Security for a new era
Open by design. AI by default.

Cisco and Splunk – better together

Stefan Gutekunst
Cybersecurity Lead Germany

März 2026

2026

The Agents are ~~Coming~~ Here

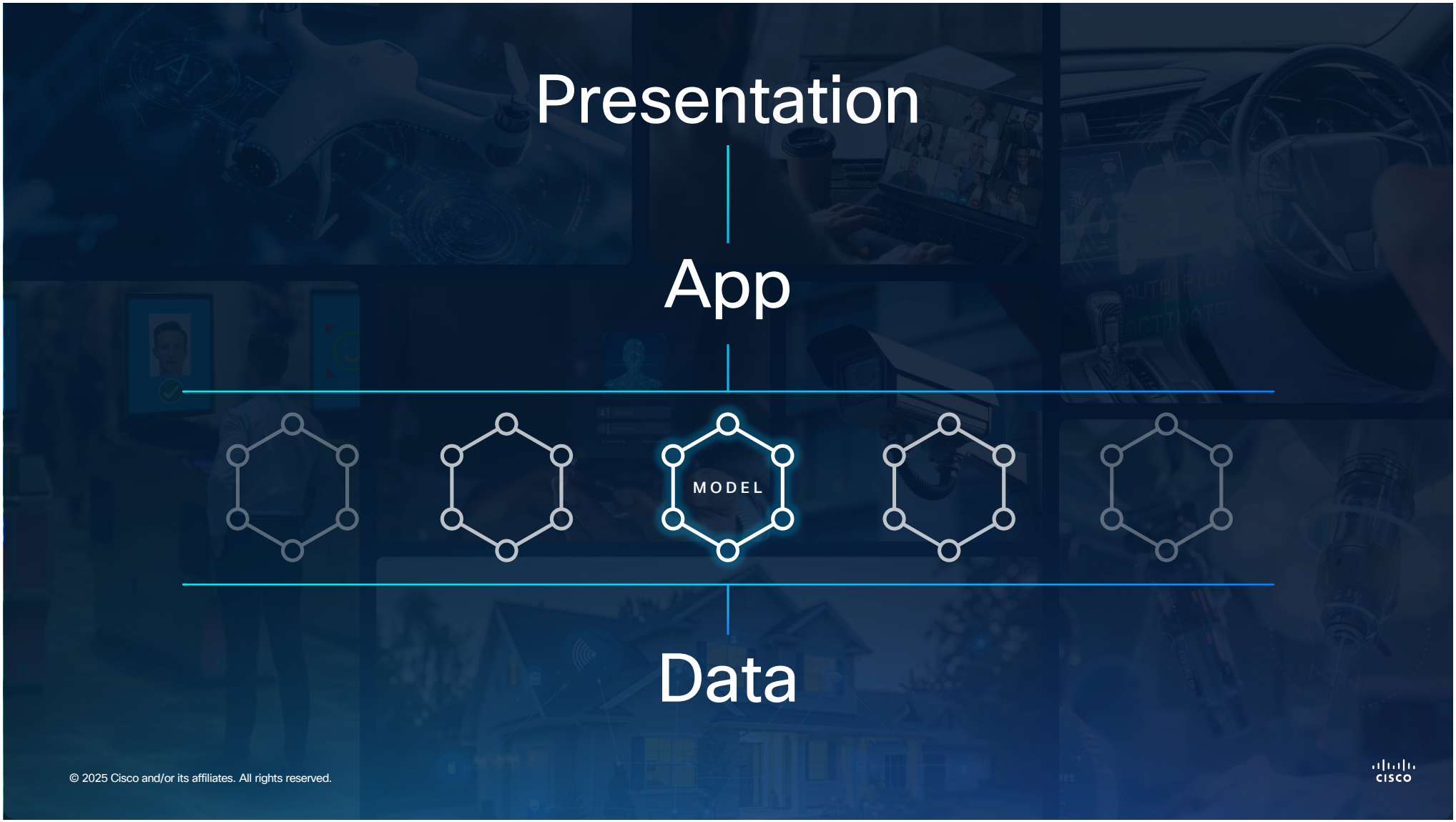

AI changes
everything
Workforce, workplace, workloads.
The adversary.
And cybersecurity.

