CISCO The bridge to possible

Zero-trust Network Access

SD-Access med Catalyst Center

Per Jensen

Technical Solution Architect

October-2023

Agenda

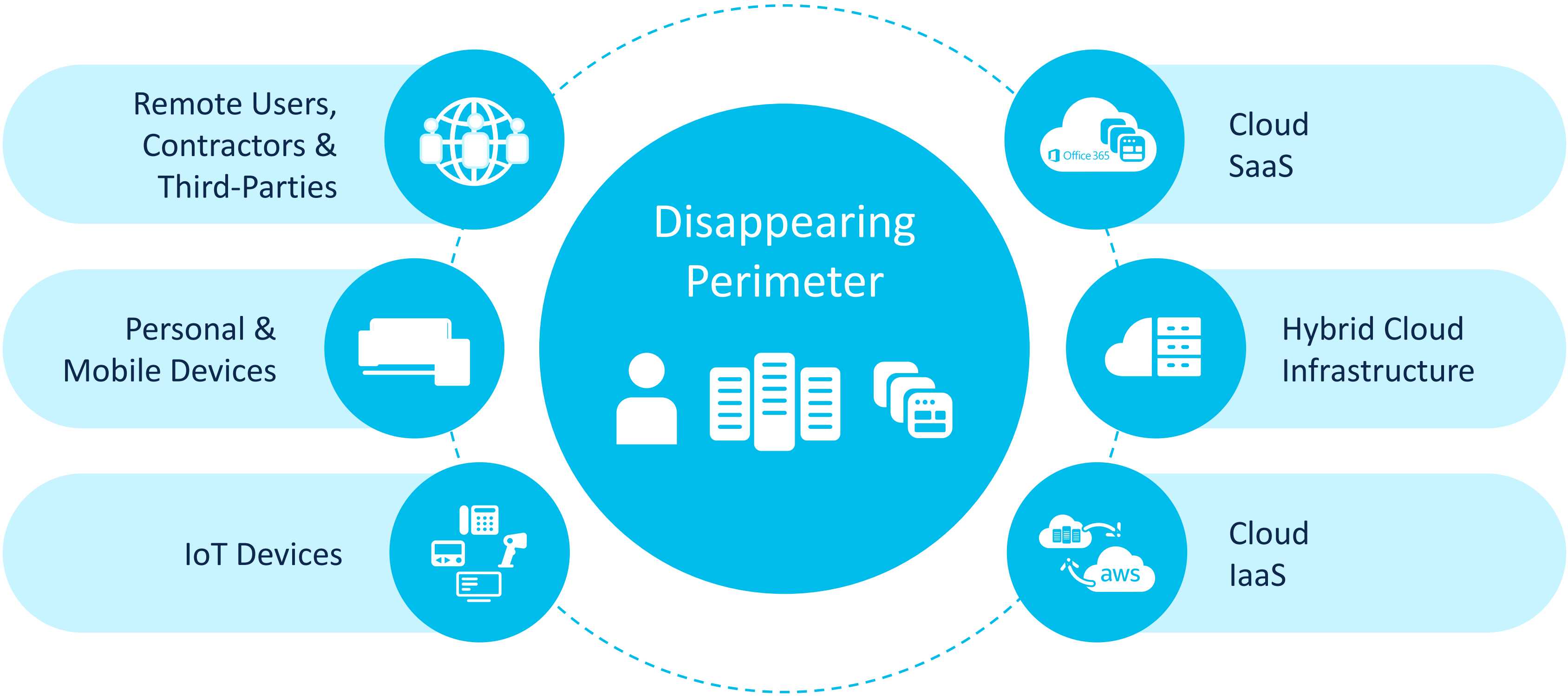
- Discussion of Zero-trust and Fabric
- ISE - overview
- Catalyst Center - overview
- Conclusion

Agenda

- Discussion of Zero-trust and Fabric
- ISE – overview
- Catalyst Center - overview
- Conclusion

