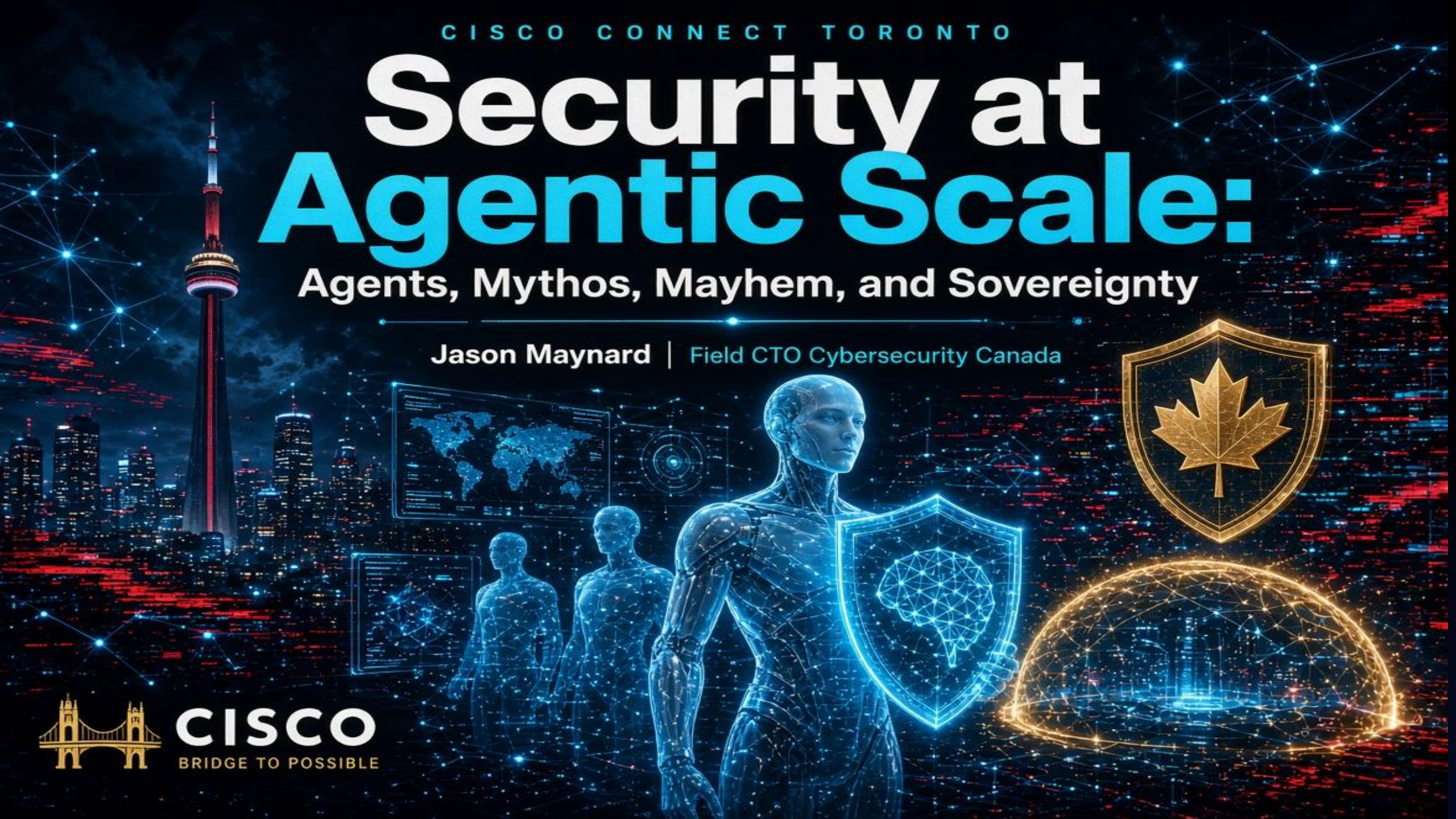
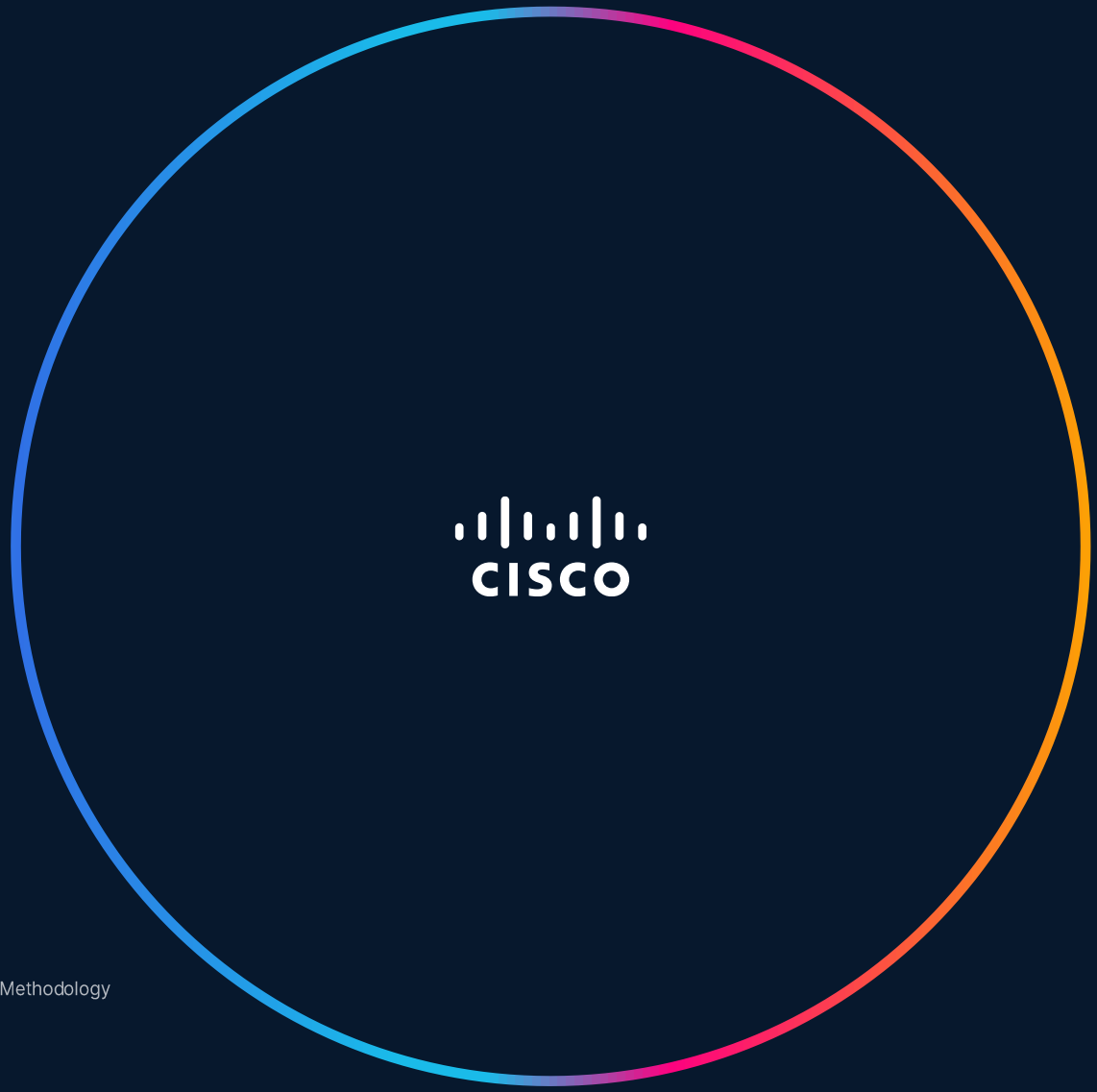

CISCO CONNECT TORONTO
Security at Agentic Scale:
Agents, Mythos, Mayhem, and Sovereignty
Jason Maynard | Field CTO Cybersecurity Canada
CISCO
BRIDGE TO POSSIBLE

