



Zero Trust Workplace with Cisco DNA

Santa Monica Networks Security Day

Taras Dmytriv
Systems Engineer
November 2022

Taras Dmytriv



- Helping customers to transform their network infrastructure with Cisco Solutions
- Background in Advanced Services and Customer Success roles
- Coffee, sci-fi, and eSports enthusiast



Helsinki, Finland

Session Objective



- Inform
- Educate
- Inspire

Agenda

- 1 Cisco Digital Network Architecture
- 2 Cisco Continuous Trust Overview
- 3 Cisco Segmented Access Overview

What is Cisco DNA?

Cisco Digital Network Architecture

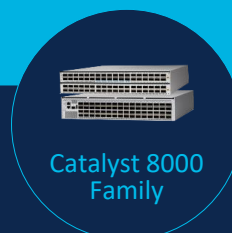
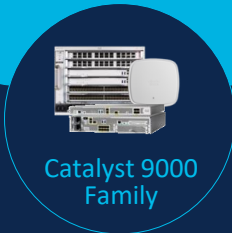
Begins with 3 pillars for secure, agile networking



**Software Defined and
Systems Thinking**



Digital-Ready Infrastructure



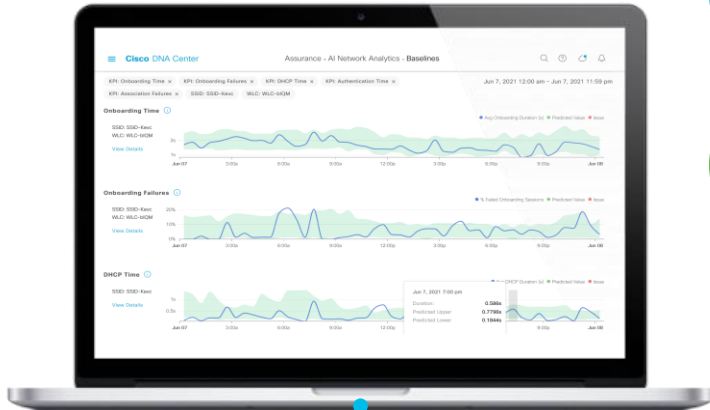
Zero Trust Security Model



Cisco DNA Center is a foundational platform technology

Command and control center for Cisco Catalyst

Cisco DNA Center



Physical and virtual infrastructure



Cisco and third party



Automation

Automation and workflows simplify building and maintaining large scale networks. AI/MR streamlines and simplifies complex tasks



Analytics

AI/ML and insights to ensure the health, performance and reliability of applications and infrastructures



Security

AI/ML and DPI Identify and classify endpoints, enforce security policies and mitigate threats for a complete workplace zero trust solution



Programmability

Mature APIs, SDKs, and closed-loop integrations, untangle the complexities of interconnecting third party systems

