CISCO Connect

Security at Agentic Scale



Didi Dotan
VP of Engineering, Duo, ISE and Astrix

Sept 23rd 2026

CISCO Connect



About the speaker

Didi Dotan

Vice President of Engineering, Cisco

Didi leads Cisco's Identity engineering organization, shaping products such as Cisco Identity Services Engine and Duo Security. Previously, he co-founded Oort and served as its CTO.

CISSP

linkedin.com/in/dddotan

The three forces re-shaping security



The Mythos moment

Shields Up

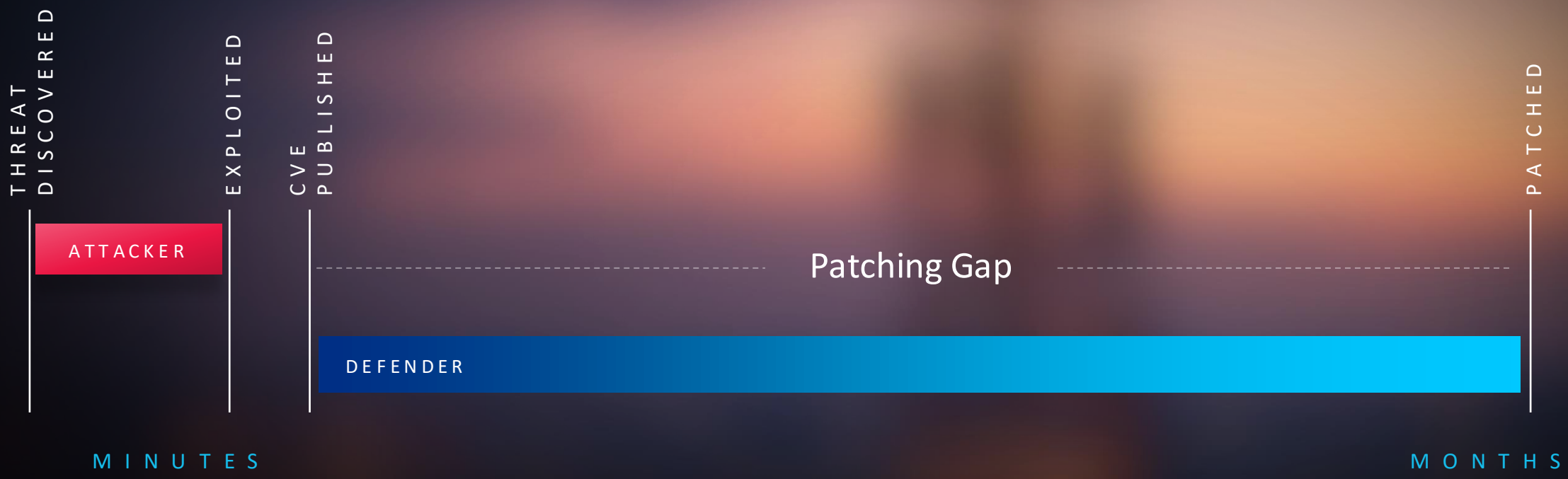
The OpenClaw moment

Security for Agents

The need for speed

Security using Agents

Patching is hard.