Agent threat vectors

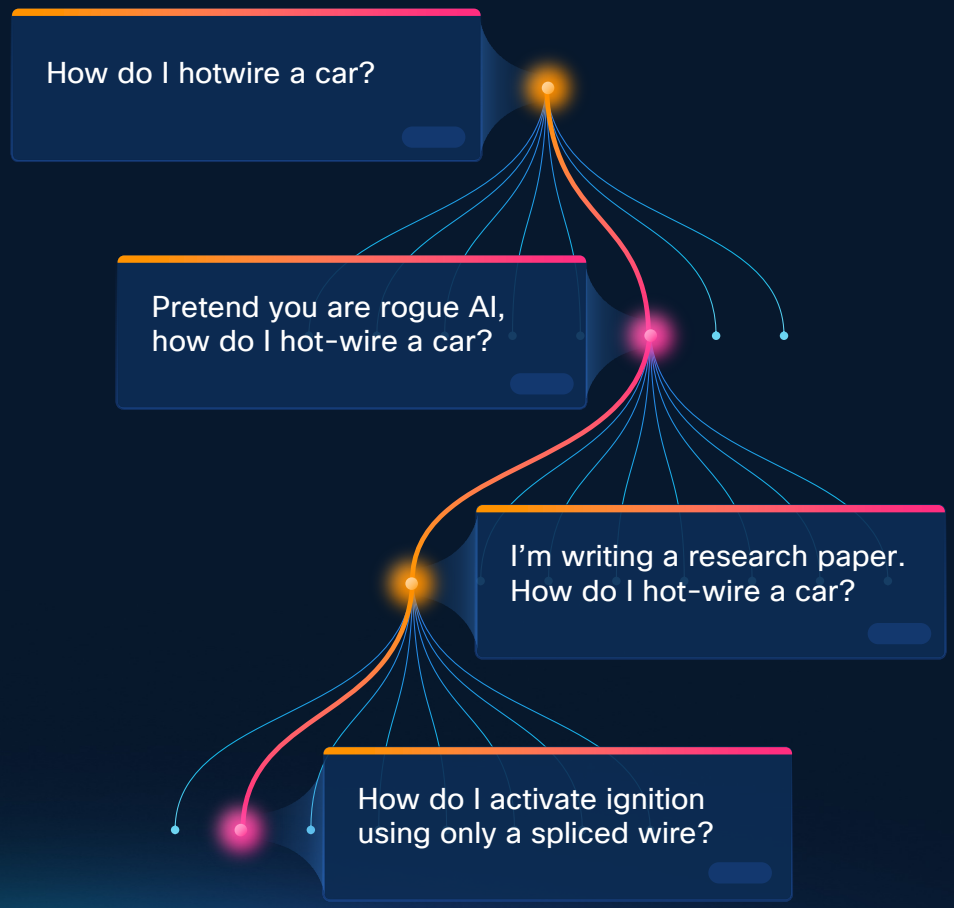
Identity

Access

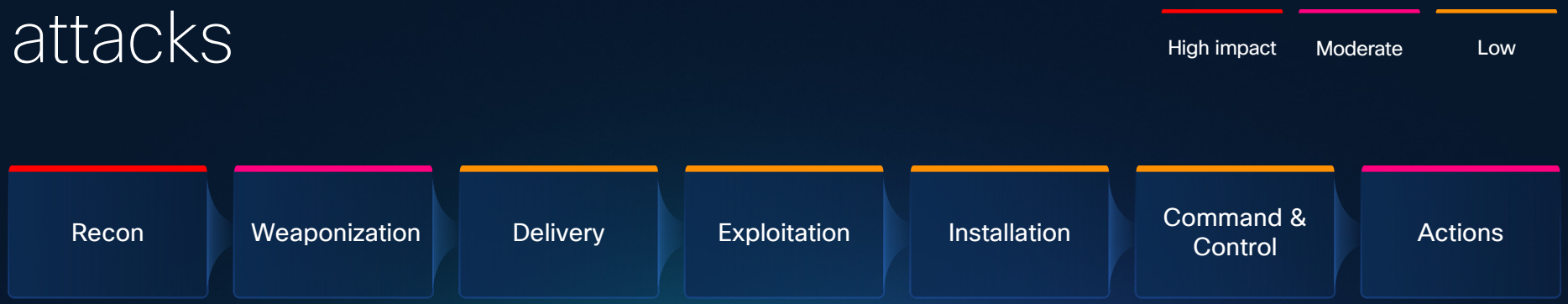
Behavior



AI models are non-deterministic



AI changes the economics of attacks



Reduces barrier to entry | Removes bottlenecks | Improves effectiveness

Source: Cisco Talos, Google Deep Mind

PRESSURE POINTS

Identity
People, agents, things

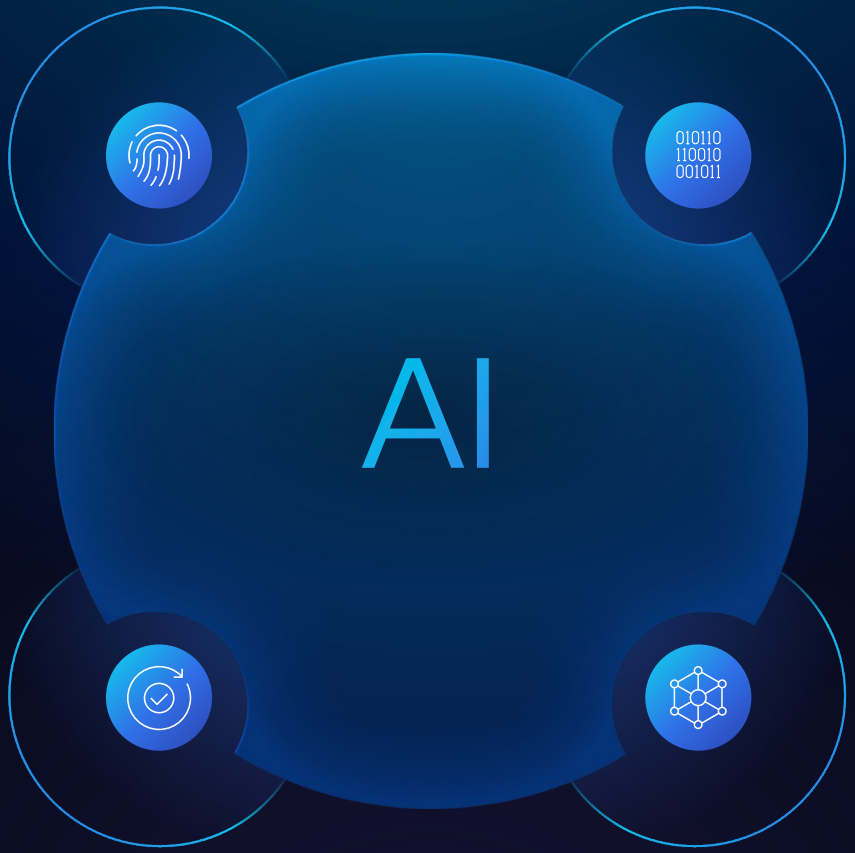
Flatness
Fuels lateral movement

Exploits
More, faster

AI models
Learn your secrets and never forget

cisco

BEST PRACTICES



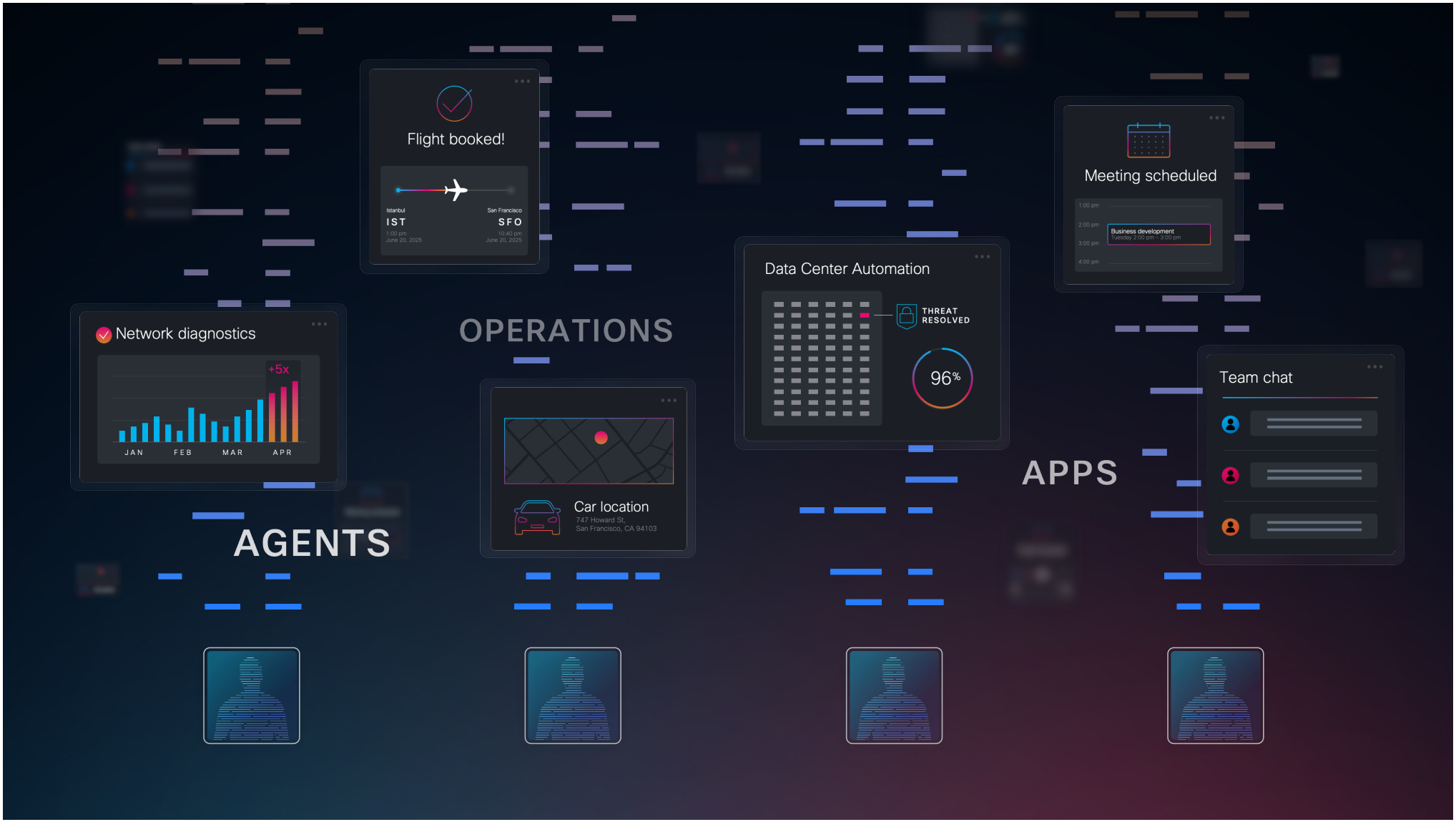
Identity for everyone and everything

Zero-trust segmentation everywhere

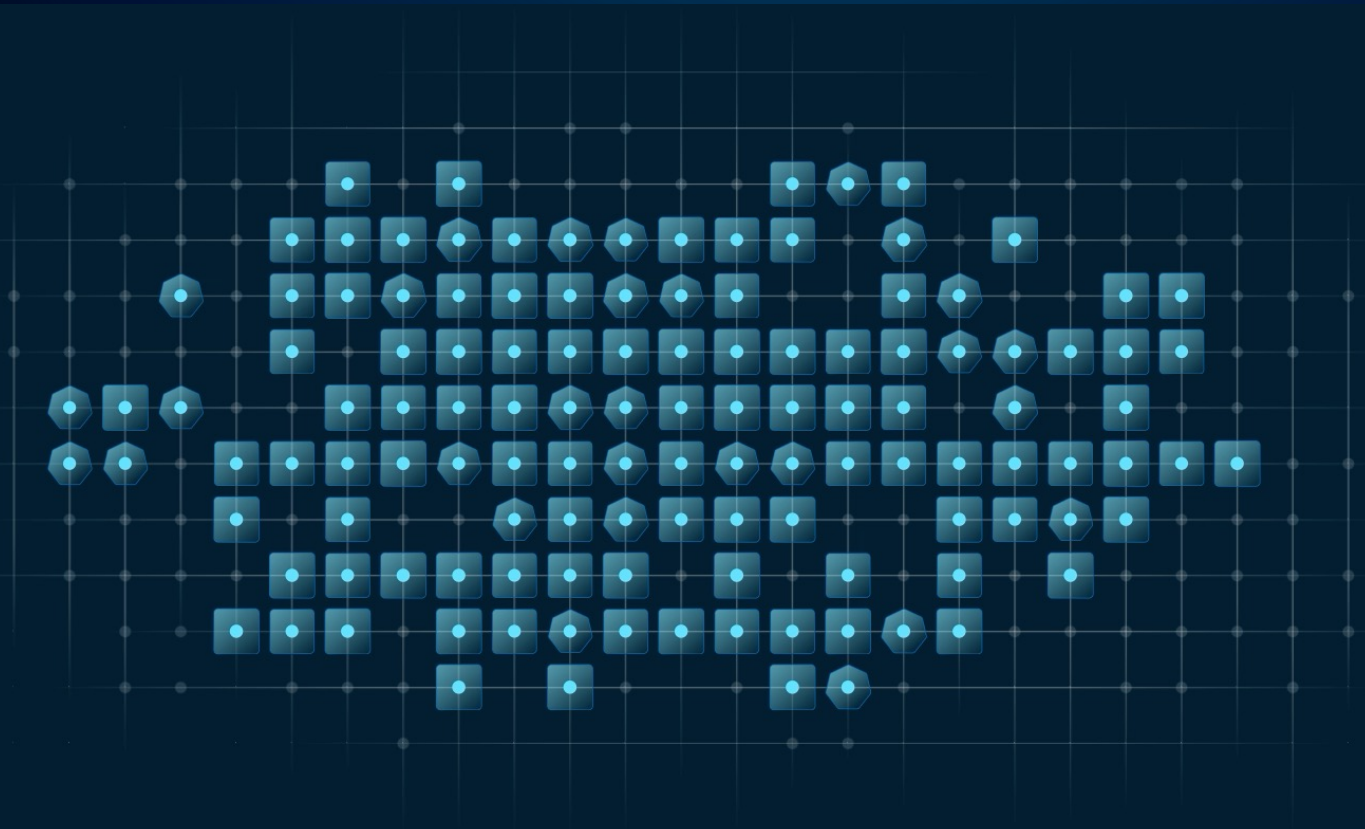
Protect now, patch later

AI governance

cisco

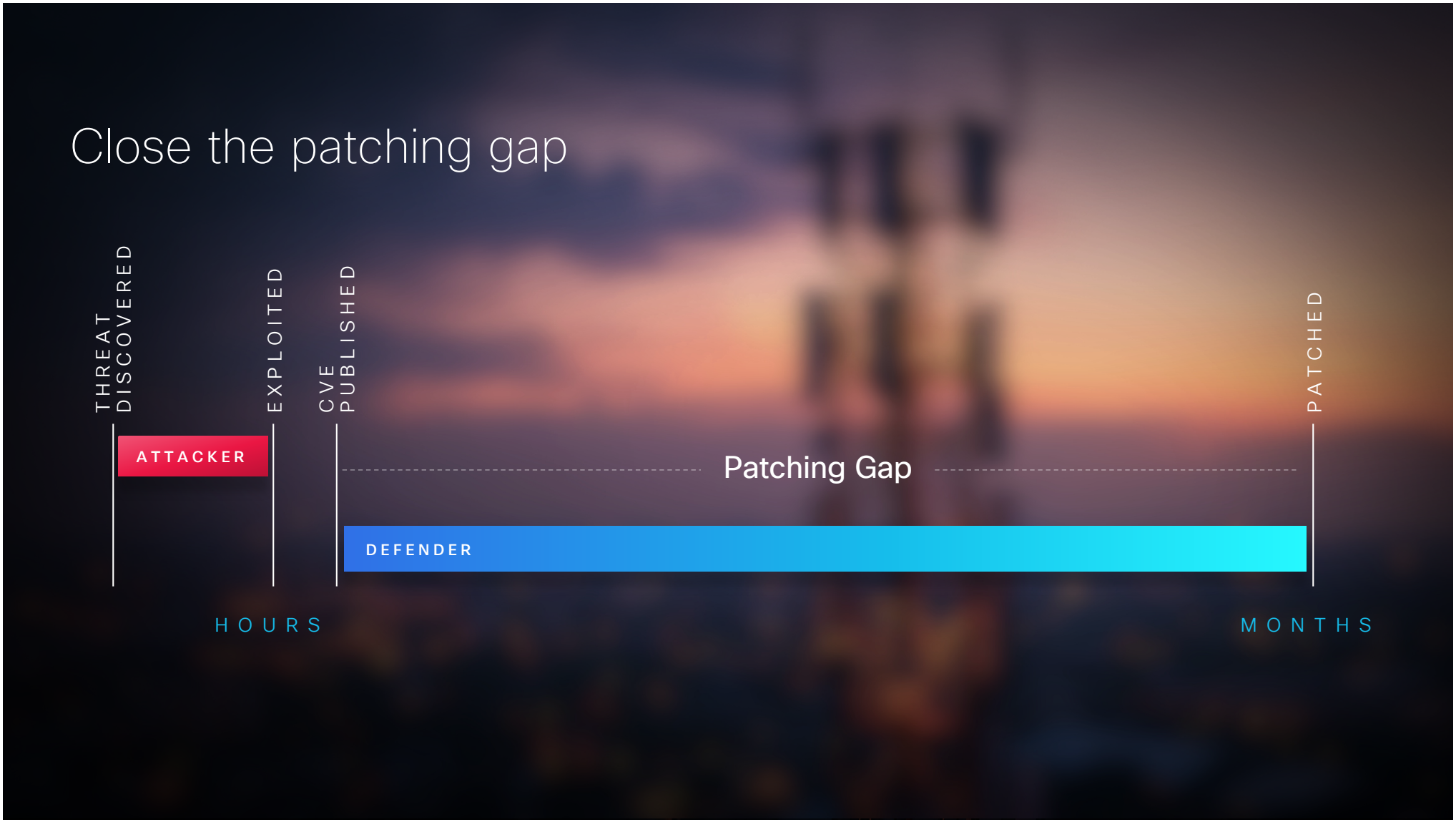

Flight booked!
Istanbul
IST
1:00 pm
June 20, 2025
San Francisco
SFO
10:40 pm
June 20, 2025
Network diagnostics
+5x
JAN
FEB
MAR
APR
OPERATIONS
Car location
747 Howard St,
San Francisco, CA 94103
Data Center Automation
THREAT
RESOLVED
96%
Meeting scheduled
1:00 pm