Cisco Catalyst 9000 Family



Cisco Catalyst
9300 Series

Cisco Catalyst
9400 Series

Cisco Catalyst
9500 Series

Cisco Catalyst
9600 Series



Cisco Catalyst
9800 Series



Cisco Catalyst
9100 Series

Cisco Catalyst
9200 Series



Access switching

Core/Dist switching

Wireless

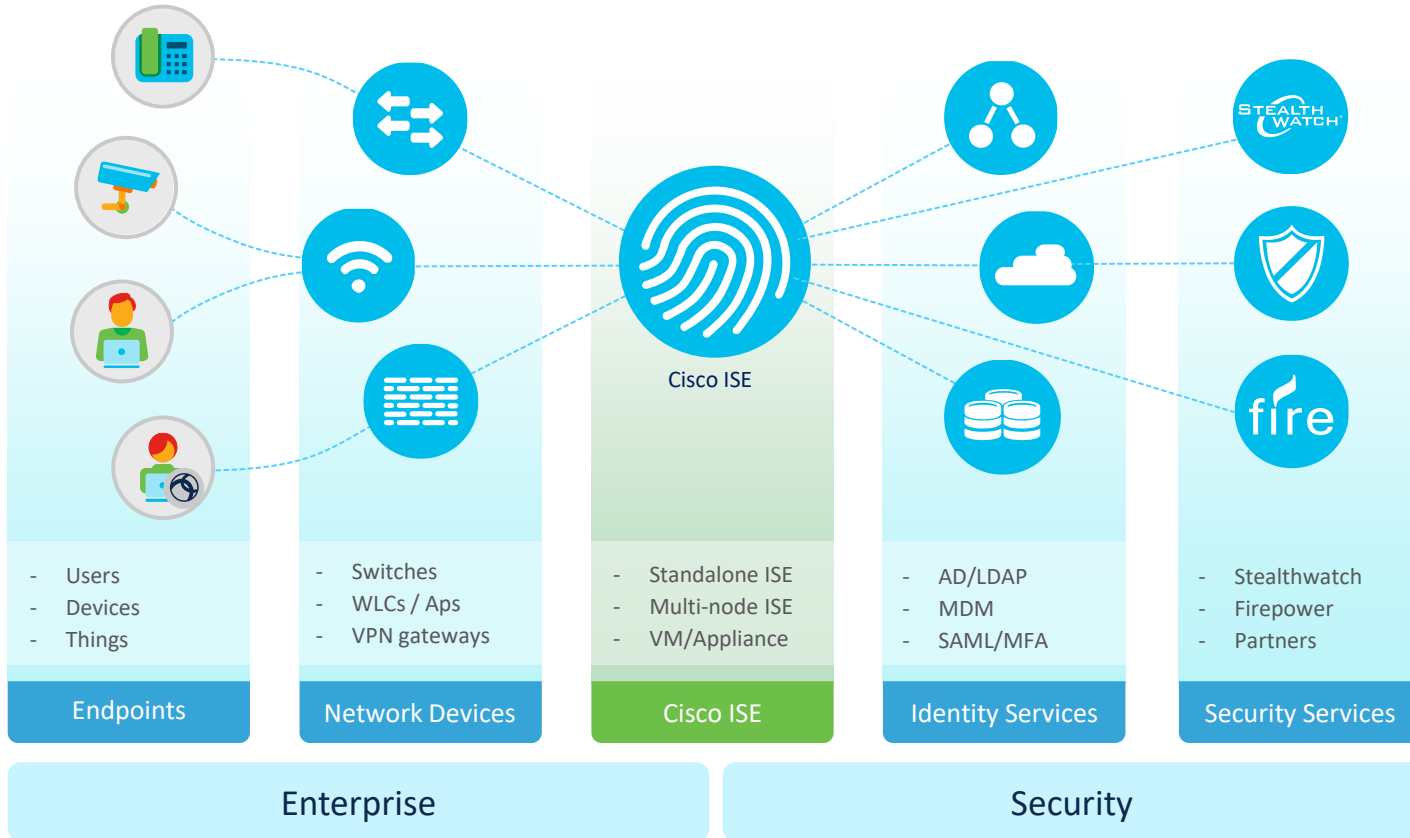
IOS-XE

Common Software Architecture

Programmable ASIC

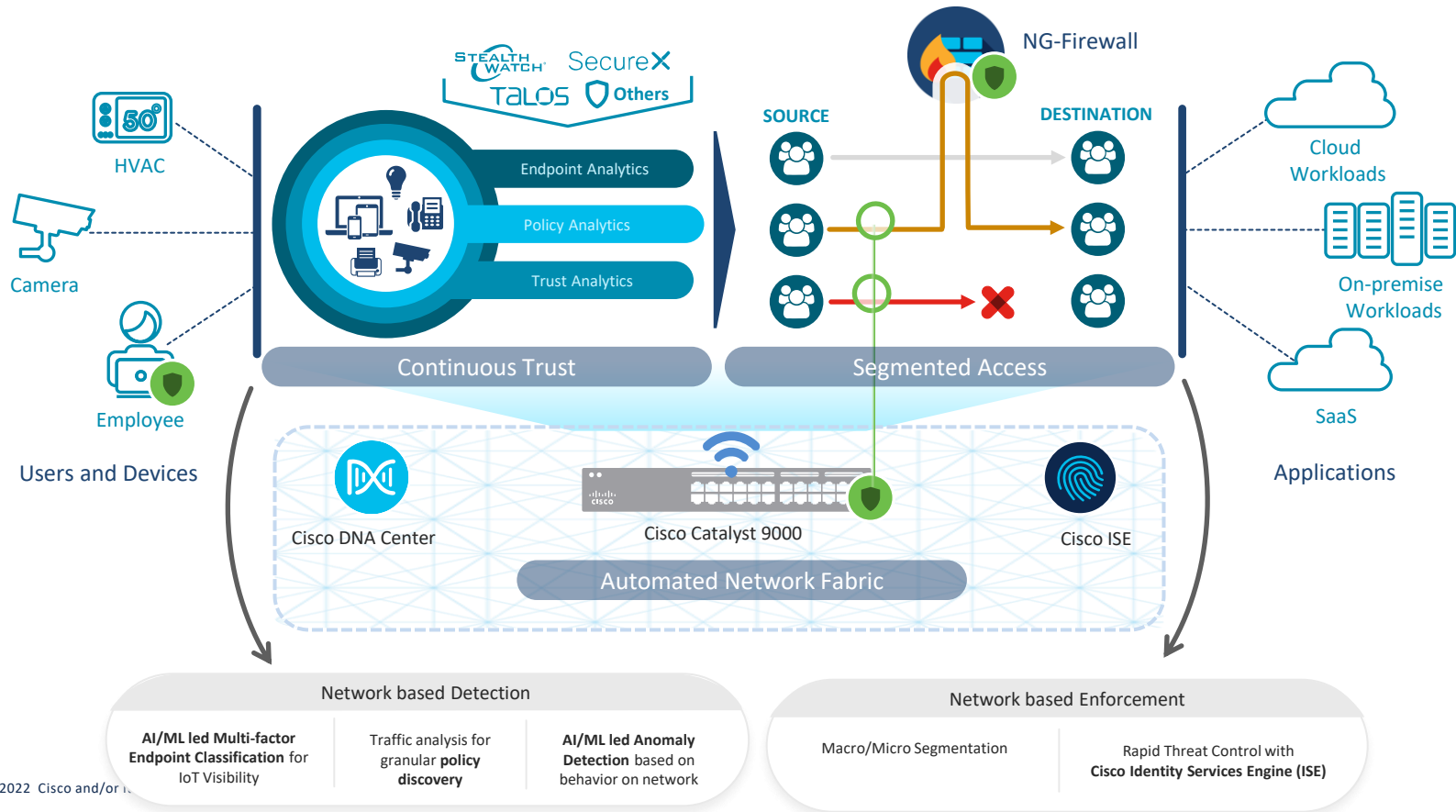
Common Hardware Architecture

Identity with ISE is Secures the Enterprise



SD-Access Delivers Trusted Workplace

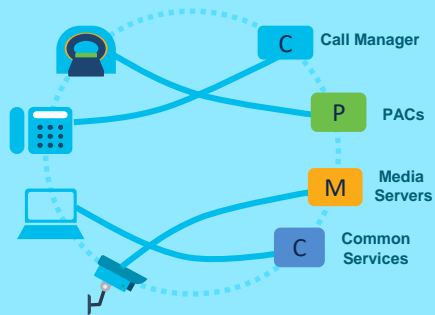
Leverage Network and ML to Scale Workplace Zero-Trust



