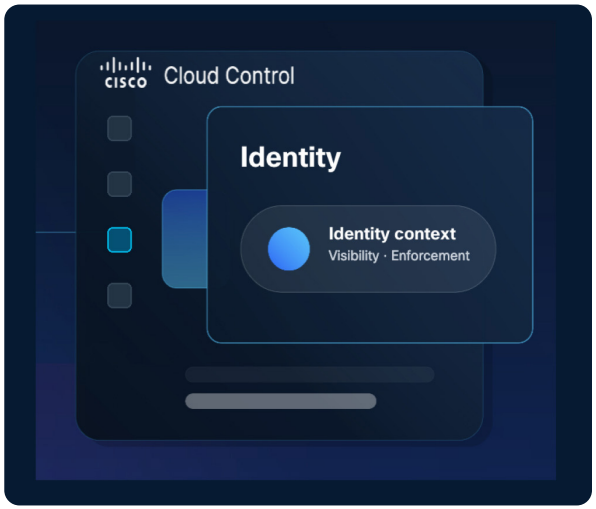
Cisco Cloud Control

Cisco Identity

Bring identity context to the network through Cisco Cloud Control

AI has turned identity ambiguity into network risk. Every unmanaged actor, credential, and privilege expands the attack surface, while AI-powered attackers can find weak credentials, stale access, exposed keys, and unprotected paths at machine speed.

For the network, the problem is direct: it often sees the connection before it understands the actor. It may see an IP address, VLAN, device, session, or flow, but not enough context to know who or what is behind it, whether it should be trusted, or what it should be allowed to reach. Cisco Identity closes that gap by making actor, posture, and risk context part of how the network understands and protects access.



The Power of Identity in the Network

The network sees activity

It connects users, devices, apps, workloads, services, and agents to the resources they need.

Identity explains the actor

Actor context shows who or what is behind access, whether posture changed, and where risk is concentrated.

Enforcement turns context into protection

Network teams can use identity context to guide policy, segmentation, and access.

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

From signal to action

Turn Identity Context Into Action

Overview

Identity in Cloud Control brings identity, device, network, application, and agentic activity into one operational view. This unified view brings together context from sources such as identity providers, endpoint security tools, developer platforms, SaaS applications, and AI-agent sources.

Capabilities

See the actors behind access

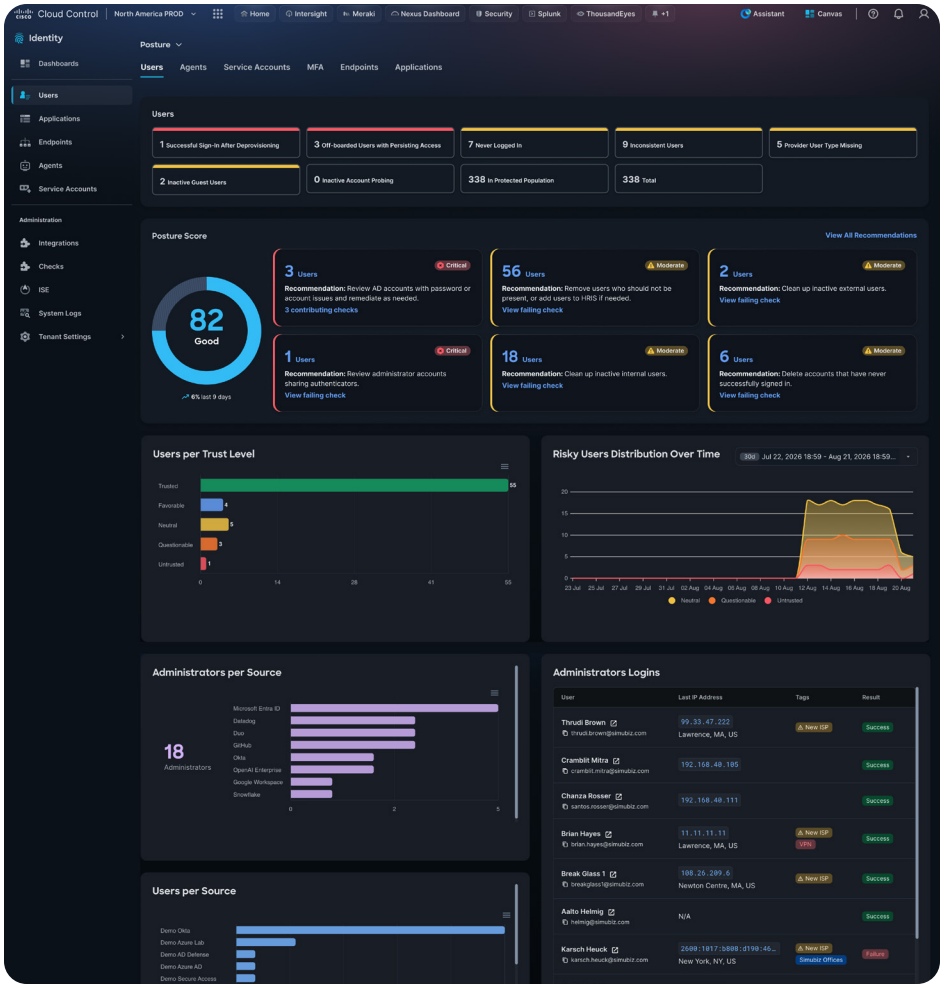
Identify humans, devices, applications, workloads, service accounts, and AI agents across Cisco and supported vendor sources.