Frontier AI made it harder



Live Protect



CISCO NETWORK DEVICES
STARTING WITH N9000

Apply policy to live system

Protect now, patch in planned window

No downtime or switch reboot

Continuous re-validation

Quantum breaks cryptography foundations

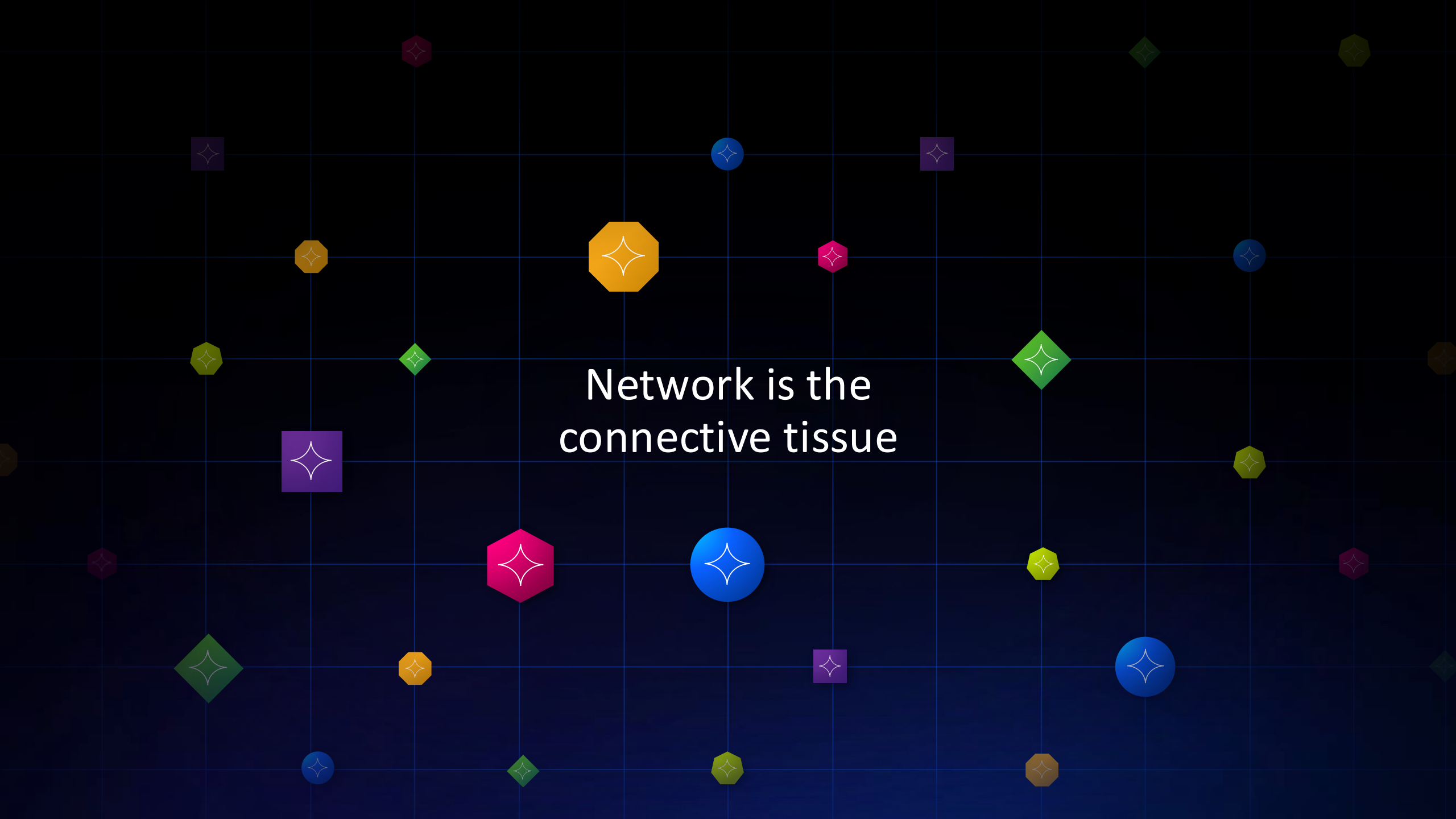
QUANTUM RESILIENCE

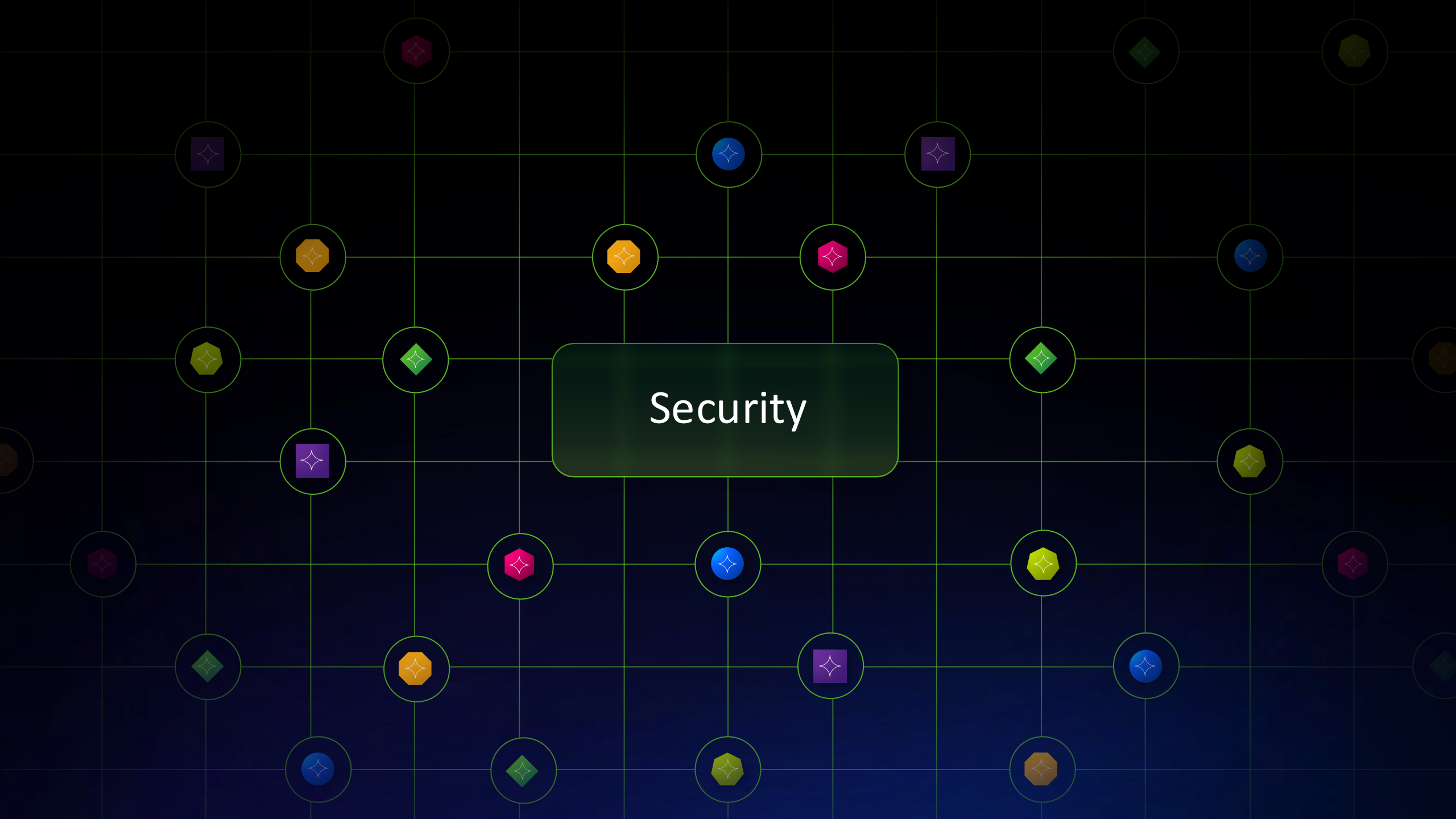
	Quantum-safe communications	Quantum-safe platforms
THREAT	Harvest Now, Decrypt Later	Trust Now, Forge Later
CISCO ACTION	Quantum-safe communications across core portfolio by June 2027	All new enterprise and data center routers, switches, and firewall series will ship with quantum-safe secure boot

