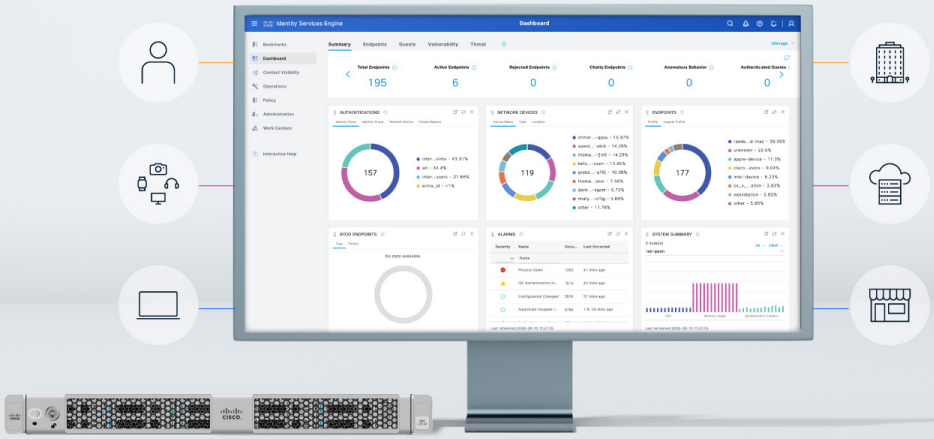
Cisco Identity Services Engine (ISE)



Key Benefits

- **See everything that connects to your network**—from users and devices to IoT endpoints
- **Enforce identity-driven policy** that follows users and devices anywhere
- **Reduce risk by limiting lateral movement** across your network
- **Extend Zero Trust protection across your entire network**—not just application access
- **Continuously enforce compliance, verify trust and respond to threats in real-time**

"Cisco ISE gives us the visibility and control we need to confidently support a secure, flexible workplace."

– IT Security Leader, Global Enterprise

Verify identities. Enforce least privilege. Contain threats.

As enterprise networks expand across campus, branch, edge, and cloud—and the number of connected users, devices, and IoT endpoints grows—securing network access is becoming increasingly complex.

With users and devices constantly moving, traditional access control methods based on network location, such as VLANs and IP addresses, built for static environments, no longer reliably identify who or what is connecting. Likewise, Zero Trust Network Access (ZTNA) solutions that primarily control access to applications are often created with broad scope, that do not prevent threats from spreading inside the network. As a result, policy is often limited to specific domains and enforced only at the point of network access. Once connected, users and devices can move laterally; expanding the attack surface and making it harder to continuously verify trust, enforce consistent access, and respond to threats.

Cisco Identity Services Engine (ISE) gives you centralized, identity-driven access control across your network. It continuously verifies users and devices, enforces context-aware access policies, and delivers consistent control across wired, wireless, and VPN environments. By shifting access decisions from network location to identity, Cisco ISE helps you adapt to changing risk and enforce Zero Trust at scale, extending protection beyond application access to control how users and devices move across your network.

With a unified platform for visibility, segmentation, and threat response, Cisco ISE helps you reduce risk, simplify operations, and enforce Zero Trust at scale.

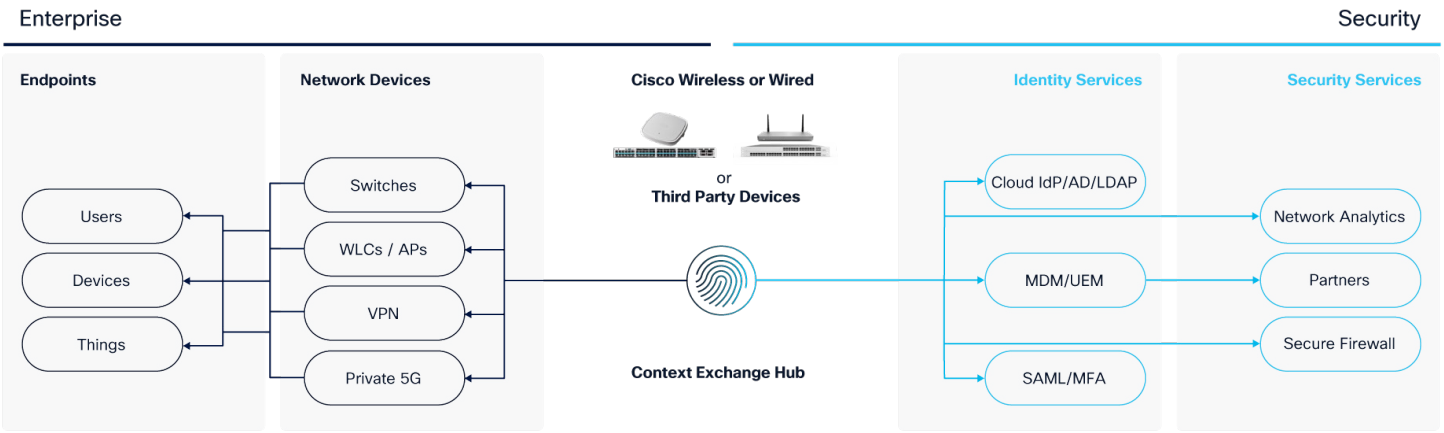


Figure 1. Cisco ISE - The Bridge between Networking and Security

Make Identity the Core of Network Access, Segmentation, and Trust

Cisco ISE goes beyond traditional network access control by making identity the foundation for access, segmentation, and threat response across your network.

- **Flexible deployment with faster time to value.** Deploy across on-premises and cloud environments to enable simplified onboarding and reduce operational overhead
- **True visibility without agents.** Discover and profile users and devices—including managed, unmanaged, and IoT devices, using AI-driven analytics without requiring endpoint software
- **Identity-based segmentation that scales.** Use Security Group Tags (SGT) to control how users and devices communicate—so policy follows them everywhere-campus, branch, data center, and cloud
- **Enforce least-privilege access and continuously verify trust** throughout the session, not just at the point of authentication—regardless of the access method (wired, wireless, VPN or cellular)
- **Dynamically isolate threats across your security ecosystem.** Share identity and device context with 70+ security solutions to automate detection and response—turning insight into immediate action

Move beyond basic access control to identity-based segmentation and real-time threat response.

Discover how Cisco ISE helps you stop lateral movement dynamically, enforce consistent policies, and extend Zero Trust protection across your entire network—while simplifying operations.

Request a demo or learn more at: https://www.cisco.com/go/ise