Industry Use Case

Industrial

majentai

IoT/OT Segmentation with Cisco ISE & TrustSec

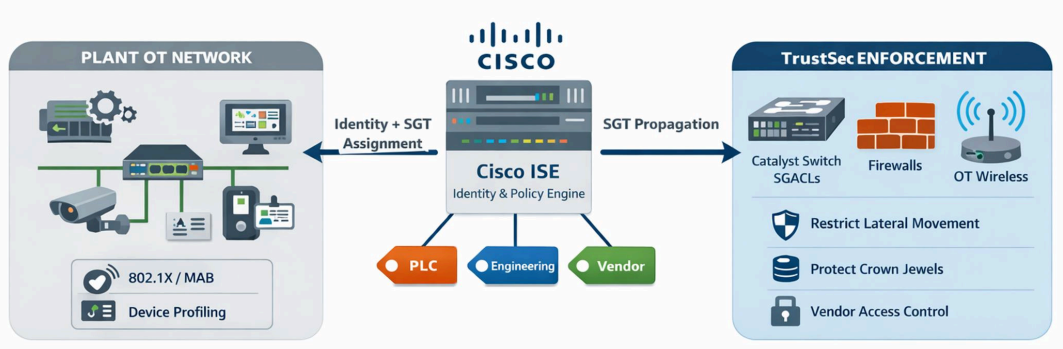
Magentai helps teams reduce OT risk by applying identity-based segmentation using Cisco ISE and TrustSec. ISE identifies and classifies OT and IoT endpoints and assigns Security Group Tags (SGTs). TrustSec enforces policy between device groups to limit lateral movement, protect critical assets like historians and SCADA, and govern vendor access without creating unmanageable VLAN and ACL sprawl.

Overview

Industrial environments often have legacy and unmanaged devices, such as PLCs, HMIs, controllers, and cameras, that cannot run agents or modern endpoint controls. They also have high availability and safety constraints, so segmentation must be phased and low risk. Magentai uses Cisco ISE to identify OT and IoT endpoints and assign TrustSec Security Group Tags (SGTs) so policy can be enforced by identity and role instead of IP addresses. This reduces unnecessary east-west movement and avoids ACL and VLAN sprawl that becomes hard to maintain across plants and sites.

How it Works

Cisco ISE discovers and classifies OT and IoT endpoints, using 802.1X where feasible and MAB plus profiling where it is not. It then assigns TrustSec Security Group Tags (SGTs) based on device role, such as PLC, HMI, engineering workstation, or vendor. TrustSec enforces an SGT-to-SGT policy matrix using SGACLs and SGT-aware enforcement points so only required services are allowed.



Prerequisites

- Defined enforcement approach and supported network infrastructure at OT access
- Agreed OT access patterns (required flows and service ports)
- Authentication strategy per device class (802.1X vs MAB + profiling)
- Change windows and a phased rollout plan to reduce operational risk

At a Glance

Primary Value: Reduce IoT/OT blast radius with identity policy

How it works: ISE assigns SGTs TrustSec enforces

Where it fits: Plants, substations, warehouses, utilities

What We Deliver

- OT zone model + SGT taxonomy (aligned to site and cell realities)
- ISE policy design (802.1X, MAB, profiling, authorization policy sets)
- TrustSec policy matrix translated to enforceable controls (SGACLs and integrations as designed)
- Pilot deployment with evidence-based validation and a scale-out roadmap
- Operational handoff package (run-state checks, monitoring, expansion plan)

Use Case	Outcome
Lateral Movement Control	Limit OT-to-OT paths to required services only, reducing overall blast radius.
Crown-Jewel Protection	Restrict access to historians, SCADA, and safety systems to approved roles and flows.
Vendor Access Governance	Provide scoped, identity-based access with time-bound policies and fast revocation when needed.
Cell/Area Separation	Segment by plant, site, line, or cell without VLAN explosion or ACL management sprawl.

Majentai is a world-class Cybersecurity services provider, dedicated to implement, integrate and operate the most resilient Cybersecurity platforms using proven state-of-the-art technologies. With a team of seasoned experts and cutting-edge technology, we deliver comprehensive solutions tailored to our clients' unique needs, ensuring their digital assets remain secure in an increasingly complex cyber landscape.

For more information or to engage our services, please contact us at info@majentai.com or visit https://majentai.com