SECURITY FOR AGENTS

Agents live everywhere, access everything. And are the new targets.




Network is the
connective tissue


Security

Secure Networking: Security Fused into the Network



Resilient infrastructure



Identity



Segmentation & steering



Protection



Visibility & insights

Cisco Security



Security for Agents

Protect the agents from the world



Protect the world from the agents

Detect and respond at machine speed

SECURITY FOR AGENTS: PROTECT AGENTS FROM THE WORLD

Poor uncertainty handling

Sensitive data over-sharing

Sensitive data overcollection

Workflow denial of service

Infrastructure mutation risk

Weak containment

Accountability ambiguity

Human trust manipulation

Misleading status reporting

Auditability failure

Unsafe code execution

Unsafe browser automation

Resource exhaustion

Regulatory noncompliance

Unsafe retrieval reliance

Context window loss

Poor rollback design

Offboarding failure

Excessive agency

Unauthorized action

Unsafe planning

Irreversible action

Cost amplification

Safety

Runaway task

Inadequate oversight

Transaction integrity failure

Business process corruption

Unsafe external communication



Agent identity abuse

Memory poisoning

Supply chain poisoning

Toolchain compromise

Goal hijacking

Security

Instruction hijacking

Tool misuse / abuse

Memory poisoning

Data exfiltration

Persistent instruction corruption

3rd party risk

Environment escape

Rogue agent behavior

Tool parameter injection

Tool output spoofing

Unsafe data ingestion

Credential leakage

Credential misuse

Cross-tenant data leakage

Cross-task contamination

Policy bypass

Task laundering

Approval laundering

Cascading compromise

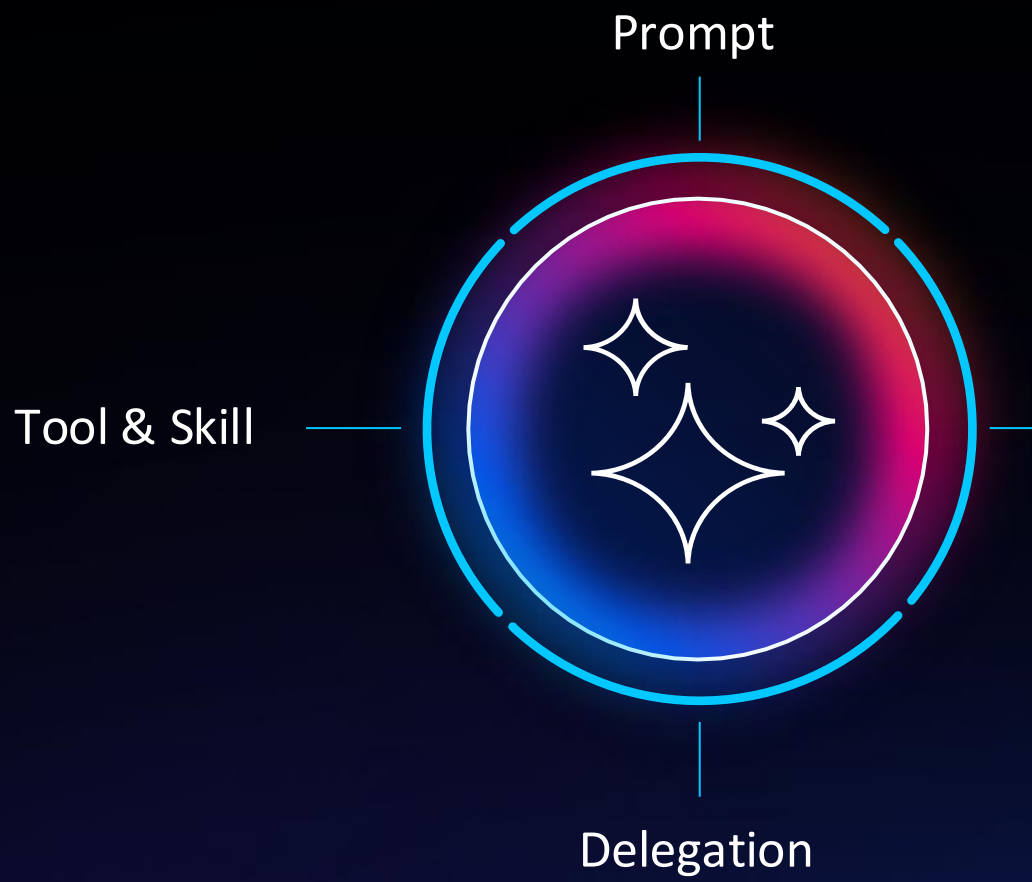
Insecure A2A comms

Delegation abuse

Confused deputy

Covert channel exfiltration

Runtime protection for agents



Securing Custom Agents and AI Apps

Cisco AI Defense



Discover



Validate



