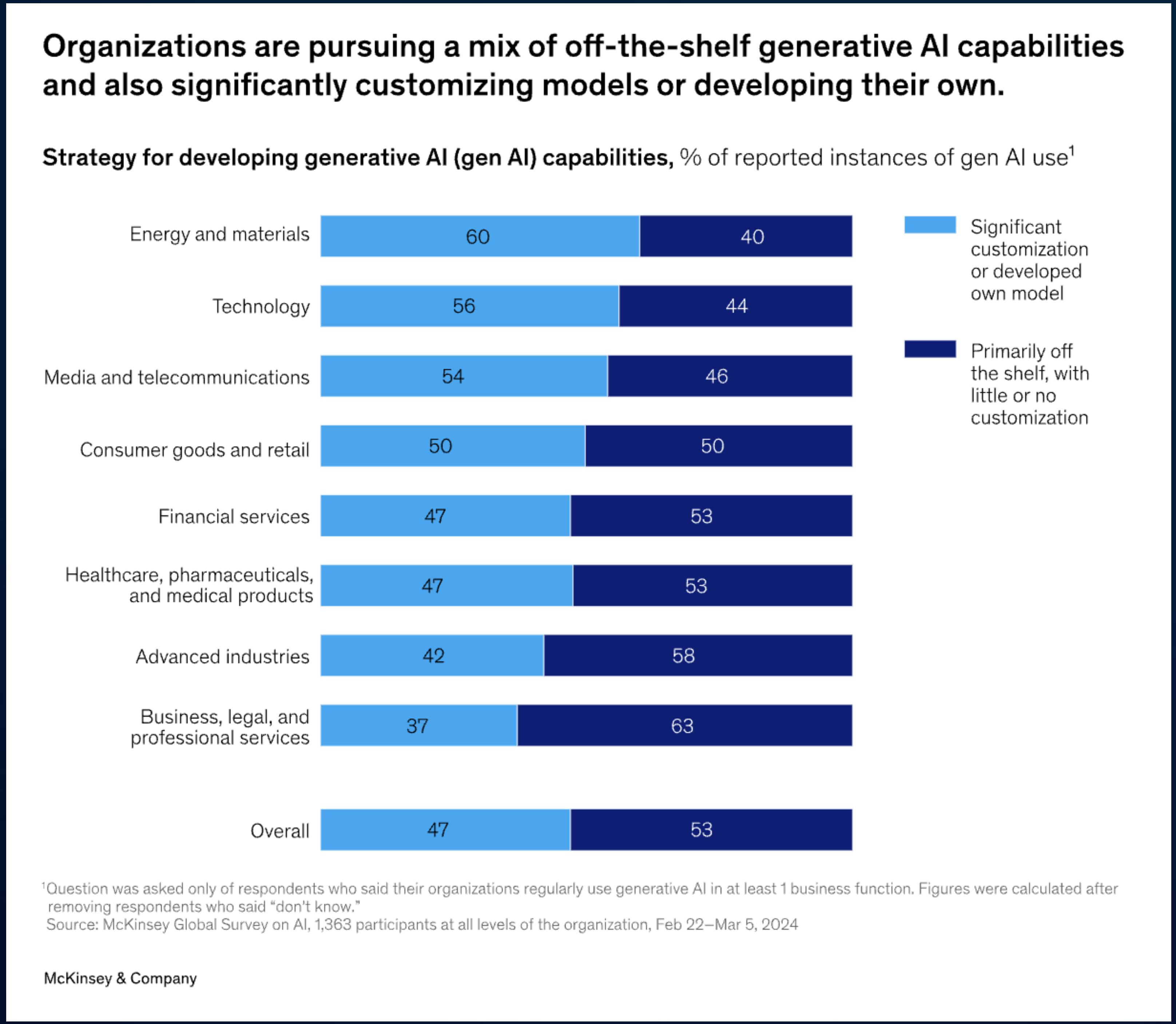
Sharing sensitive data

Ensure safe use of AI Apps

Destination for sensitive data by AI account type

(By volume of data)





Organizations are pursuing a mix of off-the-shelf generative AI capabilities and also significantly customizing models or developing their own.

Strategy for developing generative AI (gen AI) capabilities, % of reported instances of gen AI use[1]

	Significant customization or developed own model	Primarily off the shelf, with little or no customization
Energy and materials	60	40
Technology	56	44
Media and telecommunications	54	46
Consumer goods and retail	50	50
Financial services	47	53
Healthcare, pharmaceuticals, and medical products	47	53
Advanced industries	42	58
Business, legal, and professional services	37	63
Overall	47	53

[1] Question was asked only of respondents who said their organizations regularly use generative AI in at least 1 business function. Figures were calculated after removing respondents who said "don't know."

Source: McKinsey Global Survey on AI, 1,363 participants at all levels of the organization, Feb 22–Mar 5, 2024

McKinsey & Company

Developing AI Apps

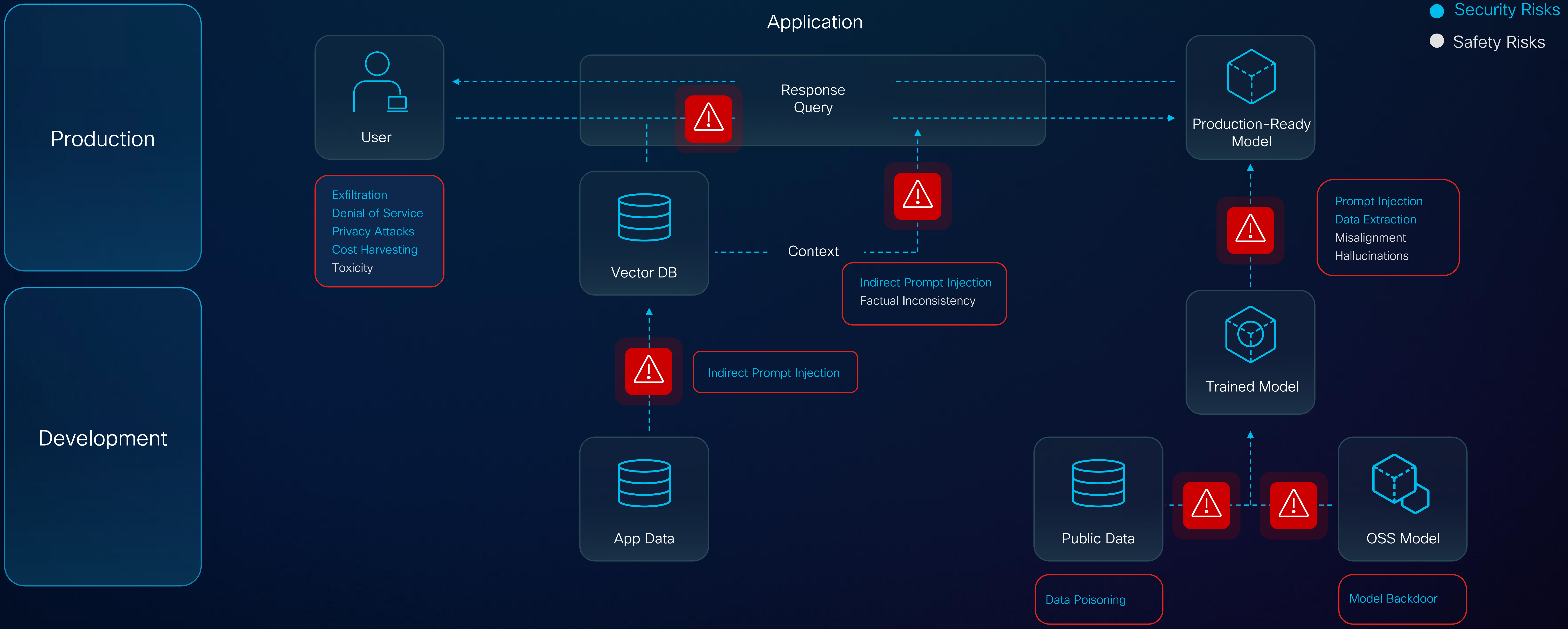
Introducing risks as they build new AI apps