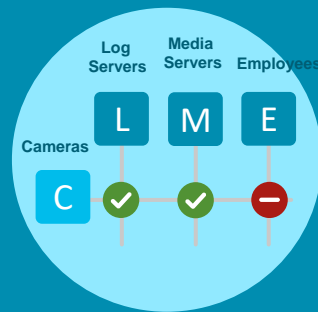
Continuous Trust



KNOW
Your
Endpoints



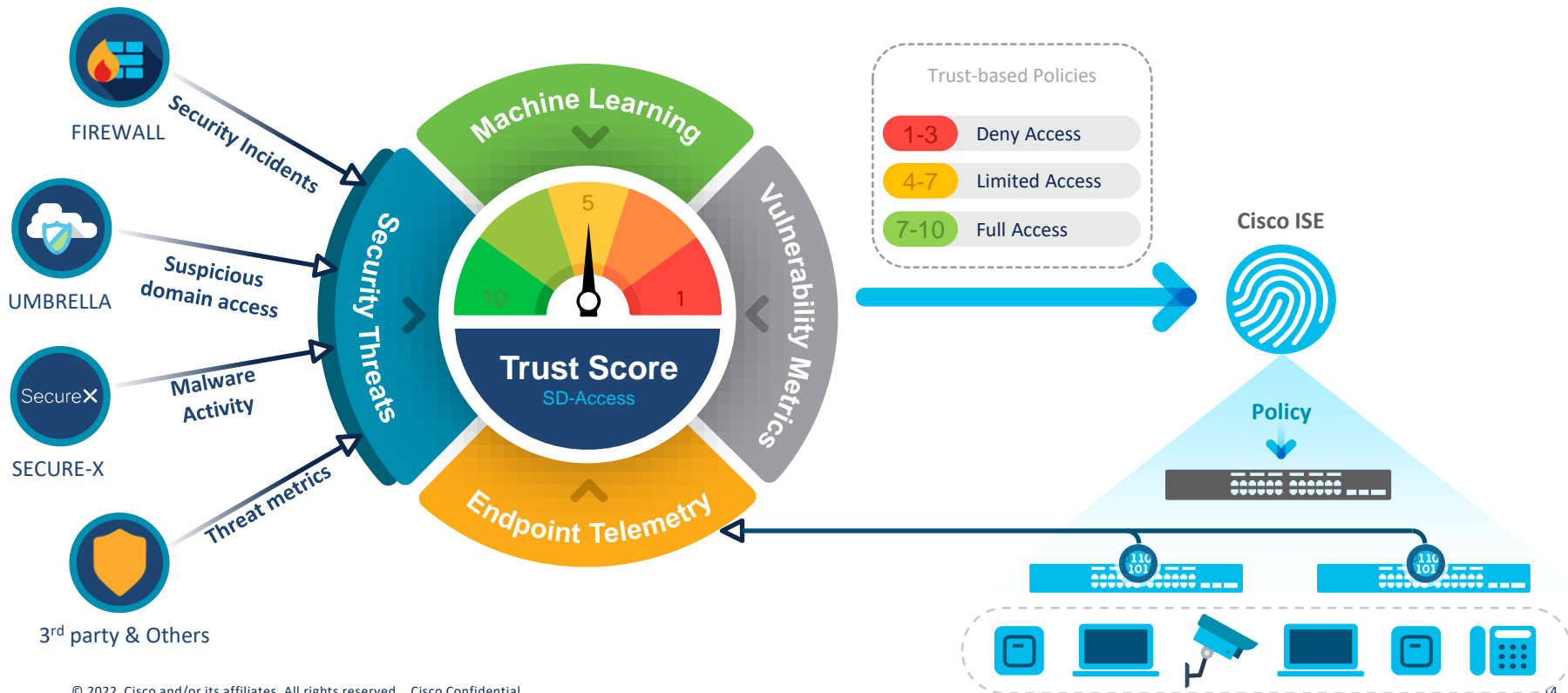
SEE
what they
talk to



DO/CREATE
the right
segmentation
policy

Workplace Zero-Trust manifested as Trust Score

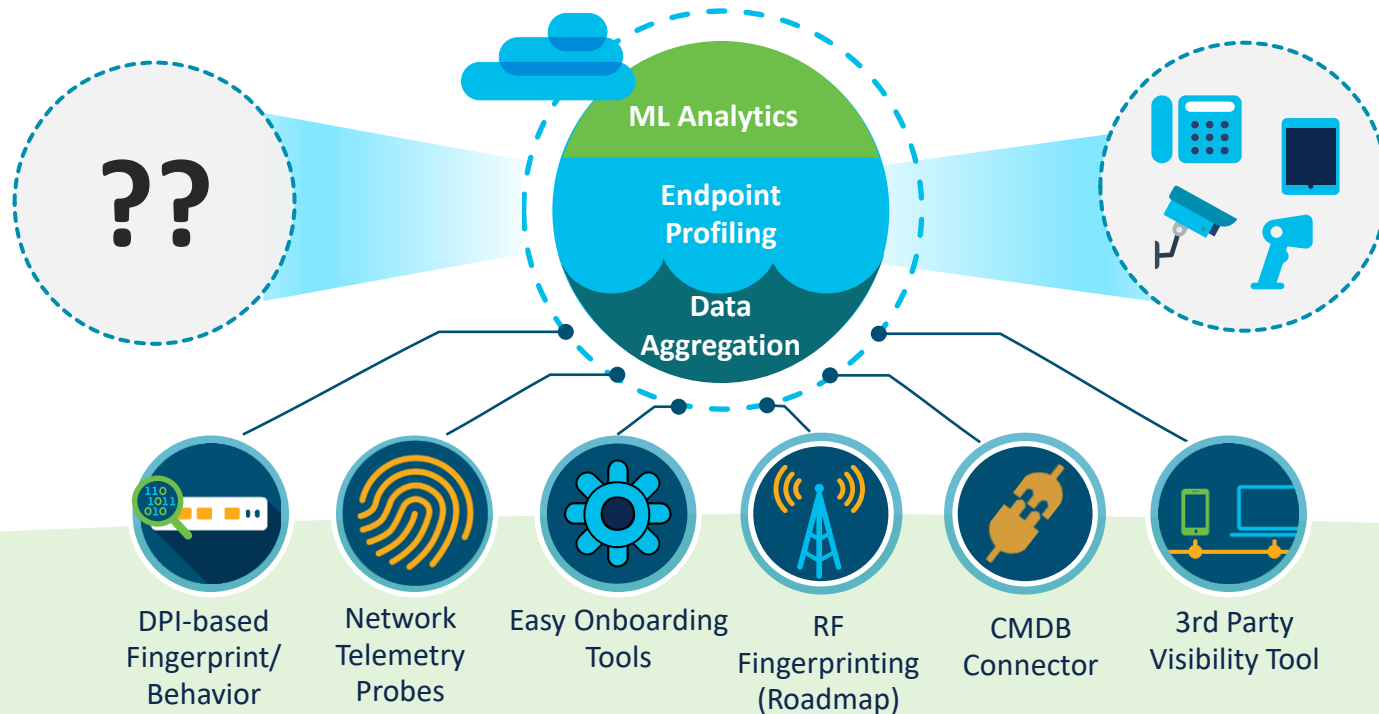
Automate Threat Response with Trust-based Policies



Endpoint Analytics

Endpoint Analytics on Cisco DNA Center

Rapidly reducing the unknowns to gain visibility on the pathway to Zero Trust



AI Endpoint Analytics: Multifactor classification

Classifying endpoints using four independent label categories for more flexible profiling



