cisco
SECURE

cisco The bridge to possible

Nova generacija segmentacije

Cisco Identity Services Engine (ISE) in TrustSec

Silvo Lipovšek
IngramMicro

Januar 2025

The World Has Changed

New Applications, Infrastructures, and Work Styles are changing the rules!

The workplace has gone hybrid

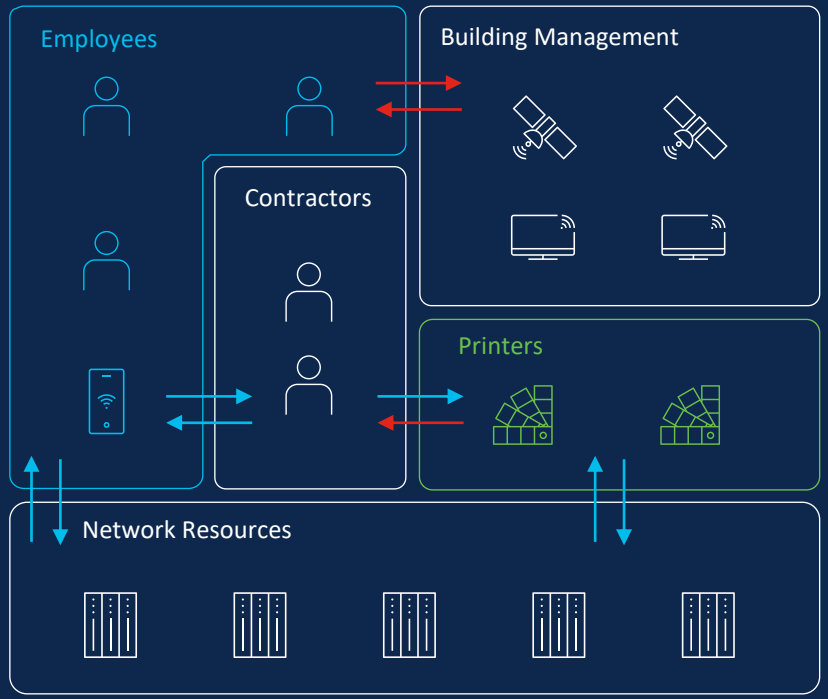
IoT is evolving

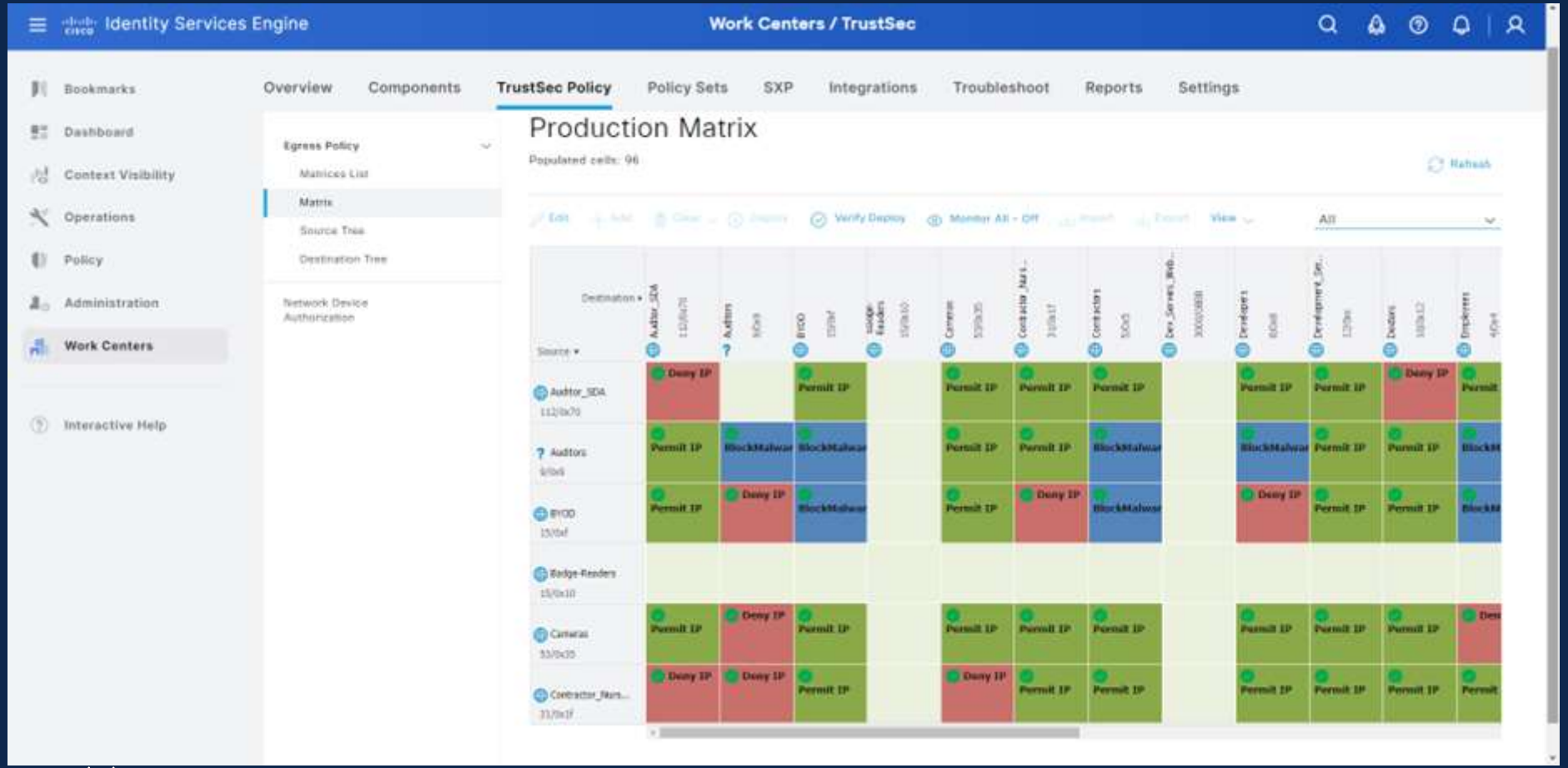