Evaluate posture and change

User Trust Level, anomaly signals, timelines, and access context to understand which actors need attention.

Investigate and resolve with context

AI Canvas can bring identity, device, network, and application context into a guided investigation path.

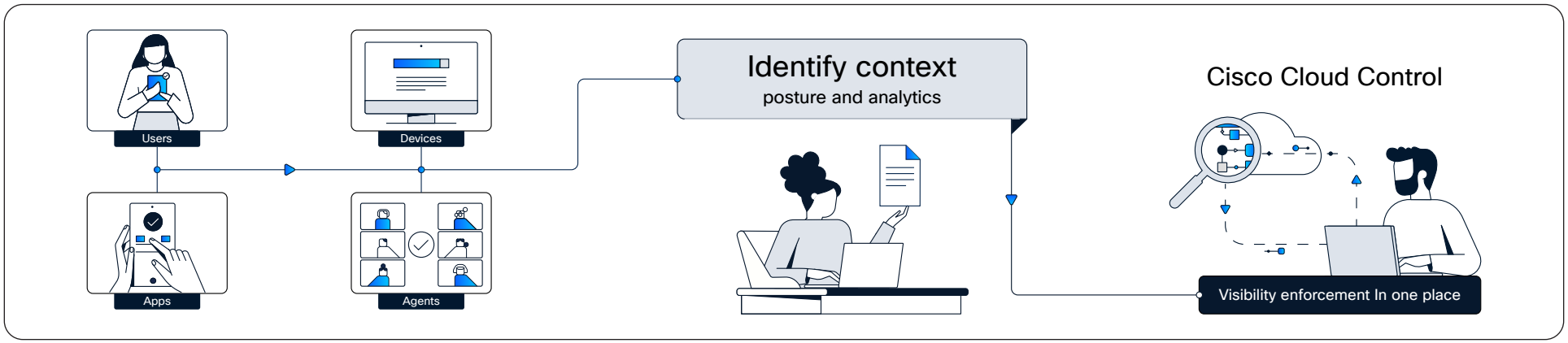


© 2026 Cisco and/or its affiliates. All rights reserved.

Identity-aware networking

Visibility Is the Starting Point. Network Enforcement Is the Outcome.

Cisco Identity is not about adding another isolated identity view. It brings actor context into Cisco infrastructure so access decisions can be informed by identity, posture, risk, and network context.



What This Makes Possible

Troubleshoot access with the full story

See identity state, device posture, network access, recent activity, and application context together.

Reduce blind spots across human and non-human identities

Bring service accounts, agents, endpoints, and application activity into the same operating conversation.

Prepare the network to make identity-aware decisions

Use actor context in Cisco Cloud Control to guide protection, segmentation, and exposure reduction.

© 2026 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)
C45-6677428-00 10/26