Device type

Laptop

CT scanner

Smartphone



Hardware model

MacBook Pro

Optima CT540

Galaxy S8



Hardware manufacturer

Apple

GE

Samsung



Operating system

MacOS 10.14.6

CTT OS 6.3.x Linux

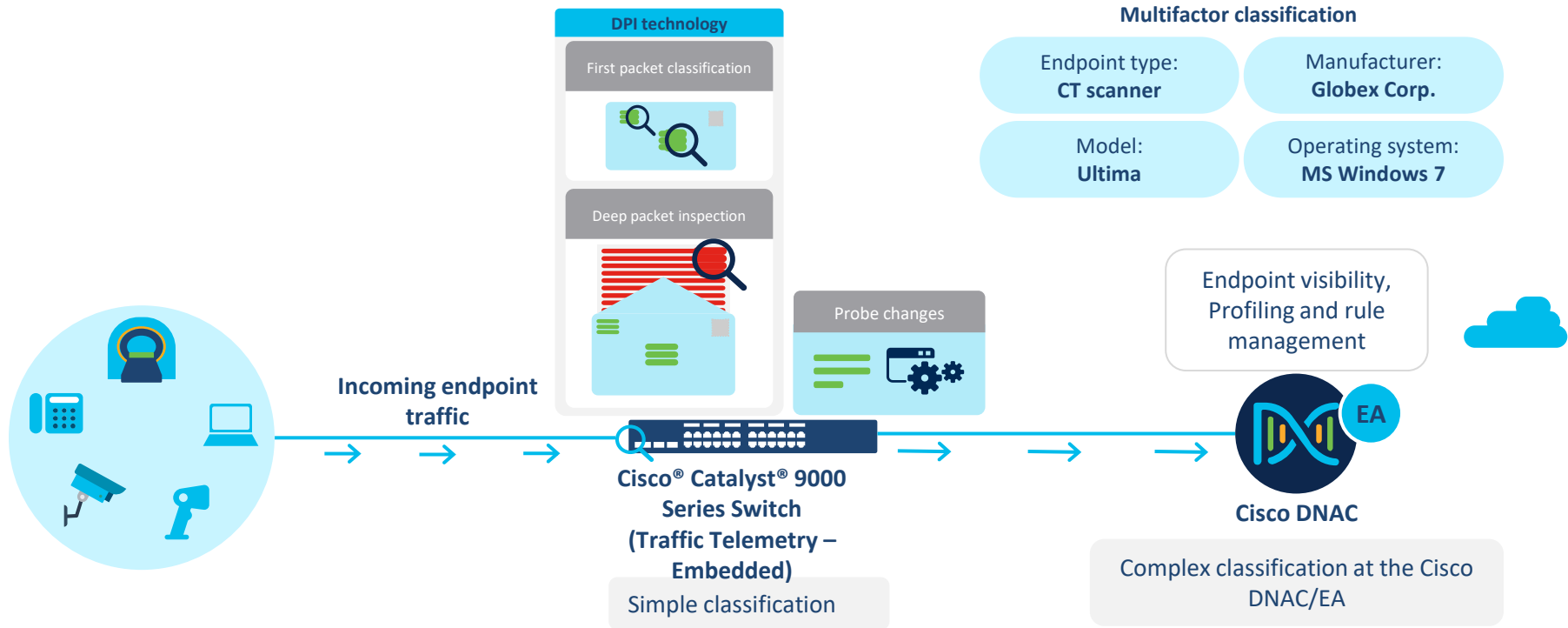
Android 9.0

Cisco ISE probes and data sources



Unique Cisco ISE probes used in EA	
ISE and Third party	RADIUS AD MDM
AnyConnect	ACIDex

EA Profiling using Embedded Traffic Telemetry



IOTAsset Attributes in Endpoint Analytics

Cisco DNA Center Policy · Endpoint Analytics

Overview **Endpoint Inventory** Profiling Rules Hierarchy

VIEW KNOWN PROFILES: Endpoint Type OS Type Hardware Model Hardware

Filter Actions 1 Selected

MAC Address	Hostname	Endpoint Type	OS Type
<input type="checkbox"/> 00:50:56:94:D0:54	kernow-w103	Workstation	Windows 7
<input type="checkbox"/> 00:50:56:A0:1A:50	kernow-w7-1	Workstation	Windows
<input type="checkbox"/> 00:50:56:A0:56:22	kernow-w7-1	Workstation	Windows
<input type="checkbox"/> 00:50:56:A0:72:89	kernow-w7-1	Workstation	Windows 7
<input type="checkbox"/> 00:50:56:A0:B9:44	kernow-w7-1	Coffee Machine	-
<input checked="" type="checkbox"/> 00:50:56:A0:C8:67	CT-Scanner-1	CT-Scanner	Linux
<input type="checkbox"/> 00:50:56:A0:D7:3F	PACS-System-1	Storage	Linux
<input type="checkbox"/> 04:6C:9D:1F:88:00	-	-	-
<input type="checkbox"/> 70:DB:98:76:1E:8A	-	-	-

00:50:56:A0:C8:67

DETAILS

MAC Address	00:50:56:A0:C8:67	OS Type	Linux
location	Cisco UK/Reading/300	Hardware Model	Magnetom Vida
Endpoint Type	Longwater Avenue CT-Scanner	Hardware Manufacturer	Siemens Healthcare

ATTRIBUTES [View Attribute Glossary](#)

> RADIUS

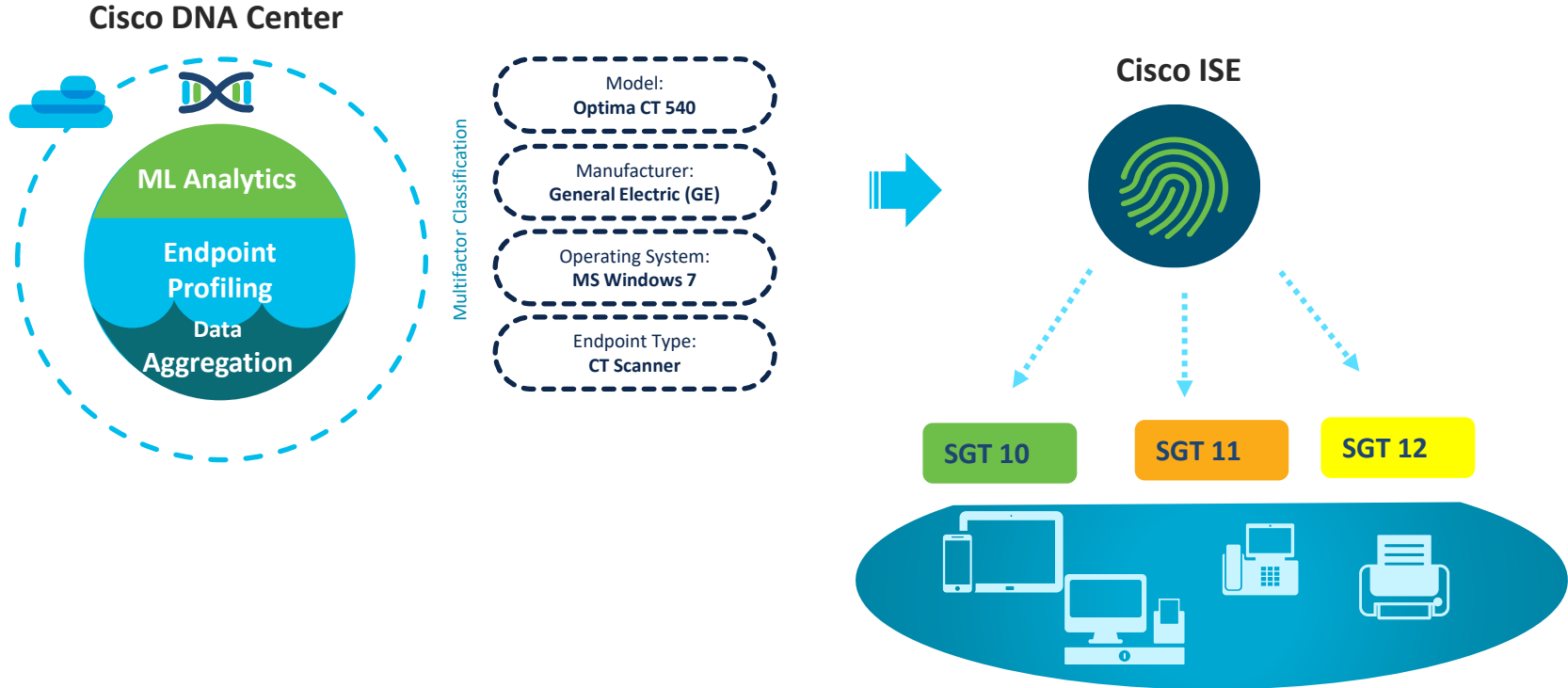
> SNMP

From Profile Label:

IOTAsset

assetDeviceType	CT-Scanner	Endpoint Type
assetHwRevision	Magnetom Vida	Hardware Model
assetIpAddress	10.4.1.124	
assetMacAddress	00:50:56:A0:C8:67	
assetSwRevision	Linux	OS Type
assetVendor	Siemens Healthcare	Hardware Manufacturer