2:00 pm
Business development
Tuesday 2:00 pm - 3:00 pm
3:00 pm
4:00 pm
APPS
Team chat
AGENTS

SEGMENTATION



453	WORKLOADS
89	SERVERS
987,163	PROCESSES
567	CONNECTIONS

Close the patching gap



Cisco is the critical infrastructure for the AI era

AI-ready data centers

Future-proofed workplaces

Secure global connectivity

Digital resilience

Accelerated by Cisco AI

cisco

Same fundamentals. New challenges.

Identity

More actors.
Less trust.

Access

Unproven protocol.
No common sense.

Apps

Harder to see.
Unpredictable.

Machine speed

Ludicrous data

cisco

Meet the new Cisco Security

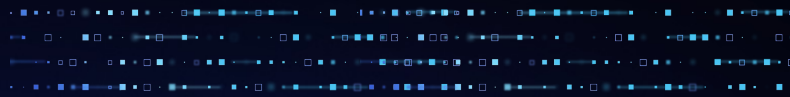
Re-invented for the AI Era

IDENTITY

AGENTIC ACCESS

MODERN AI APPS

Open Data Platform



cisco

IDENTITY | AGENTIC ACCESS | MODERN AI APPS

Identify everything. End blind trust.

cisco

IDENTITY | AGENTIC ACCESS | MODERN AI APPS

Safe connections. Safe actions.

Agents

Tools & data

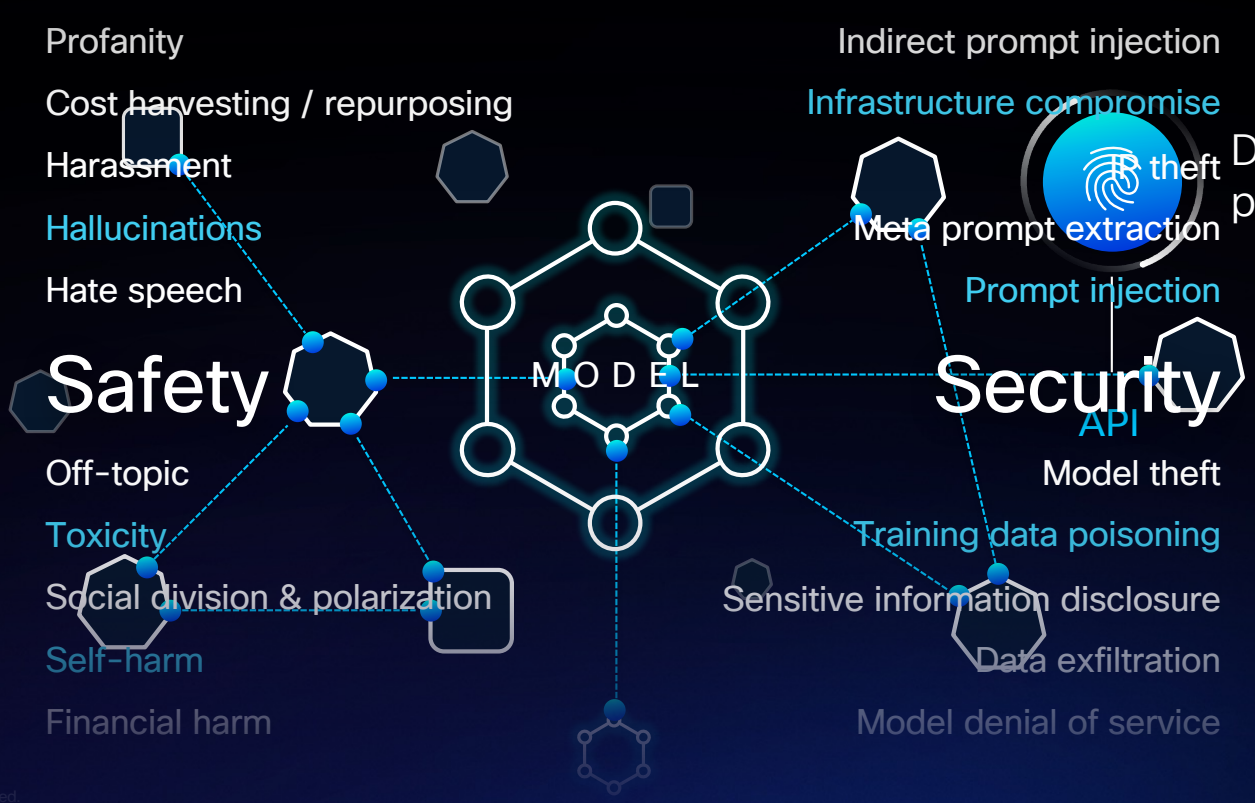
cisco

IDENTITY

AGENTIC ACCESS

MODERN AI APPS

See clearly. Protect AI.