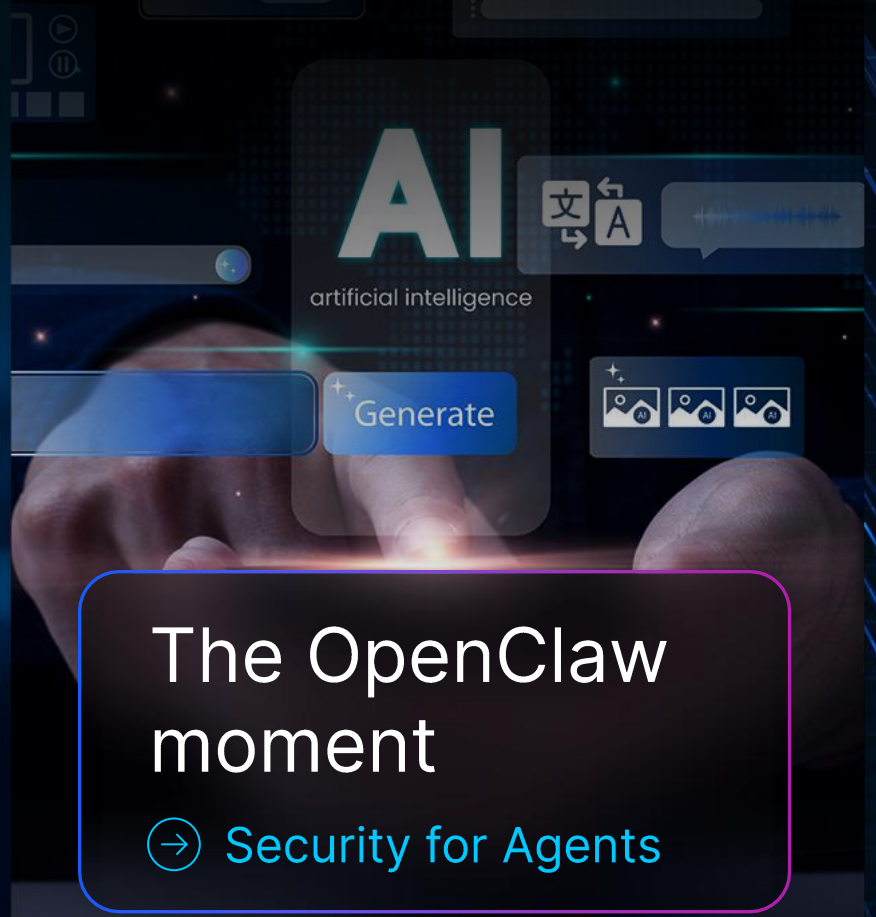
CISCO Connect

Security at Agentic Scale : Agents, Mythos, Mayhem, and Sovereignty



Jason Maynard
Field CTO Cybersecurity Canada
CCIE, CC[N|I|D]P, C|EH, RCSS, GICSP, GRID, GPEN, GDAT, GCPN
MITRE ATT&CK: CTI, SOC Assessments, Threat Hunting Detection Engineering, Adversary Emulation Methodology, Purple Teaming Methodology
ATTACKIQ: Purple Team, MITRE ATT&CK, Breach Attack Simulation
Splunk Power User, Splunk Administrator