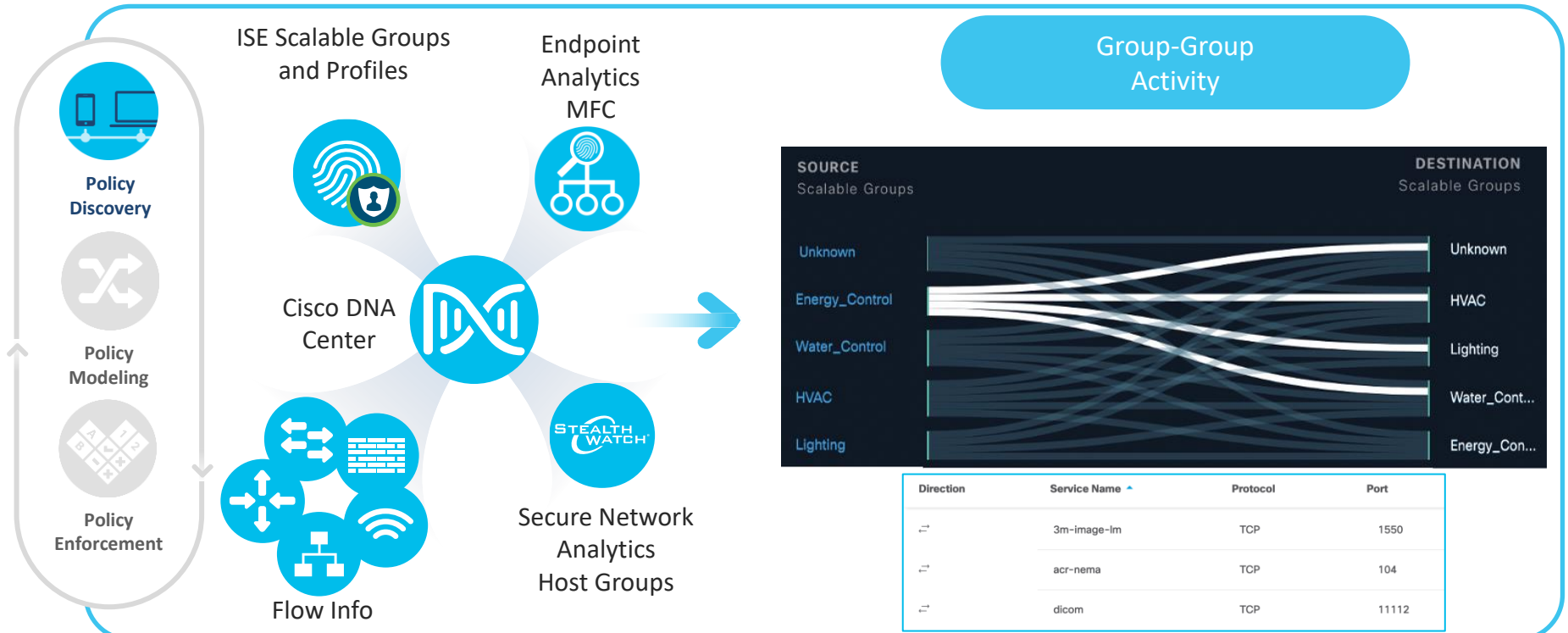
Better Classification reduces unauthorized access



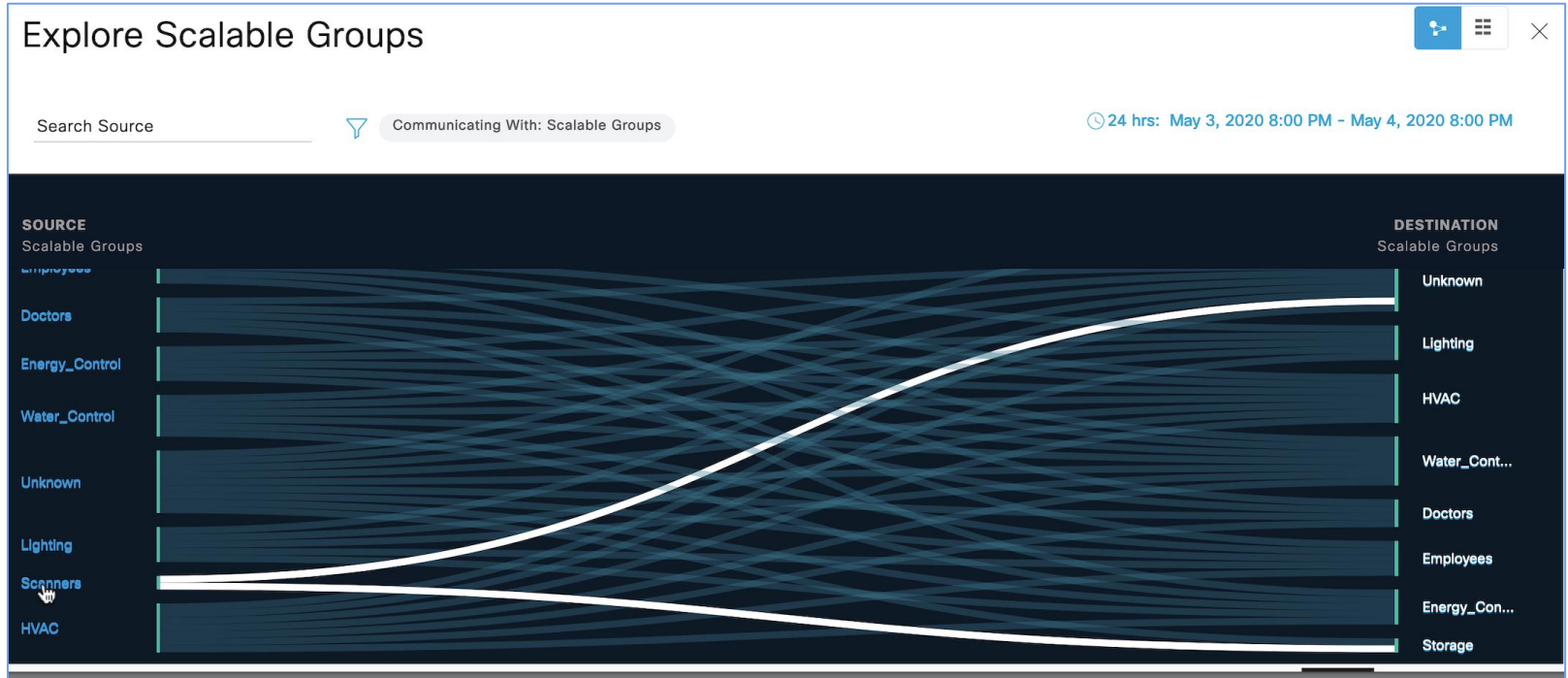
Policy Analytics

Group-Based Policy Analytics

Application on Cisco DNA Center: Turn policy on incrementally!