Shift in IT Landscape

Users, devices, and apps are everywhere



Disappearing Perimeter

Remote Users, Contractors & Third-Parties

Personal & Mobile Devices

IoT Devices

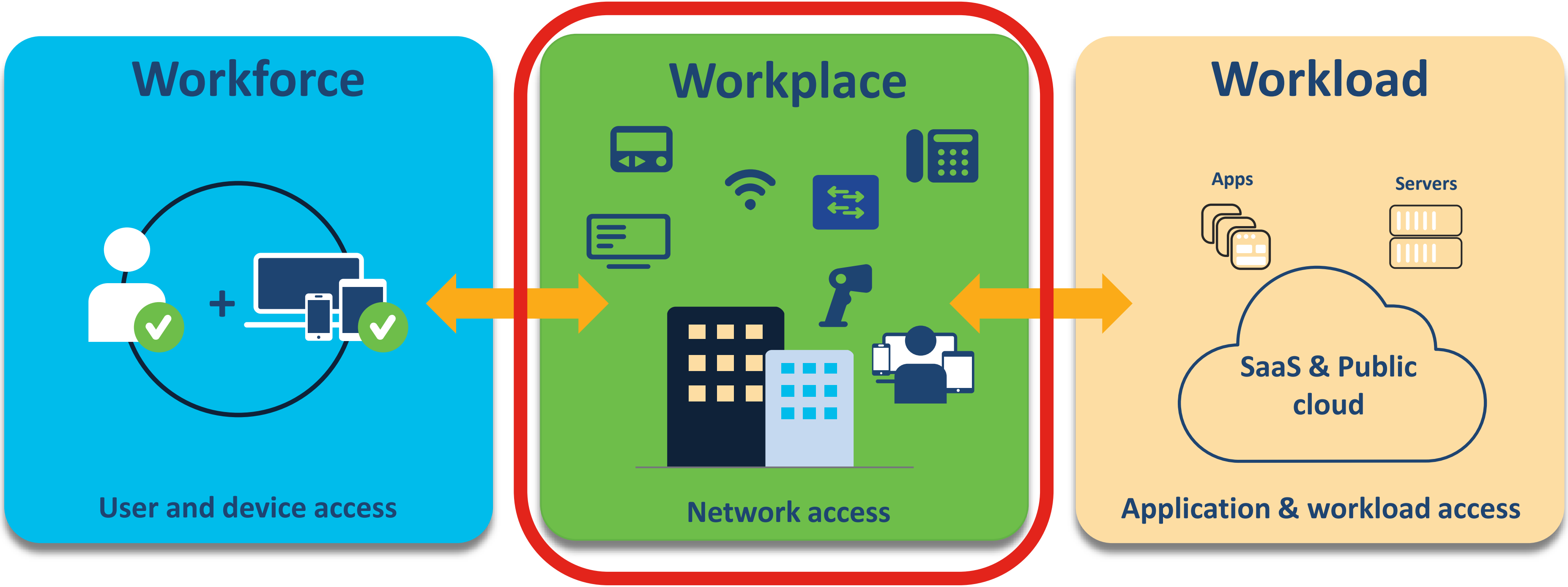
Cloud SaaS

Hybrid Cloud Infrastructure

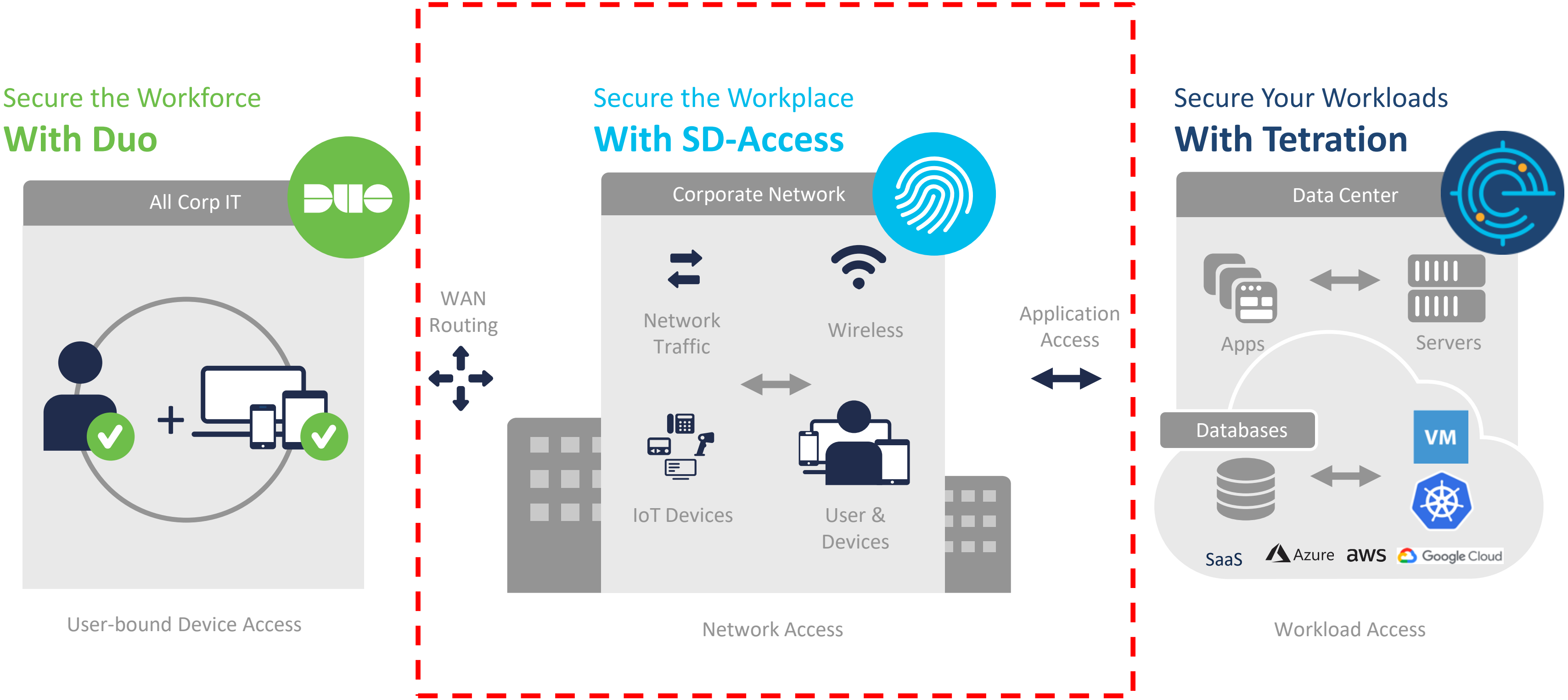
Cloud IaaS

Cisco Zero Trust

A zero-trust approach to securing all access across your applications and environment, from any user, device, and location



Cisco Zero Trust



Secure the Workforce
With Duo

User-bound Device Access

Secure the Workplace
With SD-Access

Network Access

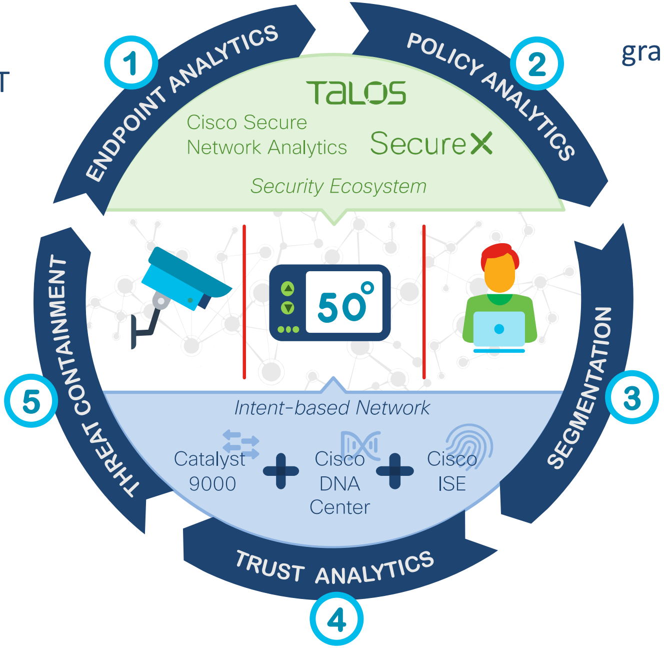
Secure Your Workloads
With Tetration

Workload Access

SD Access solution for Zero Trust for Workplace

AI/ML based multi-factor endpoint classification for IoT Visibility

Traffic analysis for granular policy discovery



Automated threat isolation and remediation

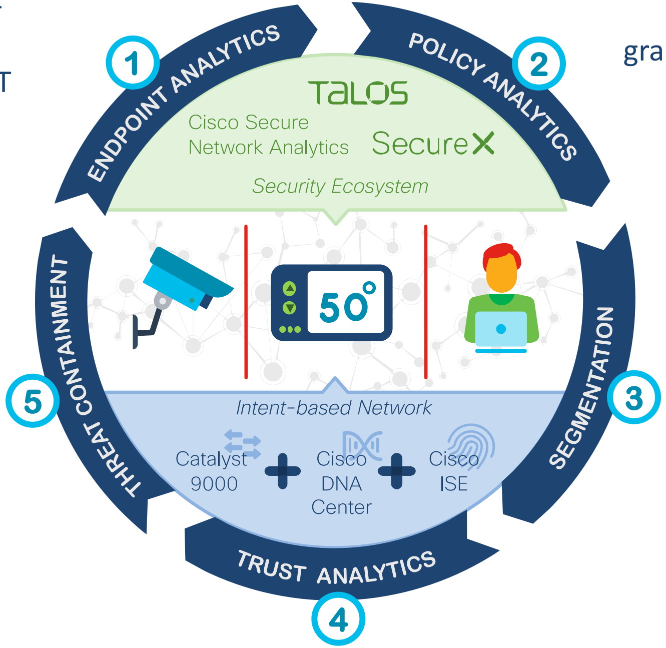
Flexible Macro/Micro segmentation

AI/ML-led network behavioral anomaly detection. Identifying endpoint weaknesses, vulnerabilities etc.