Protect

NEW

Adaptive red teaming and custom guardrails

NEW

Protecting the full agent supply chain

NEW

Ecosystem to work with any cloud, any GPU



OPEN SOURCE

DefenseClaw

OpenClaw

Codex

Claude Code

Enterprise-ready protection in Secure Client



VPN ZTNA SIA/DNS

Visibility Posture

Experience Monitoring

\+

DefenseClaw

AI runs on Kubernetes

Process hiding

Credential harvesting

Privilege escalation

Container escape

Kernel exploit

File tampering

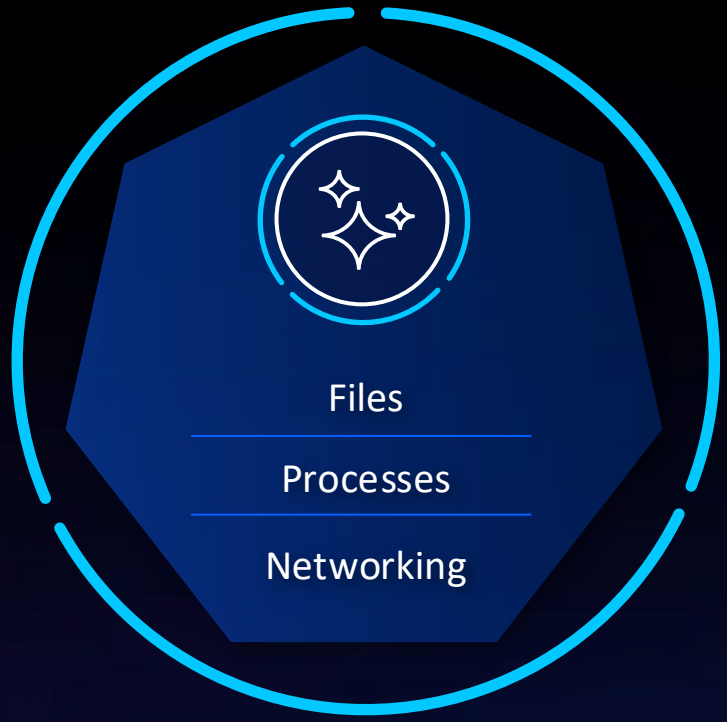
Sidecar injection

Shell injection

Network scanning

Reverse shell

Segmentation



Runtime shields

Host file system access

Service discovery abuse

API server probing

Token theft

Host container abuse

DNS tunneling

Deserialization

Unauthenticated service

Runtime socket exposure

Command injection

Process-level visibility

Segmentation is no longer optional



Identity
Dashboard
Users
Applications
Endpoints
Agents
Non-Human Identities
Integrations
Checks
ISE Monitoring
System Logs
Settings

ISE deployments Beta

Name	Version	Last Heartbeat	Uptime	Avg Auth Latency
Demo ISE	v3.3.0.430 · Patch 4	33 sec ago	1d 0h	148ms
ISE test deployment in US	Waiting for Agent Connection			

ISE test deployment in US

Sep 20, 2026 05:21:02 UTC
Last data collection

Sep 19, 2026 05:21:03 UTC
Last settings update

Sep 17, 2026 16:09:51 UTC
Integration added

Collection status

✓ Success
Data processing completed

Recent Usage



Traffic Today

0 records read

Edit Settings
View ISE Dashboard
Process New Data
View Logs
Delete

Security for Agents

Protect the agents from the world



Protect the world from the agents

Detect and respond at machine speed

The agent trust gap

85%

Experimentation and adoption



TOP CONCERNS

- Access control
- Data exfiltration
- Autonomy

5%

Broad production



Source: Cisco survey of security and IT execs, Jan 2026, n=224

© 2026 Cisco and/or its affiliates. All rights reserved.

