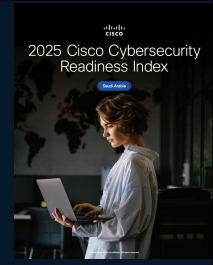
Securing Enterprise AI and Agentic Workflows with Cisco

Alexey Zhukov
Cybersecurity Regional Sales Leader
(Turkiye, Romania and CIS)

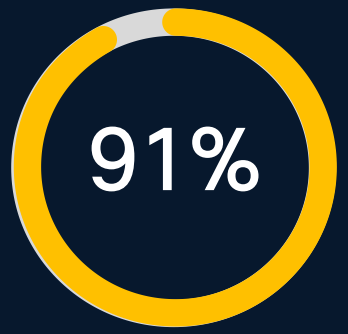
SOFTPROM SECURITY FORUM
Baku, Azerbaijan

April 2026



As companies grapple with complexities of AI

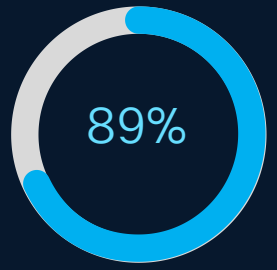
Say their organizations have experienced AI-related security incidents in the past 12 months



Organizations have experienced AI-related security incidents in the past 12 months

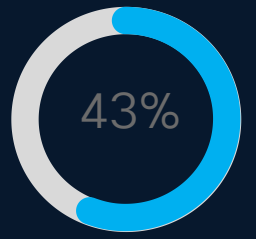
Employees are utilizing third-party GenAI tools for work through different methods

Approved, publicly available tools accessed through a security service

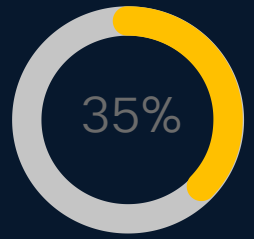


Say employees are accessing company networks from unmanaged devices

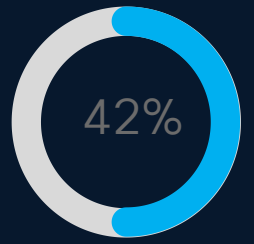
AI incidents respondents dealt within the last 12 months