Every app is an AI App

Security teams lack visibility

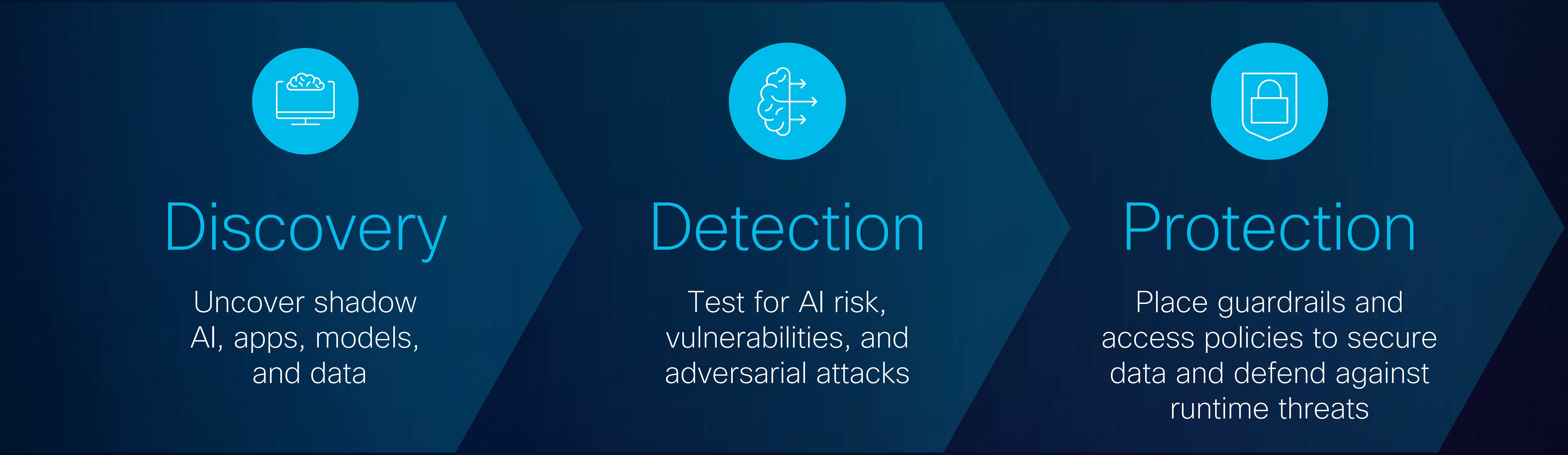
Common safety and security risks

Risk are present across the GenAI lifecycle



AI Security Journey

Safely enable GenAI across your organization



Discovery

Uncover shadow AI, apps, models, and data

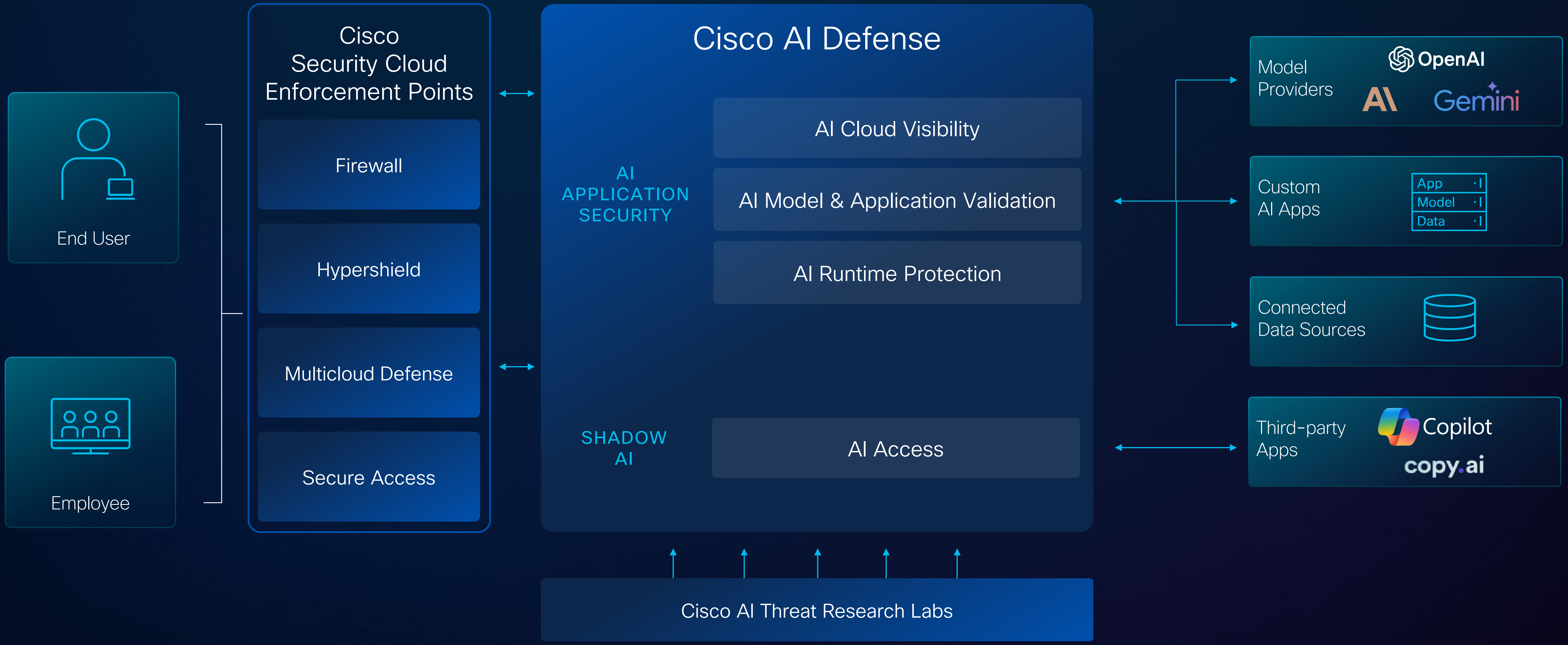
Detection

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



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

OpenAI

Gemini

Custom AI Apps

App

Model

Data

Connected Data Sources

Third-party Apps

Copilot

copy.ai

AI for Security

Hybrid Mesh Firewall

Securing the enterprise is increasingly challenging

Highly distributed, fine-grained apps

- Spanning data center, cloud
- Containers
- 1000s of microservices

Nothing can be trusted

- Distributed perimeter necessary but no longer sufficient
- Need security in every flow to stop lateral movement