The three forces re-shaping security



The Mythos moment

Shields Up

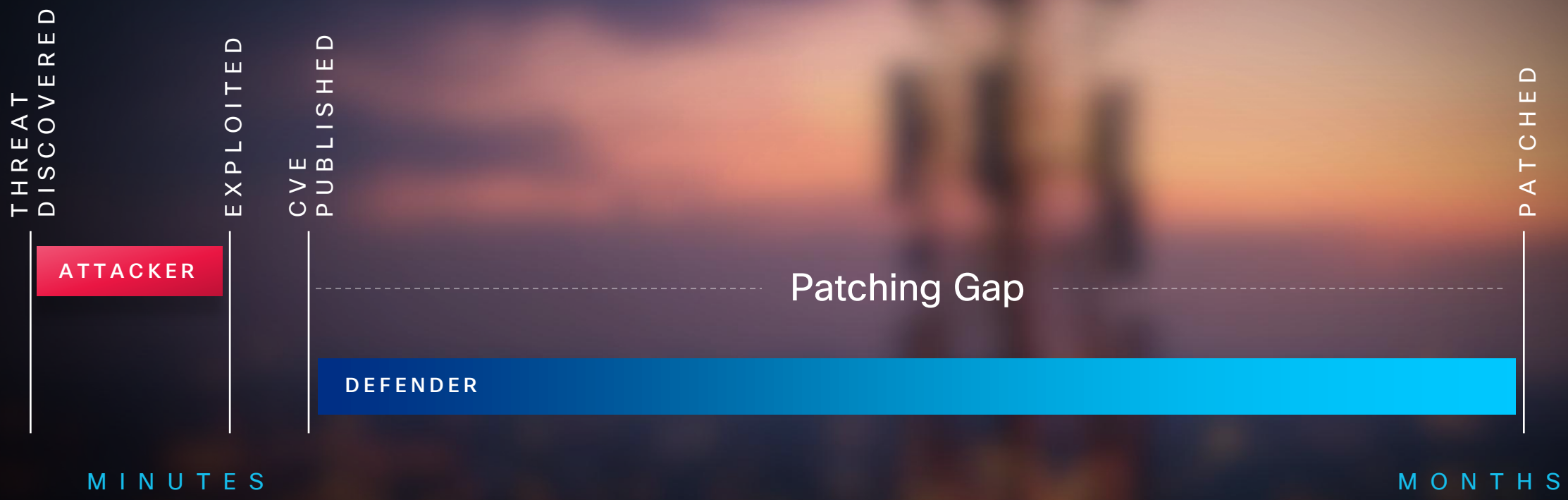
The OpenClaw moment

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

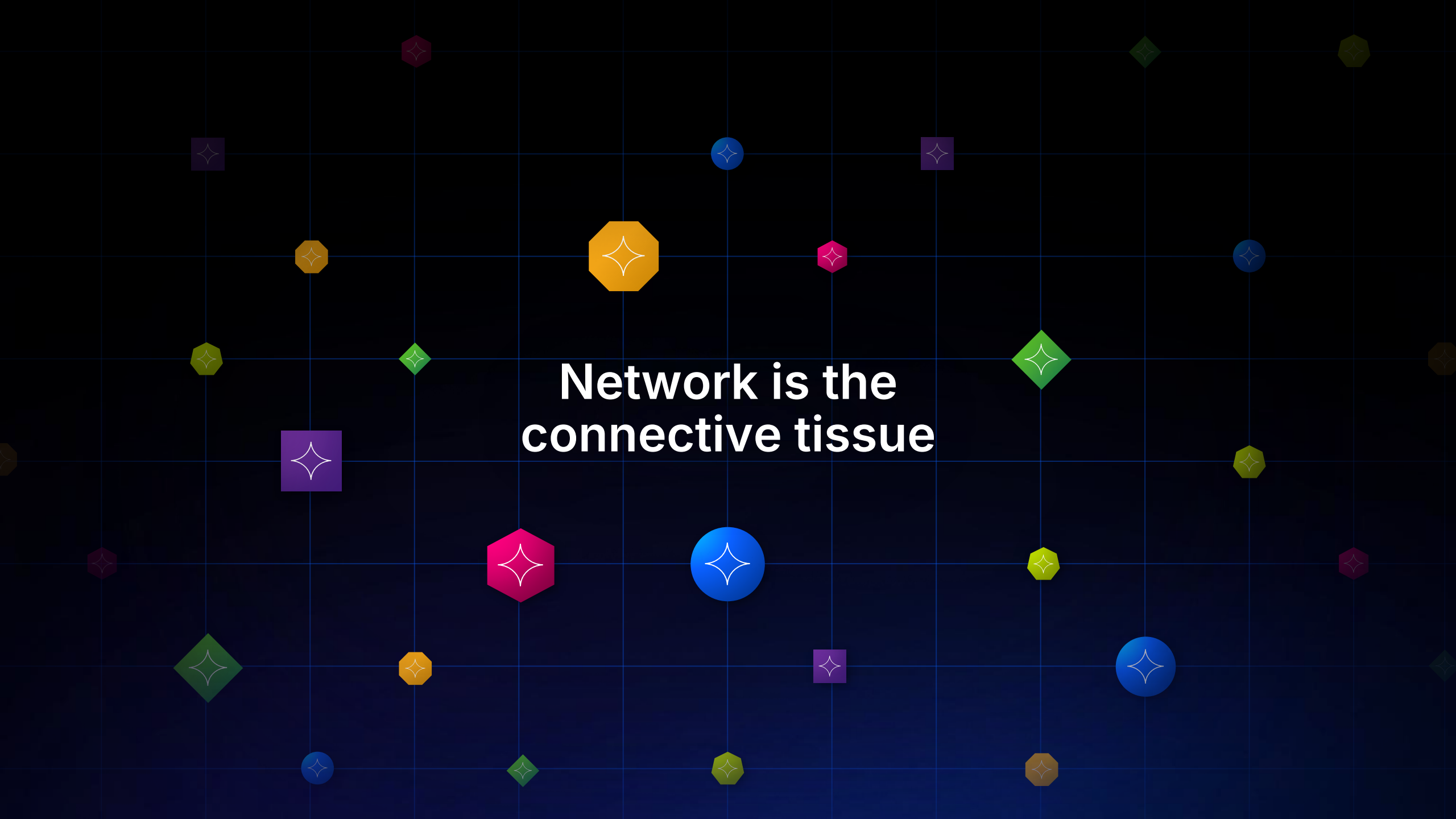
QUANTUM RESILIENCE

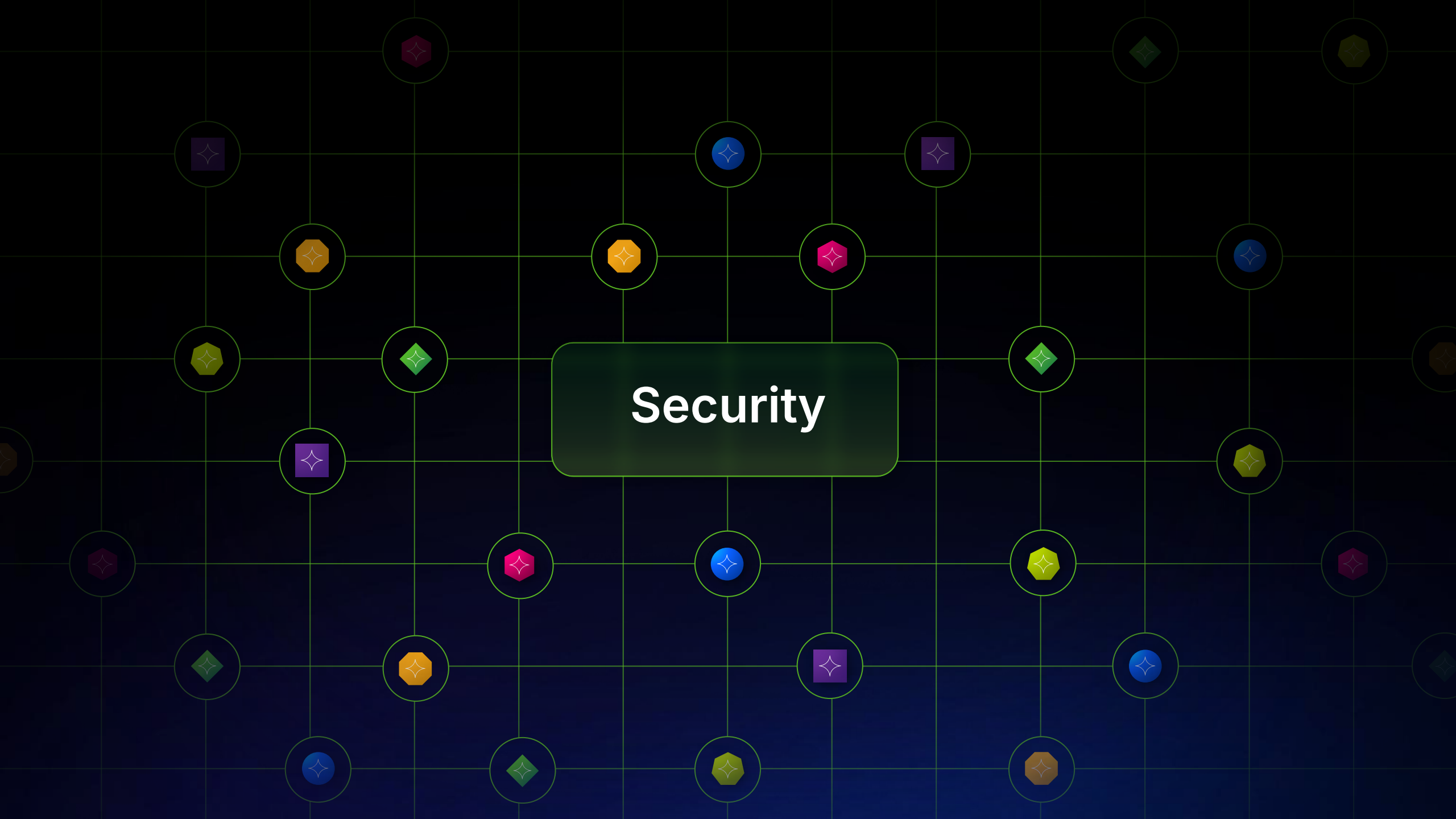
	Quantum-safe communications	Quantum-safe platforms
THREAT	Harvest Now, Decrypt Later	Trust Now, Forge Later
CISCO ACTION	Quantum-safe communications across core portfolio by June 2027	All new enterprise and data center routers, switches, and firewall series will ship with quantum-safe secure boot

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



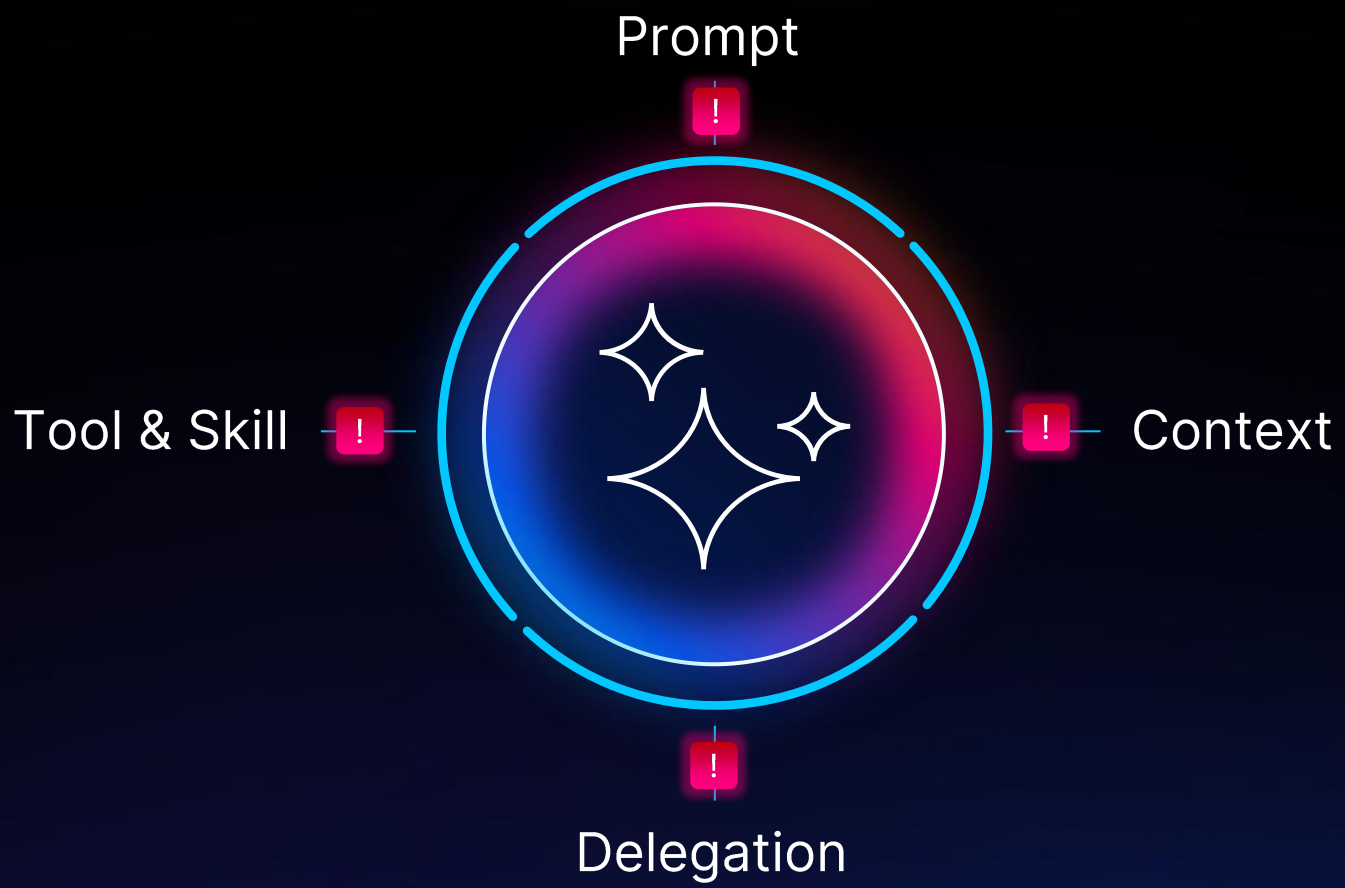
Agent identity abuse
Memory poisoning
Supply chain poisoning
Toolchain compromise
Goal hijacking