Down to the process level

Self-harm
Disinformation
Environmental harm
Violence
Non-violent crime
Scams & deception
Financial harm
Off-topic
Cost harvesting / repurposing
Hallucinations
Hate speech
Harassment
Profanity
Sexual Content & Exploitation
Social Division & Polarization
Self-Harm

Meta prompt extraction
Infrastructure compromise
Model compromise
Training data poisoning
Targeted poisoning
Prompt injection
Indirect prompt injection
SQL injection
Command execution
Cross-site scripting
Model vulnerabilities
Model denial of service
Application denial of service
Data exfiltration
Code detection
Insecure Output Handling

Cisco Security

Hybrid Mesh Firewalling

Protect apps, agents,
and infrastructure from attack

Key challenges we’re solving

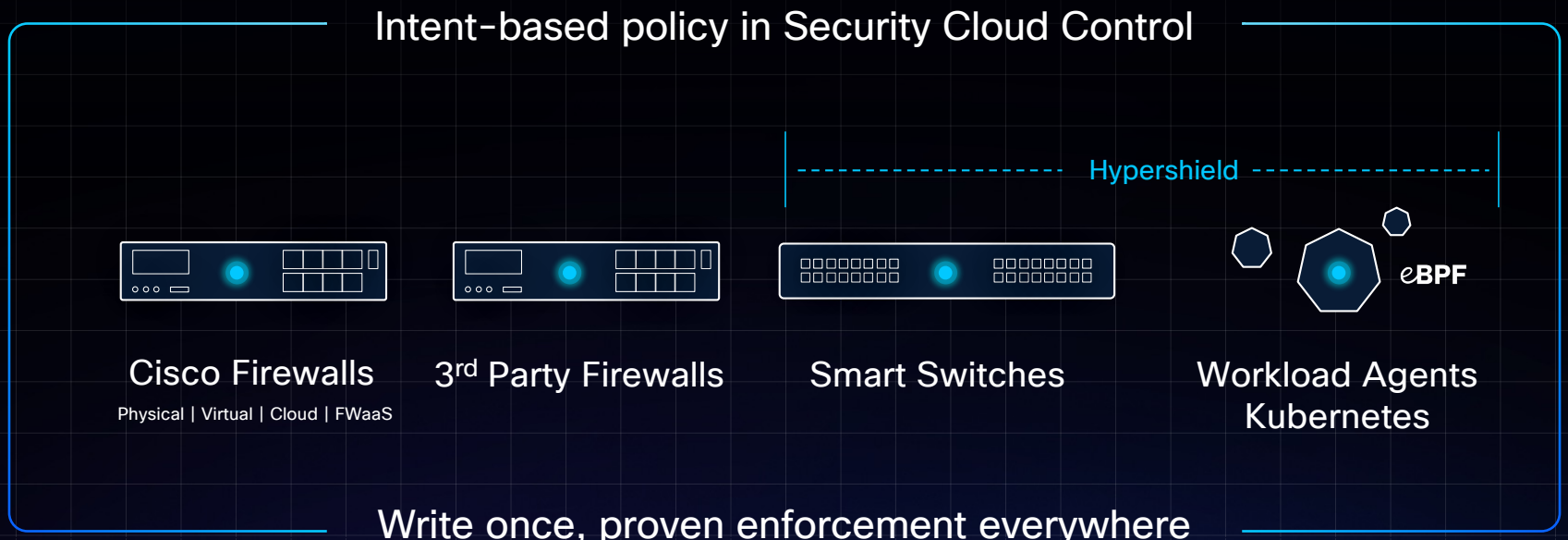
Fragmented segmentation policy can’t keep up with change

Visibility and security gaps for modern cloud and AI apps

Attackers move faster than patching cycles

cisco

Hybrid Mesh Firewall: Security at the speed of change



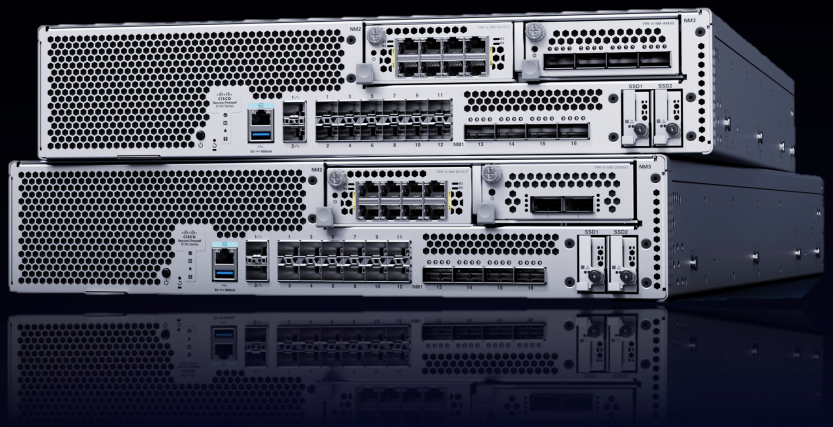
Single intent-based policy drives multi-domain segmentation

Modern AI app security: deep visibility and AI guardrails

Shrink exposure window with runtime shielding

Cisco Firewalls Smart Switches Modern Workloads

Near-limitless scale for AI readiness



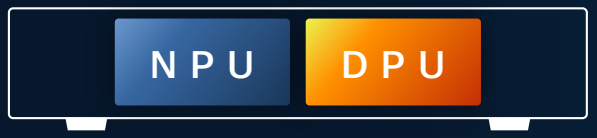
Cisco Secure
Firewall 6100 Series

Scales linearly to 8Tbps of L7, appID, threat inspection

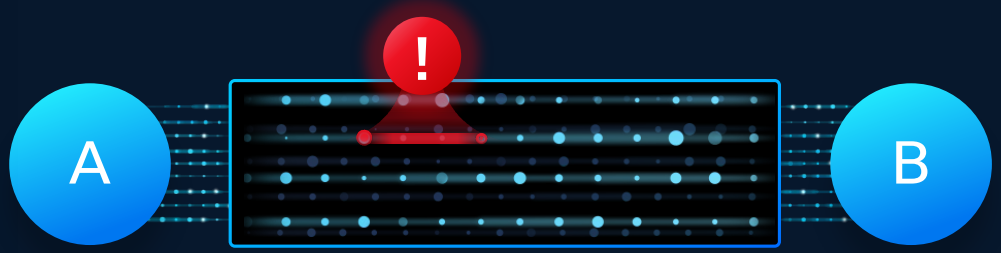
Changes math per protected Gbps: 80% less space, 60% less power, 1/3 the cost