More vulnerabilities, exploited faster

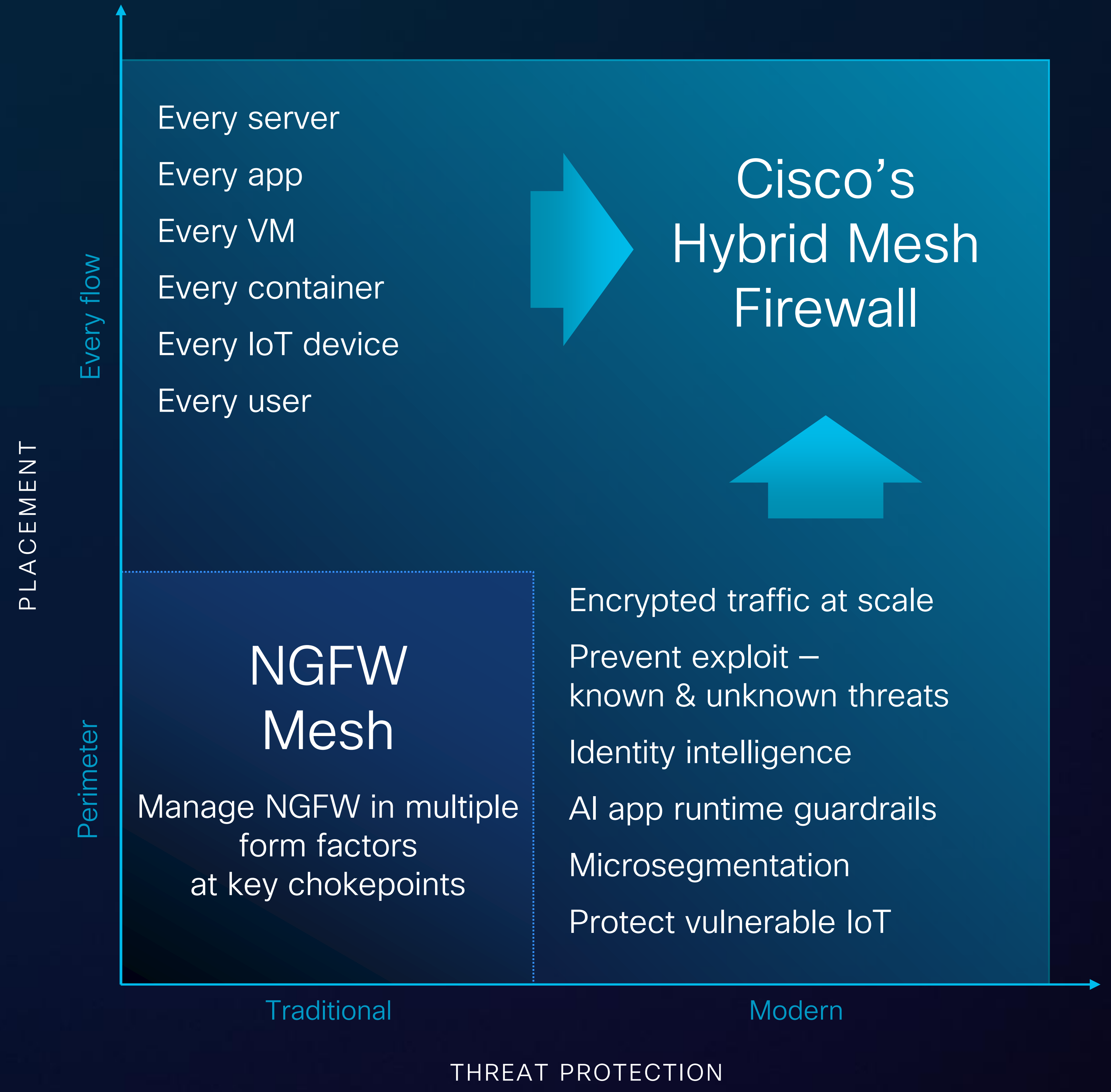
- Weeks to hours to minutes
- Patching can't keep up
- New AI model risks

AI increasing attack surface and attack sophistication

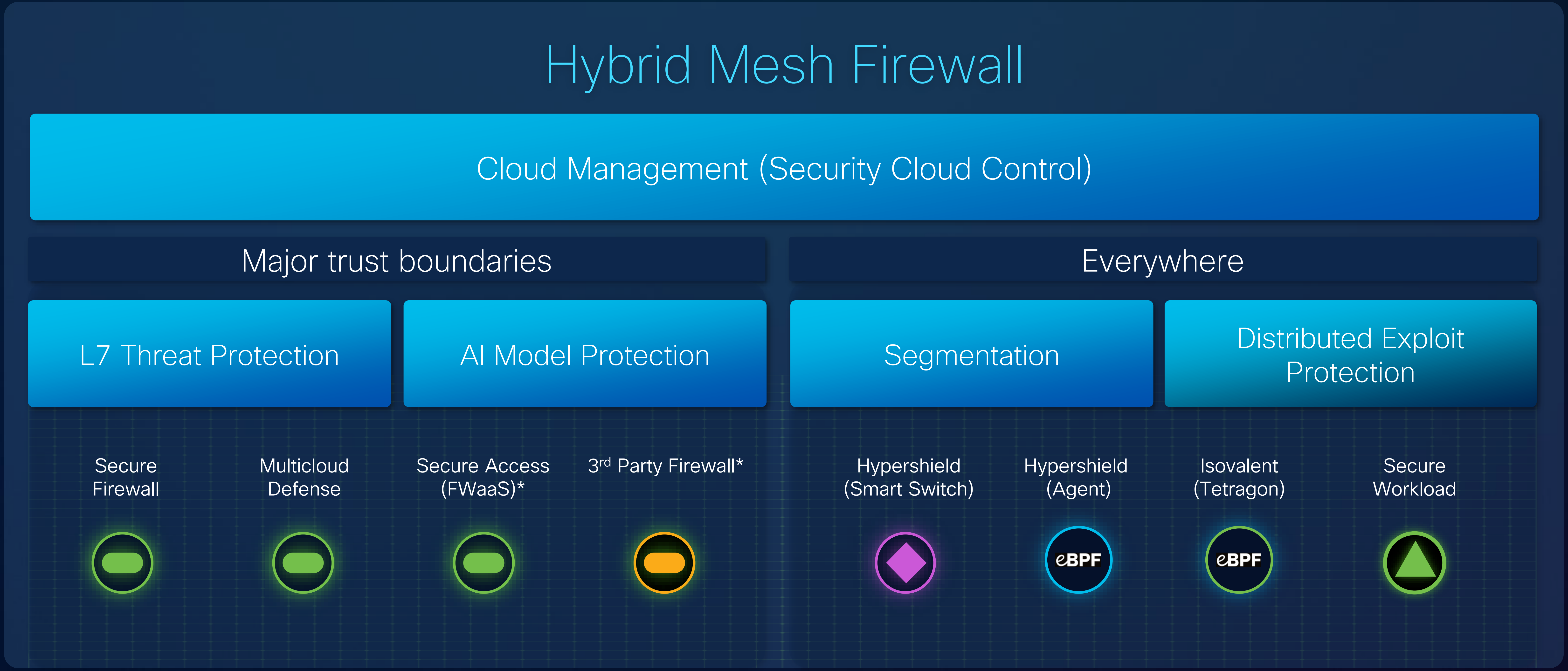
Firewalling needs to evolve to meet today's challenges

OUR NORTH STAR

Make it easy for organizations to reduce attack surface, prevent compromise, and stop lateral movement in the modern data center, cloud, campus, and factory



Cloud Protection Suite



Hybrid Mesh Firewall

Cloud Management (Security Cloud Control)

Major trust boundaries

- L7 Threat Protection
- AI Model Protection

Everywhere

- Segmentation
- Distributed Exploit Protection

Secure Firewall

Multicloud Defense

Secure Access (FWaaS)*

3rd Party Firewall*

Hypershield (Smart Switch)

Hypershield (Agent)

Isovalent (Tetragon)

