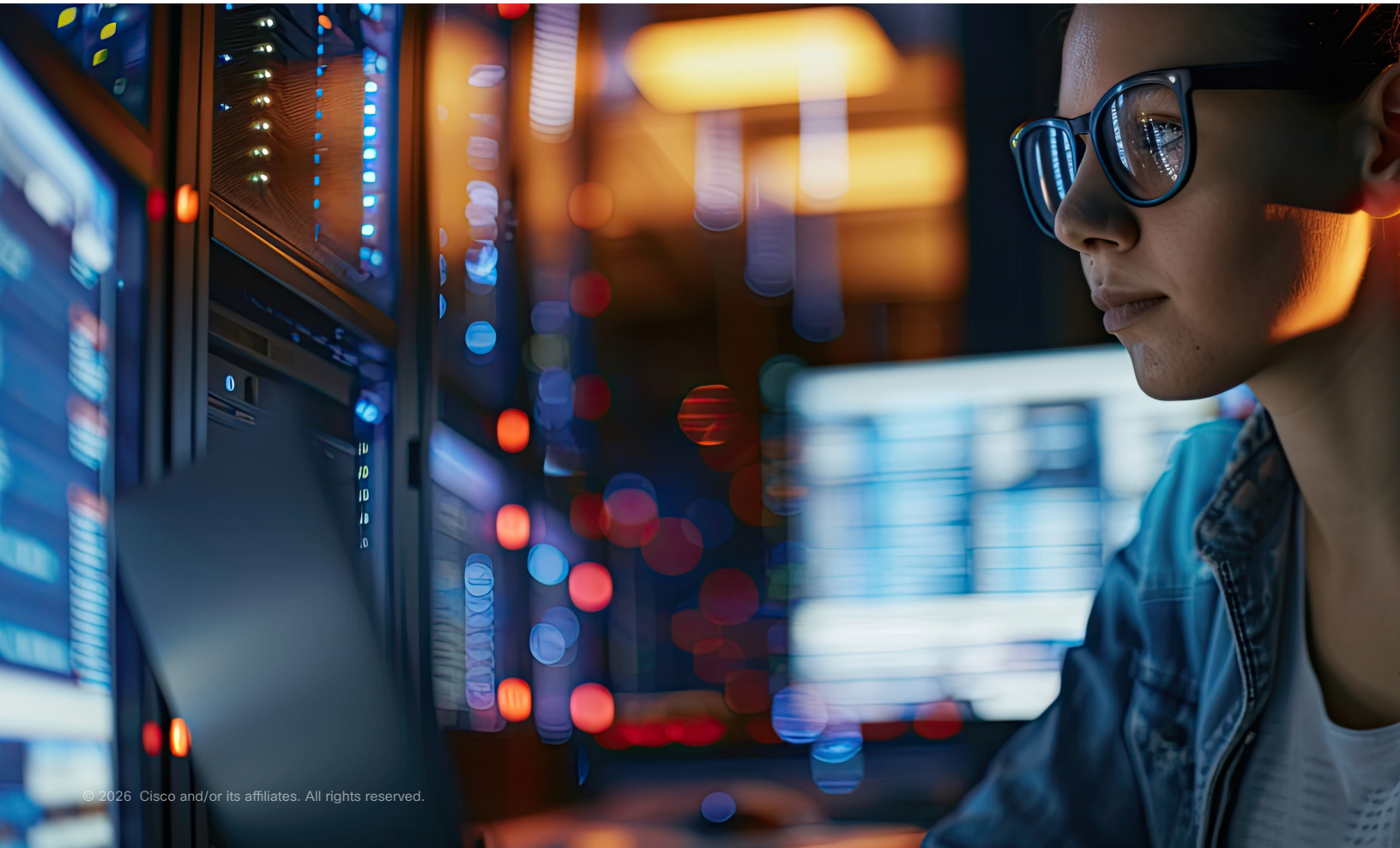
Cisco Identity Services Engine (ISE)