Cyber attacks are on the rise

Apps and environments are cloud-powered

Least Privilege Access: Expectation vs. Reality

Expectation

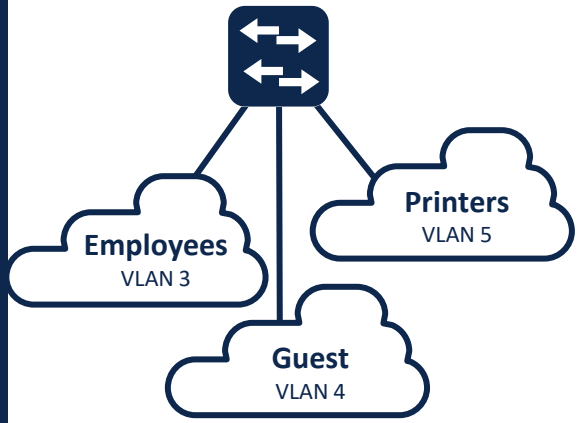




ISE Segmentation Technologies

VLANs

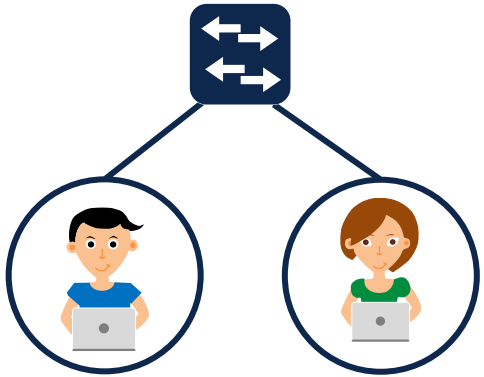
Dynamic VLAN Assignments



Per port / Per Domain / Per MAC

ACLs: DL, Named, DNS

Downloadable ACL (Wired) or
Named ACL (Wired + Wireless)



