CISCO
SECURE

Implement zero trust and regain control with Cisco Identity Services Engine (ISE)

The phone rings. It is your CIO, and he informs you that the digital transformation of your business is about to take the next step. You will be required to onboard an unprecedented number of connected Internet of Things (IoT) devices to enable and propel productivity. You are already dealing with the great cloud migration. And the growing requirements for bring your own device (BYOD) and the mobile workforce are causing you to shudder every time the phone rings.

No one wants that call – the one that says you have just been the latest casualty of the malware economy. Or just as bad, if not worse, the call that says your access policy has just shut down a critical function of your business. How do you balance these innovations that are pushing your business forward, and increasing risk?

Cisco Identity Services Engine (ISE) solves for this massive problem. ISE ensures secure network access for trusted users and endpoints to the trusted apps they need to meet business objectives. The ISE ecosystem allows for proper and accurate asset inventories that are leveraged to classify endpoints into profiled groups for automated policy implementation in order to enable granular control within segmented zones of trust and to enable rapid threat containment.

Benefits

- **Gain visibility with context and control:** Know who, what, where, and how endpoints and devices are connecting. Look deep into devices to ensure compliance and limit risk, with or without the use of agents.
- **Extend zero trust to contain threats:** Software-defined network segmentation shrinks the attack surface, limits the spread of ransomware, and enables rapid threat containment.
- **Accelerate value of existing solutions:** Integrate with Cisco and third-party solutions to bring an active arm of protection into passive security solutions and increase your return on investment (ROI).
- **Future proof your network security:** ISE provides the foundation for policy control within Cisco DNA Center™ and is the linchpin for SD-Access.

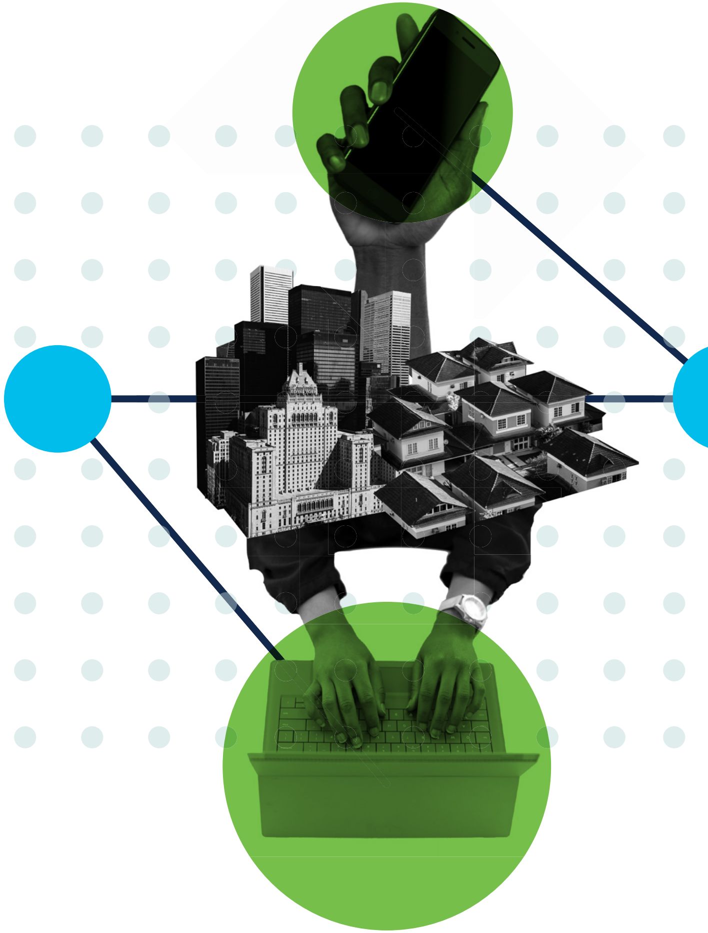
The secure network access challenge and zero trust

Providing secure access to trusted users and endpoints is getting more and more difficult to achieve. The problem of identifying and controlling endpoints as they request access to trusted resources has been exasperated by trends around cloud migration, mobility, and the proliferation of IoT-connected devices. But as the cloud, mobility, and IoT all possess great possibilities to unlock innovation as well as save organizational resources, these new paradigms have introduced more questions and complexity when it comes to securing data and maintaining compliance across the expanding perimeter.