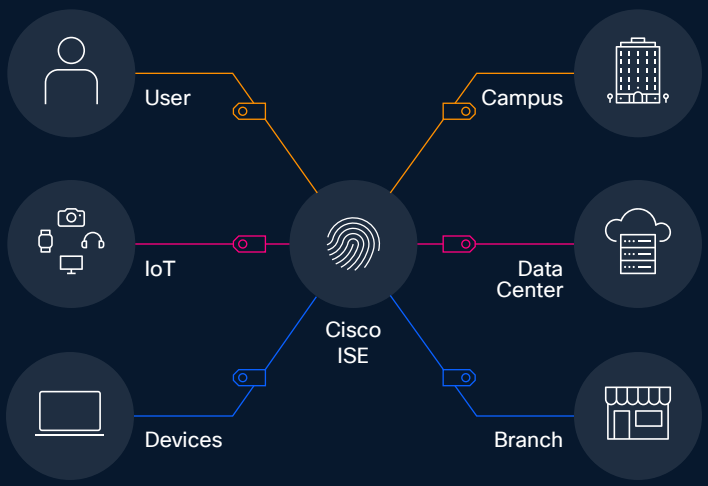
See everything that connects, control what happens next



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

Cisco ISE gives you the visibility, context, and enforcement to make precise, real-time decisions—so you can continuously verify trust and control every connection across your hybrid environment.

Networks are more dynamic than ever, with users, devices, and IoT endpoints connecting across wired, wireless, VPN, and cloud environments. Yet visibility remains fragmented, identity context is incomplete, and enforcement is often inconsistent. Most solutions focus only on granting access—leaving a critical gap in controlling what happens after connection.



Cisco Identity Services Engine (ISE) bridges this gap by unifying visibility, identity, and enforcement into a single platform. It discovers and profiles every user and device—including unmanaged and IoT devices—without requiring agents, then enriches that data with identity context from across your ecosystem.

With this foundation, Cisco ISE continuously verifies trust and enforces least-privilege access—not just at the point of entry, but throughout the entire session. It extends control beyond access using identity-based segmentation, ensuring users and devices only communicate as intended. The result: stronger security, reduced risk, and a complete Zero Trust posture across your hybrid network.

Figure 1. Cisco ISE as a centralized identity-based control plane across hybrid environments

Trends and challenges

Fragmentation Across Identity, Visibility, and Enforcement Is Slowing Security Outcomes

Rising Complexity Slows Zero Trust Maturity

As organizations adopt Zero Trust frameworks such as NIST and CISA models, many remain stuck in early stages of maturity. Initial efforts often prioritize identity and access, but advancing to continuous verification and adaptive, policy-based control across the entire environment is far more difficult.

A primary obstacle is fragmented identity. Identity data is distributed across directories, MDMs, CMDBs, and security tools—with little real-time exchange of context. This creates inconsistent and incomplete identity context, limiting the ability to make accurate, risk-aware decisions. Without a unified identity foundation that can drive enforcement, Zero Trust cannot evolve beyond basic access control.

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

SSE and SASE Improve Access—But Not Full Network Control

SSE and SASE architectures including ZTNA solutions have become central to securing application access, especially for remote and hybrid users. However, they primarily focus on north-south traffic and application-layer control. They provide limited visibility into unmanaged and IoT devices and lack the ability to govern how users and devices interact within the network (east-west traffic).

Traditional NAC solutions were designed for static, location-based environments. They rely on IP addresses and VLANs to enforce access at the point of connection but lack the flexibility to adapt to dynamic, hybrid environments or to enforce policy consistently beyond initial access.

As a result, organizations often deploy multiple disjointed solutions— each solving part of the problem but none providing unified, continuous control. Visibility, identity, and enforcement remain fragmented across these solutions and operate independently. Without a common control plane, context is lost between systems.

The Missing Link: Identity-Driven Enforcement

When identity, visibility, and enforcement are not unified, policy becomes inconsistent and reactive. Enforcement points lack full context, policies don't follow users and devices, and response actions are delayed or manual.

To reach higher levels of Zero Trust maturity, organizations must move beyond isolated capabilities and make identity the foundation for continuous, network-wide control. Without this, the gap between access and control persists—leaving networks exposed to lateral movement, operational complexity, and increased risk.

Market Insights

Recent industry research shows that while organizations are investing heavily in identity and segmentation, most still operate with fragmented tools—limiting their ability to turn insight into real-time enforcement.

Identity sprawl creates operational complexity

IT and security teams use an average of 5 tools to resolve a single identity issue—highlighting how identity, visibility, and enforcement remain fragmented across systems.

Limited visibility leads to identity risk

75% of organizations lack full visibility into identity vulnerabilities, and 94% say identity complexity reduces overall security, making it harder to make accurate, risk-based access decisions.

Segmentation is a priority—but hard to scale

79% of organizations identify segmentation as critical, yet only 33% have fully implemented segmentation across their environments, citing complexity and lack of visibility as key barriers.

Disconnected tools delay response

Only 52% of organizations have fully integrated identity and device telemetry, leaving nearly half without the unified context needed for accurate, real-time policy enforcement.