Employee

```
permit ip any any
```

Contractor

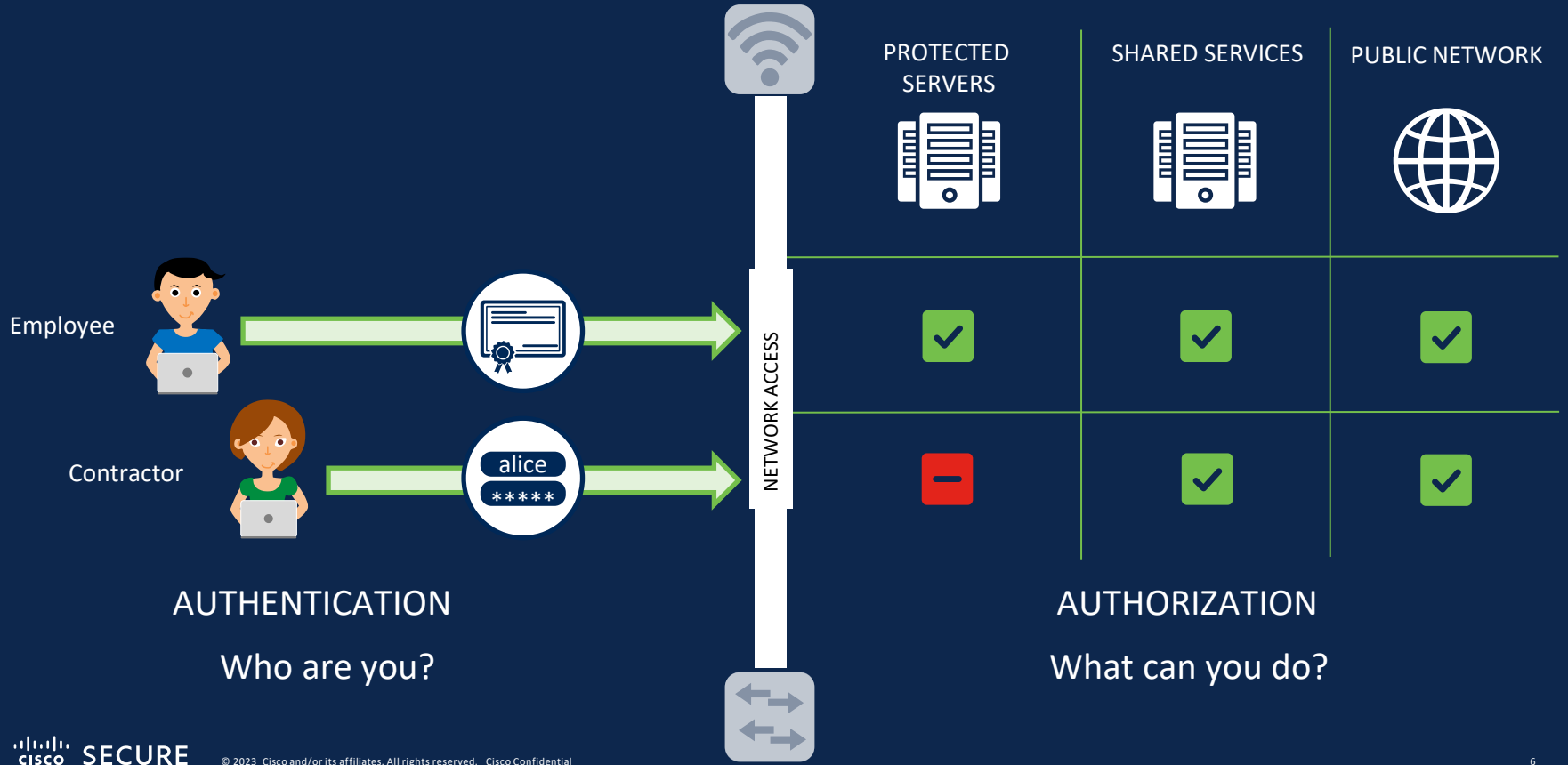
```
deny ip host <critical>
permit ip any any
```