Group to Group Activity



Detecting Ports/Protocols Between Groups

Scalable Groups Traffic > Scanners ↔ Storage

SOURCE
Scalable Groups

DESTINATION
Scalable Groups

Scanners Storage

Scanners → Storage

Search Table

Create Report Download Report **View Contract**

Direction	Service Name	Protocol	Port
↔	3m-image-lm	TCP	1550
↔	acr-nema	TCP	104
↔	dicom	TCP	11112

N.B. DICOM: Digital Imaging and Communications in Medicine

Ports 104, 1550 and 11112 detected between Scanners and Storage groups, all used for DICOM interaction

Identify the specific ports/protocols needed in access control policies

Contract and Discovered Information Side-by-Side

(GBPA App on Cisco DNA Center)

The screenshot displays the Cisco DNA Center interface for Group-Based Access Control (GBPA). The top navigation bar includes the Cisco DNA Center logo, the current page title 'Policy · Group-Based Access Control', and search, help, and refresh icons. The main navigation menu shows 'Policies', 'Scalable Groups', 'Access Contracts', and 'Analytics', with 'Analytics' selected. The breadcrumb trail is 'Overview > Policy Analytics for Scalable Groups > Scanners → Storage > Contract Page'. The current view is 'Scanners → Storage' and 'Policy Details'.

The interface is split into two main panels, both highlighted with orange borders:

- Left Panel (Configured Contract):** Titled 'Contract: Permit_Scanner2PACS_DICOM' with an 'Edit' link. It contains a table with columns: #, Action, Application, Protocol, Source Port, Destination Port, Logging, and Action. The table lists three entries, all with 'PERMIT' action and 'advanced' application. A blue arrow points from the 'View traffic' link of the first entry to the right panel.
- Right Panel (Discovered Traffic Flows):** Titled 'All Unique Traffic Flows' with a time filter '24 hrs: Jan 17, 2021 3:00 PM - Jan 18, 2021 3:00 PM'. It contains a table with columns: Direction, Service Name, Protocol, and Port. One entry is shown: 'acr-nema' service, 'TCP' protocol, and port '104'. The text 'DISCOVERED via GBPA' is overlaid in large yellow letters.

#	Action	Application	Protocol	Source Port	Destination Port	Logging	Action
1	PERMIT	advanced	TCP	104		OFF	View traffic
2	PERMIT	advanced	TCP	1550		OFF	View traffic
3	PERMIT	advanced	TCP	11112		OFF	View traffic

Direction	Service Name	Protocol	Port
→	acr-nema	TCP	104

Create/Edit Contract Easily Based on Discovered Flows (GBPA App on Cisco DNA Center)

The screenshot displays the Cisco DNA Center interface for managing Group-Based Access Control (GBAC) contracts. The breadcrumb trail indicates the path: Overview > Policy Analytics for Scalable Groups > Water_Control → Energy_Control > Contract Page. The current view is for the contract 'Permit IP'.

CONTRACT CONTENT (2)

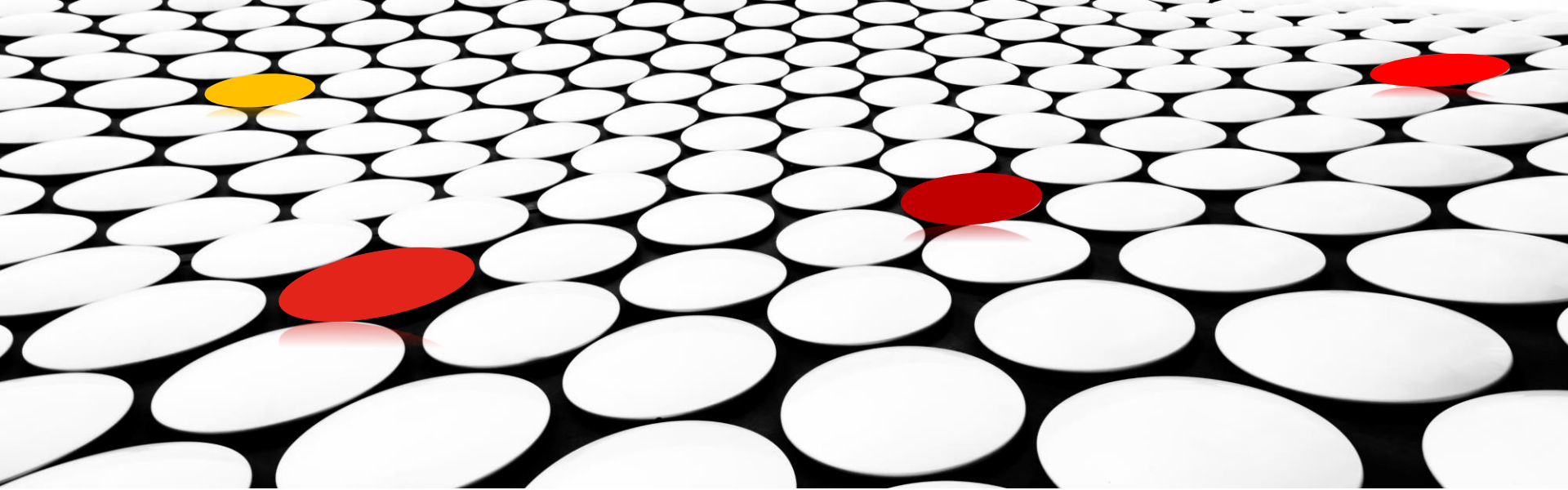
#	Action*	Application*	Transport Protocol	Source / Destination	Port	Logging	Action
1	Selec...▼	Select...▼		Destination		<input type="checkbox"/>	+ X
2	Selec...▼	ftp	TCP	Destination	21	<input type="checkbox"/>	+ X

All Unique Traffic Flows (24 hrs: Jan 18, 2021 5:00 PM - Jan 19, 2021 5:00 PM)

Direction	Service Name	Protocol	Port	Action
↔	ftp	TCP	21	Add to contract
↔	https	TCP	443	Add to contract
↔	telnet	TCP	23	Add to contract
→	tftp	UDP	69	Add to contract
→	Unassigned	ICMP	0	Add to contract

A green arrow points from the 'Add to contract' link in the traffic flow table to the 'Add to contract' link in the contract content table, illustrating the process of adding a discovered flow to a contract.

Trust Analytics



Trust Analytics:

Continuous evaluation of endpoint behavior /anomalies to provide right level of access.

Trust context and impact on Trust score

Positive Influence

- Secure Authentication
- Posture Compliance



Negative Influence

- Suspicious behavior (Impersonation using MAC spoofing)
- Connections to Low reputation IP's.
- Insecure interface (Unauthorized ports/weak credentials)
- ...
- ...