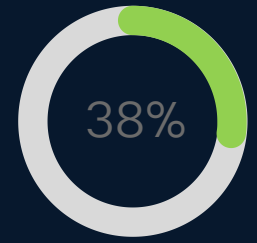
Model theft or unauthorized access



Prompt injection attacks

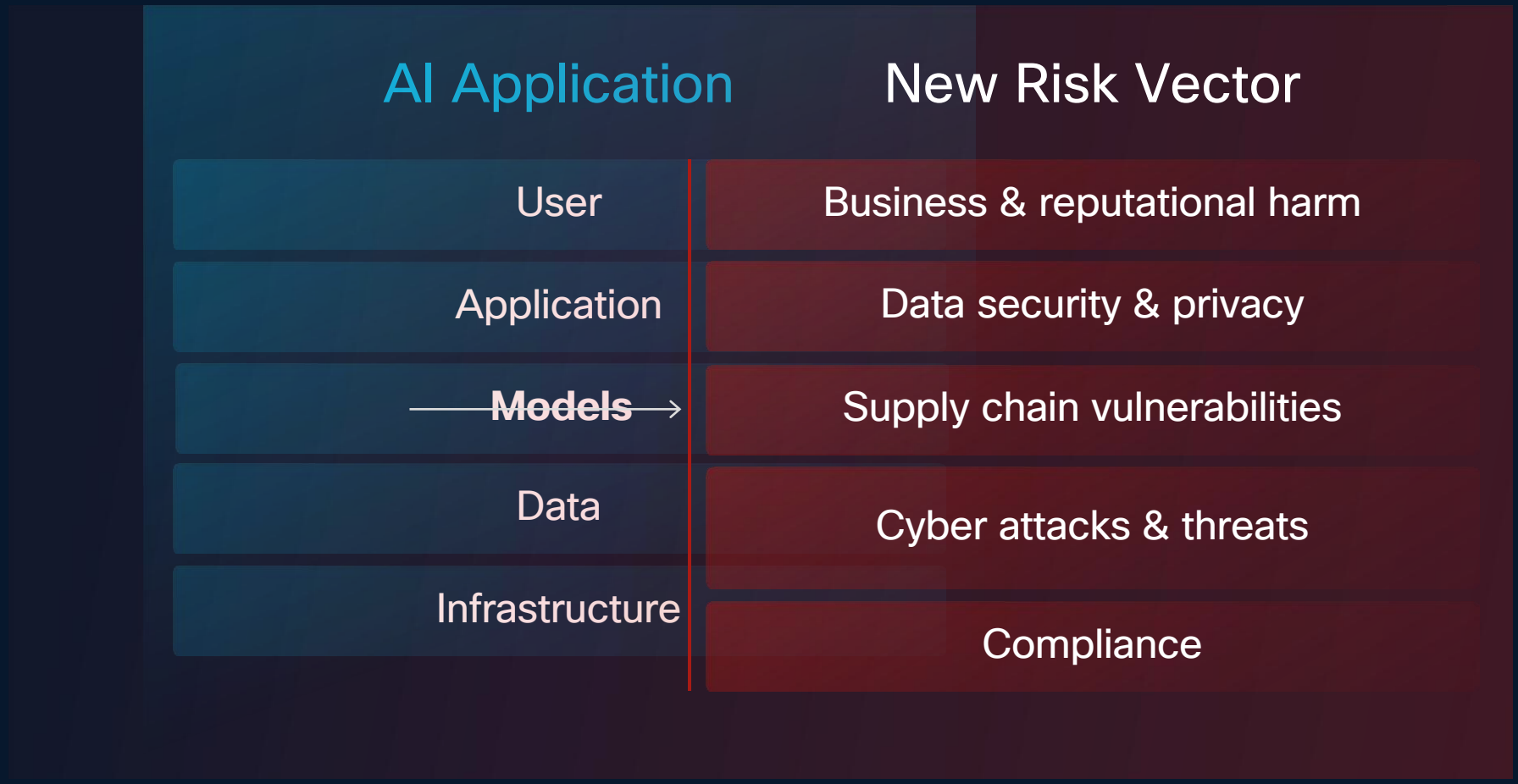


AI enhanced social engineering



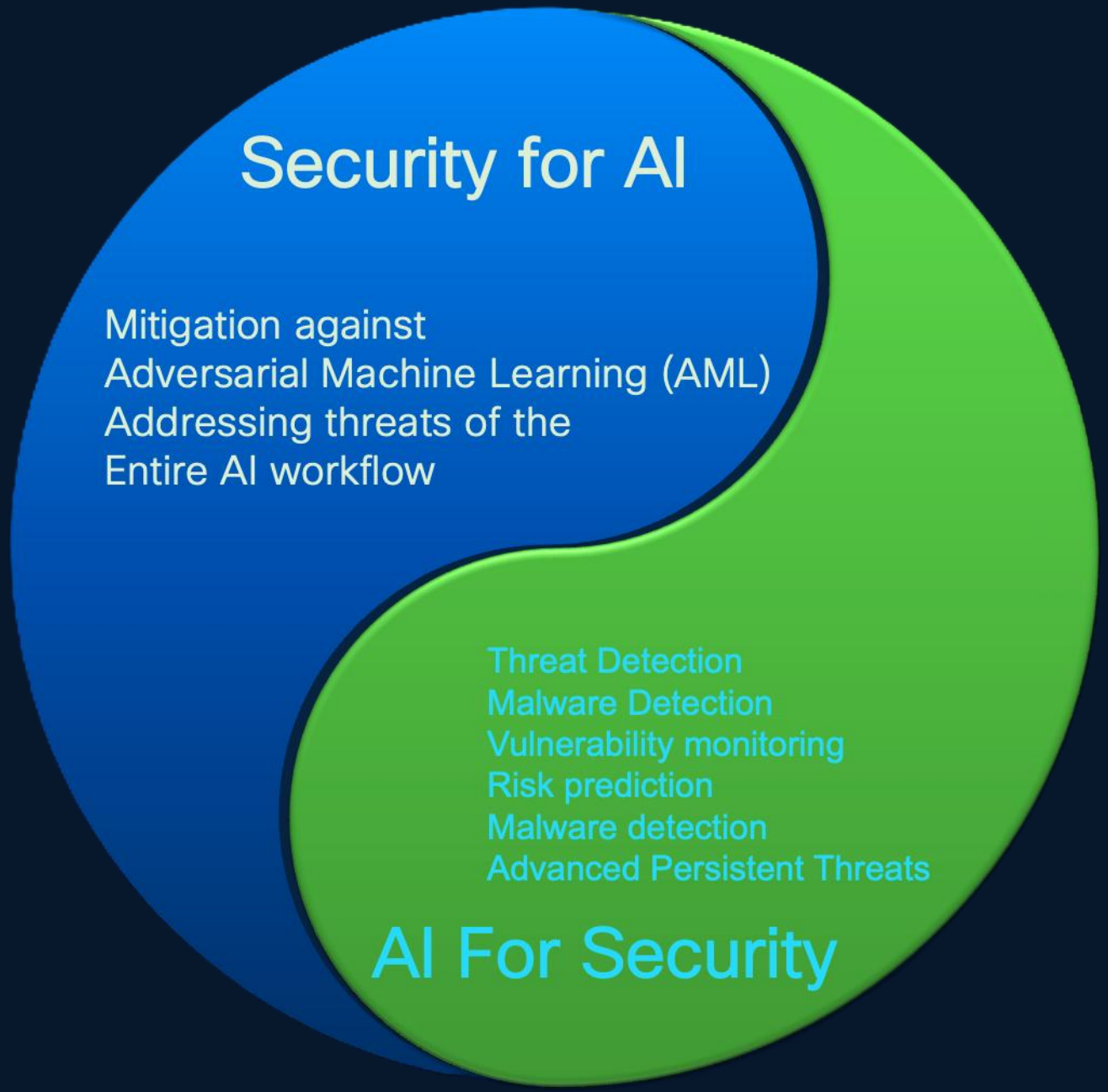
Data poisoning attempts

AI Applications Introduce a New Risk Vector



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 EXECUTION & RULES