Identity Gaps Are Driving Financial Losses

More than 50% of organizations have experienced financial losses from identity-related breaches, demonstrating that gaps between detection and enforcement have real business consequences.

The takeaway:

Organizations are not lacking tools—they are lacking integration. When identity and segmentation operate in silos, policies are inconsistently enforced, threats spread more easily, and response is delayed. Unifying identity, visibility, and enforcement into a single control plane is essential to reduce risk, limit lateral movement, and achieve Zero Trust at scale.

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

How it works

Unify visibility, identity, and enforcement into a single control plane.

Cisco Identity Services Engine (ISE) unifies visibility, identity, and enforcement into a single, network-wide control plane. By connecting context to action, it ensures policy is applied consistently—before, during, and after access—across your entire hybrid environment.

True visibility without agents

ISE discovers and profiles every user, device, and IoT endpoint—including unmanaged assets—using AI-driven analytics and behavioral profiling. This agentless approach eliminates blind spots and accelerates time to value without requiring endpoint software.

One identity-driven control plane, across your network

Cisco ISE builds a unified identity context by integrating with directories, MDMs, and asset systems. Policies enforced across campus, branch, data center, and cloud, based on identity and device posture—not just location—eliminating gaps between environments.

Consistent enforcement and continuous verification

Whether access is established through wired, wireless, cellular, VPN, or ZTNA, Cisco ISE acts as a centralized policy engine—ensuring consistent enforcement across on-premises and cloud environments while continuously verifying trust throughout the session, not just at the point of authentication.

Identity-based segmentation at scale

Using Security Group Tags (SGT), ISE controls how users and devices communicate across campus, branch, data center, and cloud. Policy follows the identity everywhere removing the need for complex network redesigns and significantly reducing lateral movement.

Automated threat containment

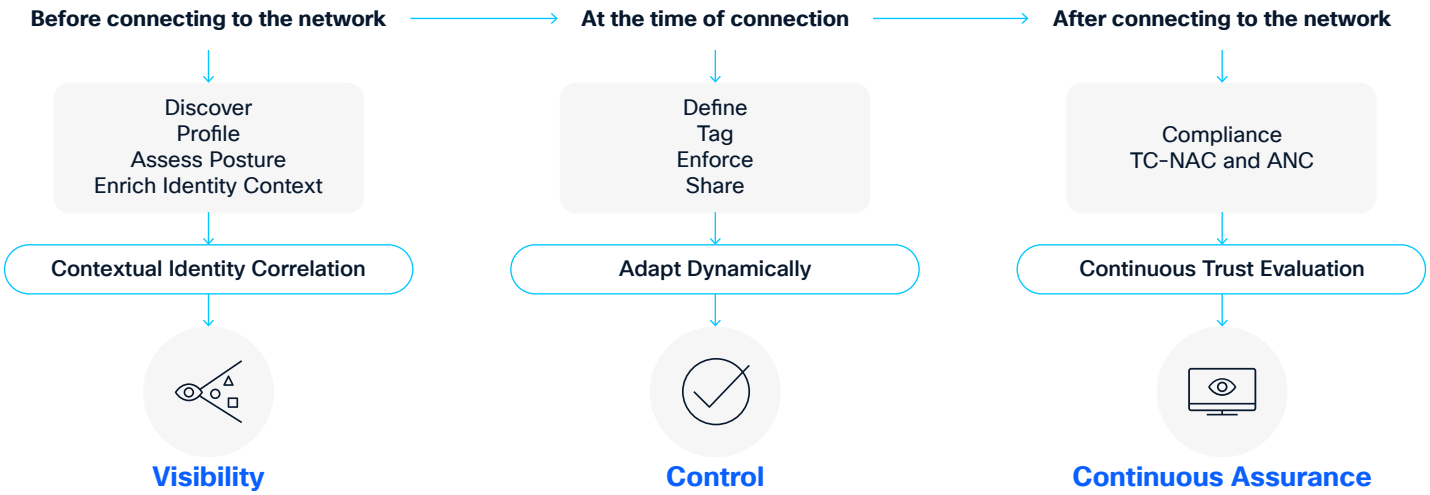
ISE shares identity and device context with 70+ Cisco and third-party security solutions through pxGrid integration. This enables automated, network-based response—allowing faster threat isolation and preventing further spread.

Flexible Deployment with Faster Time to Value

Cisco ISE supports deployment across on-premises and cloud environments, giving you the flexibility to align with your architecture and operational model. Its agentless approach simplifies onboarding, reduces operational overhead, and accelerates time to value.