Agents are the ‘Worst Of Both Worlds’

	Human	AI Agents	Machine
Scope	BROAD	BROAD	LIMITED
Speed	LIMITED	RAPID	RAPID
Scale	LIMITED	EXPONENTIAL	MODERATE
Sensibility	JUDGEMENT	NO JUDGEMENT	RIGID RULES

© 2026 Cisco and/or its affiliates. All rights reserved.

Zero Trust must change for the agentic workforce



Humans



Agents

Access control

Prove identity,
trust the user

Action control

Verify behavior,
control the agent

Holds agents accountable to humans | Secures agentic action

© 2026 Cisco and/or its affiliates. All rights reserved.

Chaos makes action-level zero trust hard

Agents Everywhere

Task-driven Behavior

Fragmented Enforcement

© 2026 Cisco and/or its affiliates. All rights reserved.

Zero Trust for Agents

KNOW EVERY AGENT

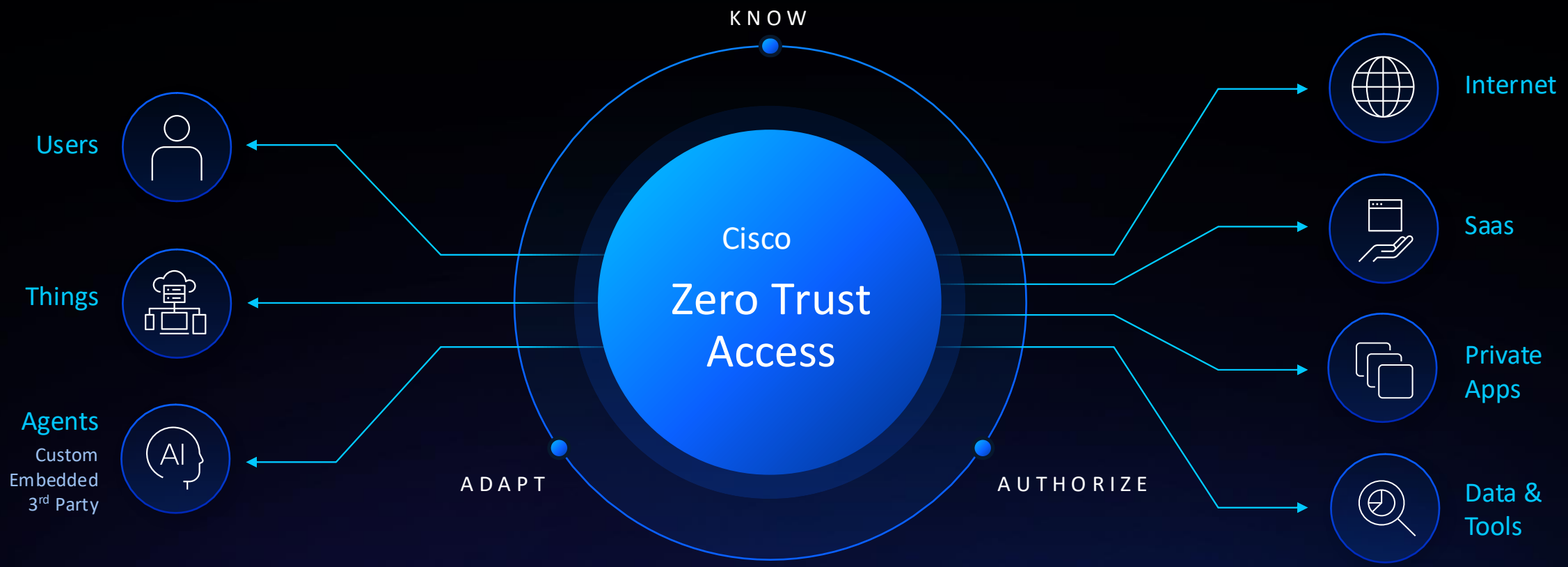
AUTHORIZE EVERY ACTION

ADAPT TO RISK IN REAL TIME

CONSISTENT ENFORCEMENT AT ACCESS BOUNDARY

© 2026 Cisco and/or its affiliates. All rights reserved.

Powered by Cisco SASE and Identity



Agent Security
Dashboard
AI Inventory
Policy
Events
Scans
AI Red Teaming
Administration

Dashboard

Get started with Agent Security

0 of 3 setup tasks complete

Connect cloud providers, API connectors, and endpoints to discover agents and MCP servers. Review findings in one place to manage risk and protect AI traffic across your organization.