Our Approach: Cisco AI Defense

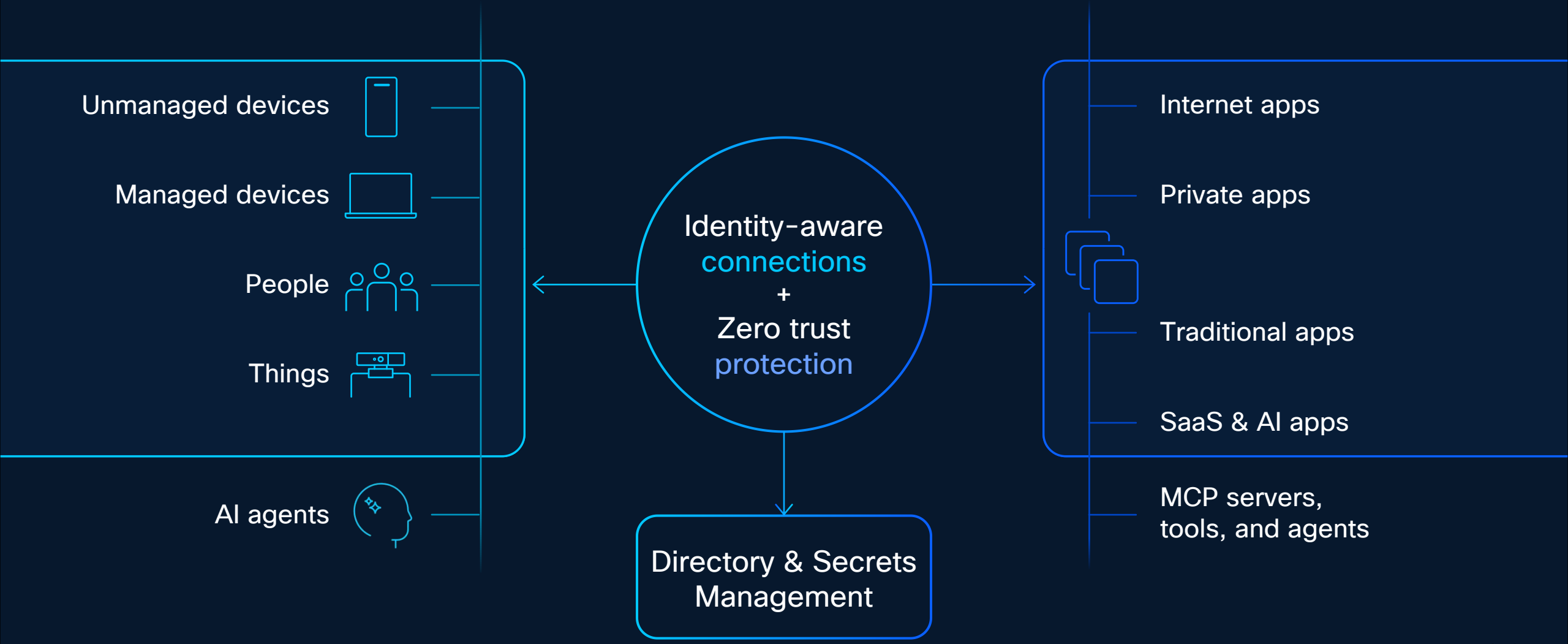
Securing AI environments across the entire lifecycle

Discover

Validate

Protect

Extending Cisco's Zero Trust Access to secure Agentic AI



KNOW EVERY AGENT | AUTHORIZE EVERY ACTION | ADAPT TO RISK IN REAL TIME

Visibility, identity, and ownership for every AI agent interacting with your environment