With Cisco ISE, you move beyond fragmented access control to a unified approach that reduces risk, limits lateral movement, and simplifies operations—while delivering consistent, scalable security across your entire network to enable Zero Trust outcomes.

Figure 2. Continuous visibility and enforcement lifecycle



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

Benefits

- **See everything that connects.**
  Gain complete visibility into every user, device, and IoT endpoint, including unmanaged devices—eliminating blind spots across your environment
- **Make identity your control plane.**
  Replace rigid, location-based controls (VLAN/IP) with dynamic, identity-driven policy that follows users and devices, and adapts to changing risk
- **Reduce risk and limit lateral movement.**
  Control how users and devices interact across your network to minimize exposure and reduce breach impact
- **Extend Zero Trust protection across your network.**
  Go beyond application access to enforce consistent policy before, during, and after access—across every connection and interaction
- **Continuously verify and stay compliant.**
  Enforce least-privilege access at all times and automatically contain threats while sharing identity context across your security ecosystem to coordinated response and support compliance

Use Cases

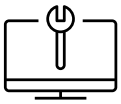
Apply identity-driven control across complex and real-world environments.

Figure 3. Cisco Identity Services Engine use cases across various industries

Industry	Use case description
Enterprise IT	Enforce consistent identity-based access across wired, wireless, and VPN users while segmenting sensitive resources to reduce lateral movement.
Manufacturing	Protect OT environments by segmenting industrial devices and controlling communication between IT and OT networks.
Healthcare	Secure unmanaged medical devices and IoT endpoints while ensuring compliant access to patient data systems.
Financial Services	Enforce least-privilege access and segmentation to meet regulatory requirements and prevent data breaches.
Any Industry	Enable Zero Trust by continuously verifying identity and enforcing policy across hybrid environments.

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

Business Value: Drive Measurable Outcomes Across Teams



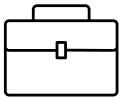
For IT teams

- Simplify operations with a centralized policy engine across wired, wireless, VPN, and cloud
- Reduce complexity by eliminating VLAN/IP-based segmentation and manual configurations
- Accelerate onboarding and reduce overhead with agentless visibility and flexible deployment



For Security Teams

- Enforce least-privilege access with continuous verification across all users and devices
- Reduce attack surface and limit lateral movement with identity-based segmentation
- Accelerate threat detection and response through automated containment and ecosystem integration



For Business Leaders

- Reduce financial risk by preventing and containing breaches more effectively
- Support compliance with consistent, auditable policy enforcement across environments
- Enable secure business agility—supporting hybrid work, IoT, and cloud adoption with confidence

Services: Accelerate Time to Value and Strengthen Outcomes with Cisco

Deploying identity-based access and segmentation at scale requires the right strategy, integration, and operational alignment. Cisco Services helps you successfully plan, implement, and optimize Cisco Identity Services Engine (ISE)—so you can achieve faster time to value and stronger security outcomes.

Cisco experts work with you to assess your current environment, identify gaps in visibility and policy, and design an architecture aligned to your Zero Trust goals. During deployment, Cisco helps integrate ISE with your existing infrastructure—including directories, MDMs, and security tools—ensuring consistent identity context and enforcement across your environment. Beyond deployment, Cisco Services helps you operationalize continuous verification, segmentation, and automated response. With ongoing optimization and best practices, you can simplify operations, improve policy accuracy, and adapt to evolving threats and compliance requirements.

The result is a faster, more predictable path to Zero Trust—reducing risk, minimizing disruption, and ensuring your investment in Cisco ISE delivers measurable, long-term value.

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

Cisco Advantage

Only Cisco delivers end-to-end identity-driven control across your network.

Cisco ISE turns identity into a true network-wide control plane. It is uniquely integrated across Cisco's networking and security portfolio—including Catalyst, Meraki, SD-WAN, and ACI, as well as Secure Access (SSE), Secure Firewall, Duo, XDR, and Hypershield—to share identity context and enforce policy consistently across every environment. With integration across 70+ Cisco and third-party security solutions, ISE connects visibility to enforcement in real time—delivering unified, continuous Zero Trust control across campus, branch, data center, and cloud in a way that siloed point solutions cannot achieve.

Take control of your network with identity at the core

See everything that connects and control how it communicates—extending Zero Trust across your entire hybrid environment. Learn more or request a demo at: **https://www.cisco.com/go/ise**

© 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)

P1707012506 07/26