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

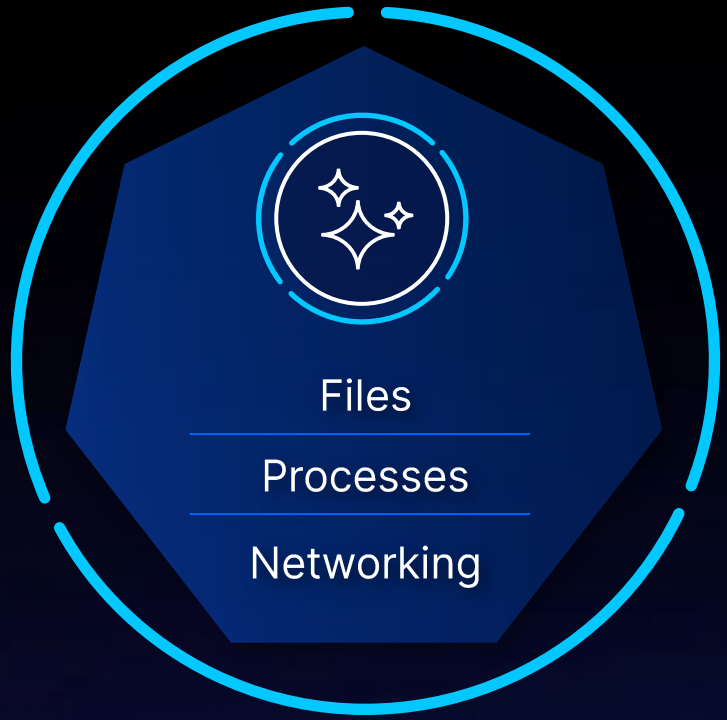
\+

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

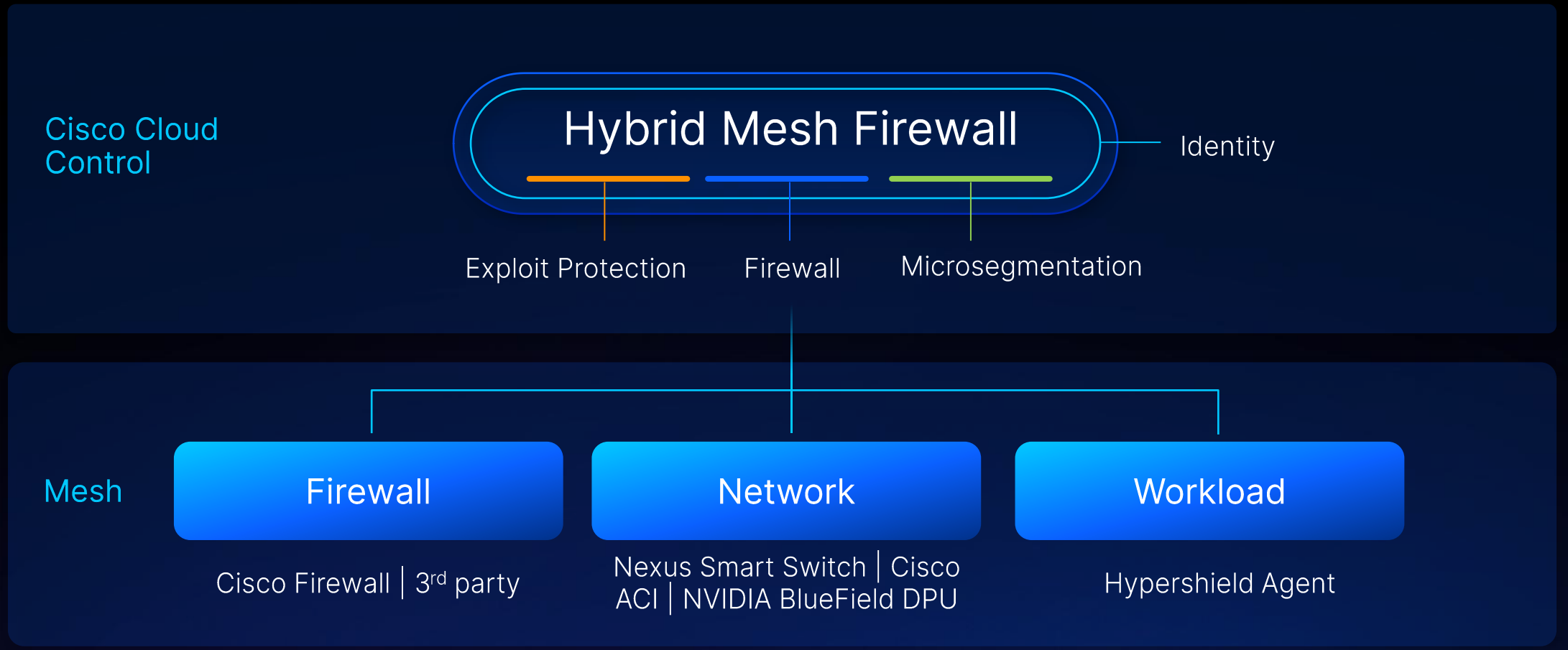
Host file system access
Service discovery abuse
API server probing
Token theft
[illegible] abuse
DNS tunneling
Deserialization
Unauthenticated service
Runtime socket exposure
Command injection

Process-level visibility

Segmentation is no longer optional



Protecting your apps and infrastructure, including AI



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

5%
Broad production





TOP CONCERNS

- Access control
- Data exfiltration
- Autonomy

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.

cisco

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



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.