SD Access solution for Zero Trust for Workplace

AI/ML based multi-factor endpoint classification for IoT Visibility

Traffic analysis for granular policy discovery



Automated threat isolation and remediation

Flexible Macro/Micro segmentation

AI/ML-led network behavioral anomaly detection. Identifying endpoint weaknesses, vulnerabilities etc.

ISE and SDA

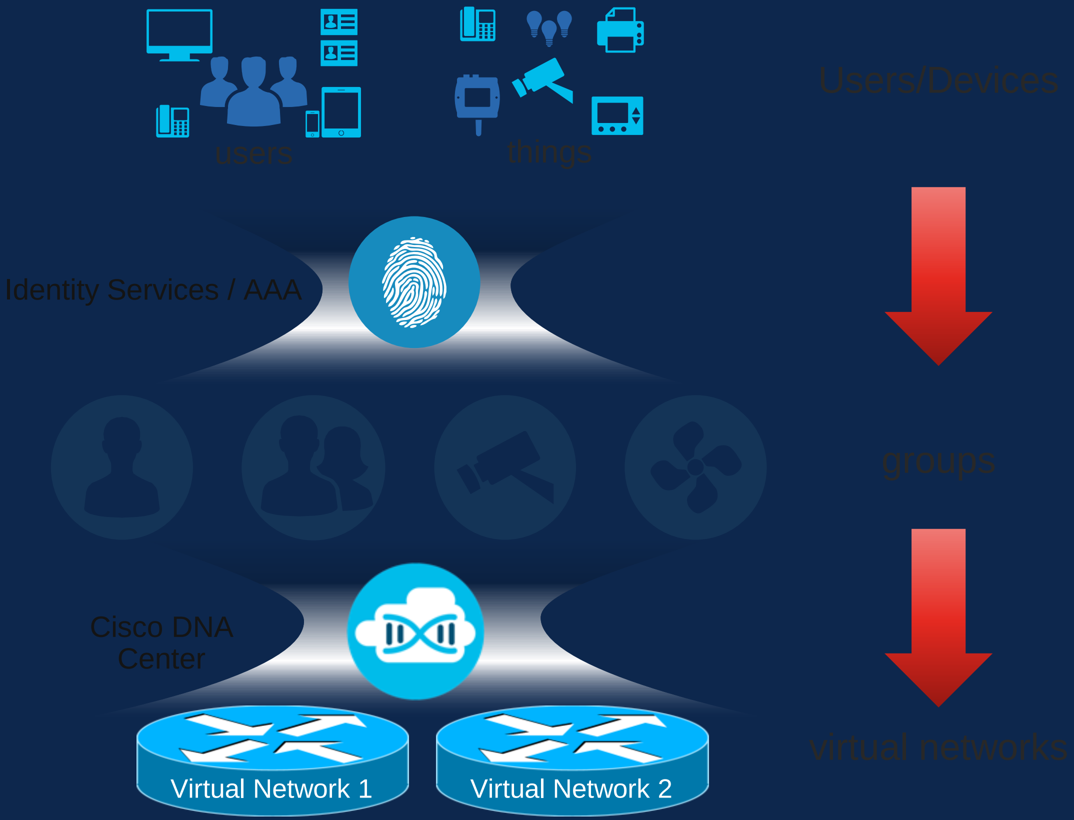
Cisco ISE
Cisco DNAC

Access Control (Host On-boarding)
User / Device Authentication

Segmentation
Role-based Segmentation

Guest Wireless Setup
Guest network automation

User/Device Groups & Virtual Networks



users

things

Users/Devices

Identity Services / AAA

groups

Cisco DNA Center

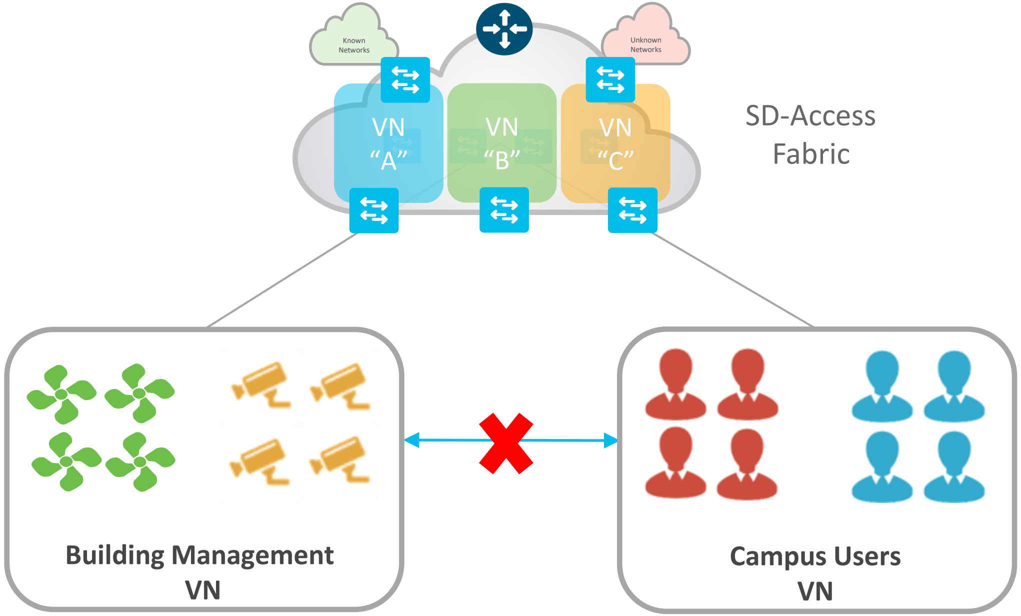
virtual networks

Virtual Network 1

Virtual Network 2

SD-Access Policy

Two Level Hierarchy - Macro Segmentation