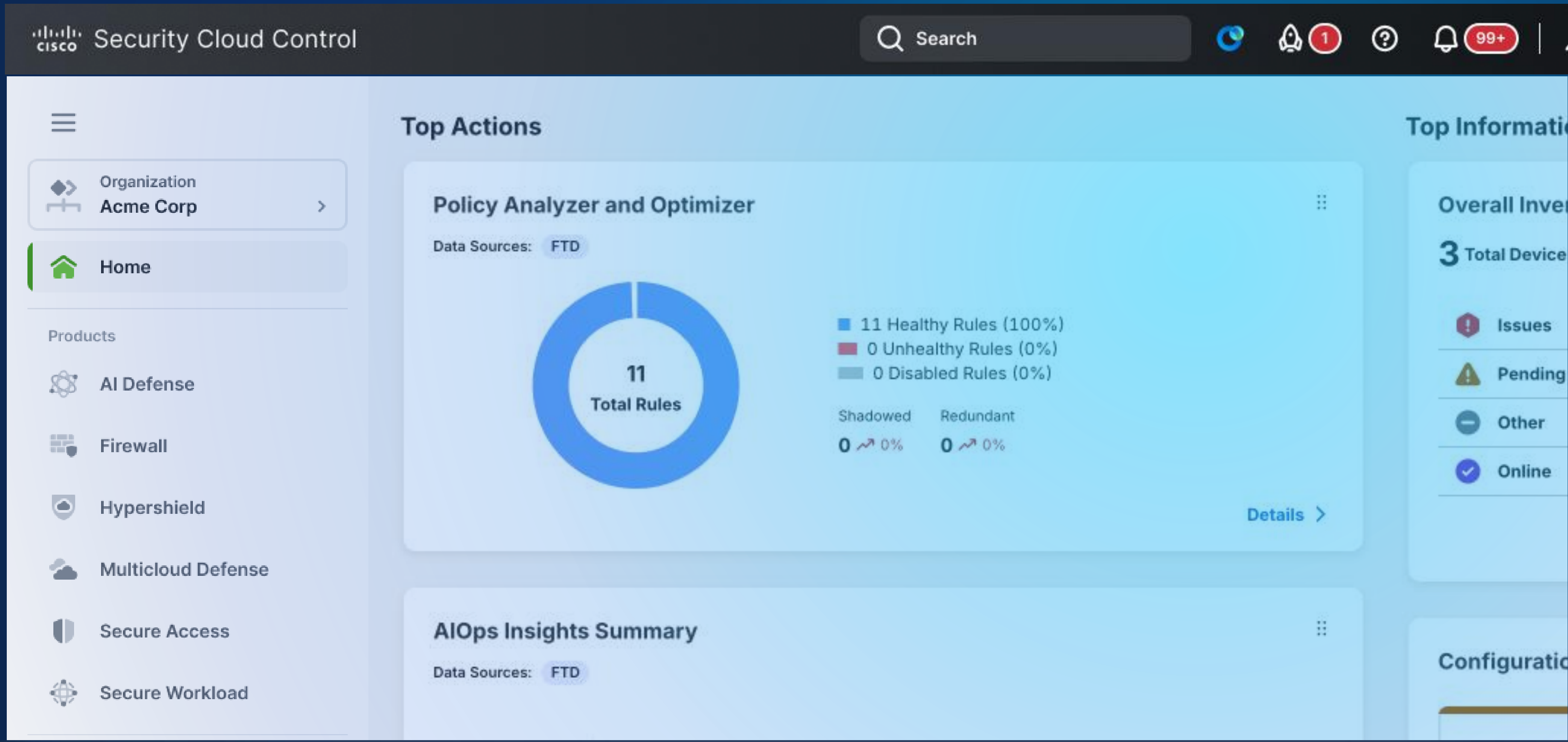
Secure Workload

Flexibility to swap components

Some capabilities are planned but not yet available or guaranteed.