Scalable Group Tags

Cisco Group-Based Policy

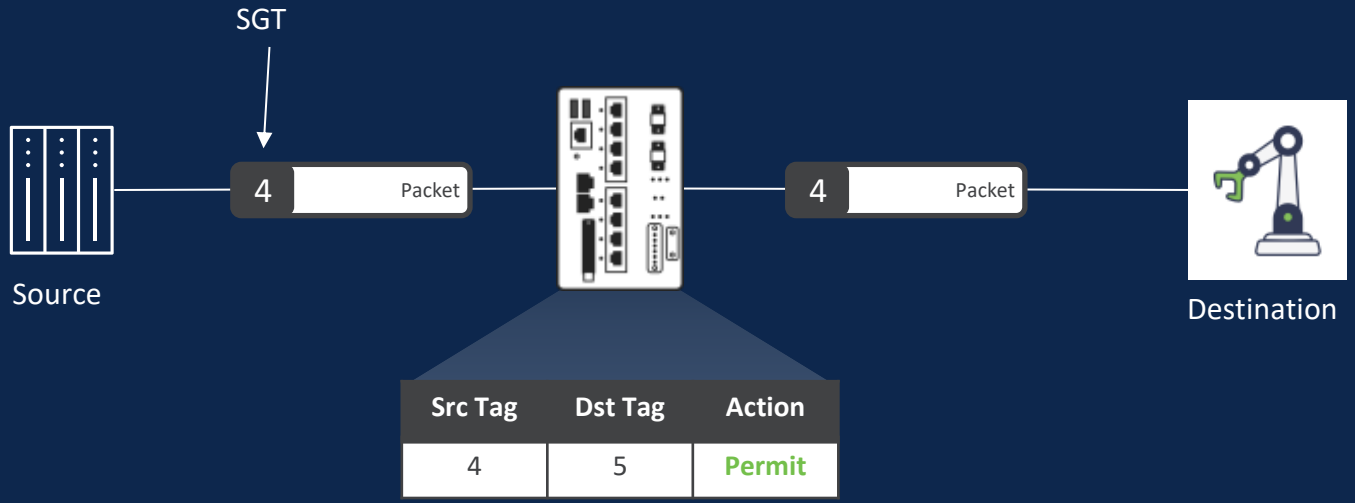
16-bit SGT assignment and SGT based Access Control

Authentication and Authorization



What are Scalable Group Tags (SGTs)?

Role Based Access Control embedded in the network



How Identity Services Engine 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 assessments to identify indicators of compromise
- Automatically Updates access policy