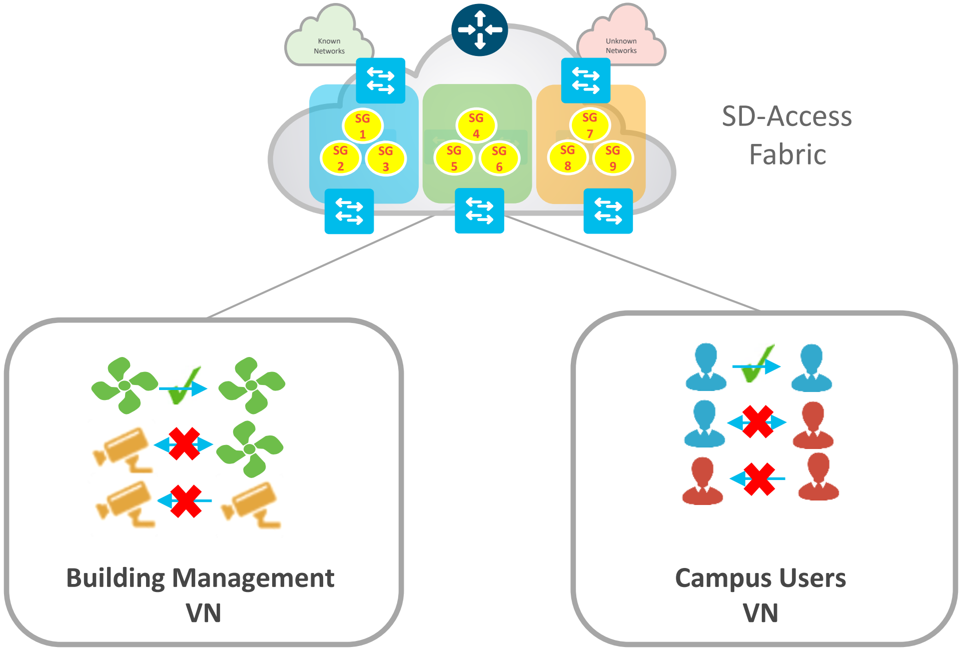


Virtual Network (VN)

First level Segmentation ensures **zero communication** between forwarding domains. Ability to consolidate multiple networks into one management plane.

SD-Access Policy

Two Level Hierarchy - Micro Segmentation



SD-Access Fabric

Building Management VN

Campus Users VN

Scalable Group (SG)

Second level Segmentation ensures **role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Design your Security Access Policy

NETWORK ACCESS

	PROTECTED SERVERS	SHARED SERVICES	PUBLIC NETWORK
EMPLOYEE	✓	✓	✓
CONTRACTOR	−	✓	✓
Guest	−	−	✓

AUTHORIZATION

What you can do?

Design your Security Access Policy

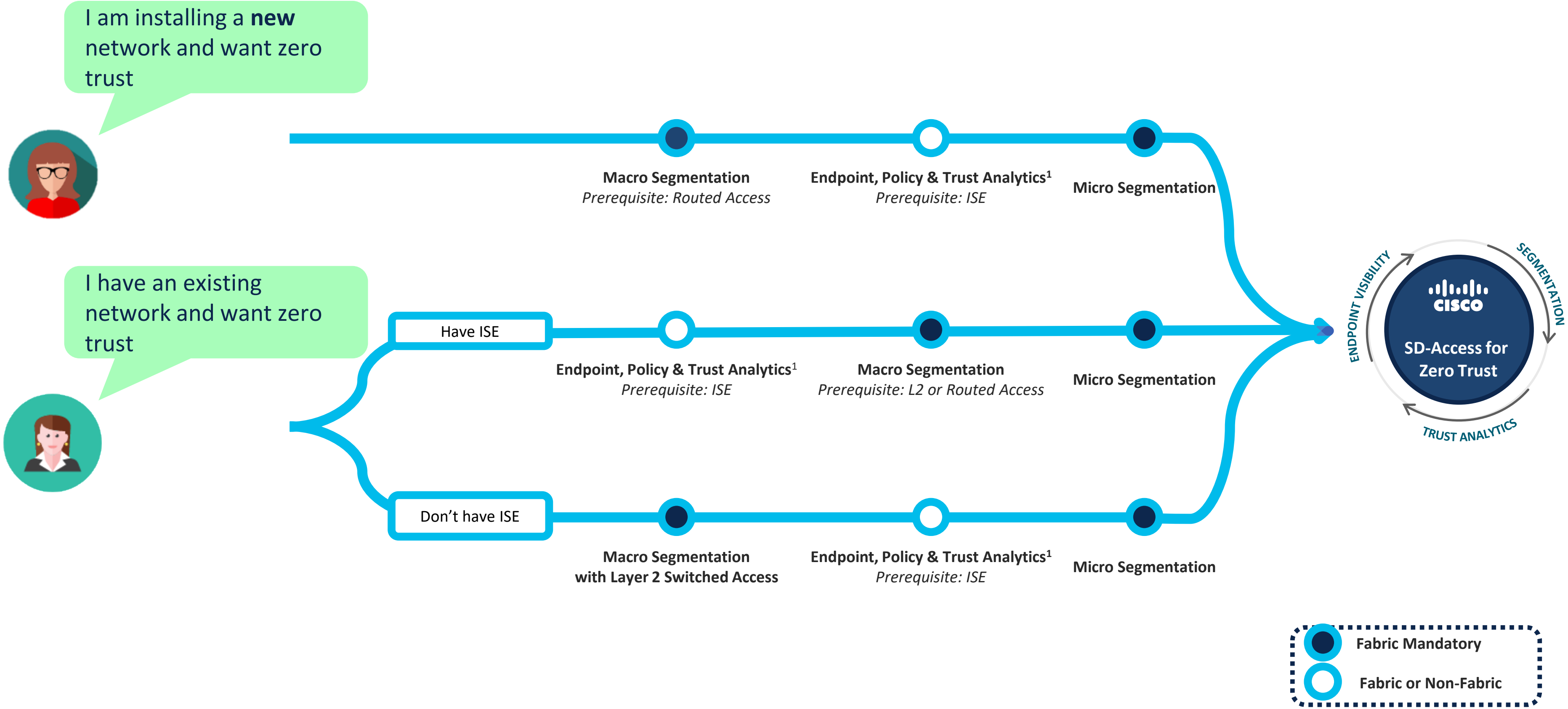
Basic Tenant of Zero Trust

The effect of Zero Trust is

Ubiquitous Least-Privilege Access

(i.e. grant access,
but make it specific!)

