Identity Services Engine (ISE)

Zero Trust for the WorkPlace

Cisco Partner
https://cs.co/1page

Cisco **Identity Services Engine** (**ISE**) is a centralized security solution that provides secure network access to users and devices. It helps gain visibility into what is happening in your network, such as who is connected, which applications are installed and running for wired, wireless, and VPN endpoints in a network.

Benefits:

Gain visibility with context and control: Know who, what, where, and how devices (e.g., endpoints, mobile devices, security cameras, printers) are connecting. Look deep into devices to ensure compliance and limit risk, with or without the use of agents.

Remote management and public cloud deployment: Enable access and management from anywhere within any consoles through APIs. ISE 3.1 supports deployment in AWS.

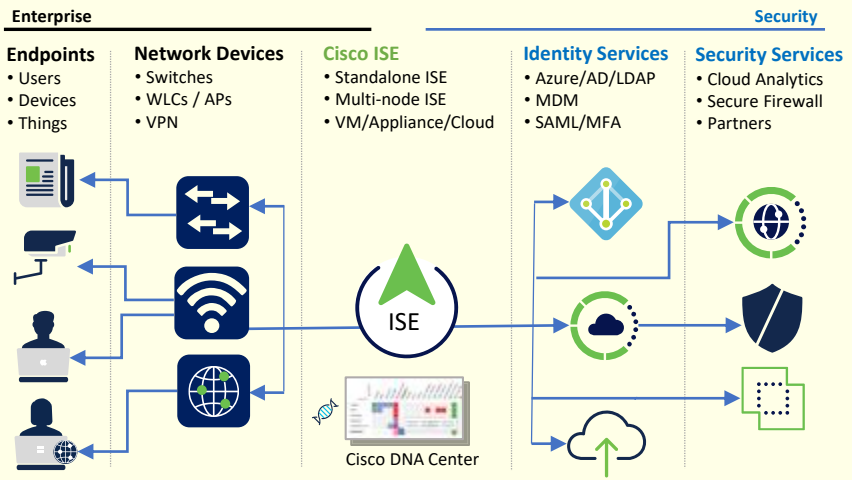
Extend zero trust to contain threats: Software-defined network segmentation shrinks attack surface, limits spread of ransomware, and enables rapid threat containment.

Future proof your network security: ISE provides the foundation of policy control for SD-Access integrating directly with Cisco *DNA Center*™.

3.x Licensing:

- **Essentials** (User Visibility & Enforcement)**:** AAA and 802.1X, Guest (Hotspot, Self-Reg, Sponsored), Easy Connect (PassiveID).
- **Advantage** (Context with Essentials)**:** Profiling, BYOD (+CA, MDP), pxGrid (Cloud & Direct), User Defined Network (Cloud), TrustSec (Group-Based Policy), Endpoint Analytics Visibility and Enforcement, Rapid Threat Containment
- **Premier** (Compliance w/Advantage)**:** Posture, MDM Compliance, TC-NAC

Zero Trust for the Workplace:



Use Cases:

Zero Trust Network Access: Allow wired, wireless, or VPN access to the network based on the user and/or endpoint. Use RADIUS with 802.1X, MAB, Easy Connect, or Passive ID.

Automated Deployment & Configuration: *InfraOps* teams can accelerate deploying USE with Ansible, Terraform pre-built playbooks. *NetOps* teams can also leverage Ansible & Terraform playbooks to automate onboarding of devices.

Guest Access: Differentiate between Corporate and Guest users and devices. Choose from Hotspot, Self-Registered Guest, and Sponsored Guest access options.

Asset visibility: Use the probes in ISE and Cisco network devices to classify endpoints and authorize them appropriately with Device Profiling. Automate access for many IoT devices.

Compliance & Posture Use agentless posture, AnyConnect, MDM, or EMM to check endpoints to verify compliance (Patches, AV, USB, etc.) before allowing network access.

Context Exchange: pxGrid is an ecosystem that allows any application or vendor to integrate with ISE for endpoint identity and context to increase Network Visibility and facilitate automated Enforcement. *Note: requires Advantage*

Segmentation: Group-based Policy allows for segmentation of the network by using Scalable Group Tags (SGT) and Scalable Group ACLs (SGACL) instead of VLAN/ACL segmentation.

Cisco SDA/DNAC: Integrate with DNA Center to automate the network fabric and enforce policy throughout the entire network infrastructure using Software-Defined Access (SDA).

BYOD: Allow personal devices to access network resources by registering device and download certificates for authentication through a simple onboarding process.

Threat Containment: Using a Threat Analysis tool, such as Cisco Cognitive Threat Analytics, to grade an endpoints threat score and allow network access based upon the results.

Device Administration: TACACS+ Migrating from ACS or building a new Device Admin Policy Server, this allows for secure, identity-based access to the network devices.

Resources:

Selling:
- SalesResources
- Instant Demos
- Data Sheet
- ISE Champions

Licensing:
- Licensing Guide
- 3.0 Migration
- Proposal Template

Platform:
- ISE Software
- EoL & EoS
- ISE in AWS

Team Space:
- ISE Bar *(public)*

Public:
- Webinars | Videos
- Product Docs
- Compatibility
- ISE & NAC Resources
- Public page

Example SKU: ***ISE-SEC-SUB***