Agentic IAM
by Duo

- Agent & Tool Discovery
- Agent Directory
- Agent Access Policy
- Human Accountability
- Lifecycle Management

Know every agent | Authorize every action | Adapt to risk in real time

STEP 1

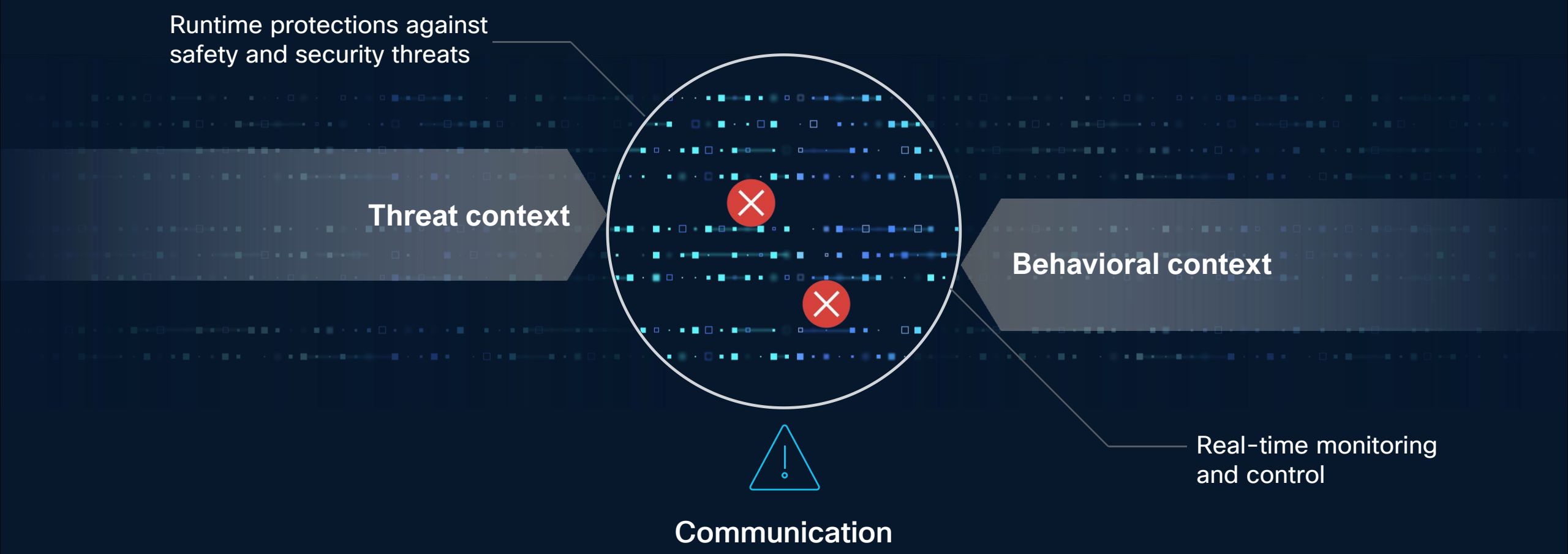
Agent Directory: discover + register + human owner + lifecycle