Flexible Start Options removes barriers to Quick Value



I am installing a **new** network and want zero trust

Macro Segmentation
Prerequisite: Routed Access

Endpoint, Policy & Trust Analytics[1]
Prerequisite: ISE

Micro Segmentation

I have an existing network and want zero trust

Have ISE

Endpoint, Policy & Trust Analytics[1]
Prerequisite: ISE

Macro Segmentation
Prerequisite: L2 or Routed Access

Micro Segmentation

Don't have ISE

Macro Segmentation with Layer 2 Switched Access

Endpoint, Policy & Trust Analytics[1]
Prerequisite: ISE

Micro Segmentation

SD-Access for Zero Trust

● Fabric Mandatory

○ Fabric or Non-Fabric

Agenda

- Discussion of Zero-trust and Fabric
- ISE – overview
- Catalyst Center - overview
- Conclusion

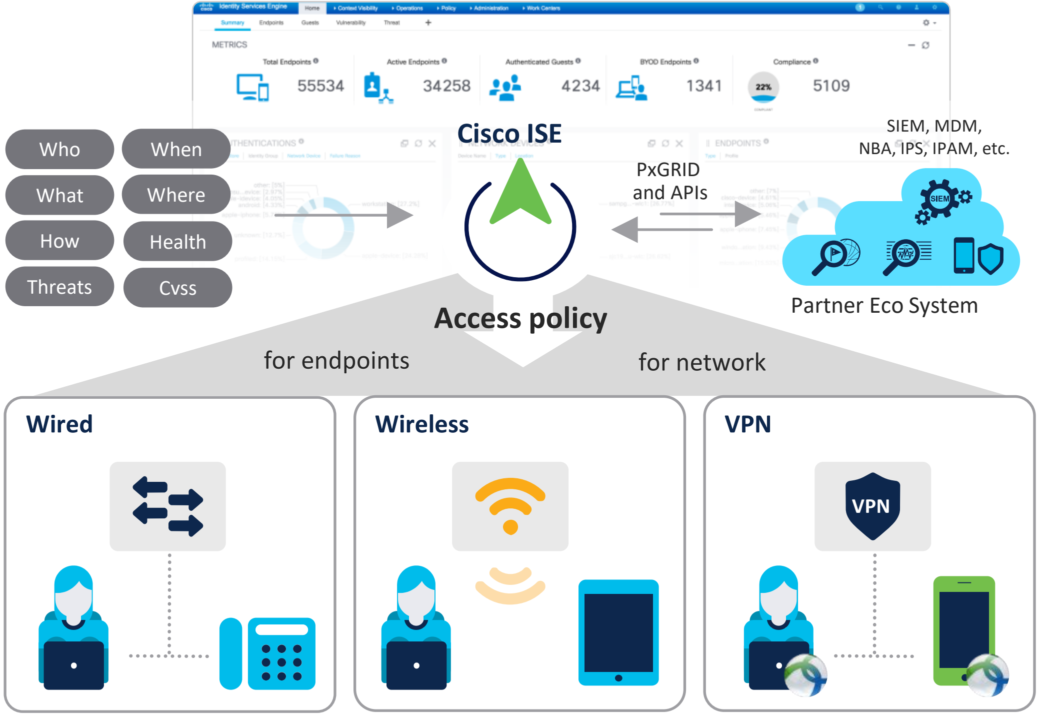
Cisco ISE for intent-based access

Cisco Identity Services Engine (ISE) is an industry leading, Network Access Control and Policy Enforcement platform, that lets you,

See
Users, endpoints and applications

Secure
By controlling network access and segmentation

Share
Context with partners for enhanced operations



METRICS

Total Endpoints	Active Endpoints	Authenticated Guests	BYOD Endpoints	Compliance
55534	34258	4234	1341	5109

Who | When | What | Where | How | Health | Threats | Cvss

Cisco ISE

PxGRID and APIs

SIEM, MDM, NBA, IPS, IPAM, etc.