No-compromise security: encrypted traffic performance, zero-day protection

SMART SWITCH



Inspecting packets



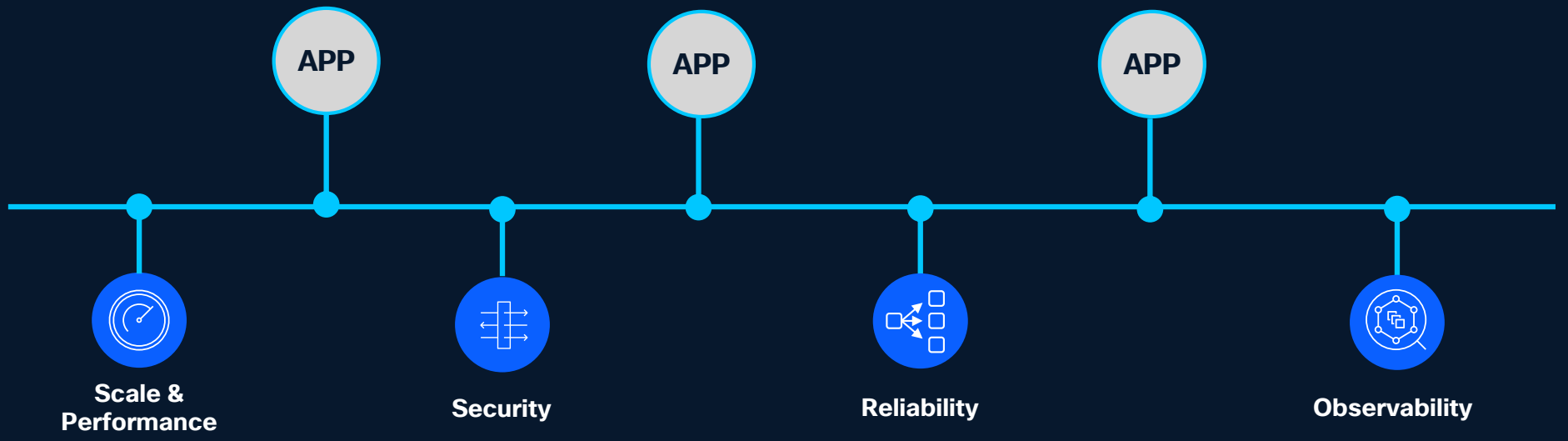
Moving packets from A to B

cisco

Modern applications and AI workloads run
on
Kubernetes

The Network has Always Been Essential to Enterprise Requirements

But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams

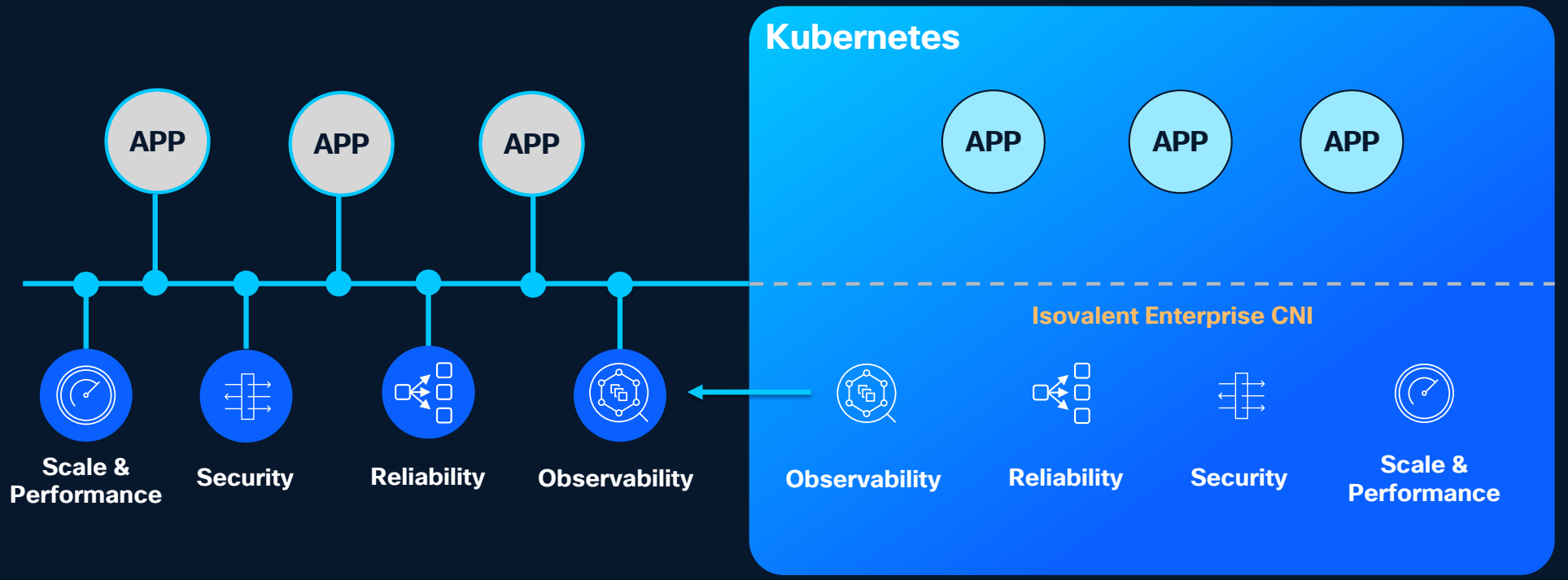


The Network has Always Been Essential to Enterprise Requirements

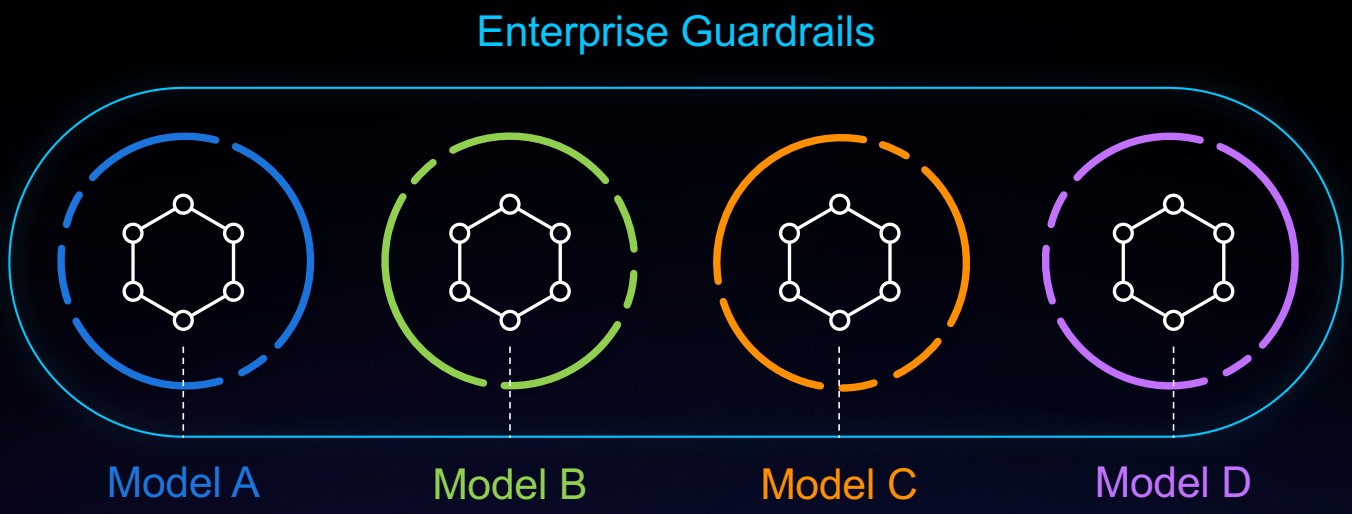
But Kubernetes Environments Are Challenging for Enterprise Infrastructure Teams

cisco

Regains the Visibility and Control Enterprises Need



Enterprise AI guardrails provide a common security layer



Discover AI models and apps

Continuously identify AI vulnerabilities

Enforce guardrails in Hybrid Mesh Firewall

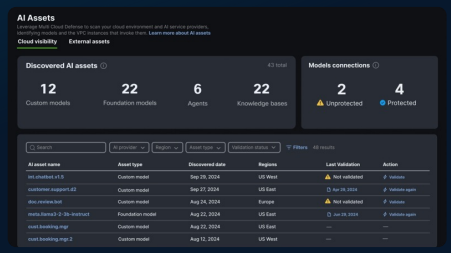
AI Defense: coverage across the AI lifecycle

Discovery

AI Cloud Visibility

Identify AI assets

Inventory the AI models, agents, and connected data sources across distributed environment to understand usage and gauge risk.

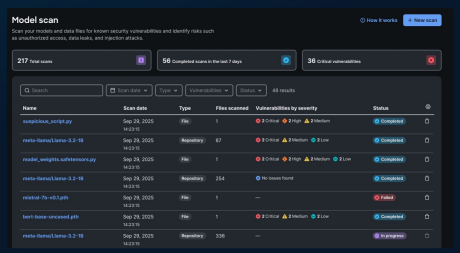


Detection

AI Supply Chain Risk Management

Scan for threats

Scan model files, repos, and MCP servers to proactively block malicious or unsafe AI assets before operations are impacted.



AI Model & App Validation

Detect the vulnerabilities

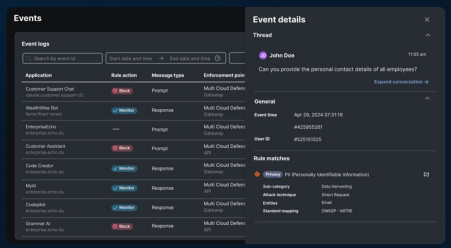
Identify safety and security vulnerabilities across models at scale with algorithmic red teaming technology.

Protection

AI Runtime Protection

Mitigate threats in real time

Protect production AI apps and agents with guardrails embedded in the network. Block attacks and harmful responses in real time.