Fine-grained Access Controls: Consistently enforced where agents access enterprise data & tools.

- STEP 2

Use intent, threat, and behavioral context to adjust protection decisions.

• STEP 3



Protect intellectual property as it flows in and out of AI systems

Secure Access: protecting the usage of AI

Threat Visibility	Leakage Prevention	Threat Prevention
Discover and Assess Activities	DLP Inspection of Prompts/Uploads	Block Apps and Control Downloads

Discovers and controls over **70** Gen AI apps (including APIs)

AI Powered Detections Today

Breach Protection

eXtended Detection and Response (XDR)
Ransomware Recovery
Endpoint detection and response (EDR)
Email threat protection
Malware protection
Network detection and response (NDR)
Threat hunting for endpoints

XDR Risk Scores NN for MITRE ATT&CK mining

XDR Alert Summarization

XDR Global Intelligence Models

TALOS Signature Generation AutoML

User Protection

Access Management
Email Security
Remote Browser Isolation
Security Service Edge (SSE)
Endpoint Security
Experience Insights
Network Access Control

Email Threat Defense (HuggingFace, spaCy, NER)

Duo Trust Monitor Unsupervised Learning

Anomaly detection in industrial processes (IoT)

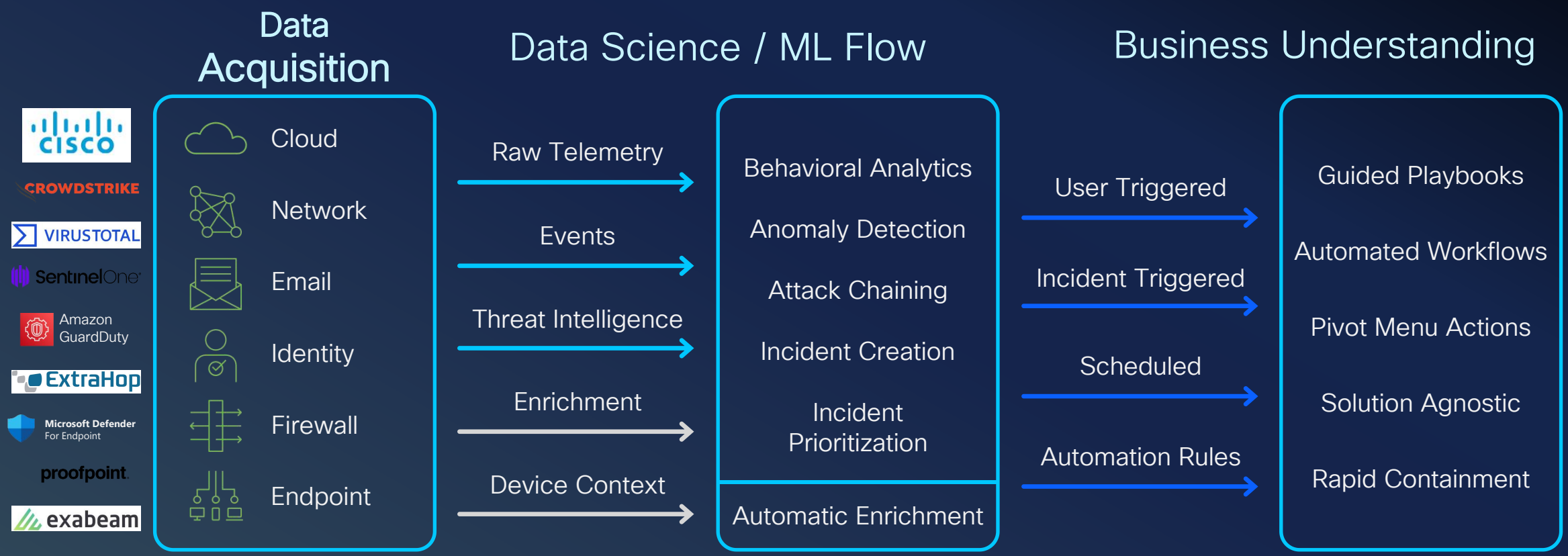
Umbrella NN (+SVM + Supervised)