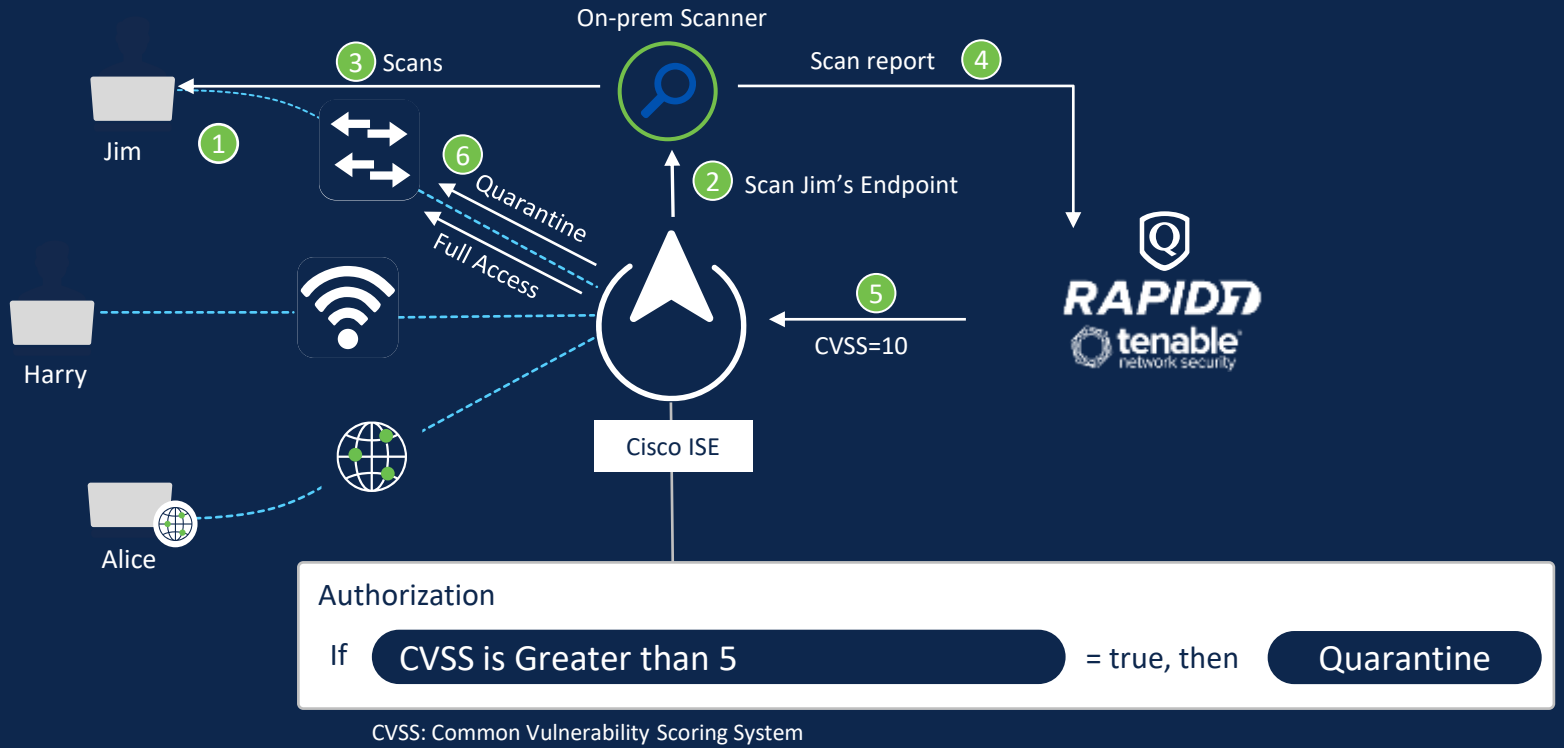
Endpoint classified, and profiled into groups

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

Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

Vulnerability Assessment (Threat-Centric NAC)

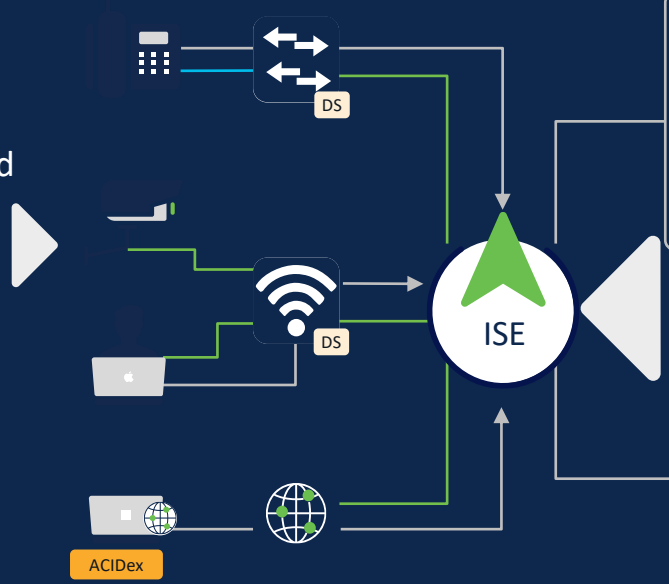


CVSS: Common Vulnerability Scoring System

Endpoint Profiling

The profiling service in Cisco ISE identifies the devices that connect to your network

Endpoints send interesting data, that reveal their device type



AnyConnect Identity Extensions (ACIDex)
Device Sensor (DS)