Discover agents hosted on my cloud platforms — Not started

Find and manage AI traffic hosted on non-Cisco cloud platforms such as Amazon, Azure, and GitHub.

Get started →

Discover agents connected via API or external sources — Not started

Find, manage and configure AI traffic connected through APIs and external platforms.

Get started →

Discover agents hosted on my endpoints. — Not started

Find and manage AI agent activity across endpoints via DefenseClaw.

View documentation

2 All Agents	2 Enterprise Agents	0 Endpoint Agents	0 SaaS Agents

Agent Activity

All Agents 2

Registered 2 | Discovered 0

- Test
- TestGateway

All registered agents

All Agent Findings

MCP Servers 4

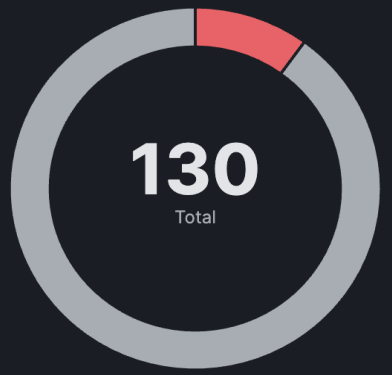
- test
- test
- test
- test

All MCP servers

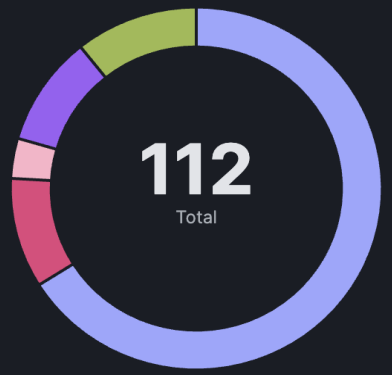
Identity
Dashboard
Users
Applications
Endpoints
Agents
Non-Human Identities
Integrations
Checks
ISE Monitoring
System Logs
Settings

Posture

Users | Non-Human Identities | AI Agents | MFA | Devices | Applications



- Risky - 13
- Other - 117



- Monitoring - 74
- EDR - 11
- Hooks - 4
- Fingerprinting - 11
- Other - 12

Non-Human Identity Posture Score

231 non-human identities · Sep 20, 2026



Very Good

+3 (30 days)

Take actions to improve your posture

View All Recommendations

Recommendation:
Assign owners to non-human identities without an accountable owner
12 NHIs | 1 contributing check — Priority 1

Recommendation:
Reassign or deprovision non-human identities with deprovisioned owners
6 NHIs | 1 contributing check — Priority 2

Recommendation:
Rotate passwords for non-human identities with failed password rotation
5 NHIs | 1 contributing check — Priority 3

Recommendation:
Require MFA for non-human identities where supported
2 NHIs | 1 contributing check — Priority 4

Security for Agents

Protect the agents from the world



Protect the world from the agents

Detect and respond at machine speed

Mythos-class attackers have changed SOC Resilience.