Cloud Protection

Workload Security
Multi-Cloud Defense
Application Security
Attack Surface Management
Vulnerability Management

Vulnerability Management Risk Scores (VM+VI)

XDR High level architecture



Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

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%**

AI security starts with identity, access, behavior — and a unified platform

- Know every agent
- Authorize every action
- Adapt to risk in real time

The question is no longer whether AI will operate inside the enterprise.
The question is whether you will govern it on a platform – or chase it with point tools.


CISCO

Back-up slides

Encrypted Visibility Engine (EVE)

Enhanced Visibility and Detection Efficacy of Encrypted Traffic

Inferenced Based Identification without Decryption in TLS & QUIC of:

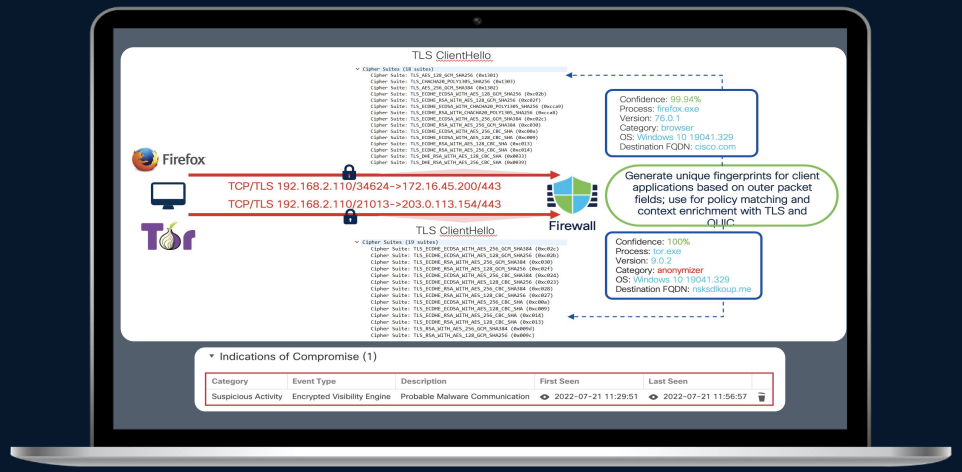
- Client Applications
- Operating Systems
- Compromised Hosts

AI @ Speed of the Network:

- Network Protocol Fingerprinting (NPF) selects classifier
- Weighted Naïve Bayes classifier with sparse updates
- Best Threat Detection efficacy in recent internal testing

Machine Learning Generated Fingerprints with data from:

- Computer Security Incident Response Team (CSIRT)
- Network Visibility Module (NVM)
- Secure Malware Analytics (ThreatGrid)