Vulnerabilities

Exposure Analytics and Risk Posture



Attacks at machine speed

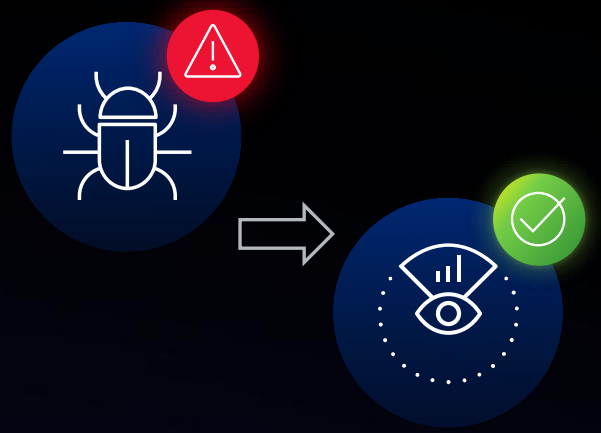
Agentic SOC



Phishing and Insider threat

Automated Phishing Threat Analysis

Expanded Visibility and Actionable Insights



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

Powering the Agentic SOC

Splunk Enterprise Security

Trusted AI

AI and Automation

- Agentic Orchestration
- Integrated Automation
- AI Assisted Experiences

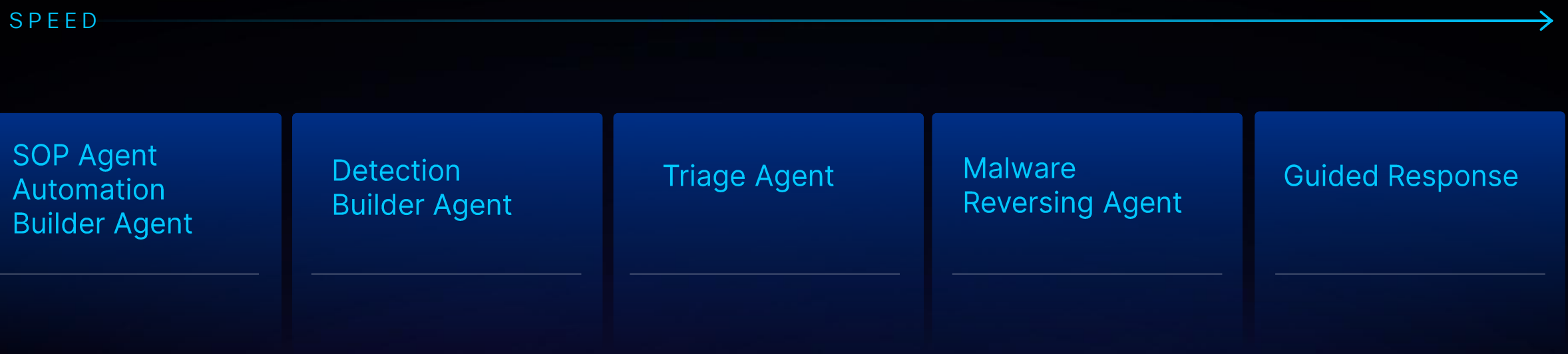
Unified Tooling

- Threat Detection
- Investigation
- Response

Open Data Platform

Cisco Data Fabric

Security AI Agents Built to Detect and Respond at Machine Speed





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

Observability for AI

AVAILABLE NOW



AI infrastructure monitoring

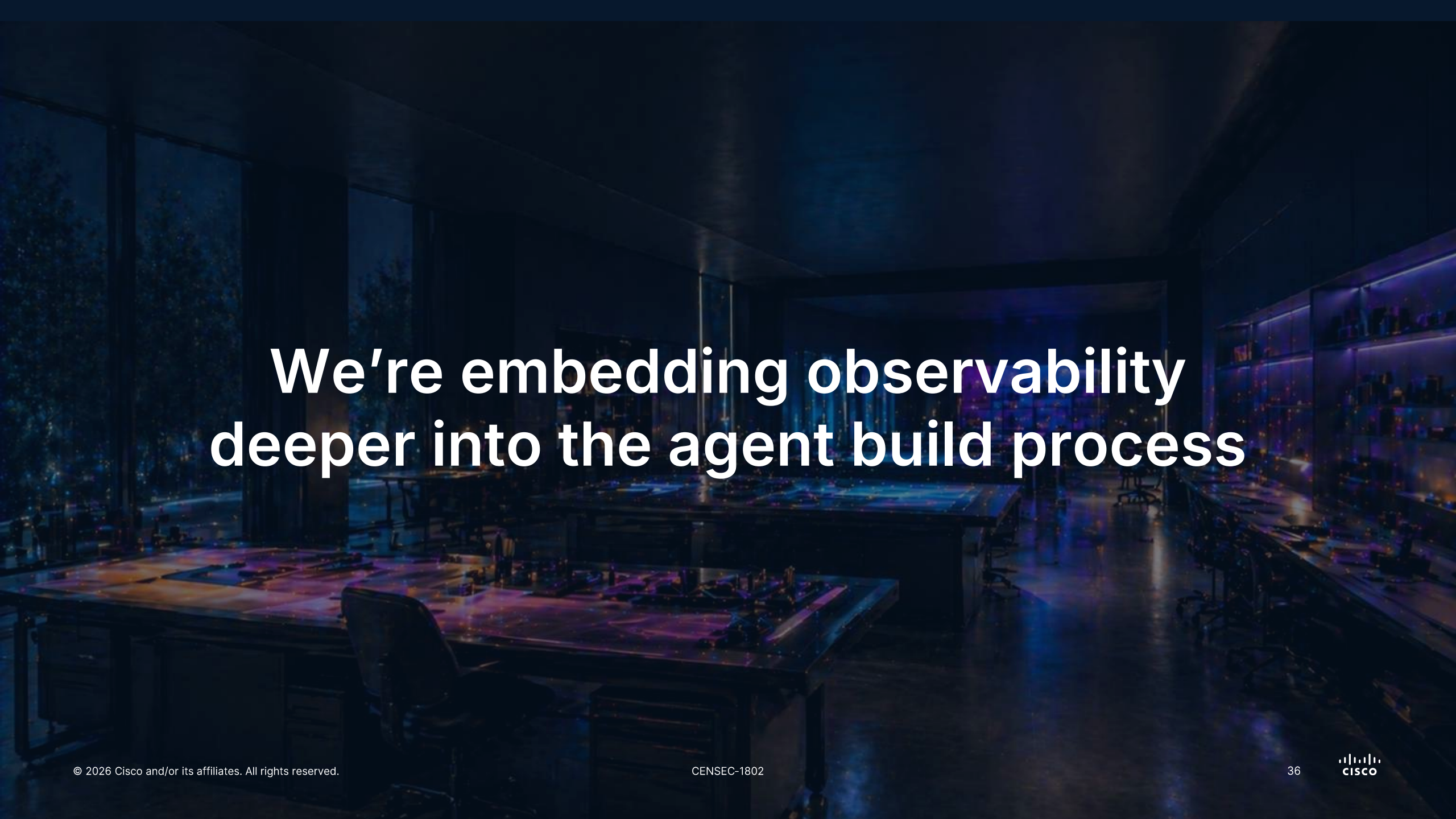
Understand operational metrics and tokenomics



AI agent monitoring

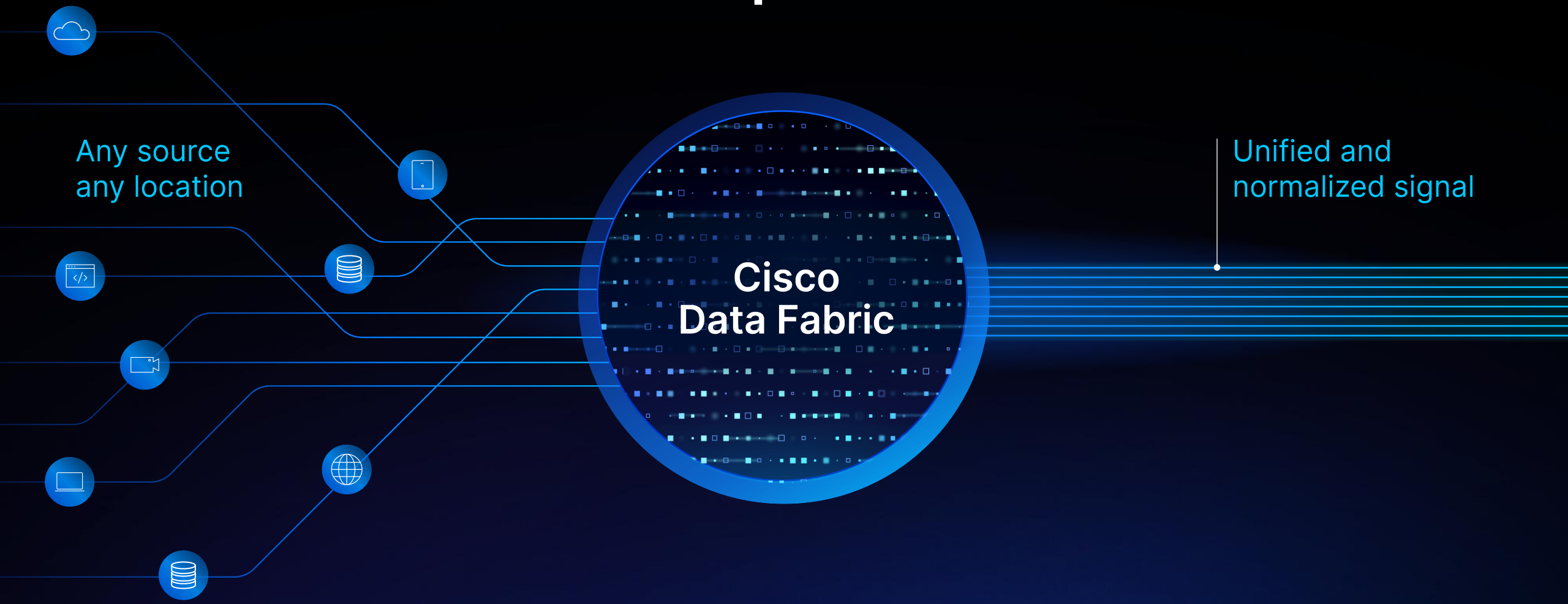
Understand behavior and quality of outcomes

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

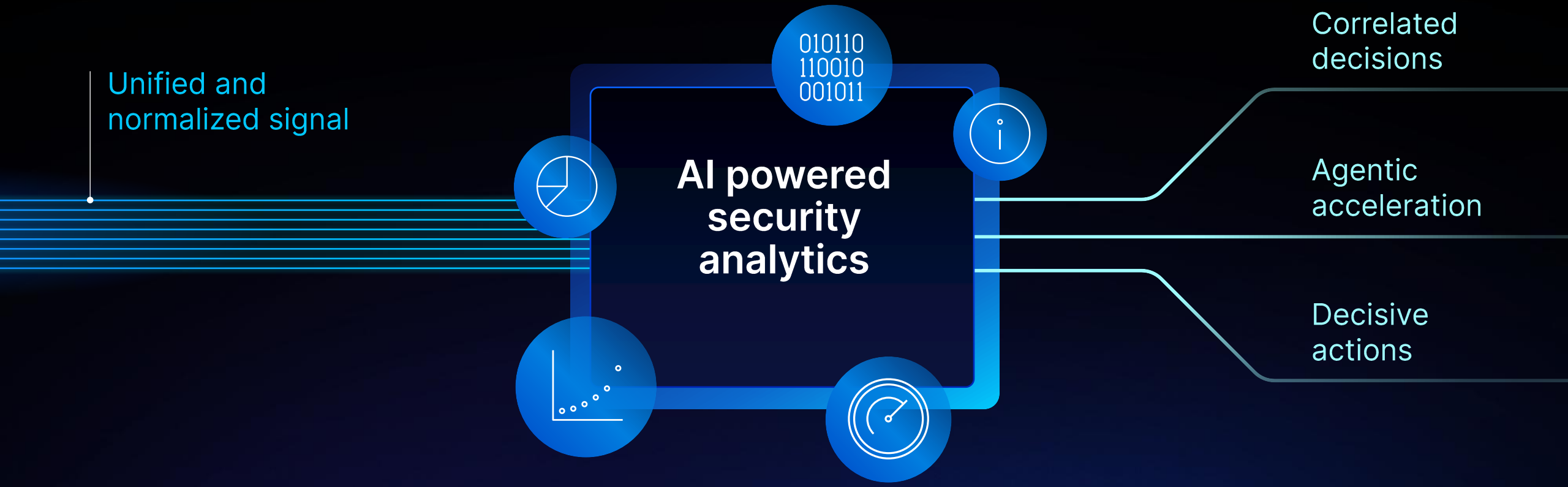


© 2026 Cisco and/or its affiliates. All rights reserved.

