Cisco Identity Intelligence

(Oort)

Cisco Partner

https://cs.co/1page

Cisco Identity Intelligence (CII) is an AI-powered solution that bridges the gap between authentication and access, enabling enterprises to quickly detect, investigate, and respond to identity threats reducing their identity attack surface. The solution is cloud-native, agentless, easy to install, and integrated with other security tools.

Benefits:

Cross-Platform Visibility:

- Identity agnostic
- Discovers the broadest identity attack surface
- Map user populations across heterogeneous IdPs & HR systems
- Agentless

High-Fidelity Identity Detections:

- Infuses identity intelligence across Cisco Security Cloud
- Low-noise identity & device detections
- Built-In AI-based behavior-based analytics and anomaly detection to accurately detect identity threats

Faster Response & Remediation:

- Provides actionable risk insights across Cisco Security Cloud empowering broad responsive measures
- One-click remediations
- 360 user & device profiling
- Integrates with XDR / existing SIEM, workflow, and communication tools

FAQs:

Q: How does Cisco Identity Intelligence work?
A: Cisco Identity Intelligence ingests data from Cisco and third-party sources and graphs the identity landscape of user, devices, services, apps, and behaviors. It then builds a behavior baseline for every identity..

Q: What can Cisco Identity Intelligence do?
A: Here is a partial list of some of the key features:

- Discovers entire identity population
- Identifies and addresses vulnerable accounts
- Eliminates unused and risky privileges
- Detect behavior anomalies
- Graduated responses to high-risk access attempts

Q: Will Cisco Identity Intelligence be an independent product?
A: For now, Cisco Identity Intelligence is an engine that will hydrate the Cisco Security Cloud with identity behavioral intelligence starting with Duo (Advantage & Premier), Secure Access and XDR.

Use Cases:

- Creating a User Inventory
- Monitoring Non-Employee Accounts
- MFA Adoption & Usage
- IAM Reporting & Analytics
- User or Session Investigation
- Continuous Threat Detection
- License Optimization

Target Customers:

Any size customer will do:

- More than one Identity Provider (IDP) is Ideal, cloud-based is important today
- Cloud Friendly

Must have Azure/Entra P1 or P2:

- Not require on Prem presence
- Can use MSFTs sync to bring AD logs into Azure for consumption by CII

Customers who already have Duo:

- It can help expand the Duo footprint

What to avoid:

- Customers with extensive on-Prem solutions installed: (PingFed, ADFS w/o Entra, or even opensource iDPs like Shibboleth)

Types of Data:

Posture Checks:

- Idle Licenses
- Inactive User Accounts
- Inactive Guest Accounts
- Weak MSF Configuration
- Unmanaged Device Access

Many more…

Threat Checks:

- MFA Flood
- Admin Impersonation
- Admin Activity Anomalies
- Compromised Sessions
- Inactive Account Probing

Many more…

Event Data:

- Sign-in / Auth logs
- Alerts
- Audit logs
- Provisioning Logs
- Risky user events

Many more….

Resources:

BDM / TDM	Oort Knowledge Base	Demo site:	Blog
At-a-Glance	FireStarter request	• *Click Log In*	Use Case Mapping
Battlecard	Identity Assessment	• *Org name:* ***genie***	Customer profiles
	Intelligene Overview	• *SSO: Use Duo account*	Public page
		• *Any Google account*	

Example SKU: **N/A, *see Duo Advantage or Premier***