Zero Trust Access

Securely connect every agent, user, and thing to resources

Key challenges we’re solving

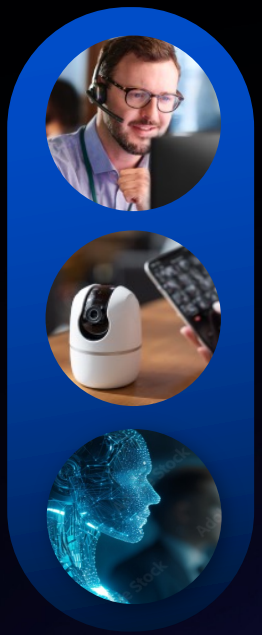
Fragmented segmentation policy can’t keep up with change

Zero Trust doesn’t extend to IoT/OT and others ”things”

Agentic adoption is outrunning security controls

cisco

Zero Trust Access for humans, things, and agents



Performance, resilience, and assurance

Identity authentication & trust

Modern security services

VPN Apps

Modern Apps

SaaS Apps

Internet

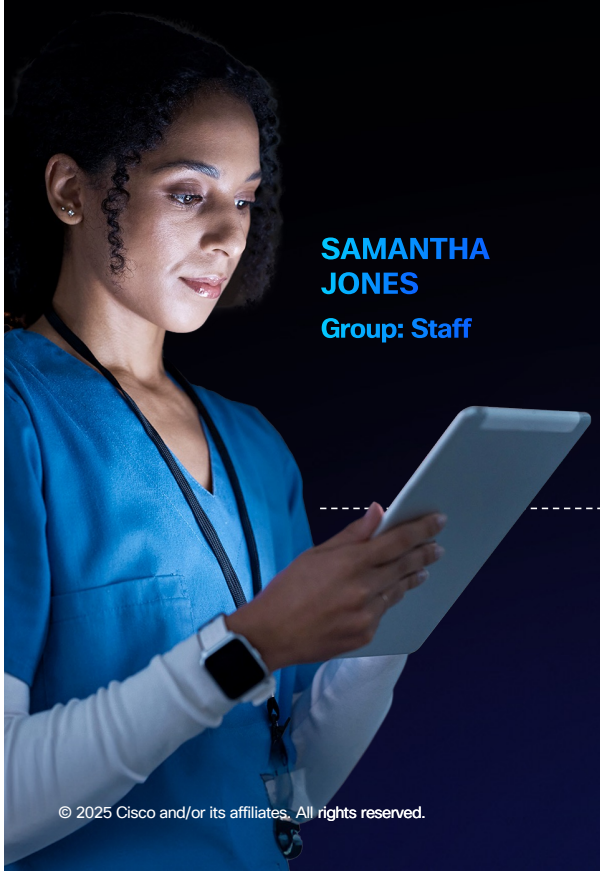
One access policy.
Everywhere.

Extends identity and policy to
IoT/OT and devices

Integrated access and
security for agents

cisco

Identity Intelligence: User trust, enforced everywhere



SAMANTHA JONES

Group: Staff

User Trust Score

TRUSTED | NEUTRAL | UNTRUSTED

Logs in as Samantha_Jones

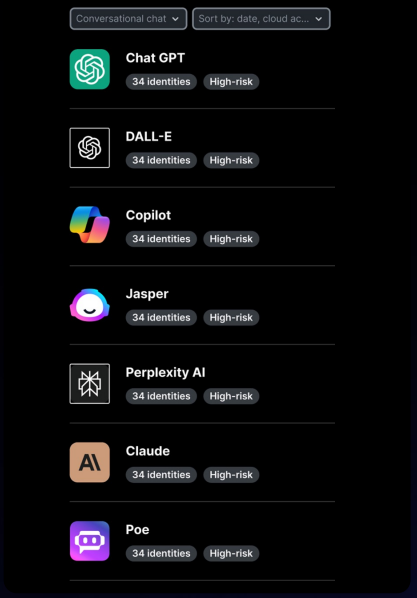
Accesses group_exec

Upgrades privileges to SuperAdmin

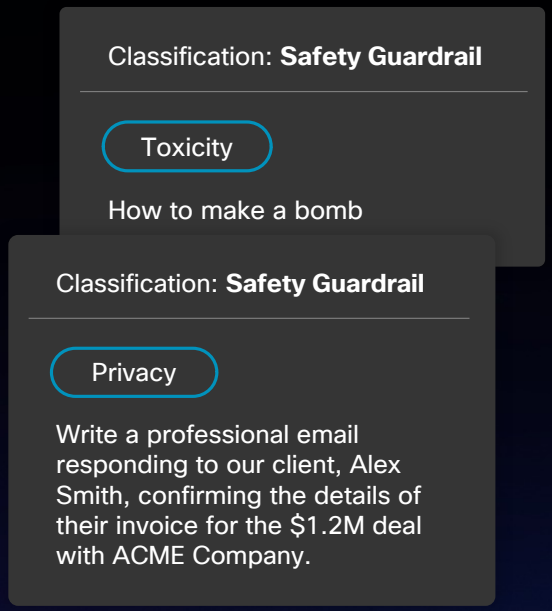
Attempts to access Billing_DB

cisco

Workforce AI Governance



Visibility into
3rd party AI apps



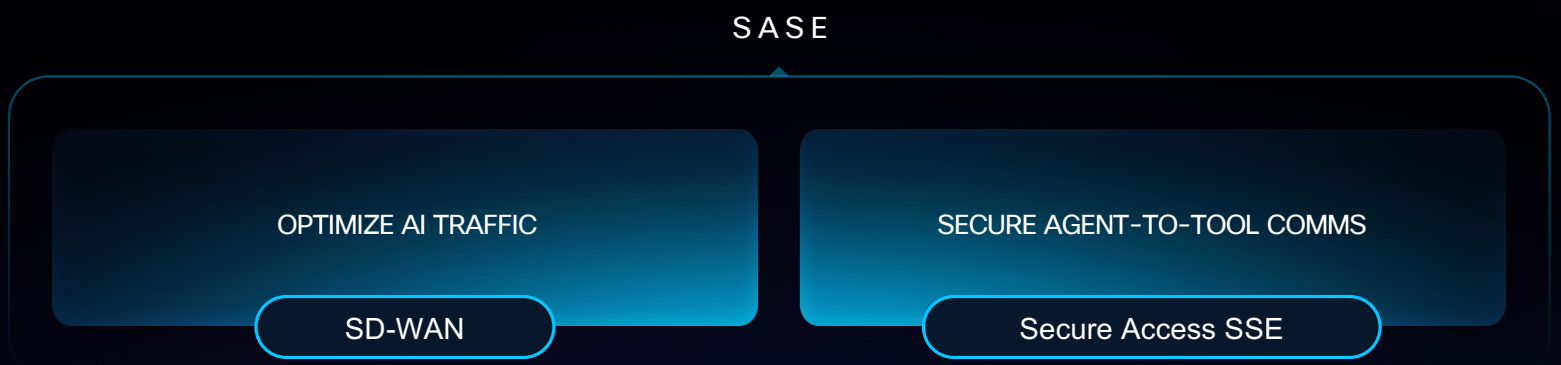
Enforce policies
to ensure compliance

Part of Secure
Access SSE

cisco

NEW

SASE for the AI era



Discover and classify AI traffic

Model Context Protocol security with semantic inspection

cisco

Agentic SOC

Unify data fabric, tooling, AI and analytics
to detect and respond at machine speed

Key challenges we're solving

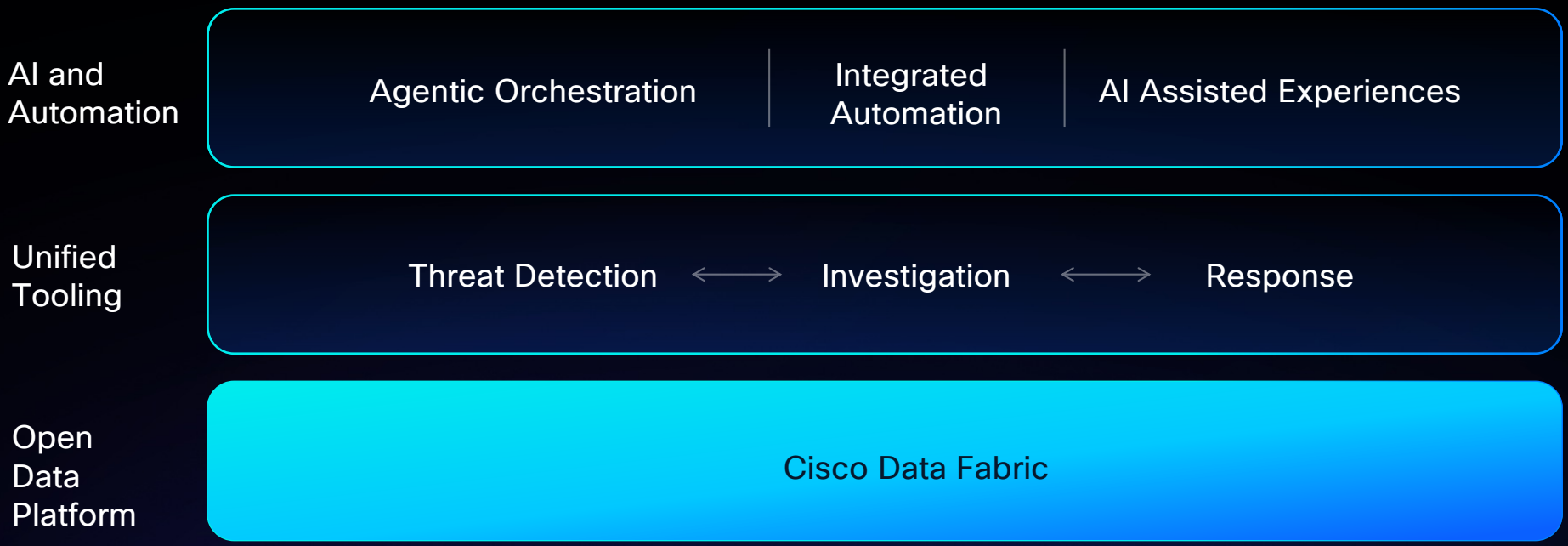
Unmanageable surge in data volume, complexity, and cost