Access Control and Threat Containment based on continuous trust evaluation



Trust-based Policies

1-3

Deny Access

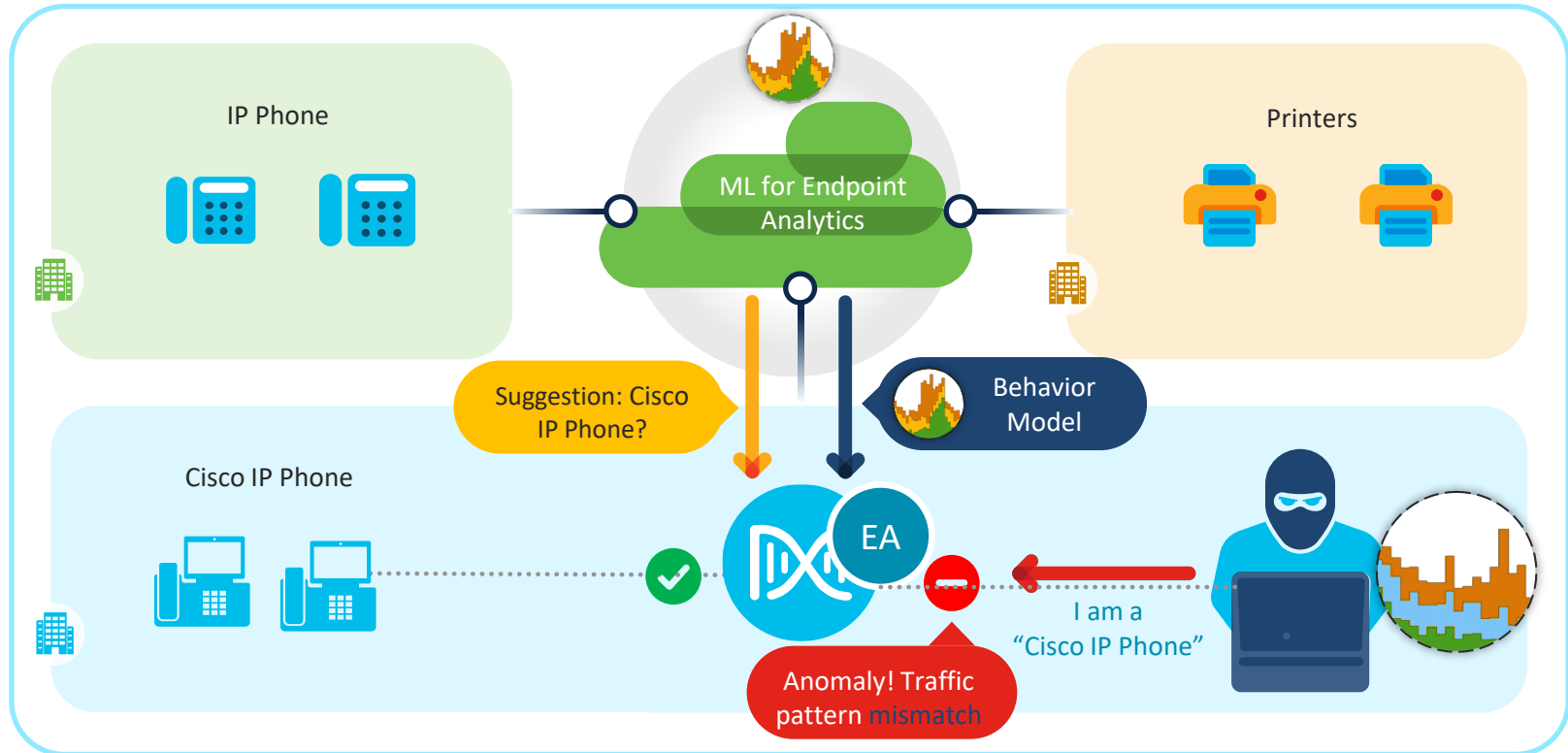
4-7

Limited Access

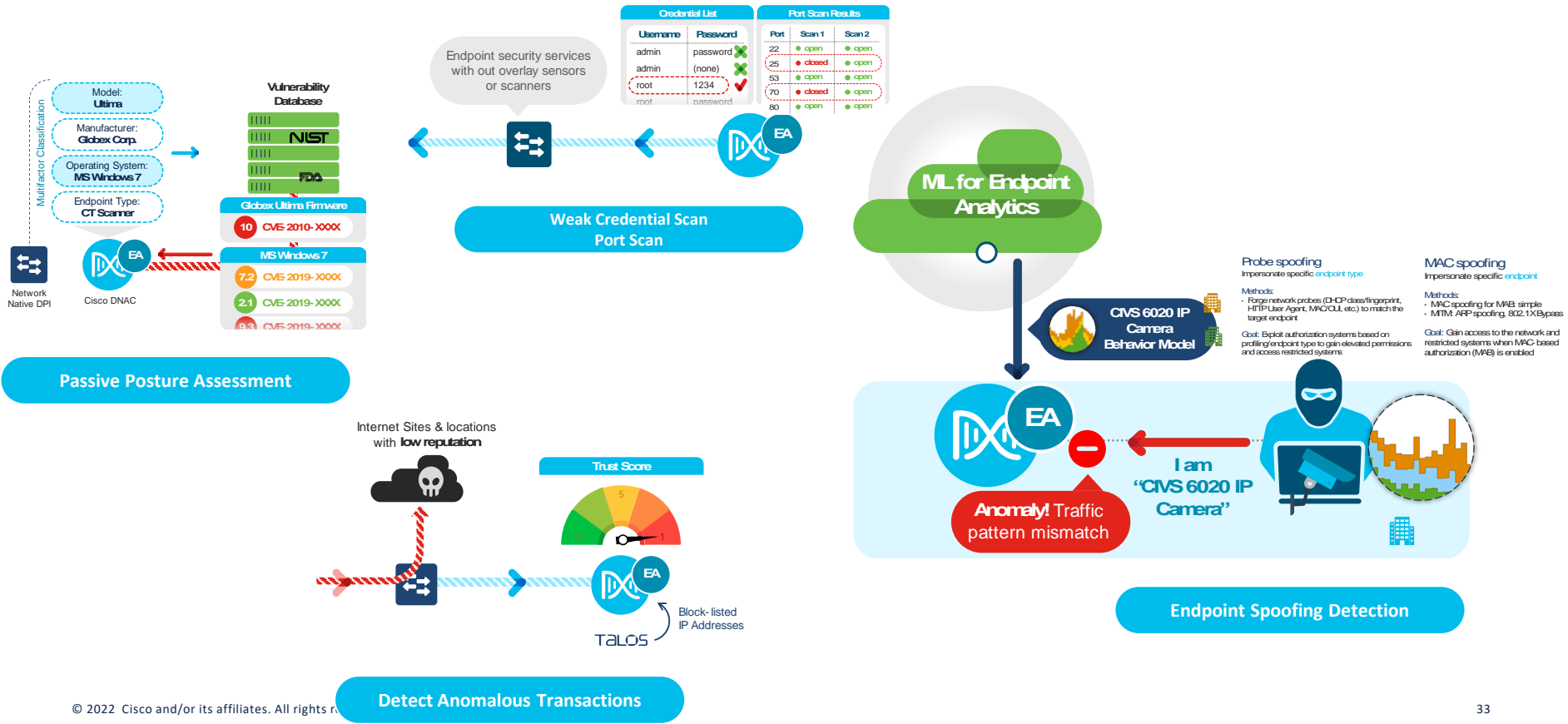
7-10

Full Access

AI Spoofing Detection



Verify Trust continuously for connected endpoints¹

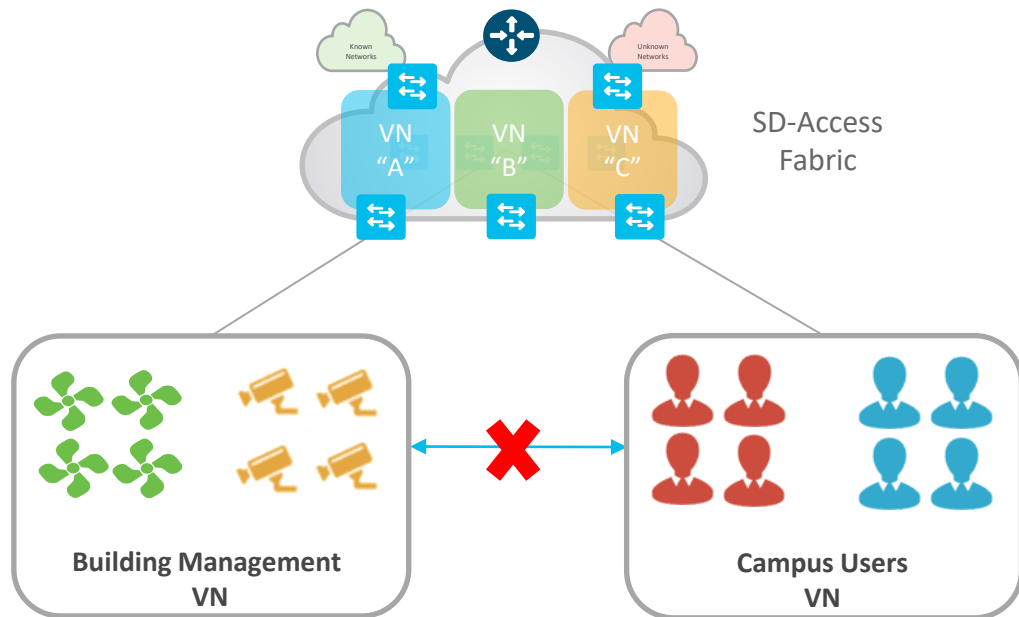


Segmented Access



SD-Access Segmentation

Two Level Hierarchy - Macro Segmentation



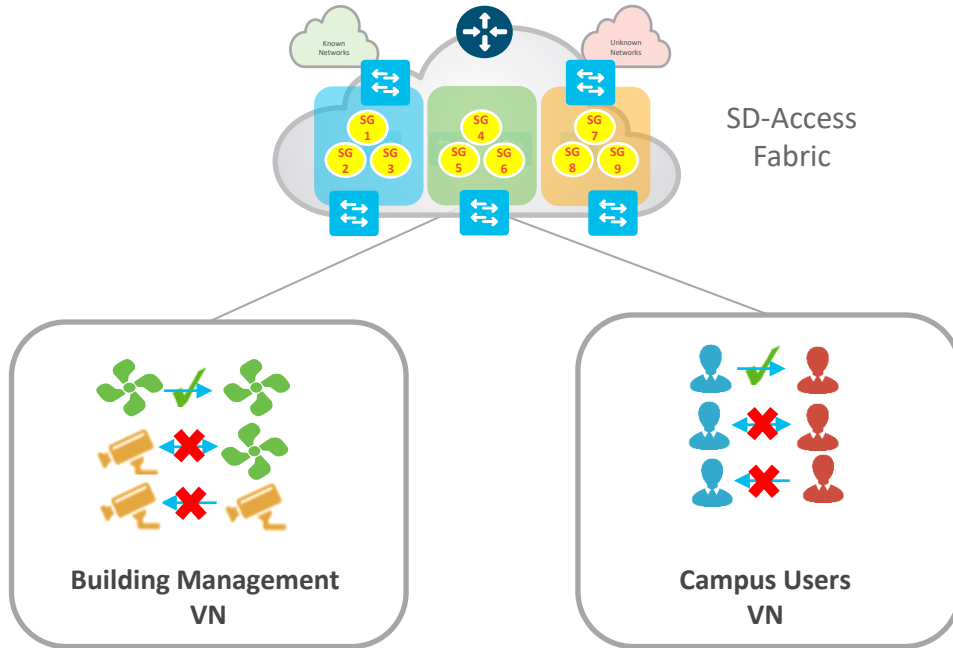
Virtual Network (VN)

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



SD-Access Segmentation