Security Cloud Control

Simplify policy administration by up to 70%



Security Cloud Control

Search

Organization
Acme Corp

Home

Products

AI Defense

Firewall

Hypershield

Multicloud Defense

Secure Access

Secure Workload

Top Actions

Policy Analyzer and Optimizer

Data Sources: FTD

11
Total Rules

11 Healthy Rules (100%)
0 Unhealthy Rules (0%)
0 Disabled Rules (0%)

Shadowed 0 0%
Redundant 0 0%

Details

AIOps Insights Summary

Data Sources: FTD

Top Informati

Overall Inve

3 Total Device

Issues

Pending

Other

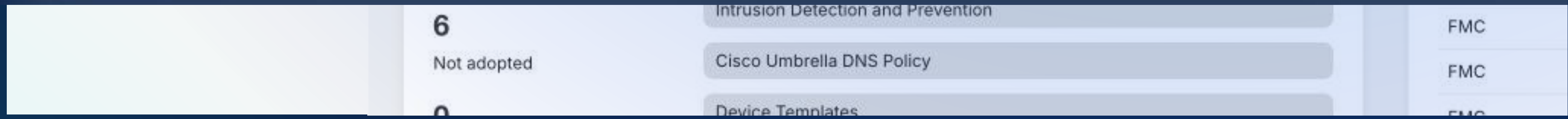
Online

Configuratio

AI assistance for policy

Proactive AIOps

Real world policy testing



6
Not adopted

Intrusion Detection and Prevention

Cisco Umbrella DNS Policy

Device Templates

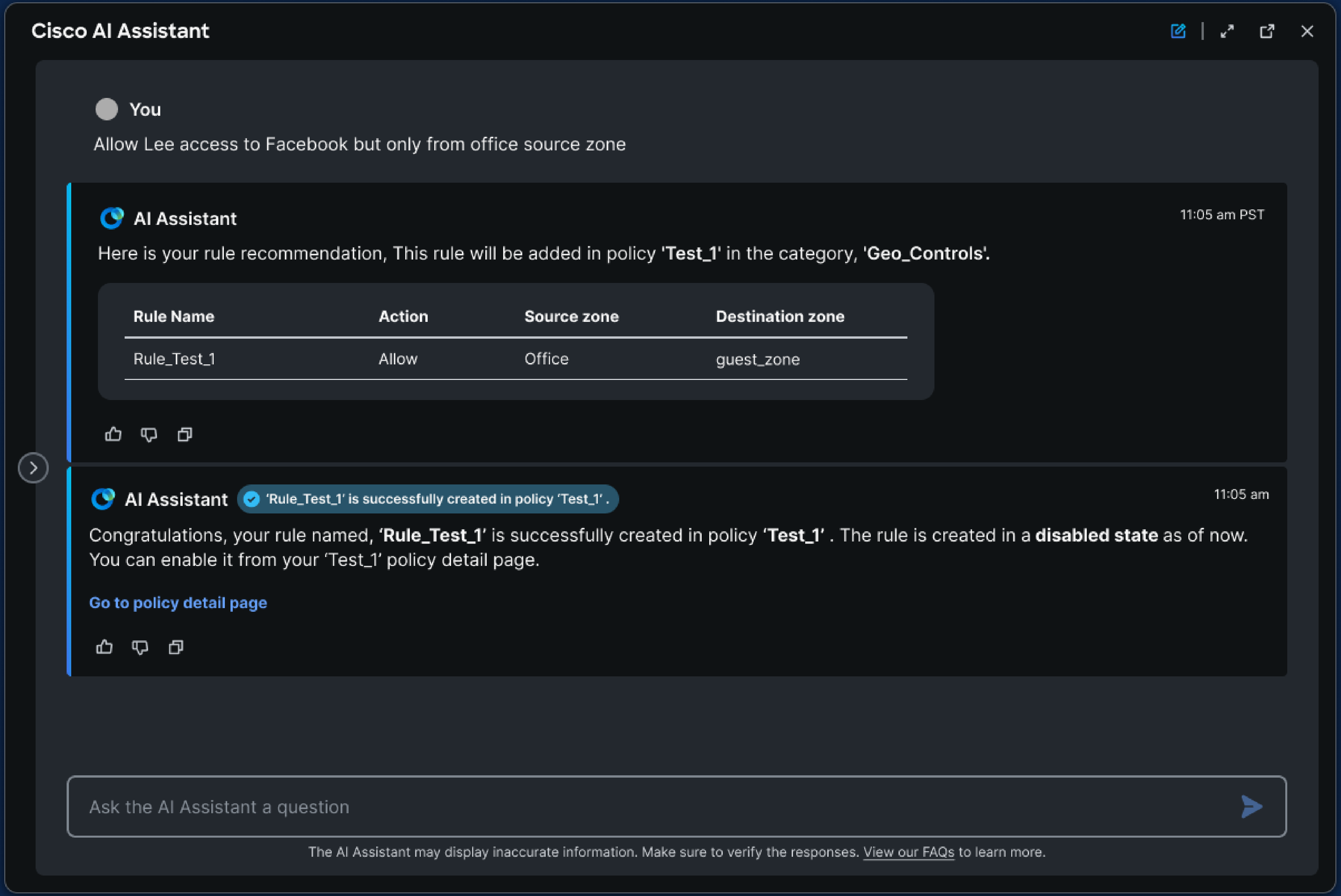
FMC

FMC

70% data source from Cisco customer conversations
Some capabilities are future.

Reduce management overhead with AI Assistant

Assist	+ Policy configuration
Augment	+ Troubleshooting
Automate	+ Policy lifecycle management



Cisco AI Assistant

You

Allow Lee access to Facebook but only from office source zone

AI Assistant 11:05 am PST

Here is your rule recommendation, This rule will be added in policy **'Test_1'** in the category, **'Geo_Controls'**.

Rule Name	Action	Source zone	Destination zone
Rule_Test_1	Allow	Office	guest_zone

AI Assistant 'Rule_Test_1' is successfully created in policy 'Test_1' . 11:05 am

Congratulations, your rule named, **'Rule_Test_1'** is successfully created in policy **'Test_1'** . The rule is created in a **disabled state** as of now. You can enable it from your 'Test_1' policy detail page.

Go to policy detail page

Ask the AI Assistant a question

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

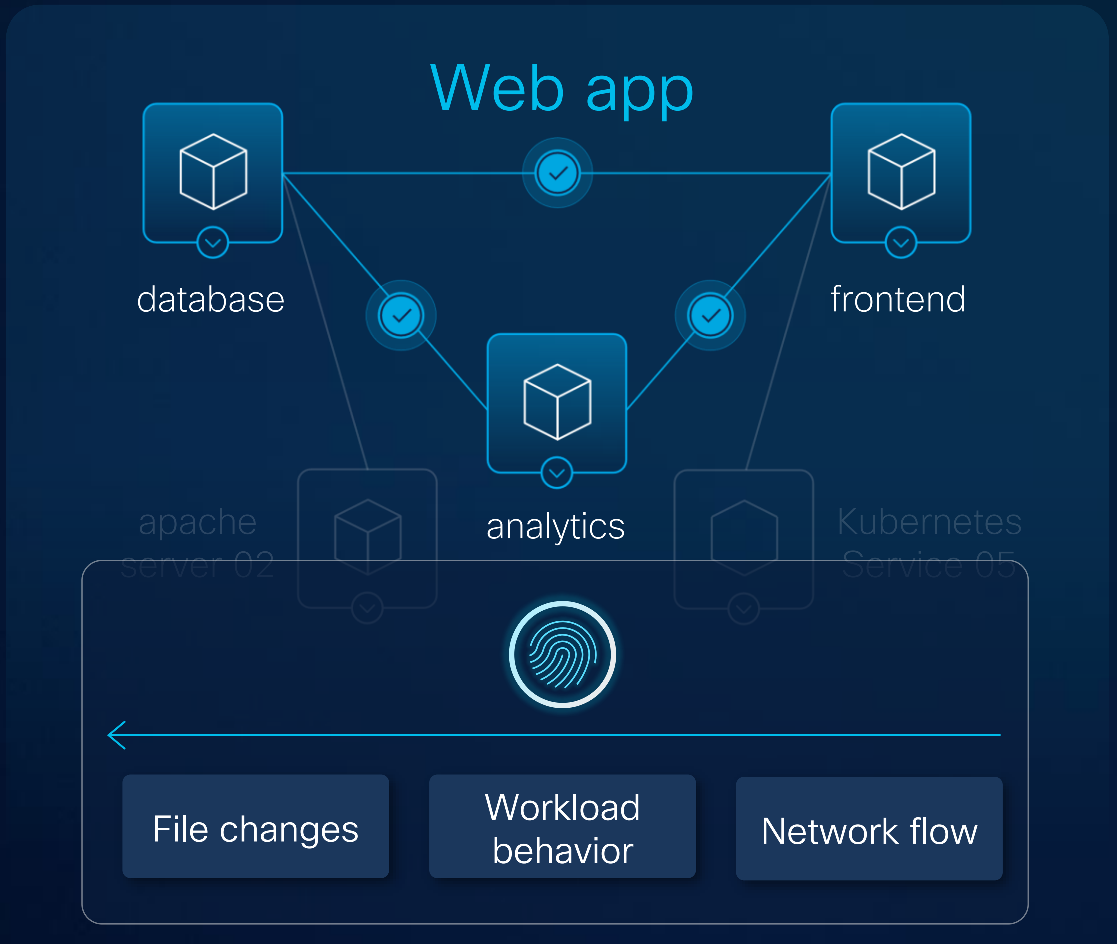
Hypershield: AI-native segmentation that works at scale