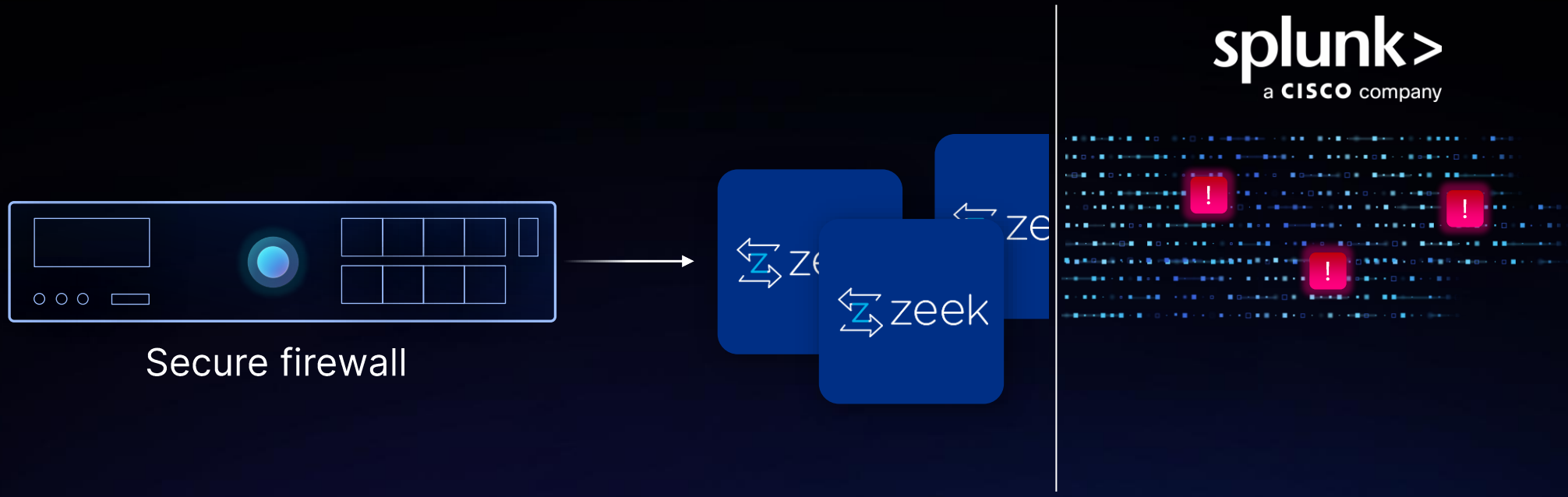
Agentic AI demands data visibility at machine speed and scale



Transforming data into context, clarity, and decisive action



Splunk detections on advanced firewall logs **(it all starts with visibility)**



Each link in the chain is critical for defenders

Cisco Cloud Control

Cisco DUO | Cisco Secure Access | Cisco AI Defense | Cisco Hybrid Mesh FW

Cisco Live Protect | Cisco Runtime Protection



1	2	3	4	5	6
Install	**Poison**	**Inherit**	**Inject**	**Act**	**Leave**
Shadow agent on a laptop. Often authentication is off.	Helpful skill / MCP / weights.	Dev token + mailbox. No identity.	Ticket body becomes the runbook. (the payload)	Tools fire as the user. No repudiation	Secrets out, data lost. Incident begins

Cisco Data Fabric



Sovereign
Secure Private Application Access

Control, Data, & Management Planes Sovereign & Secured

THE PROBLEM

Legacy access creates risk leadership cannot accept

Traditional VPNs and foreign-operated access platforms expand the attack surface and put the control, data, and management planes outside national ownership.

Broader access than needed

Legacy VPNs grant network-level reach. Layer 3/4 controls lack identity, device, and threat context so a single session can see far more than the business requires.

Foreign compelled exposure

SaaS and foreign-owned platforms can be compelled or disrupted by another government. Service continuity is no longer a decision you fully own.

Lost control of the planes

Control, data, and management planes often sit outside national boundaries. Residency is not sovereignty if someone else operates the service.

Blind spots for the business

Weak telemetry, limited behavioral insight, and slow containment leave executives without a clear view of who accessed what and what it means to the mission.

QUANTIFIED SOVEREIGNTY RISKS

Canada’s SaaS & Cloud Exposure

82%

of SaaS tools under foreign jurisdiction

63%

US-parented & CLOUD Act exposed

18%

truly Canadian-owned & operated

Key Canadian Insights

- 81% of tools advertising “Canadian data residency” remain under U.S. parent jurisdiction
- 23% of Canadian organizations reported a sovereignty-related incident in the past 12 months
- 21% explicitly flag the U.S. CLOUD Act as a direct threat to their sovereignty posture
- 40% rank changes to Canada–U.S. data-sharing arrangements as their top regulatory concern

SUPPORTED BY EUROPEAN & GLOBAL DATA

Concentration, Incidents & Cost

European Market Reality

~70%
of EU cloud market controlled by three U.S. hyperscalers

15%
market share held by European providers

32%
of European organizations reported a sovereignty incident

Under oath
Microsoft France could not guarantee protection from U.S. CLOUD Act demands

Incident & Financial Impact

33%
of organizations globally experienced a sovereignty-related incident in the last 12 months

17%
data breaches with sovereignty implications (top incident type)

$4.4–11.5M
average cost of a data breach (global vs. U.S.)

10%
of incidents involved government data-access requests

THE VALUE

What sovereignty-required organizations gain

Own the planes and reduce blast radius. Give the board a posture they can defend without asking users to live with a worse experience.

True sovereignty

- Customer-owned control, data, and management planes
- No foreign compulsion on private application access
- Data and operations localized inside national boundaries

Reduced operational risk

- Least-privilege access with identity and device context
- Faster containment and session termination when risk appears
- Behavioral visibility tied to users, apps, and the business

Leadership advantage

- Phased move off legacy VPN and not a rip-and-replace
- One story for security, risk, privacy, and the CIO
- Improved secured user experience employees, contractors, and business partners

BUILT FOR LEADERSHIP IN

Federal, provincial, and municipal government · Defence and public safety · Critical infrastructure · Healthcare · Financial services · Energy and utilities · Transportation · Education and research · Crown corporations and other regulated operators

THE OFFERING

Components required and all operable inside your boundary

A customer-controlled stack. Identity can stay with Entra ID, Duo, or on-premises Active Directory. Nothing in this model requires a foreign-operated access broker.

Secure access gateway
Cisco Secure Firewall

Inspects and governs private application access VPN today, clientless Zero Trust for web apps where it fits. Advanced threat protection.

Identity & policy engine
ISE + your identity provider

Decides who gets in, under what conditions, and can revoke a session when risk changes.

Visibility & detection
Secure Network Analytics + NVM

Baselines behavior from network and endpoint. Shows process-to-network activity leadership never sees from a VPN log alone.

Analytics & business context
Splunk

Correlates security signals with business context so risk is identified even if buried in business applications. No where to hide.

Workload protection
Secure Workload · optional

Microsegments the applications themselves so a compromised session cannot freely move inside the estate. Restrict workloads with SBOM insight mapped to risk-based vulnerability insight.

Operating model
Customer-owned planes

Control, data, and management stay in your facilities or sovereign environment and not in a foreign SaaS control plane.