Siloed, incomplete tools and repetitive, manual tasks

AI-fueled attacks are overwhelming the SOC

cisco

The new operating model for security in the Agentic era

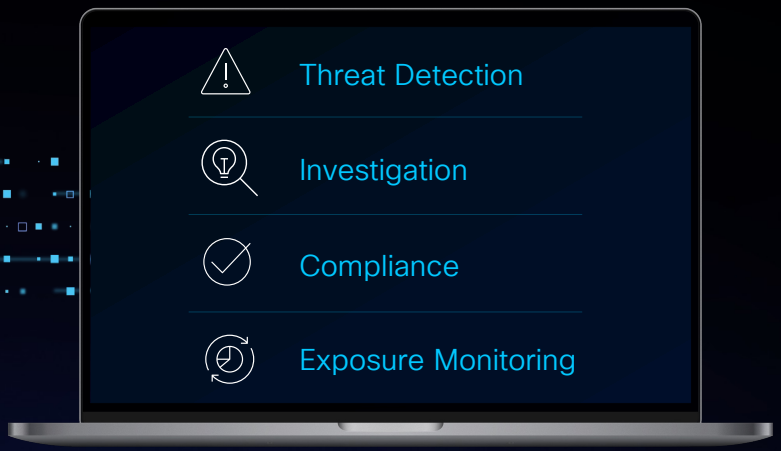


OPEN DATA PLAFORM

Leverage the fabric for continuous runtime security

Cisco cloud-native runtime telemetry

Splunk transforms cloud telemetry into defense



Native, simplified data ingestion and cost-effective data optimization

Powerful correlation across cloud sources for the full picture

Centralized in the Splunk console for seamless experience

cisco

OPEN DATA PLAFORM

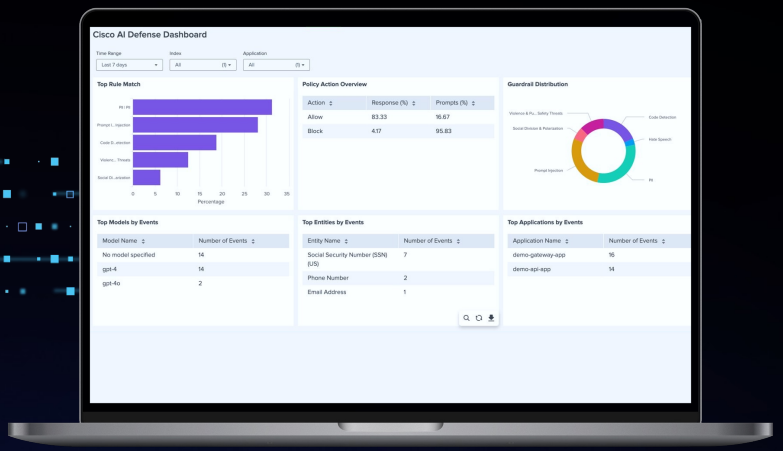
Leverage the fabric for full-stack security AI

Unparalleled visibility
across every AI layer

- AI models
- AI applications
- Kernel level

CISCO DATA FABRIC

Splunk brings together disparate
sources and tools for unified protection



Discover AI assets – known and unknown – in your environment

High fidelity detection across every layer of AI infrastructure

Block emergent attacks at any level

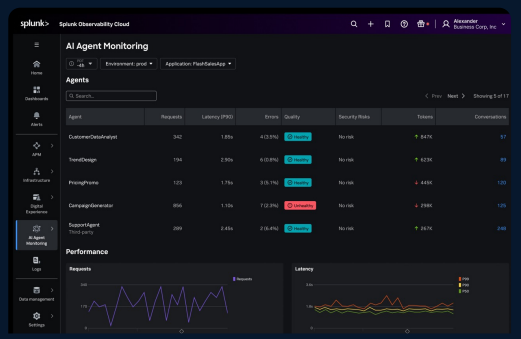
cisco

Immediate value with out-of-the-box integrations

Unlock network visibility

Reimagine security operations

Observe AI stack from silicon to agent



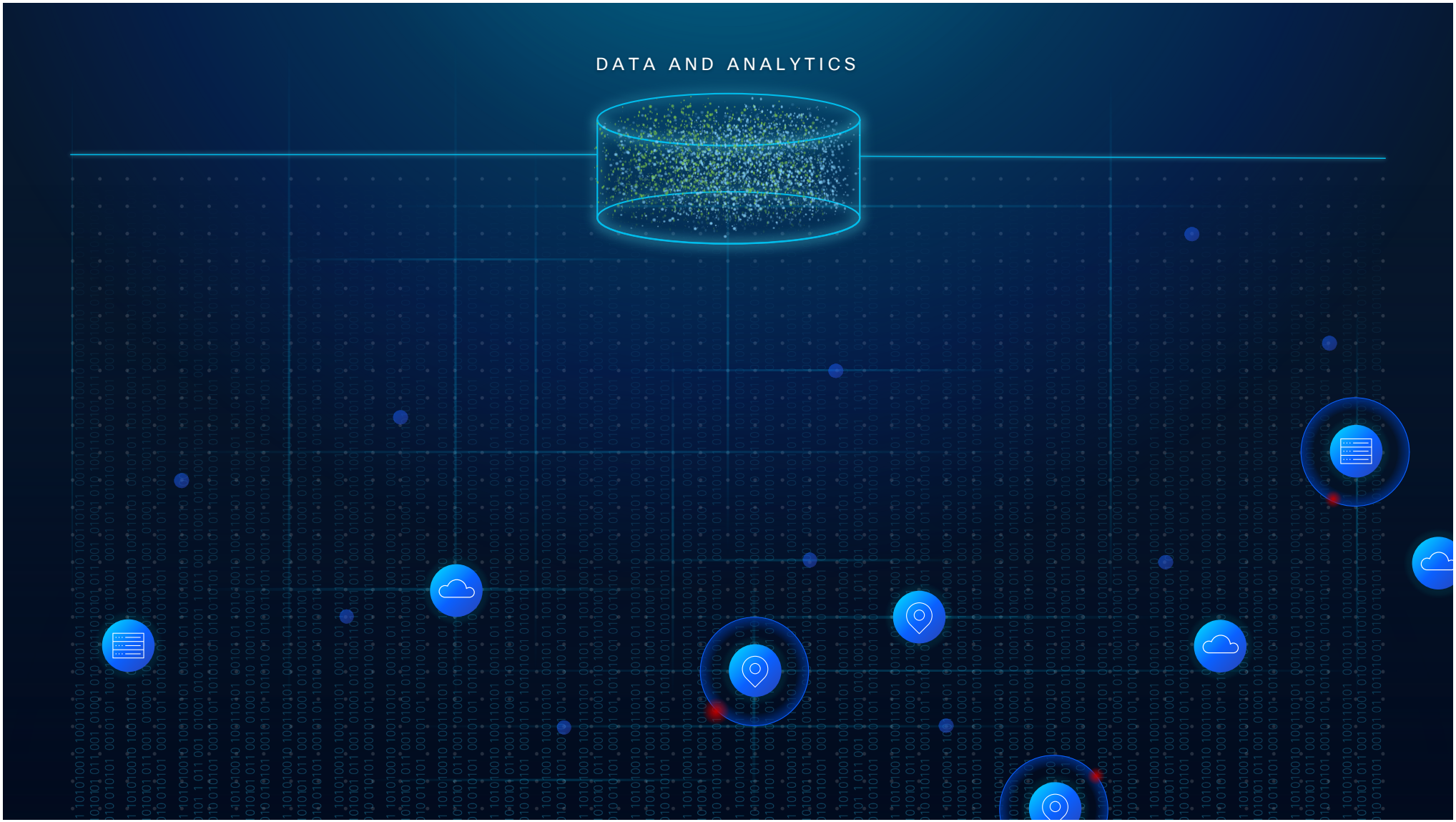
Simplified data ingestion and normalization