Manual

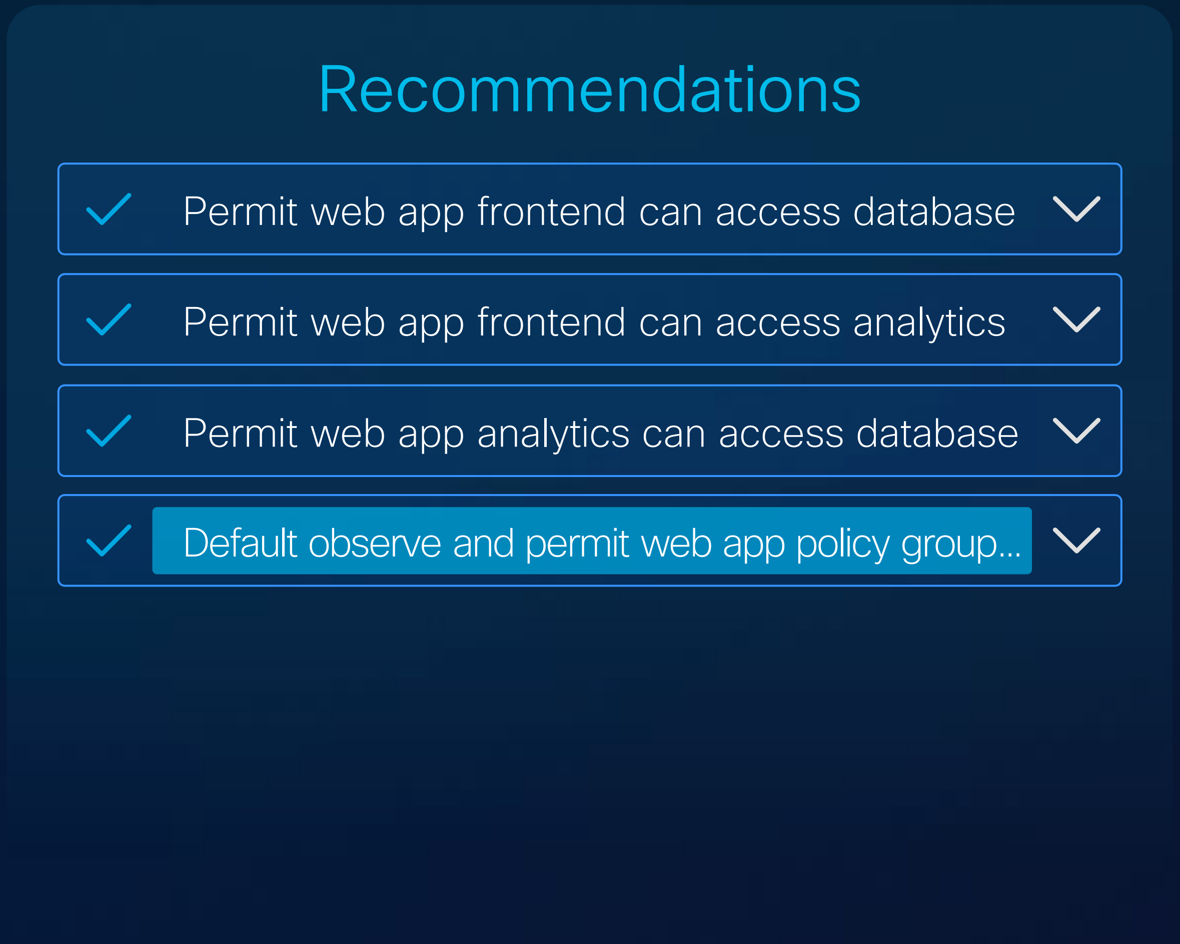
Autonomous

Autonomous segmentation

FUTURE



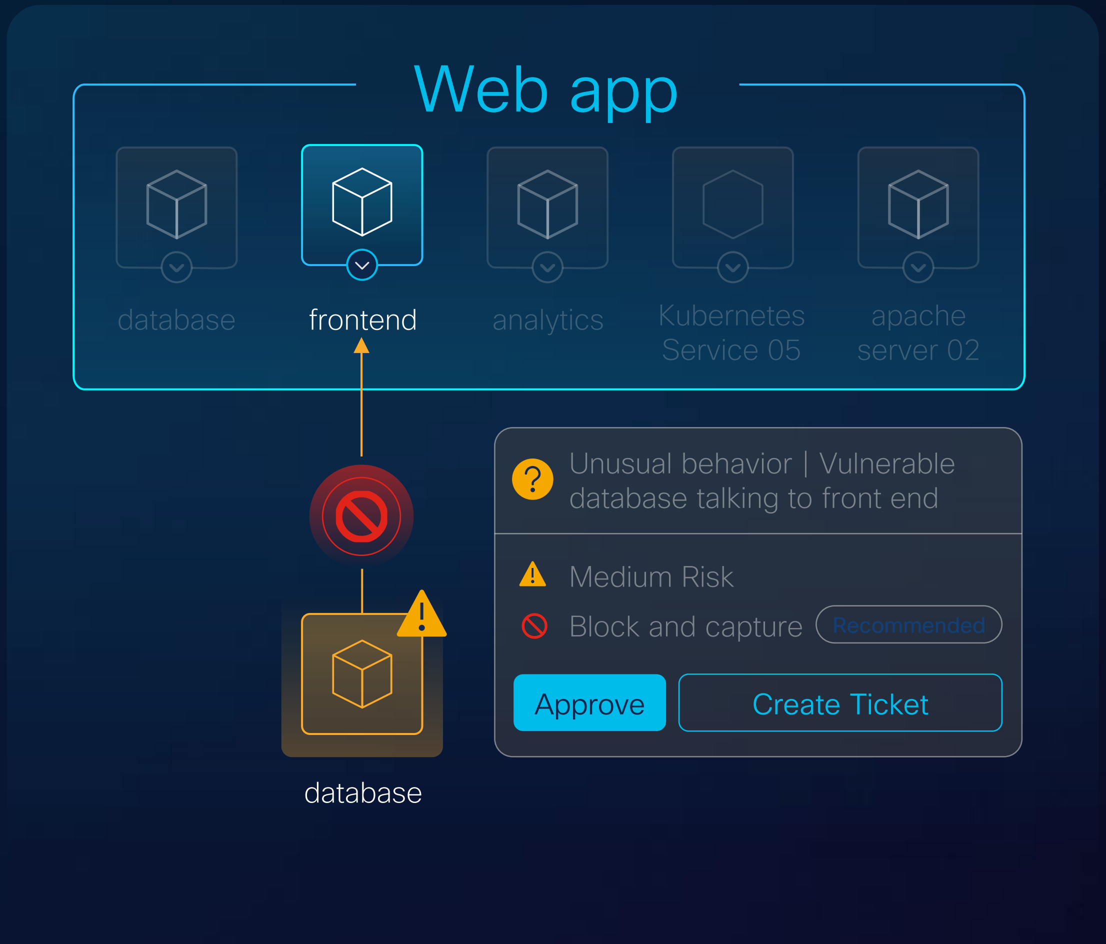
Complete understanding of changing app behavior from network to workload to pre-prod



Recommendations

- ✓ Permit web app frontend can access database
- ✓ Permit web app frontend can access analytics
- ✓ Permit web app analytics can access database
- ✓ Default observe and permit web app policy group...

