# Secure Every Connection with Cisco ISE

From visibility to automated threat containment—build Zero Trust at every stage

# Zero Trust is a journey, not a feature

Cisco ISE enables security at every stage and progression aligns with security maturity model below.

## 01

### ISE Essentials

Verify who connects

**What you get**

Visibility into all users & devices across wired, wireless, and VPN

Secure onboarding (employees, guests, IoT)

Consistent access policy across your network

**Business outcome**

Baseline security

Audit-ready access control

## 02

### ISE Advantage

Control what they can access

**What you get**

Device profiling & classification

Identity-based segmentation (TrustSec / SGT)

Integration with security ecosystem (pxGrid)

**Business outcome**

Reduced lateral movement

Stronger Zero Trust posture

## 03

### ISE Premier

Enforce compliance and contain threats

**What you get**

Device posture validation (health checks)

Compliance enforcement (MDM/ EMM integration)

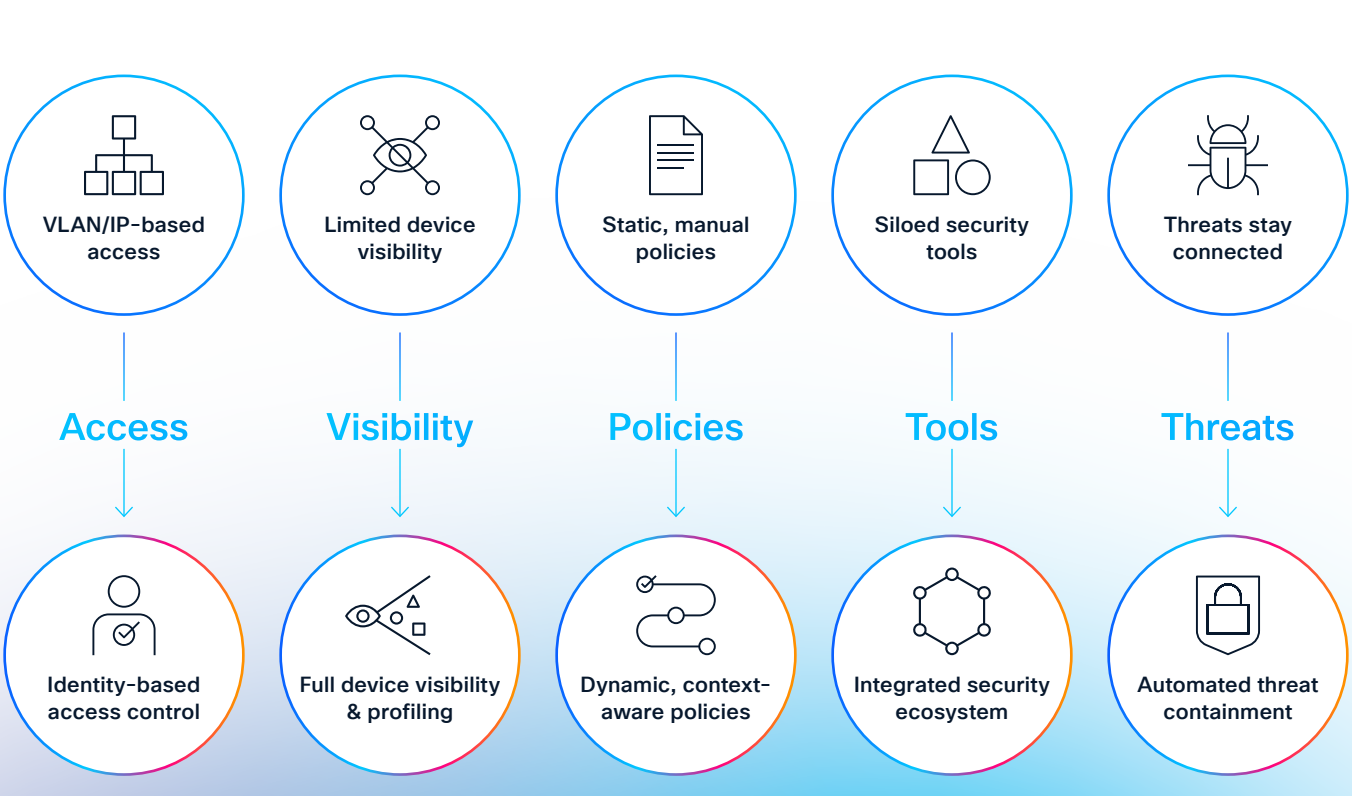
Automated threat containment

**Business outcome**

Continuous device trust

Automated threat response

# Transformation




# Quick decision guide

| Upgrade to Advantage if you need | Upgrade to Premier if you need |
|---|---|
| Device classification (IoT, printers, cameras) | Device compliance checks before access |
| Identity-based segmentation (not VLANs) | Integration with MDM (Intune, Jamf, etc.) |
| Policies based on user/device context | Continuous compliance for audits |
| Integration with security tools | Automatic isolation of compromised devices |

**View the in-depth guide to find the right plan for your network.**

Explore Cisco ISE