Zero trust and least privilege is a vital cybersecurity principle that addresses these challenges. It recommends granting only the minimum level of system/network access based on the least level of privilege required to allow users and endpoints to carry out their missions as required by business objectives. Unrequired access extends the network attack surface, increases the risk for the organization, and allows the lateral movement of threats. By controlling access to only what is needed to reach business outcomes, the organizational risk is reduced, and compliance is assured.

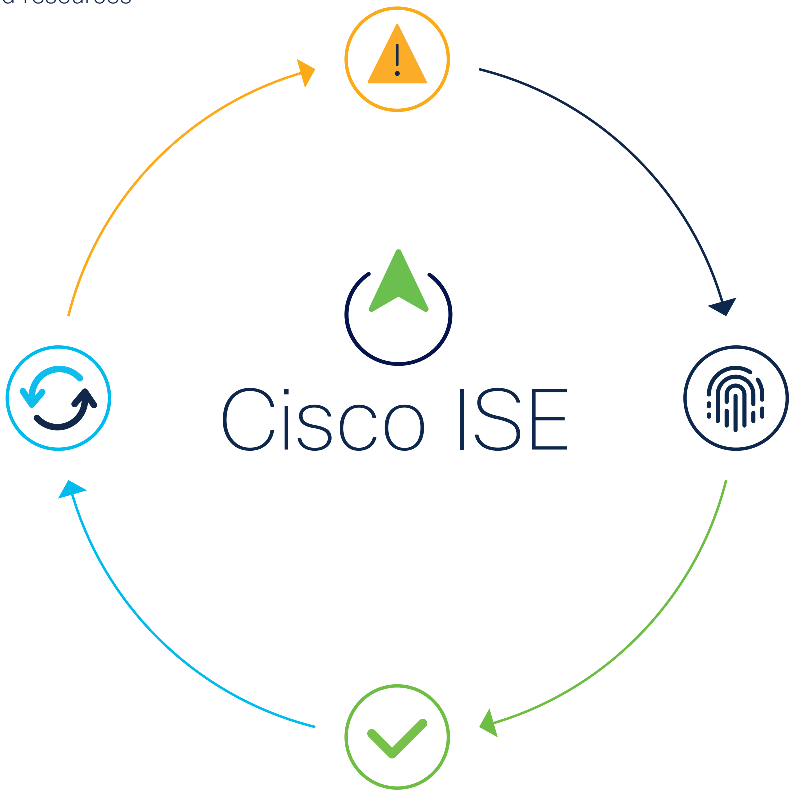
The complexity of today's networks makes the implementation of least privilege a daunting challenge. Without having the visibility to continually identify and verify network endpoints, controlling access with segmented zones of trust is not recommended, as it could cause disastrous effects in the workplace, shutting down business-critical functions, especially in IoT environments.

Cisco Identity Services Engine (ISE) is the core of your Zero Trust approach for the Workplace. It delivers complete visibility by identifying, classifying, and assembling the necessary context on users and endpoints. It continually authenticates and authorizes them based on your business intent -- your security policy --and grants an appropriate level of network access based on the principle of least privilege to limit access based only on the needs of their roles or functions.



How 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

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

Trust continually verified

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

Use Cases

Cisco ISE addresses these challenges with a broad set of mission-critical secure network access and control use cases to support zero trust in the workplace.

Dynamic endpoint visibility

See and know everything connecting. The first step to zero trust is gaining the ability to see and know everything that is connecting to the network. ISE identifies, classifies, and tracks all endpoints connected to the network to allow the automation of policy provisioning. 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 changes the policy to control access, ensure compliance, reduce risk, and contain threats.

Visibility-driven segmentation

Confidently build security into your network. ISE extends zero trust to contain threats with trusted zones of access and builds network segmentation and policy enforcement directly into the network, without the configuration complexity seen in legacy approaches. Organizations can shrink the attack surface, limit the spread of ransomware, and enable rapid threat containment, all while continually ensuring that this level of protection will not disrupt business outcomes.

Automated threat containment

Don't just block threats, remove them. ISE integrates with Cisco security products and third-party ecosystem partners through pxGrid and pxCloud** to share contextual information with on-premises and cloud-native solutions. This open integration ecosystem brings an active arm of enforcement into passive security solutions to automate threat containment, remove threats, and reduce mean time to repair, all while increasing the value of existing solutions and the overall security posture of the organization.