Partner Eco System

Access policy

for endpoints

for network

Wired

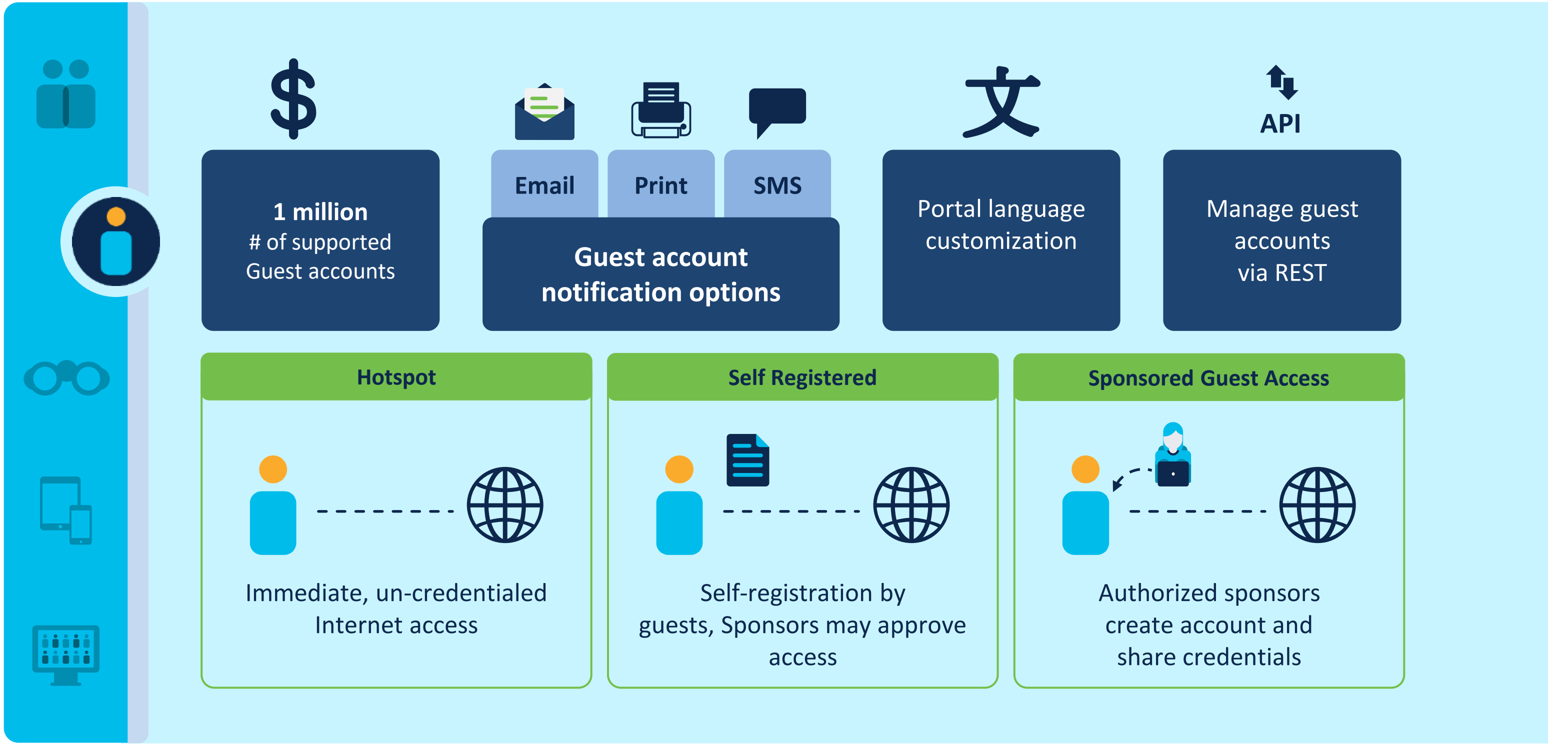
Wireless

VPN

Role-based Access Control | Guest Access | BYOD | Secure Access

Guest access

Smart ways of onboarding Guest



$

1 million
# of supported
Guest accounts

Email

Print

SMS

Guest account notification options

文

Portal language customization

API

Manage guest accounts via REST

Hotspot

Immediate, un-credentialed Internet access

Self Registered

Self-registration by guests, Sponsors may approve access

Sponsored Guest Access

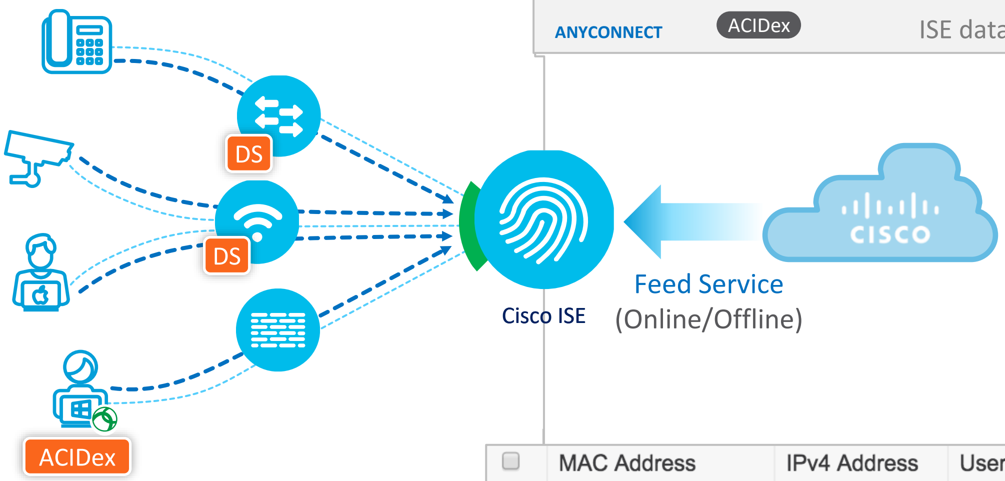
Authorized sponsors create account and share credentials

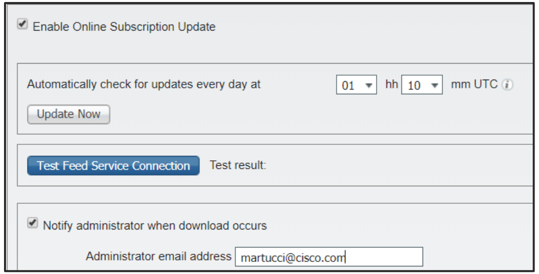
Profiling and probes

ACTIVE PROBES	Netflow, DHCP, DNS, HTTP, RADIUS, NMAP, SNMP, AD
DEVICE SENSOR	CDP, LLDP, DHCP, HTTP, H323, SIP, MDNS
ANYCONNECT	ACIDex

ISE data collection methods for Device profiling

Endpoints send interesting data, that reveal their device identity




☑ Enable Online Subscription Update

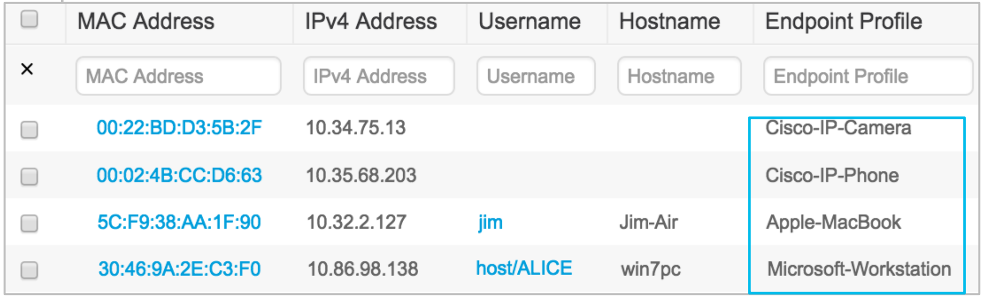
Automatically check for updates every day at 01 hh 10 mm UTC

Update Now

Test Feed Service Connection Test result:

