The bridge to possible

# Cisco Identity Services Engine (ISE)

Flexibility and choice power security resilience for zero-trust architectures

The bridge to possible

Organizations continue to be vulnerable to unauthorized devices and individuals obtaining access to their networks via unapproved connections. That's because hundreds of devices are connecting to your network every day. The simple fact is that many of these devices aren't meeting the proper qualifications to make sure that they're right for your network. Malware, bad actors, devices lacking the proper security can all leave your data—your most prized possession—at severe risk of being compromised.

## Resilience begins with a zero trust strategy

When you have clear visibility into everything that's trying to connect to your network and a consistent and secure policy that can be deployed automatically and be trusted to authenticate and authorize devices to allow network connection, you have fought the bulk of the battle. Continuously checking to make sure that not only the right devices are connecting to the network, but also the right end users are connecting is incredibly important.

But how do you make sure that these people and devices are the right ones for your network and do so on a continuous basis? This avalanche of devices is much too large from one team—never mind one person—to make sure that all are properly authorized and authenticated. Help is needed to make sure that the security of the network is consistent and strong over all areas.

Many customers aren't aware how many devices running on their network are unprotected, unmanaged and have unauthorized access.

This is especially true with IoT devices because they aren't built with a tough security as its number one job. A zero trust strategy strengthens that security by not providing network access until trust is established through authentication.

There are also non-critical assets being given unrestricted access, usually by default. This is due to endpoints being provisioned outside of IT. This is a problem because it's not what the endpoint has access to but what has access to the endpoint. Zero trust confines access to essential services through network segmentation based on least privilege. In other words, resources are only given based on what they need to accomplish.

The problem with compromised endpoints is that they tend to infect other assets on the network. Zero trust not only continues to evaluate trust, but it also isolates threats in real time.

More than the industry's only complete Network Access Control (NAC) solution

Cisco ISE is also the cornerstone of a tenacious zero trust strategy that helps enable secure access for user and devices within apps, across network and clouds. Zero trust needs to be embedded across the fabric of a multi-environment IT for a user experience without compromise.

In addition to a strong zero trust strategy, Cisco ISE gives customers the flexibility and choice they require to tether NAC workloads to multiple clouds and maintain business continuity through uncertainty. Customers gain a modernized way to deploy NAC services. Moving from managing infrastructure in a box to leveraging Infrastructure as Code (IaC) across hybrid deployments, teams can accelerate the delivery of pervasive visibility and dynamic control to secure access across the distributed network and preserve the integrity of the business.

The bridge to possible

## Benefits

- **Fully mature zero trust:** Integrate intelligence from across your stack into policy enforcement points throughout the network for continuous trusted access.
- **Security resilience:** Rapidly deploy Network Access Control workloads across multiple clouds and achieve security resilience for the self-managed infrastructure.
- **Pervasive visibility and dynamic control:** See, know, and control what is connecting to your network and ensure their posture doesn't jeopardize your business.
- **Automated threat containment:** Don't just block threats—remove them with integrated intelligence into enforcement points within the network.
- **Merge speed and agility:** Move Ops from managing infrastructure in a box to Infrastructure in Code (IaC) with automated deployments to accelerate secure network access.

## In today's connected world

### Uncertainty has become the new normal

Because change comes faster than ever, businesses are making massive investments across the enterprise to strengthen resilience. From financial resilience to operations resilience, from organizational to supply chain resilience, these initiatives are designed to help businesses operate in the new normal. And these investments will fall short without security resilience because security cuts through every aspect of these initiatives. Security resilience is the ability to protect the integrity of every aspect of your business to withstand unpredictable threats, or changes, and then emerge stronger.

### Resilience begins with securing the network connection

If organizations are to be resilient, they require flexibility and choice in deploying secure Network Access Control services to protect the integrity of the business amidst unpredictable threats and change. To emerge stronger from security incidents, pervasive visibility and dynamic control into users and endpoints connecting to network resources is a top concern for IT as they secure network access across multiple environments.

The bridge to possible

"We now have better visibility, more granular segmentation, better policy enforcement, and better identity and access management."

CIO, Financial Services Organization

From the commissioned study conducted by Forrester Consulting on behalf of Cisco, March 2022, "The Total Economic Impact™ of Cisco Identity Service Engine (ISE)"

Read the report

## Reducing risk, and emerging stronger

As uncertainty breeds risk, resilient organizations are reducing risk by closing the gaps between siloed solutions and looking to activate intelligence across the entire security stack. Integrated intelligence with a platform approach enables continuous trusted access that goes beyond building trust just at authentication and provides security throughout the entire session for mature zero-trust architectures.