**Feature planned for release in the first half of CY 2021. Please contact sales for early access.

More Use Cases

Endpoint compliance

Maintain compliance and reduce organizational risk. ISE continually verifies that device posture complies with your security policy so that risky, unpatched, and outdated devices cannot threaten the network. Limit organizational risk and maintain compliance with granular controls based on organizational risk tolerances for any one endpoint, or profiled group of endpoints without deploying agents and risking performance for protection

Secure access

Accelerates value by simplifying the provisioning of policies and devices. ISE enables self-registration, automates device configuration, 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.

Why ISE?
The Cisco advantage

Other standalone solutions end up "bolting on" security to the network, often resulting in operational complexity and performance issues. 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 built into the network.** Cisco is the only vendor who leads in both enterprise networking and cybersecurity, and ISE builds advanced security directly into the network. It enables secure network access yet converts the workplace network into a zero-trust security enforcer.
2. **Integrations and partner ecosystem.** Effective cyber programs require integrated technologies, and ISE has the most extensive partner ecosystem for automated solution integrations with Cisco DNA Center as a part of the SD-Access solution. ISE also integrates with premier Cisco security products like Cisco Firepower®, Cisco Cloud Analytics, Cisco Cyber Vision, and Cisco Advanced Malware Protection. ISE is the only solution with an IETF standards-based integration platform, and only Cisco stands behind technology integrations through testing, validation, and support. With ISE, we extend this ecosystem into the cloud with pxCloud to support cloud-native solutions.
3. **Unrivaled scalability.** ISE is the only solution that is proven to support up to 2 million concurrent endpoint sessions.
4. **Network admin access control.** ISE is the only NAC solution that includes TACACS+ for role-based administrative access control to networking equipment.

> "Cisco ISE [Identity Services Engine] allows you to control not only the types of devices connecting to your network but also allows you to control the compliance of the devices connecting."
>
> Steven van Jaarsveld, Engineer, Dimension Data

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

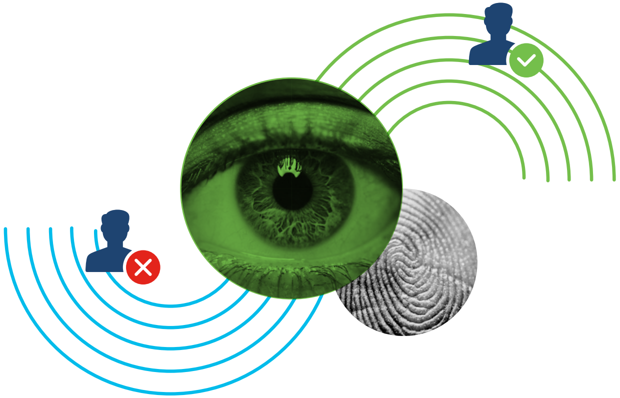
Check out ESG’s whitepaper; **Removing Complexities Around Network Segmentation** to gain further insights on achieving network segmentation.

To learn more visit:

cisco.com/go/ise

With Cisco ISE, customers gain:

1. **Cloud-enabled visibility*:** Open integrations extend interoperability into the cloud. The team can integrate with cloud software-as-a-service (SaaS) security solutions to enhance visibility for access policy enforcement decisions while enabling the flexibility required to be cloud driven and automate rapid threat containment.
2. **A simplified user experience:** A user experience with a focus on simplicity guides users through workflows to enable advanced use cases to rapidly accelerate value and protection while building the confidence required to enable and accelerate secure access.
3. **Added flexibility:** Agentless posture allows the visibility required to ensure compliance. IT no longer has to choose between the speed of delivery of services and protection; teams can now have the flexibility to decide between an agent or an agentless approach to balance the need for the connection and the obligation for protection.
4. **Increased visibility through integration:** With AI-augmented visibility, customers can leverage machine learning to properly identify, classify, and verify device identification for effective policy management and network control.
5. **Secure access from the cloud:** With ISE deployments being supported from the cloud, customers will enable their cloud-first approach and unify visibility and control across campus and branch deployments.



*Feature planned for release in the first half of CY 2021. Please contact sales for early access.