Flexible segmentation rules that help avoid app fragility



Unusual behavior | Vulnerable database talking to front end

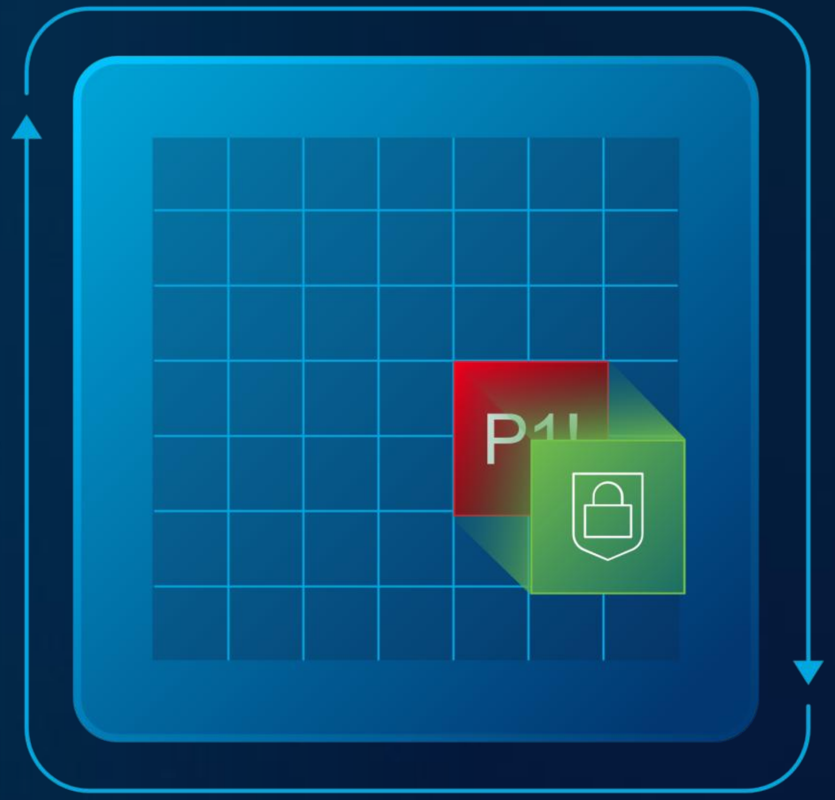
Medium Risk

Block and capture Recommended

Approve | Create Ticket

Policies updated to stricter rules in response to suspicious events

Defender’s dilemma



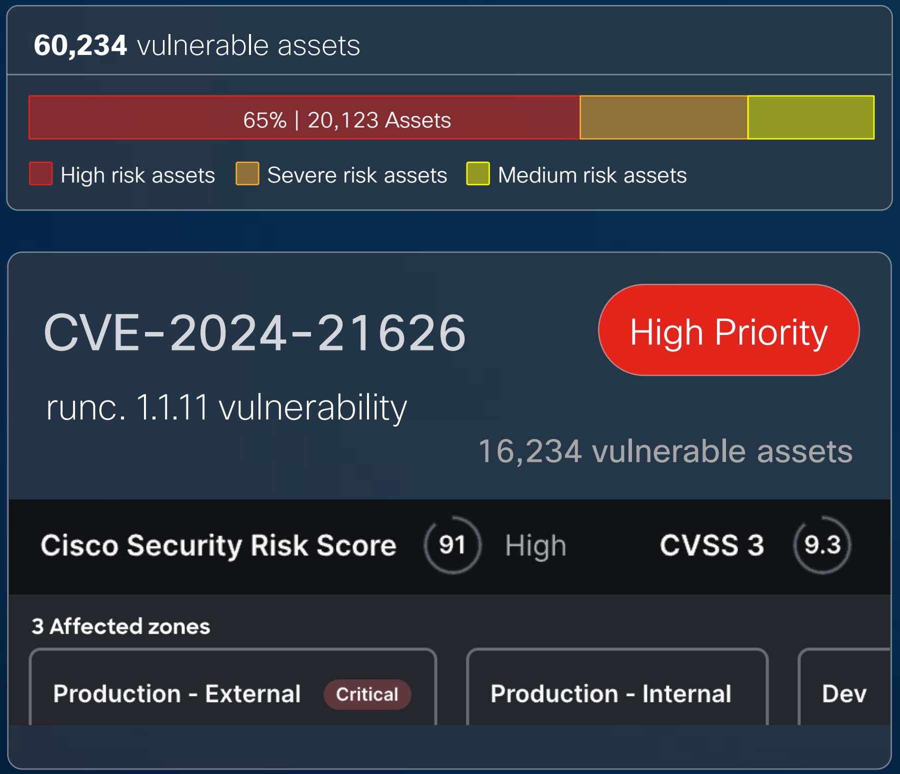
Mitigate known and unknown vulnerabilities

Do it in minutes, not months

All while keeping the app and business running

Closing the exploit gap with automated workflows

FUTURE



60,234 vulnerable assets

65% | 20,123 Assets

🟥 High risk assets 🟧 Severe risk assets 🟨 Medium risk assets

CVE-2024-21626

High Priority

runc. 1.1.11 vulnerability

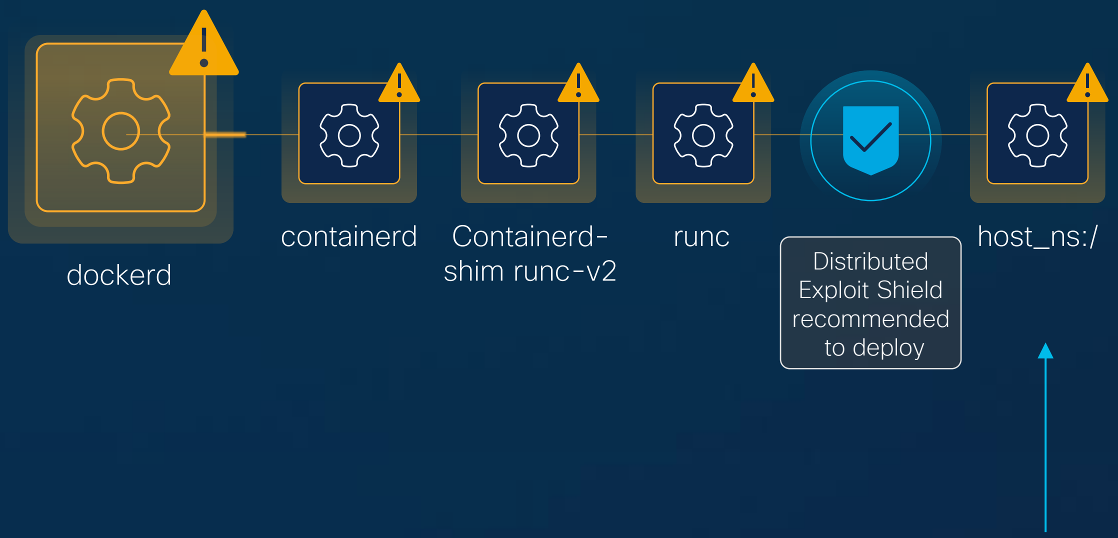
16,234 vulnerable assets

Cisco Security Risk Score 91 High **CVSS 3** 9.3

3 Affected zones

Production - External Critical | **Production - Internal** | **Dev**

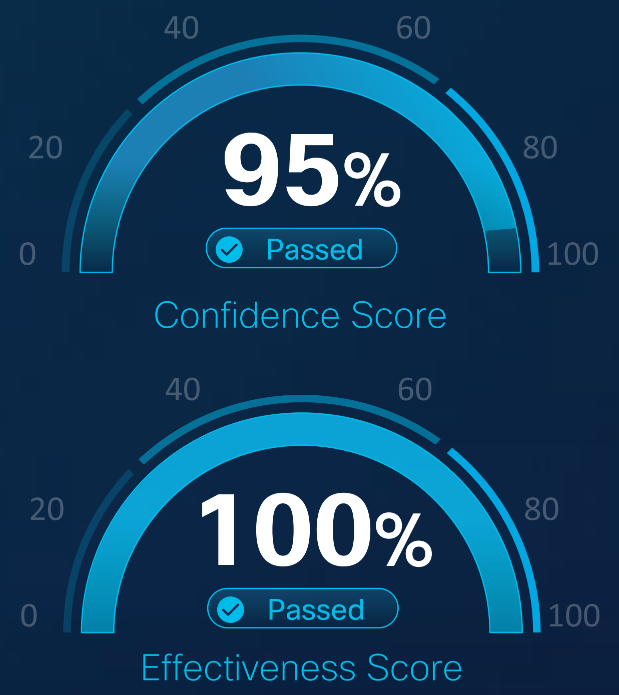
Data-driven vulnerability prioritization
+19 threat and exploit intel feeds
+12.7B managed vulnerabilities
+1B security events processed monthly



✓ The Distributed Exploit Shield blocks new container processes with a current directory of ”/” in the host name space.