AI-powered email threat detection for stronger breach protection

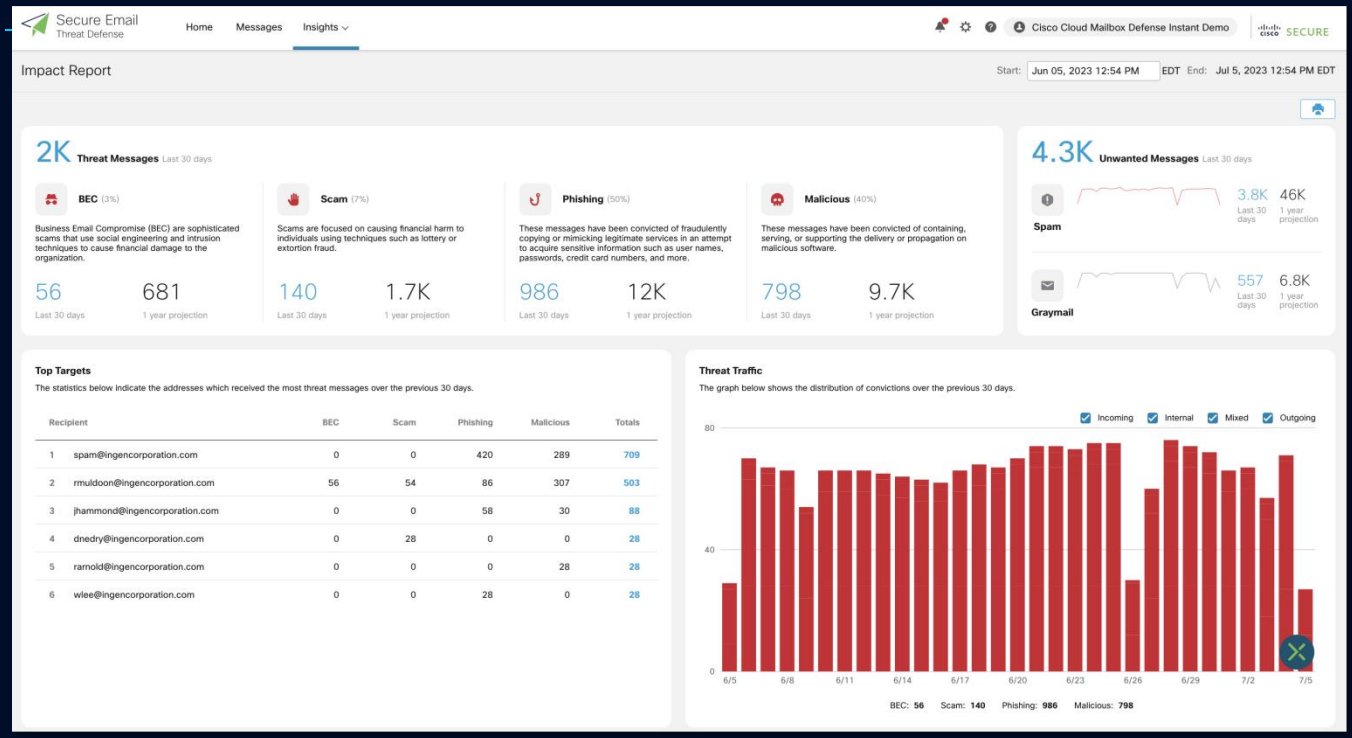
Email Threat Defense

AI-powered detections

- Uses various detectors to simultaneously evaluate different portions of an incoming email for markers of malicious intent.
- Empowers admins to act confidently and pursue more strategic initiatives.

Availability:

- Limited Availability: Now!
- GA: May 2024



The only vendor with end-to-end security embedded in the network

77%	Too many security solutions*	Cisco Security Cloud Consolidating Controls at scale
60%	Integrated multi-cloud networking and security management platform**	Cisco Security Cloud Consolidating Controls at scale
38%	Distributed workforce***	ISE, Duo, Identity Management, End to End Zero Trust
	Network most challenging to protect*	Only vendor with end to end security embedded in the network
30%	Increasing costs****	Vendor Consolidation

75% of customers considering vendor consolidation

Sources: *2025 Cyber Security Readiness Index, **2024 Global Networking Trends Report, Cisco, ***Flair HR 2025, **** Gartner 2022