ISE Data Collection Methods for Device Profiling

Probes: AD | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | NetFlow

Device Sensor: CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDex

Feed Service
(Online/Offline)

MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

Enhancing ISE profiling with Cyber Vision data

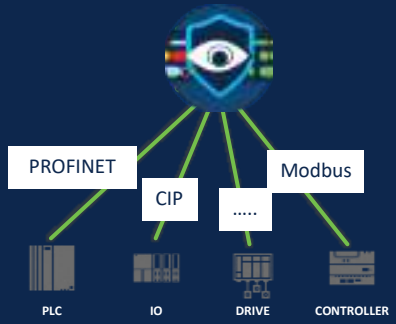
ISE Data Collection Methods for Device Profiling

Active Probes: AD | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | NetFlow

Device Sensor: CDP | LLDP | DHCP | HTTP | H323 | SIP | MDNS

AnyConnect: ACIDec

Industrial Asset
Management for OT users



Cyber Vision classifies the OT devices based on the results of DPI

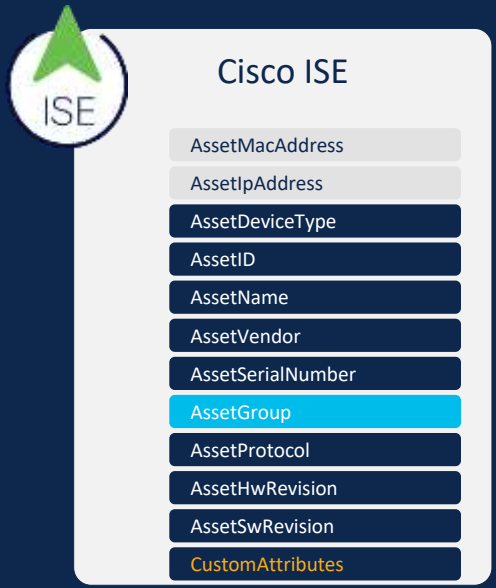
Asset Identity

This is a…

- CompactLogix Controller…
- Manufactured by Rockwell Automation …
- With serial number xxx …
- Running firmware xxx …
- Speaks CIP industrial protocol …
- Attached to switch xxx …
- Cell-1 in the Austin Plant.

The attributes are then sent up to ISE via pxGrid

pxGrid



ISE populates the custom attributes with the ones received via profiling pxGrid probe