⊘ Block and alert

Surgical mitigating control
that keeps application running

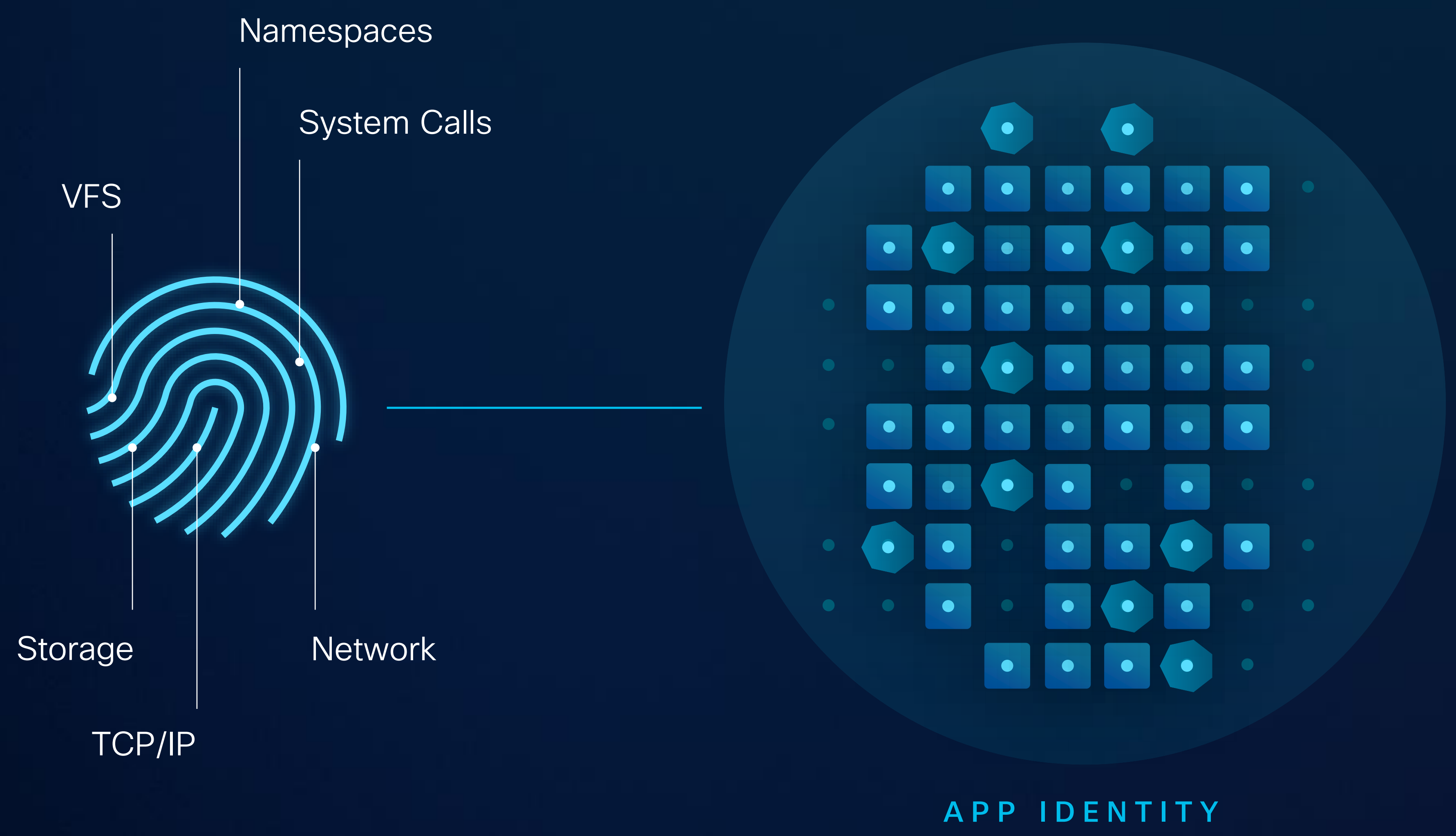


✓ The Distributed Exploit Shield was already tested in your environment

Tested against live production
traffic to earn trust and
increase confidence

Proactive defense with unknown vulnerability protection

FUTURE



VALIDATED

/var/www → dir traversal → httpd → file read → /etc/apache2/httpd_conf

SUSPICIOUS

CWE-78
OS command injection

CWE-200
Unauthorized access to sensitive information

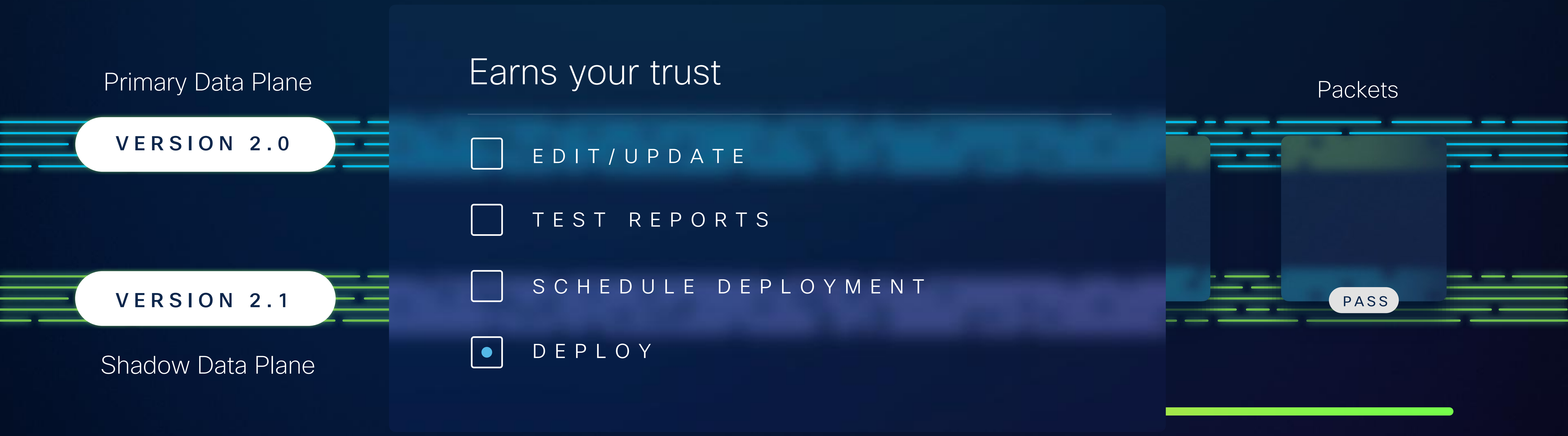
MALICIOUS

Web shell payload → Saved in PHP dir → Execute web shell

Application-specific behavior analysis | Common weakness enumeration and analysis

Digital Twin: Upgrades

FUTURE



Earns your trust

□ EDIT/UPDATE

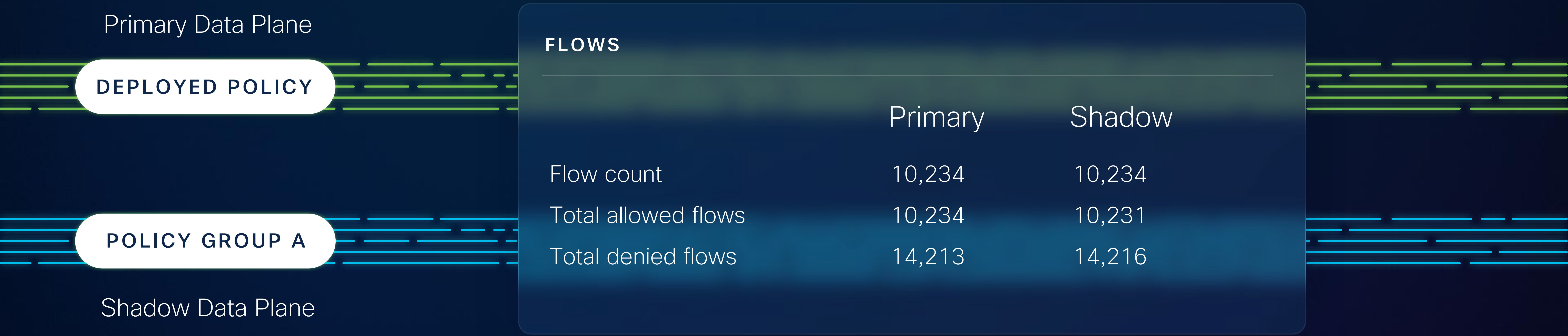
□ TEST REPORTS

□ SCHEDULE DEPLOYMENT

▣ DEPLOY

Digital Twin: Policy verification

FUTURE



FLOWS

	Primary	Shadow
Flow count	10,234	10,234
Total allowed flows	10,234	10,231
Total denied flows	14,213	14,216

Q&A

Contatti: lpomelli@cisco.com, https://www.linkedin.com/in/lpomelli/
averri@cisco.com, www.linkedin.com/in/averri-theoriginal