## IT is Hybrid—Don't forget your infrastructure in your network security

The hybrid reality of IT is driving resiliency. Organizations are demanding solutions that provide the flexibility and choice they need to tailor deploying network resources in line with reducing risk. In addition, the self-managed infrastructure remains a critical environment for IT as they look to secure their most prized IT assets from unknown threat vectors and enable the connect-from-anywhere and connect-on-anything workforce.

## How Cisco ISE enforces Zero Trust

Connecting trusted users and endpoints with trusted resources

### Endpoint request access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

### Trust continually verified

- Continually monitors and verifies endpoint trust level
- Vulnerability to identify indicators of compromise
- Automatically updates access policy

The bridge to possible

"Without ISE, we would be spending a lot more time helping people connect. Now, we can diagnose 90% of the problems in 10 minutes. Doing it the old-school way would have taken a lot more time."

**Network engineering services assistant director,** Higher education

From the commissioned study conducted by Forrester Consulting on behalf of Cisco, March 2022, "The Total Economic Impact™ of Cisco Identity Service Engine (ISE)"

Read the report

## Cisco ISE

**Endpoint classified, and profiled into groups:**

- Endpoints are tagged w/SGTs
- Policy applied to profiled groups based on least privilege

**Endpoint authorized access based on least privilege:**

- Access granted
- Network segmentation achieved

## How it works

Cisco Identity Services Engine (ISE) activates intelligence from across the security stack to become the policy decision point in a zero-trust architecture for the workplace. Cisco ISE enables an automated approach to discover, profile, authenticate, and authorize trusted endpoints and users connecting to the self-managed network infrastructure, regardless of access medium. Cisco ISE has maintained market dominance for over ten years with its unique ability to receive and share context from the network as well as integrate intelligence. With integrated intelligence, Cisco ISE builds zero-trust policy decision points into the network for continuous trusted access and automated threat containment.

Network administrators can develop and maintain dynamic risk-based polices to ensure that only trusted users and devices gain access to trusted resources, moving protection beyond authentication and maintaining trust throughout the entirety of the session.

With Cisco ISE, organizations are confidently moving from a point solution approach that only solves for a single, immediate "compliance task" and aligning to strategic business objectives with a zero-trust policy enforcement platform that will handle what's now, and what's next, in the self-managed infrastructure.

## Use cases

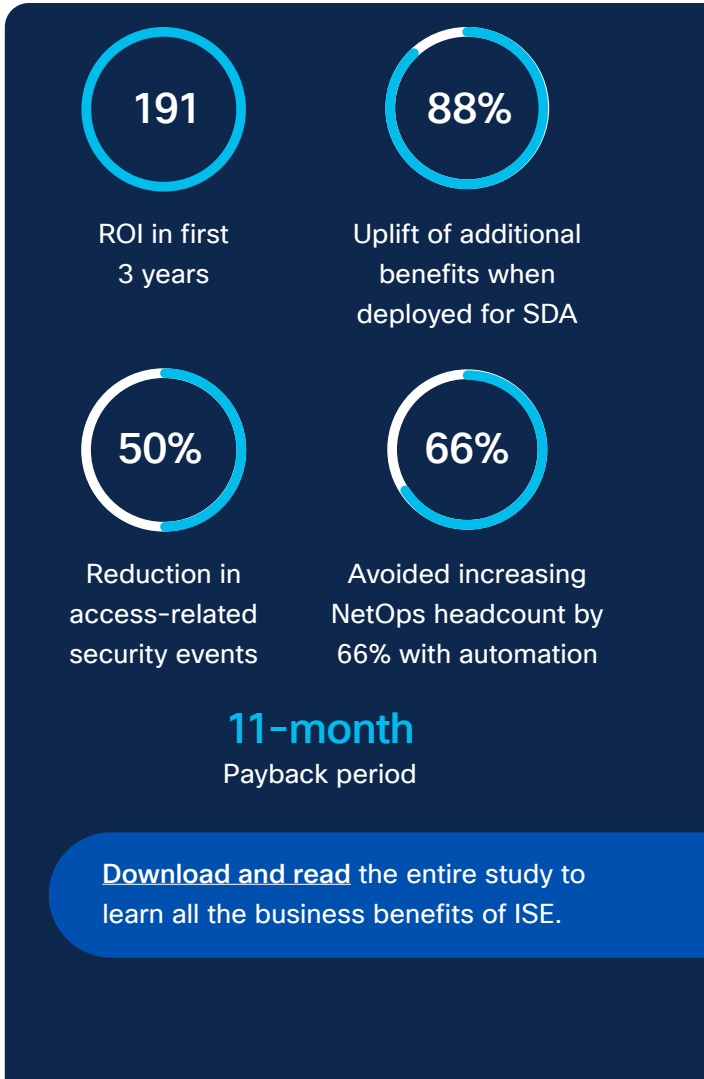
Cisco ISE addresses these challenges with a broad set of mission-critical Network Access Control (NAC) use cases to support zero trust across the distributed network.