The power of integration, the simplicity of operations

More Cross-Team Use Cases Simplified with Visibility and Automation

Cisco Security

- Network
- Applications
- Endpoint
- Cloud

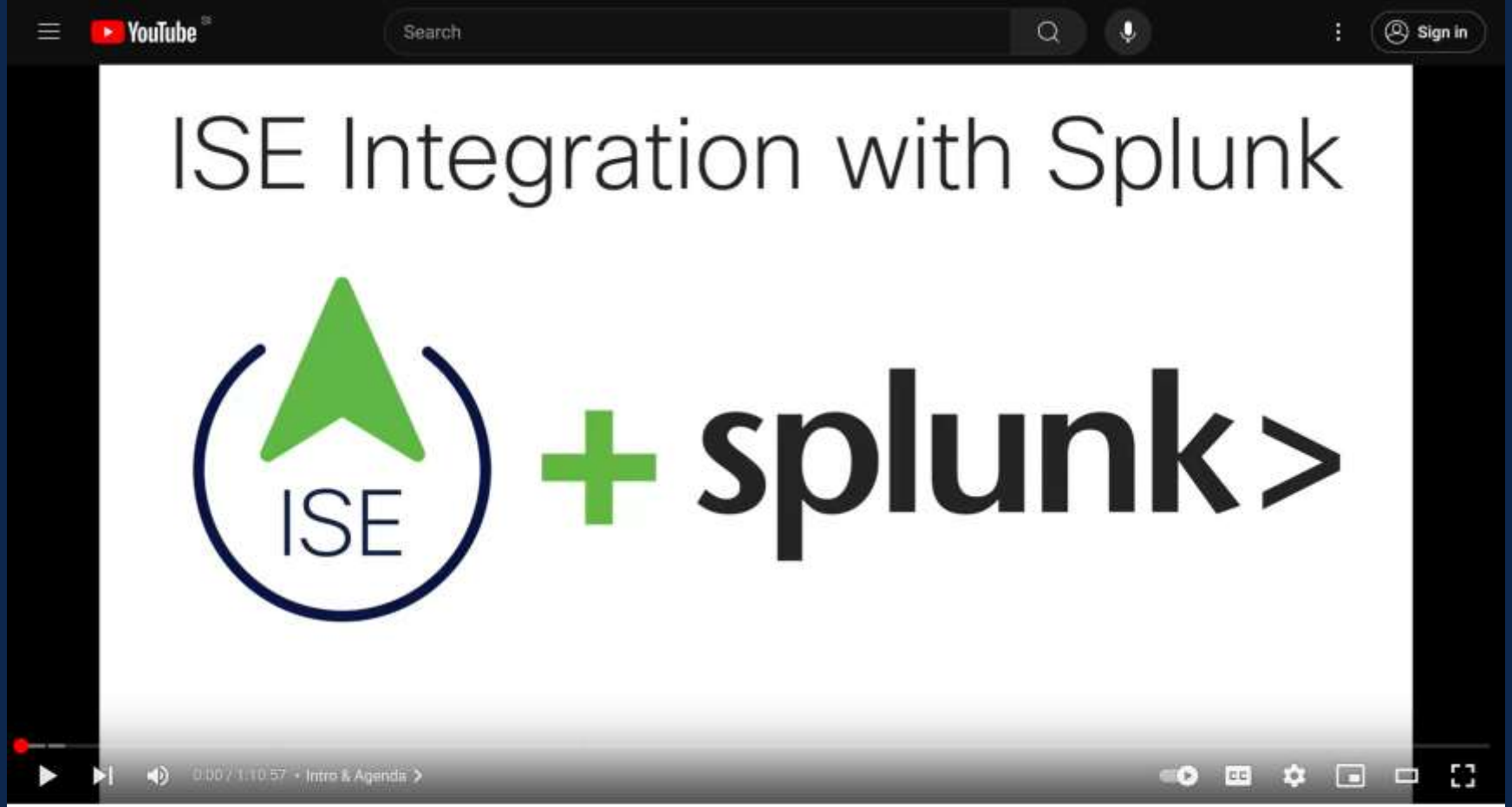
cisco SECURE X

More Integrated Products Across Partner Ecosystem and Beyond

- 3rd Party/ITSM
- Intelligence
- Identity
- SIEM/SOAR

+

Your infrastructure



Cisco ISE Integration with Splunk

Cisco ISE - Identity Services E...
23.7K subscribers

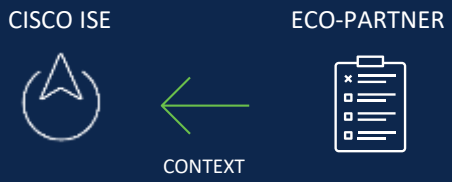
Subscribe

27 Share Save ...

Power of integration pxGrid:

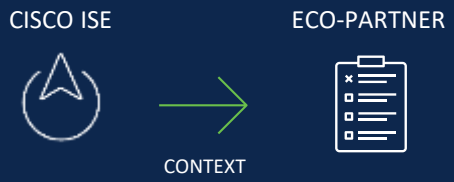
Enabling a platform approach into the Cloud

ISE CONTEXT IN



Enrich ISE context. Make ISE a better Policy Enforcement Platform

ISE CONTEXT OUT



ISE makes Customer IT Platforms User/Identity, Device and Network Aware

Rapid Threat Containment

Enforce dynamic policies into the network based on Partner's request

The foundations to zero-trust in your workplace

Visibility

Grant the right level of network access to users across domains

Segmentation

Shrink zones of trust and grant access based on least privilege

Containment

Automate containment of infected endpoints and revoke network access

ISE — The first step to Software-Defined Access

Business drivers can define network intent and dictate the mechanics of network connectivity, not the other way around