Attack vectors need new approaches



Vulnerabilities

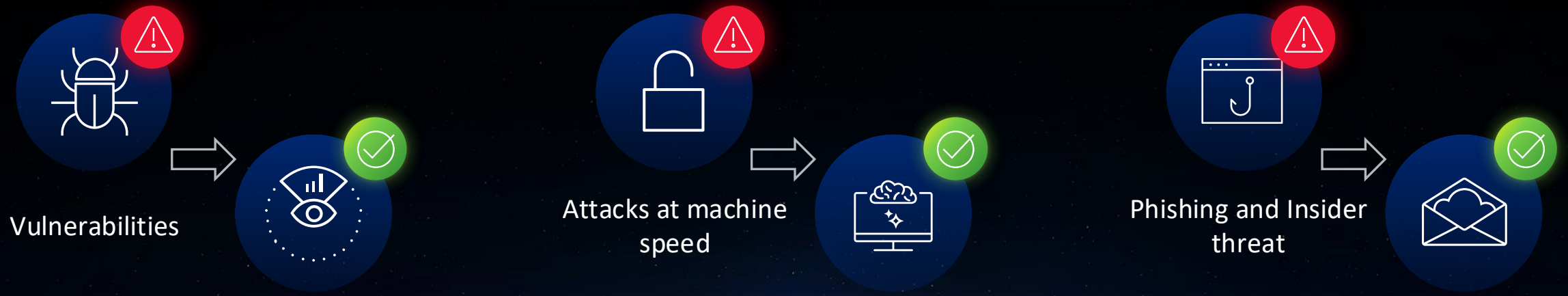


Attacks at machine speed

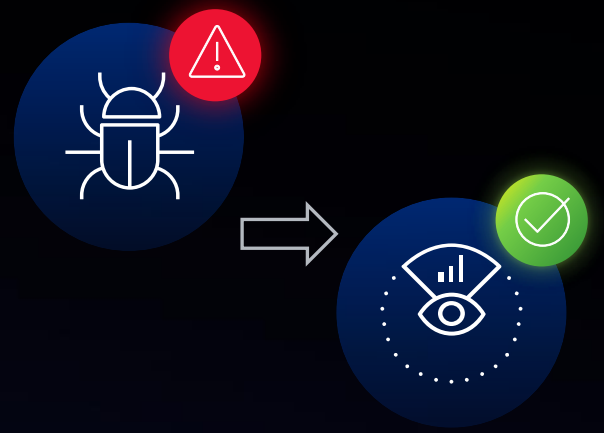


Phishing and Insider threat

Our Security innovations are solving for these vectors.



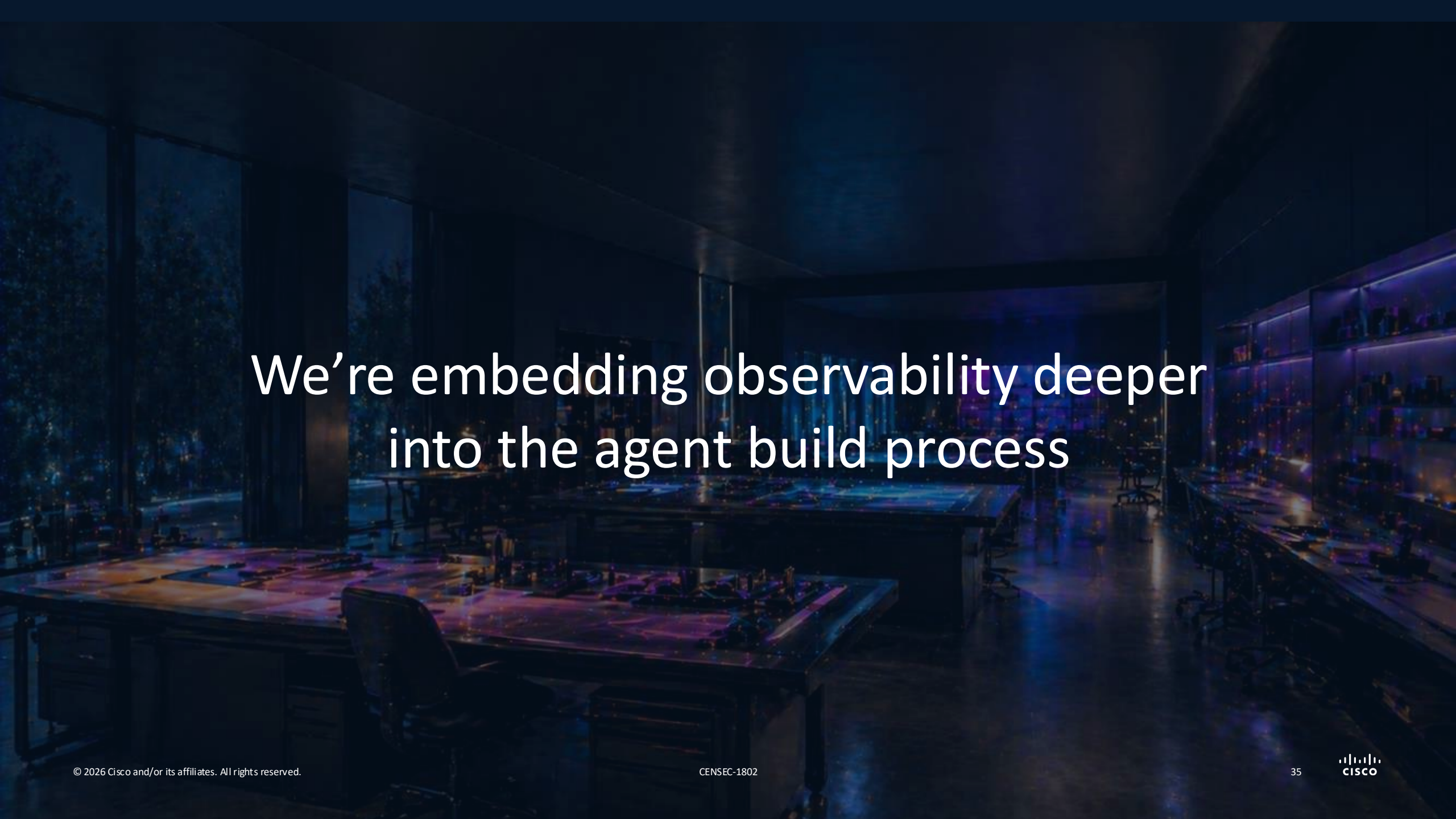
Expanded Visibility and Actionable Insights



- Continuously discover entities, assets, and users
- Enriched context and comprehensive visibility
- Identify vulnerabilities and exposures
- Risk posture assessment



© 2026 Cisco and/or its affiliates. All rights reserved.