- **Pervasive visibility:** See and know everything connecting. The first step to building a resilient security posture is gaining the ability to see and know everything that is connecting to the network. Cisco ISE automates the discovery of devices connecting to the network. With Cisco ISE, teams can identify, classify, and track

endpoints connected to the network to allow the automation of policy provisioning before allowing access to network resources. IT teams have the flexibility they need to balance business objectives with security and can choose between an agent or agentless approach to gain the visibility required to look deep into the device and ensure endpoint compliance. Any changes to the overall posture of any endpoint automatically and dynamically updates the policy to control access, ensure compliance, reduce risk, and contain threats.

- **Dynamic control:** Confidently build security into your network with visibility-driven network segmentation. Network segmentation builds zero trust into the network with policy-based access to contain and prevent the lateral movement of threats. Organizations can shrink the attack surface, limit the spread of ransomware, and enable rapid threat containment, all while continually assuring this level of protection will not disrupt business outcomes.
- **Automated threat containment:** Don't just block threats—remove them. Cisco ISE integrates with Cisco Security products and third-party ecosystem partners through pxGrid and pxGrid Cloud to gain contextual information from onprem and cloud-native solutions. This open integration ecosystem brings an active arm of policy enforcement into your security stack to automate threat containment, remove threats, and reduce mean time to repair.
- **Endpoint compliance:** Business continuity relies on a strong, resilient security posture. ISE continually verifies that device posture complies with your security policy so that risky, unpatched, and outdated devices cannot threaten the network. Cisco ISE 3.x increases organizational posture with a customizable approach to gaining continuous posture assessments for endpoints connecting to your managed infrastructure. With a limitless number of posture checks, customers can now customize and enforce dynamic policy and gain continuous trusted access to ensure business resiliency, while limiting organizational risk without disrupting business objectives.
- **Secure access:** Accelerates value by simplifying the provisioning of policies and devices. Cisco ISE enables self-registration, automates device configuration and manages certificates and mobile policy compliance. With granular visibility and controls IT admins can confidently and quickly provision new resources to allow connection to the network without sacrificing protection.

Forrester Consulting recently conducted an independent analysis of five organizations using Cisco ISE. The commissioned study conducted by Forrester Consulting on behalf of Cisco, March 2022, "The Total Economic Impact™ of Cisco Identity Service Engine (ISE)," highlighted:



The bridge to possible

## Learn more

Check out the Cisco ISE web page for more information.

Check out ESG's whitepaper on strategic zero trust: Zero Trust Must Include the Workforce, Workloads, And Workplace.

## Why Cisco ISE?

Other standalone solutions end up "bolting on" security to the network, often resulting in operational complexity and performance issues. Cisco ISE has gained market dominance with a focus on security that is built directly into the network. Our customers can provide secure network access to trusted users and endpoints through a flexible, simple solution that accelerates their value.

**Our key differentiators are:**

1. **Security Resilience built into the network.** Cisco is the only vendor who leads in both enterprise networking and cybersecurity, and Cisco ISE builds pervasive security directly into the network. With flexibility and choice in deployment and purchasing, Cisco ISE enables organizations to tether secure network access across the distributed network their way.
2. **Integrations and partner ecosystem.** With integrated intelligence, Cisco ISE builds zero-trust policy decision points into the network for continuous trusted access and to automate threat containment. Effective cyber programs require integrated technologies to break down silos and reduce complexity. Cisco ISE has the most extensive partner ecosystem for Cisco Secure and third-party solutions through pxGrid and pxGrid Cloud to bring a platform approach to secure network access and zero trust.
3. **Unrivaled scalability.** With the rise of the connected everything, organizations need scale more than ever before. Cisco ISE is the only solution that is proven to support more than two million concurrent endpoint sessions.
4. **Network admin access control.** Cisco ISE is the only NAC solution that includes TACACS+ for role-based administrative access control to networking equipment.

Visit the ISE webpage to learn how we can enable your secure network access initiatives, and SD Access webpage to learn more about our complete secure access solution.



C22-4432329-00 06/24