☑ Notify administrator when download occurs

Administrator email address martucci@cisco.com

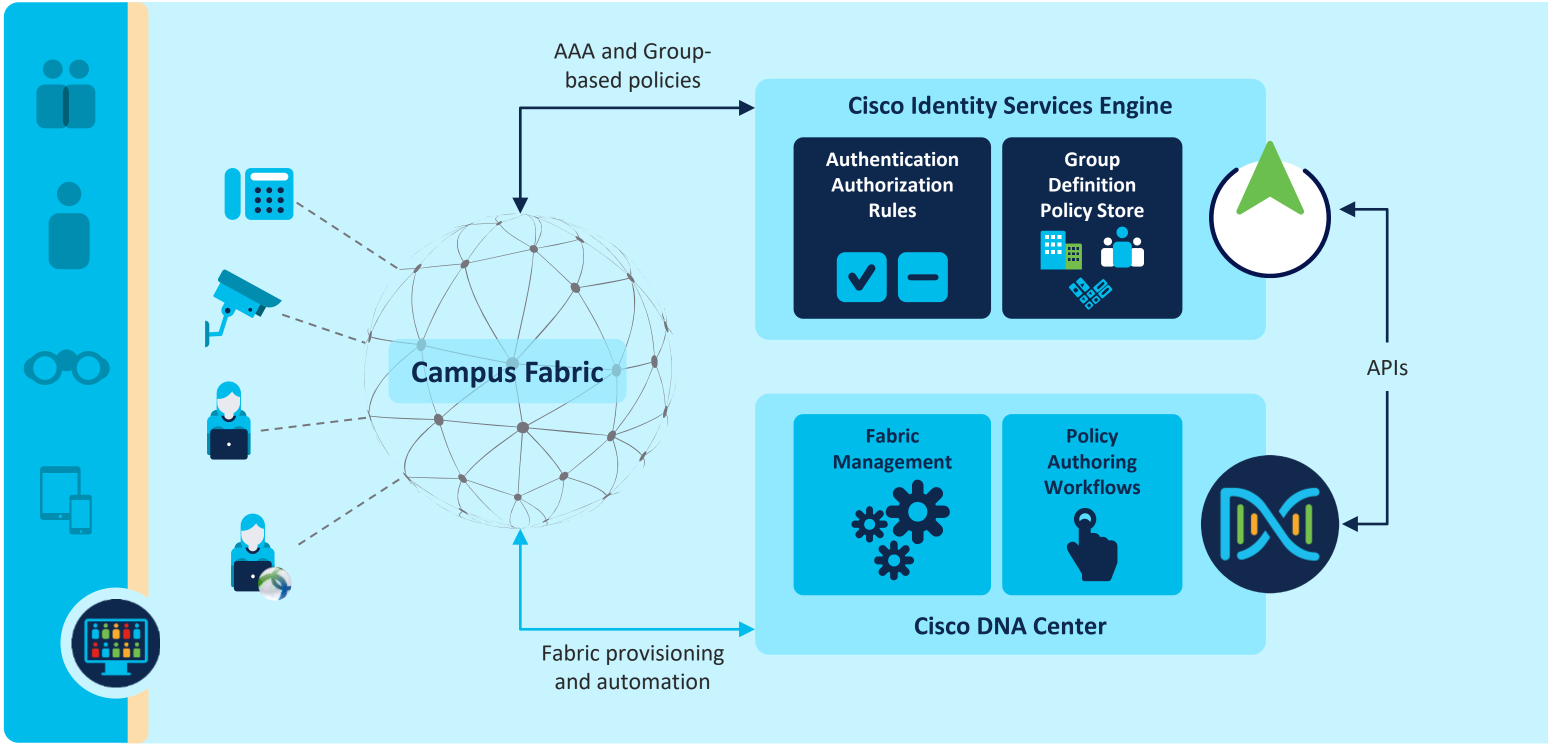


□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
×	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
□	00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
□	5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
□	30:46:9A:2E:C3:F0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

Profling helps with differentiated access also for authenticated devices

Network segmentation with policy

Segmenting with software defined access

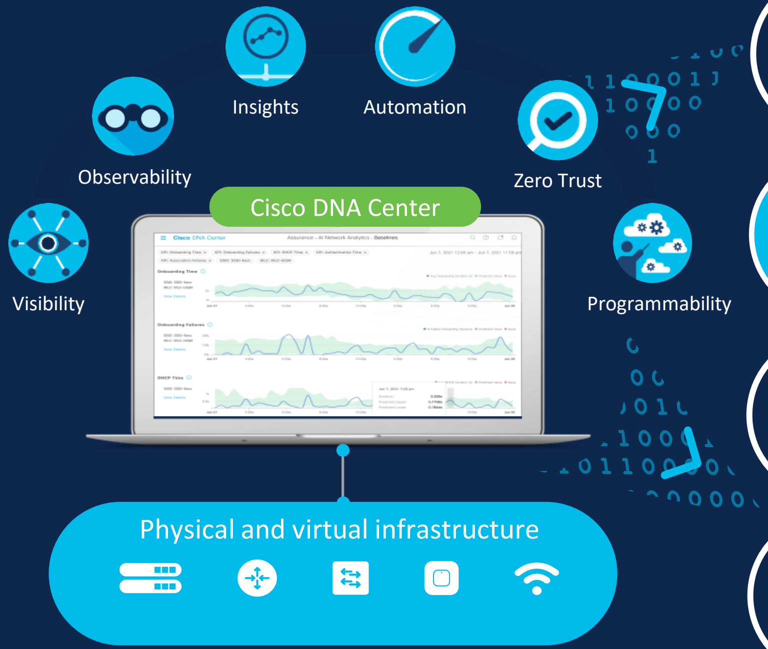

AAA and Group-based policies
Cisco Identity Services Engine
Authentication Authorization Rules
Group Definition Policy Store
Campus Fabric
APIs
Fabric Management
Policy Authoring Workflows
Cisco DNA Center
Fabric provisioning and automation

Agenda

- Discussion of Zero-trust and Fabric
- ISE – overview
- Catalyst Center - overview
- Conclusion

Cisco Catalyst Center

Provides that digital agility to drive network insights, automation, and security



AIOps

AI-driven visibility, observability, insights, and troubleshooting to ensure the health of your ***users***, applications, and infrastructure

NetOps

Automation to simplify the creation and maintenance of your networks with flexibility to move from manual to AI-assisted to ***selectively autonomous*** network management

SecOps

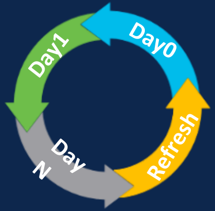
AI-driven security to classify endpoints and enforce security policies for a complete ***zero trust*** workplace solution

DevOps

Mature APIs, SDKs, and closed-loop integrations to simplify and streamline ***ecosystem integration***

Cisco DNA Center NetOps

Simplify change management at scale and accelerate remediation



Cradle to grave element management

- ❖ E2E device lifecycle Management
- ❖ Insights into network Inventory
- ❖ Zero-touch onboarding
- ❖ Simplified RMA
- ❖ Device refresh
- ❖ Wireless Maps (3D, Ekahau Site planning)
- ❖ Simplified Telemetry Enablement
- ❖ Security Advisories

Empowering users with Intent based Configuration Automation and turnkey compliance remediation

- ❖ Intent Based Configuration for Wireless and Wired
- ❖ CLI Templates (Jinja, Velocity)
- ❖ Software and Config Compliance
- ❖ Security Compliance
- ❖ Template Compliance
- ❖ Compliance Reports and Acknowledgement
- ❖ Model based Configurations

Orchestration and optimization of network services end-to-end

- ❖ Support for Network Services such as QoS, Security, Site-Site VPN, Traffic SPAN.
- ❖ Support for Wireless AP refresh, AP config workflow, RLAN config, Brownfield Learn
- ❖ Topology-agnostic Services Framework including
  - ✓ Discovery
  - ✓ Management