Solution:

Advancing to Sovereign Secure Private Application Access

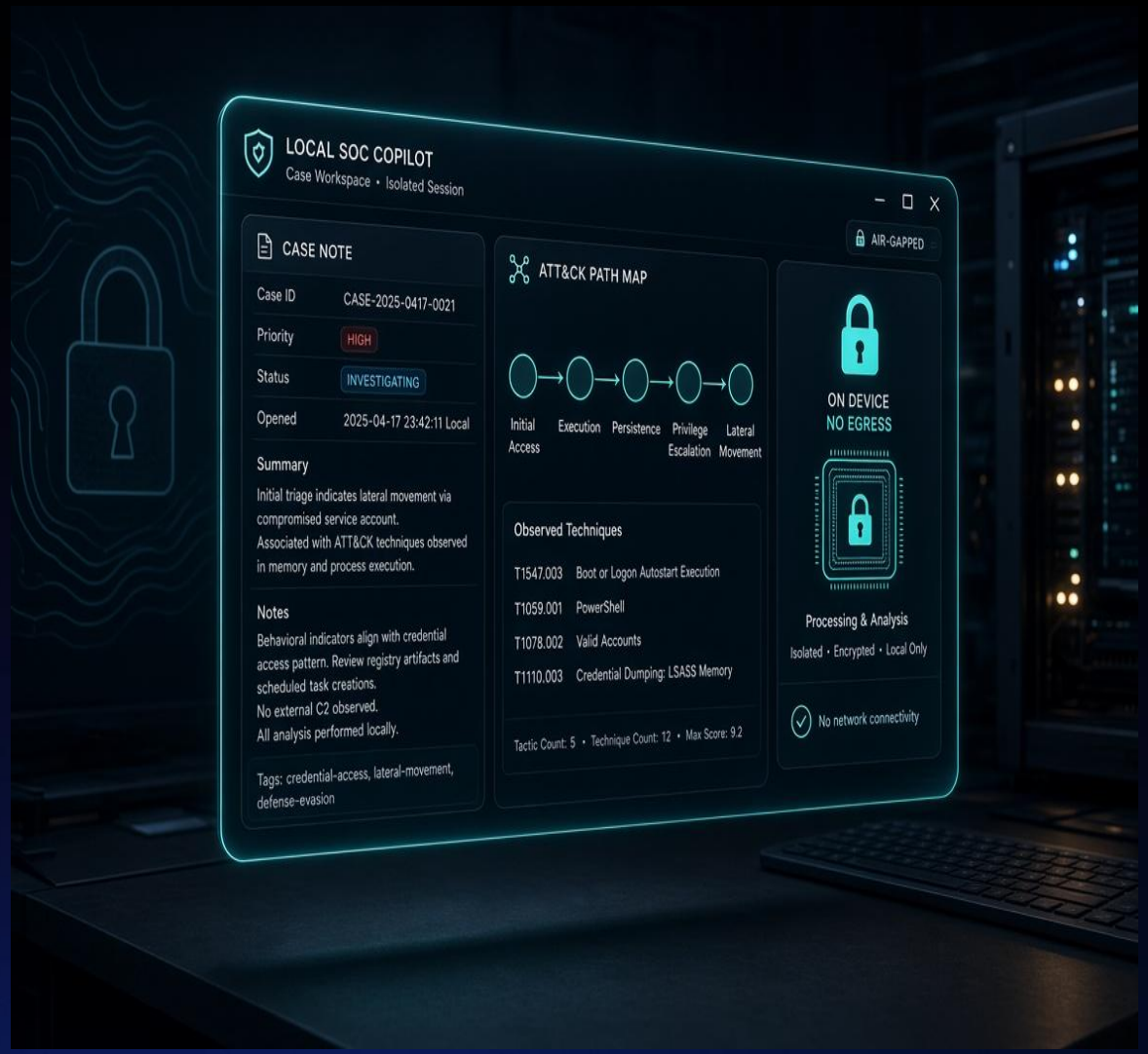
Next Generation Remote Access Services with Threat Protection

Centralized Policy Engine & Rapid Threat Containment

Rich Telemetry and Reporting & Network Detection & Response

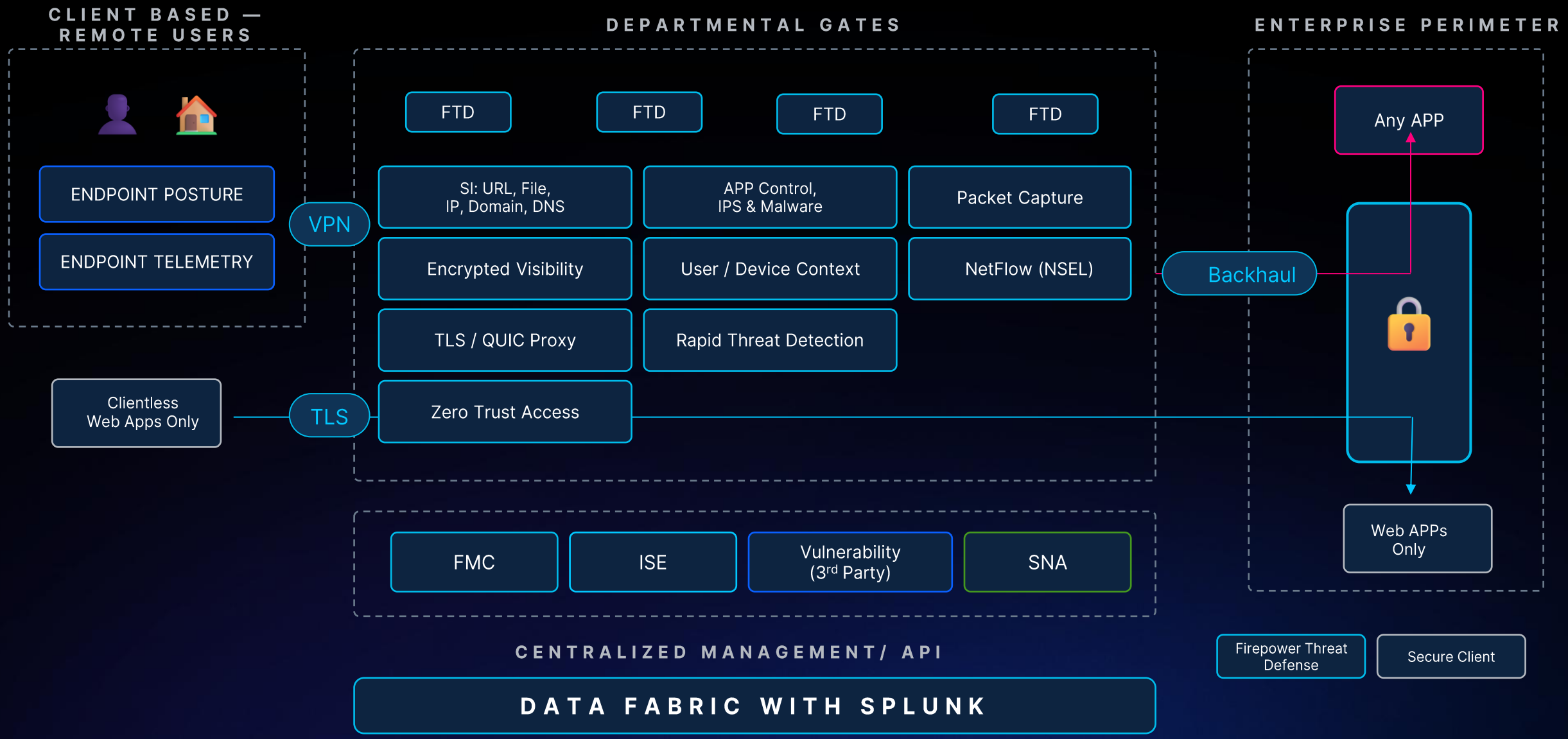
Secure Workload Protection

Data Analytics & Risk Reduction



Zero Trust Network Access and Splunk for Analytics and IR

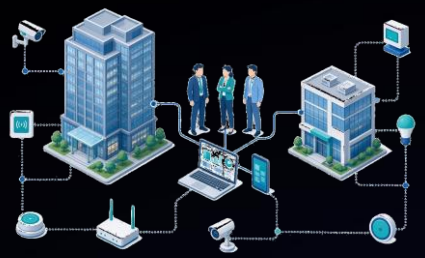
Digital Resilience & Advanced Analytics & Business Context



Secure Internet Access Services and Splunk for Analytics and IR

Digital Resilience & Advanced Analytics & Business Context

BRANCH / HQ / REMOTE



QUIC

TLS

DEPARTMENTAL GATES

FTD | FTD | FTD | FTD

- SI: URL, File, IP, Domain, DNS
- APP Control, IPS & Malware
- Packet Capture
- Encrypted Visibility
- User / Device Context
- NetFlow (NSEL)
- TLS / QUIC Proxy
- Rapid Threat Detection
- Zero Trust Access