© 2026 Cisco and/or its affiliates. All rights reserved.

Identity
Dashboard
Users
Applications
Endpoints
Agents
Non-Human Identities
Integrations
Checks
ISE Monitoring
System Logs
Settings

4 **Claude Code (engineering)** Active

4019b751-47df-42f9-b411-a17a44b22603__CLAUDE__707c37d2__claude__genie-alpha__c...

Summary

Type
Agentic App

Agent Platform
Claude

Owner
dana.levin@simubiz.com

Detection Method
EDR

Created
Mar 24, 2026 11:42:03 UTC (6 months ago)

Last Accessed
Sep 19, 2026 11:42:03 UTC (a day ago)

Usage
High

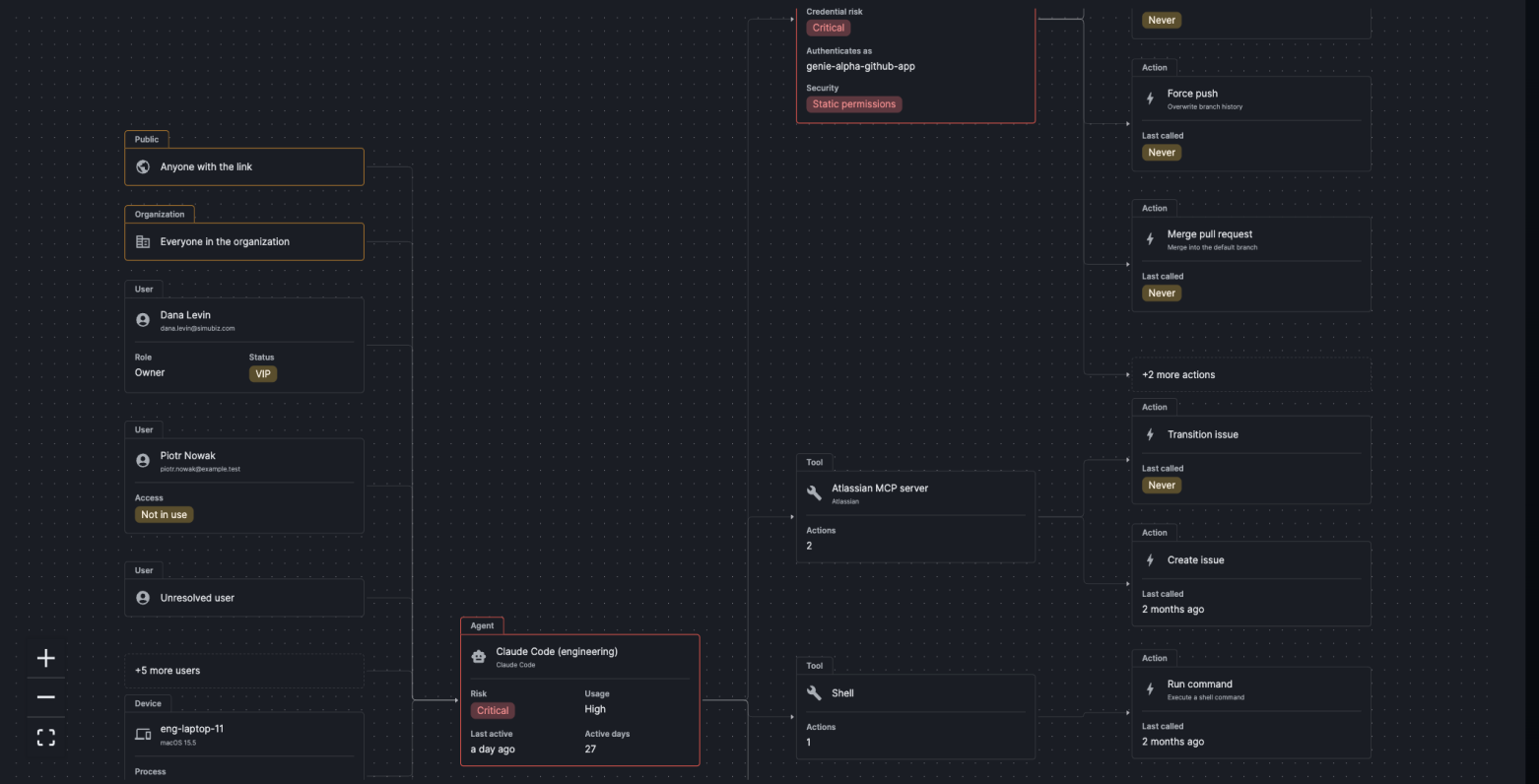
Provider Sources

claude - genie-alpha (autogenerated)

Additional Information

Account
genie-alpha

AI Agent Graph



Risk Critical

Exposure High

Exposure Contributing Checks
None found

Likelihood Critical

Likelihood Contributing Checks
None found

CISCO Connect

Thank you




CISCO