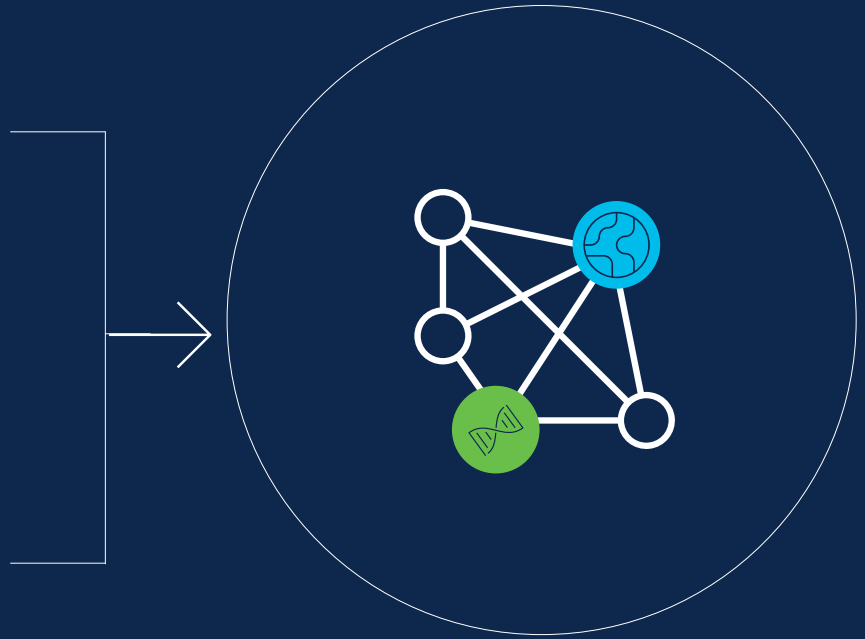
Cisco Identity Services Engine

Network access visibility, control, and policy enforcement

+

Cisco DNA Center (Catalyst Center)

Network design, policy, provisioning, and assurance



Gain balance with ISE- The complete NAC solution

- Better User Experience
- Simplified network segmentation

Endpoint Compliance

Endpoint Visibility

Secure Access

Network Segmentation

Threat containment

Security Ecosystem Integration

TrustSec vs. SDA

- Cisco TrustSec and Cisco Software-Defined Access (SDA) are both security solutions, but they serve different purposes and operate in distinct ways:
- **Cisco TrustSec**
  - **Purpose**: TrustSec is primarily focused on network segmentation and access control.
  - **Functionality**: It uses Scalable Group Tags (SGTs) to classify and enforce policies based on user roles and device types. This allows for dynamic and scalable security policies across the network.
  - **Implementation**: TrustSec can be implemented on existing network infrastructure without requiring a complete overhaul. It integrates with various Cisco products to provide consistent security policies across the network.

- **Cisco Software-Defined Access (SDA)**
  - **Purpose**: SDA is a broader solution aimed at automating and securing campus networks.
  - **Functionality**: It uses a fabric-based architecture to provide network virtualization, automation, and policy enforcement. SDA integrates TrustSec for micro-segmentation and policy enforcement within the fabric.
  - **Implementation**: SDA requires Cisco DNA Center for management and orchestration. It involves creating an overlay network on top of the existing physical network, allowing for easier management and segmentation.

- In summary, while TrustSec focuses on scalable and dynamic access control, SDA provides a comprehensive solution for automating and securing campus networks, incorporating TrustSec for enhanced segmentation and policy enforcement.

Additional Resources

- Visit:
  cisco.com/go/ise
- Technical Communities:
  https://cs.co/ise-community
- Resources:
  https://cs.co/ise-resources
  https://cs.co/sda-resources
- Support page:
  Cisco Catalyst Center Support Page
- ISE YouTube page
  https://www.youtube.com/user/CiscoISE
- Cisco DemoZone – Search ISE


cisco SECURE