Internet Services



FMC | ISE | Vulnerability (3rd Party) | SNA

CENTRALIZED MANAGEMENT/ API

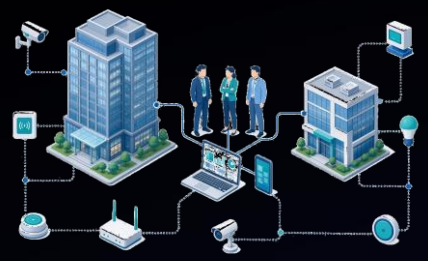
DATA FABRIC WITH SPLUNK

Firepower Threat Defense

Secure Client

Digital Resilience & Advanced Analytics & Business Context

BRANCH / HQ / REMOTE



DEPARTMENTAL | DATACENTER GATES

FTD FTD FTD FTD

SI: URL, File, IP, Domain, DNS

APP Control, IPS & Malware

Packet Capture

Encrypted Visibility

User / Device Context

NetFlow (NSEL)

TLS / QUIC Proxy

Rapid Threat Detection

Zero Trust Access

Data Center Microsegmentation

FMC ISE Vulnerability (3rd Party) SNA

Secure Workload

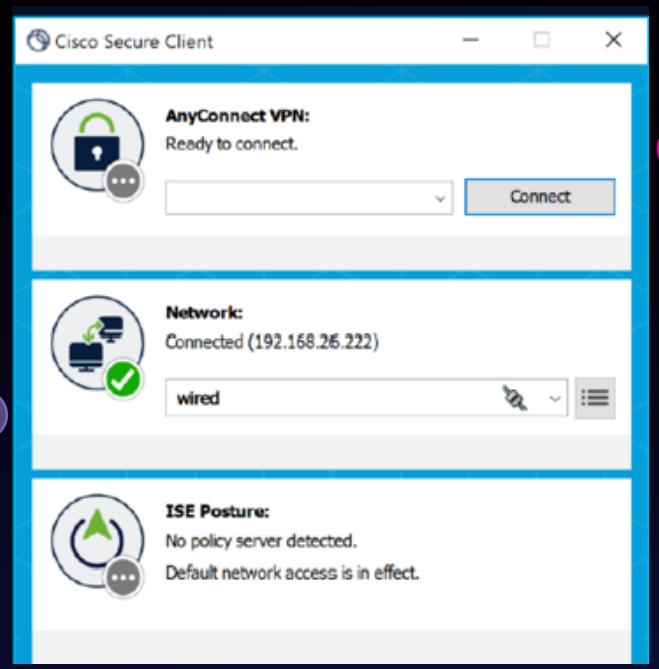
CENTRALIZED MANAGEMENT/ API

Firepower Threat Defense

Secure Client

DATA FABRIC WITH SPLUNK

Cisco Secure Client:



ANYCONNECT VPN

Remote network access

Reporting and Endpoint Telemetry

Identity and Endpoint Posture

Sovereign Private Application Services Catalog

Comprehensive Security Services

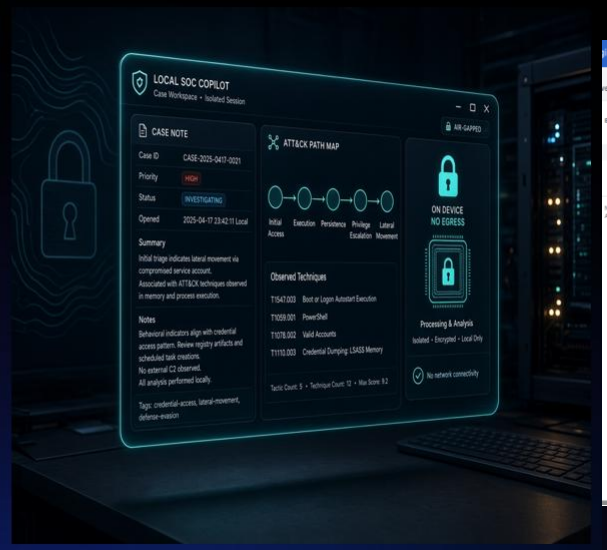
Next Generation Remote Access Services with Threat Protection

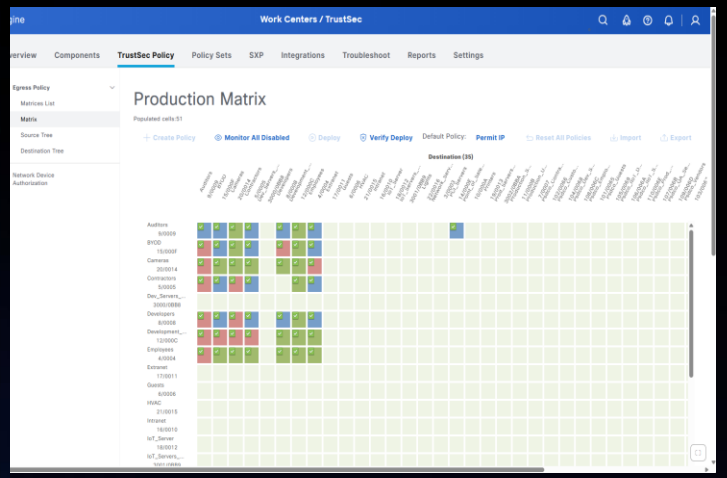
Centralized Policy Engine & Rapid Threat Containment

Rich Telemetry and Reporting & Network Detection & Response

Secure Workload Protection

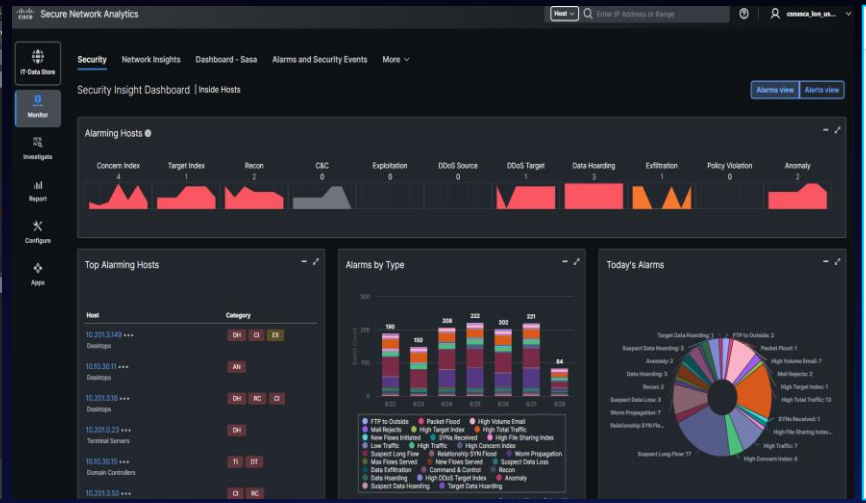
Data Analytics & Risk Reduction

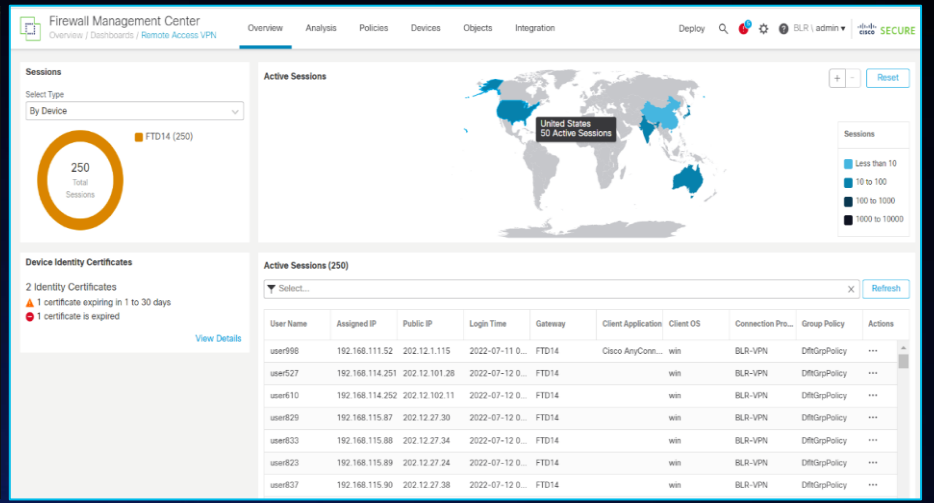












CISCO Connect

Thank you




CISCO