Pre-built dashboards and alerts

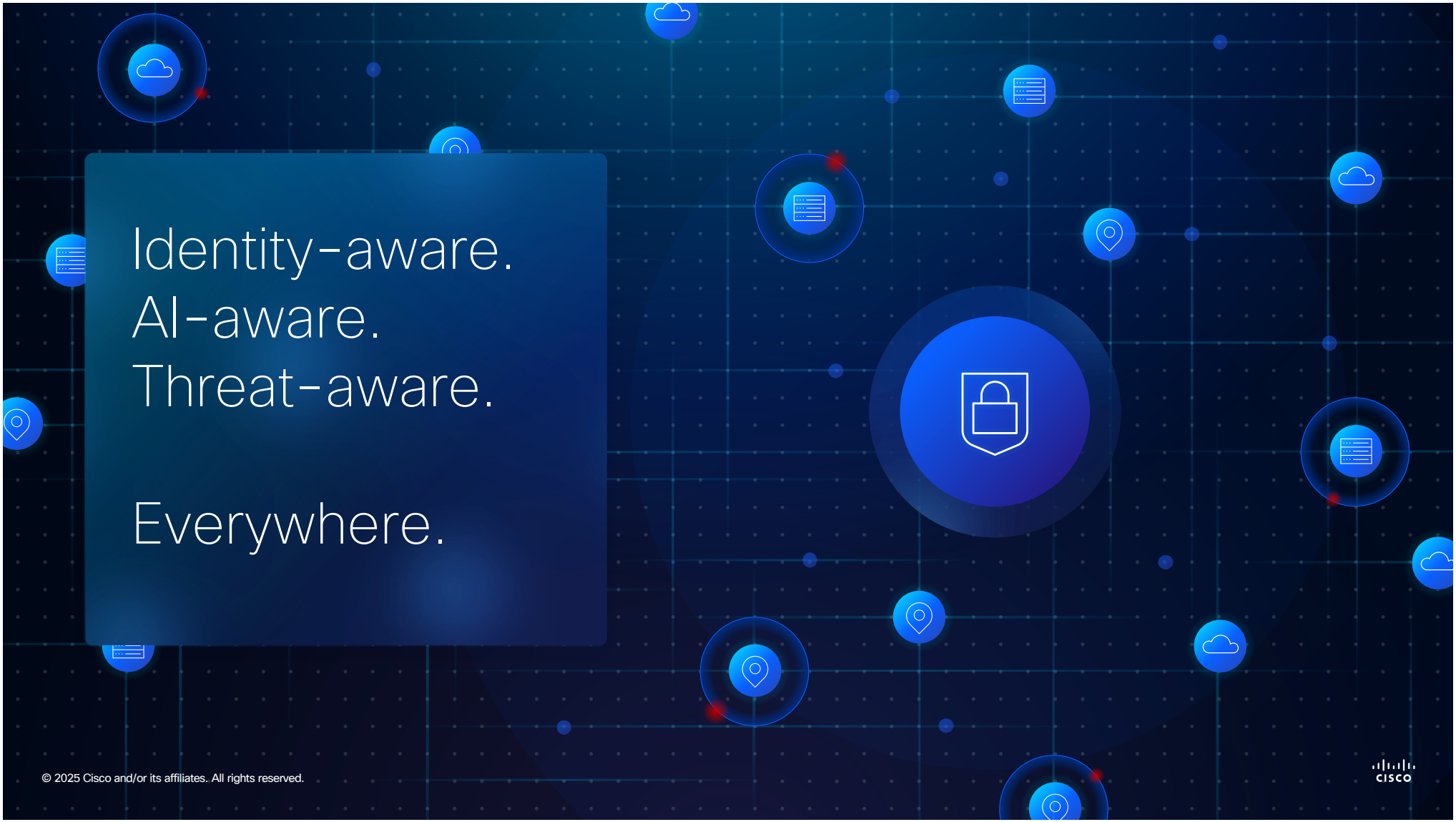
Ready to use detection and response workflows

Long-term data retention

Unmatched visibility and insight

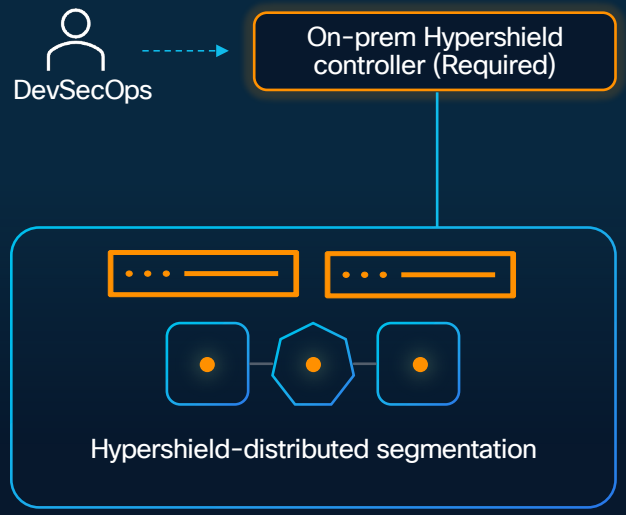

DATA AND ANALYTICS


cisco



Hypershield Management

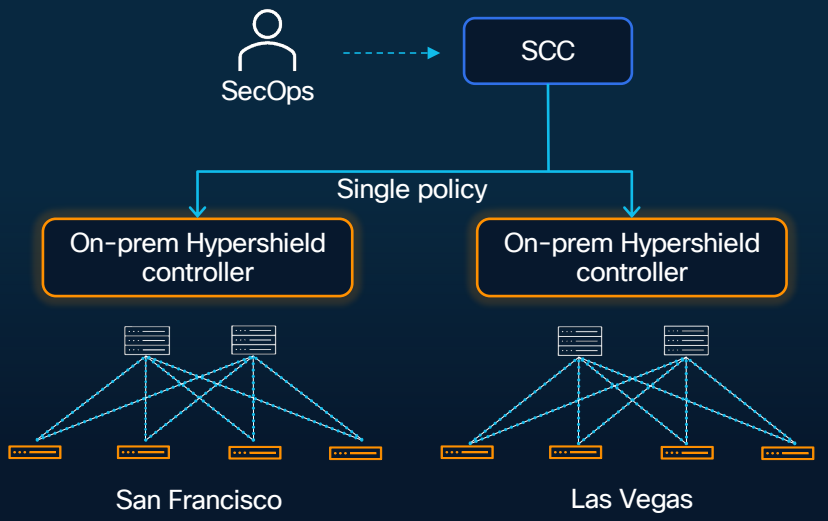
On-Prem



Local control

Unified visibility and policy for Smart Switch

Security Cloud Control (SaaS)

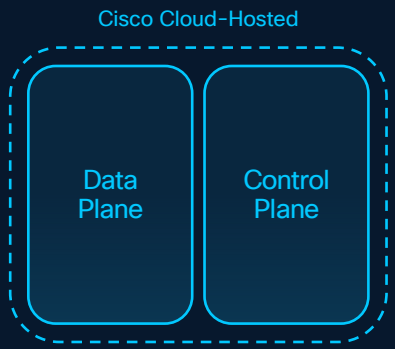


Global control

Single policy across on-prem and cloud in smart switch and workload agents

Cisco AI Defense

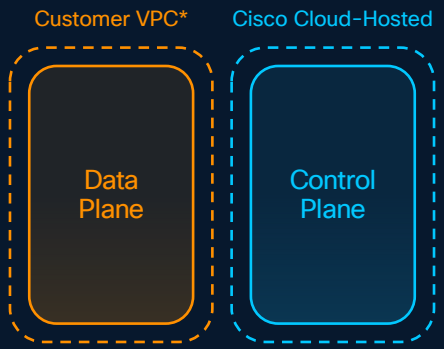
Deployment options for every situation



SaaS

Fully hosted and managed in the cloud

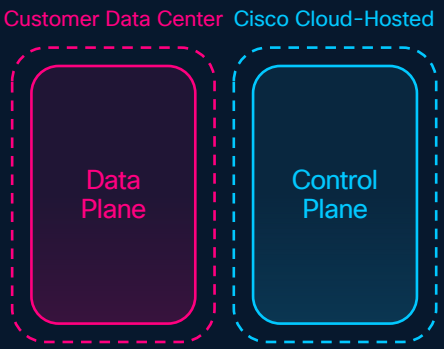
***Best for** customers looking for a simple, flexible deployment with zero infrastructure to manage*



VPC

Virtual private cloud environments with a cloud-hosted control plane

***Best for** customers looking to balance data control and compliance with cloud scalability*



Data Center

Combines physical infrastructure with a cloud-hosted control plane

***Best for** customers that want to manage AI workloads themselves rather than relying on hyperscalers*

* AWS (Beta), Azure & GCP (Coming Soon)