Resource Lifecycle Management

Configuration Management Lifecycle

Workflows for Advanced Use Cases

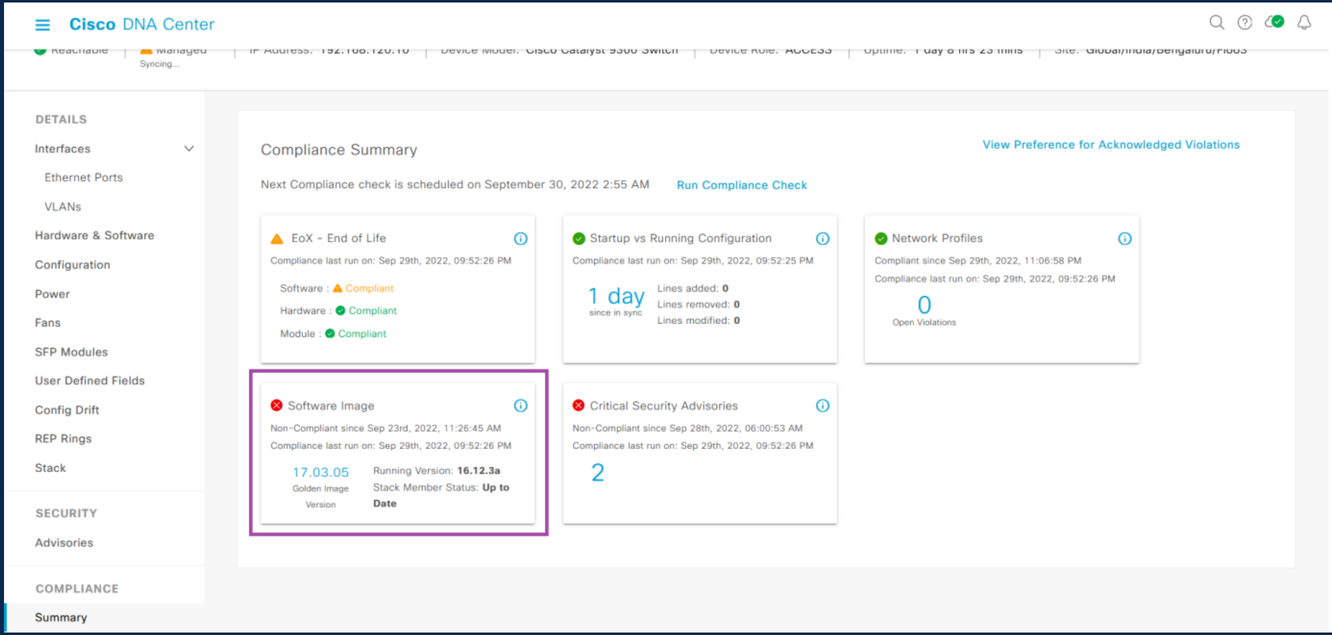
Catalyst Center - compliance

Delivered

Visibility into Non-Compliant Devices SWIM

Stack Switch version mismatch

- Compliance helps identify software version mismatch
- The Software Version mismatch is based on Golden image tagged in DNAC vs Image running on the device



Reachable | Managed Syncing... | IP Address: 192.168.120.10 | Device Model: Cisco Catalyst 9300 Switch | Device Role: ACCESS | Uptime: 1 day 8 hrs 23 mins | Site: Global/India/Bengaluru/Floo3

Compliance Summary

Next Compliance check is scheduled on September 30, 2022 2:55 AM

EoX - End of Life
Compliance last run on: Sep 29th, 2022, 09:52:26 PM
Software : Compliant
Hardware : Compliant
Module : Compliant

Startup vs Running Configuration
Compliance last run on: Sep 29th, 2022, 09:52:25 PM
1 day since in sync
Lines added: **0**
Lines removed: **0**
Lines modified: **0**

Network Profiles
Compliant since Sep 29th, 2022, 11:06:58 PM
Compliance last run on: Sep 29th, 2022, 09:52:26 PM
0 Open Violations

Software Image
Non-Compliant since Sep 23rd, 2022, 11:26:45 AM
Compliance last run on: Sep 29th, 2022, 09:52:26 PM
17.03.05 Golden Image Version
Running Version: **16.12.3a**
Stack Member Status: **Up to Date**

Critical Security Advisories
Non-Compliant since Sep 28th, 2022, 06:00:53 AM
Compliance last run on: Sep 29th, 2022, 09:52:26 PM
2

Agenda

- Discussion of Zero-trust and Fabric
- ISE –overview
- Catalyst Center - overview
- Conclusion

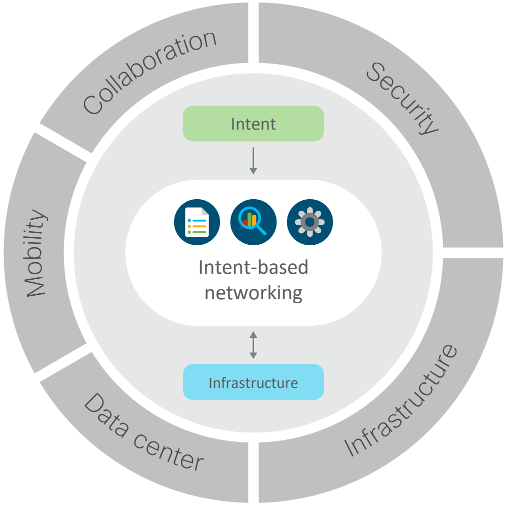
Conclusion

What helps customer:

- Know what's on your network, Secure Access - ISE
- Automation, Intent-Based Networking, Assurance (insights) – Catalyst Center
- Power the Platform

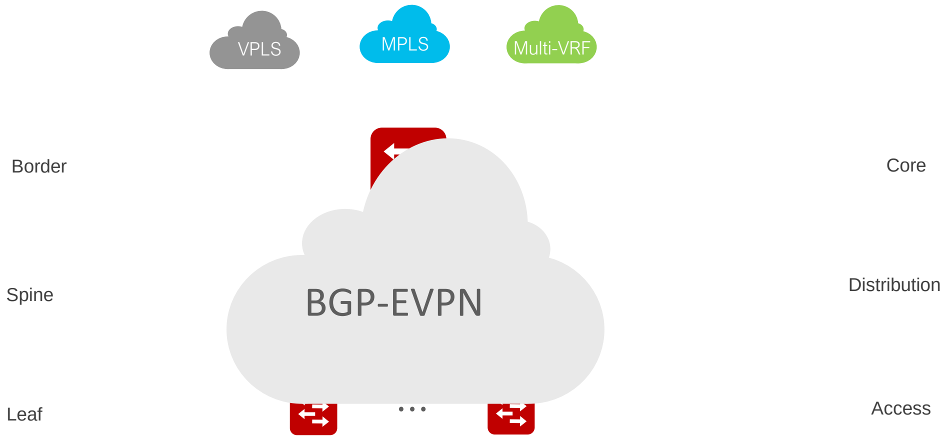
Enterprise fabric architectures

SD-Access



- Leading architecture for enterprise providing **seamless mobility and enhanced security**
- Integrated Automation, Assurance Analytics capabilities **driven from Cisco DNA-Center**
- Integrated Wireless capabilities driving **consistent policies across wired and wireless networks**

BGP EVPN



- Industry based solution providing **interoperability with 3rd party devices**
- Solution for **Brownfield environments** – MPLS, VPLS, Multi-VRF, GRE.
- **Single Overlay Solution** from campus to datacenter, all the way to cloud
- **DIY based provisioning and automation** for fabric deployment

The bridge to possible