Two Level Hierarchy - Micro Segmentation



Security Group (SG)

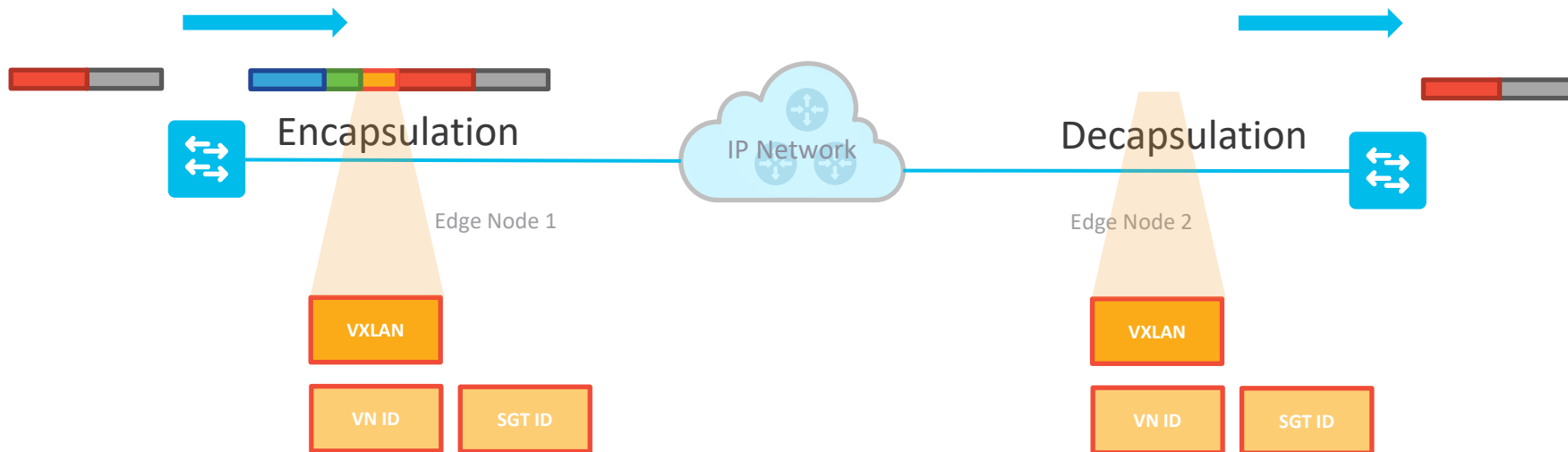
Second level Segmentation ensures **role based access control** between two groups within a Virtual Network. Provides the ability to segment the network into either line of businesses or functional blocks.

Identity-Based Segmentation

- 802.1x/RADIUS
- Passive Authorization Policy based on Endpoint Analytics attributes
- Static Port Assignment via DNA Center UI

Packet Flow in SD-Access Fabric

VN & SGT in VXLAN-GPO Encapsulation



Classification
Static or Dynamic VN
and SGT assignments

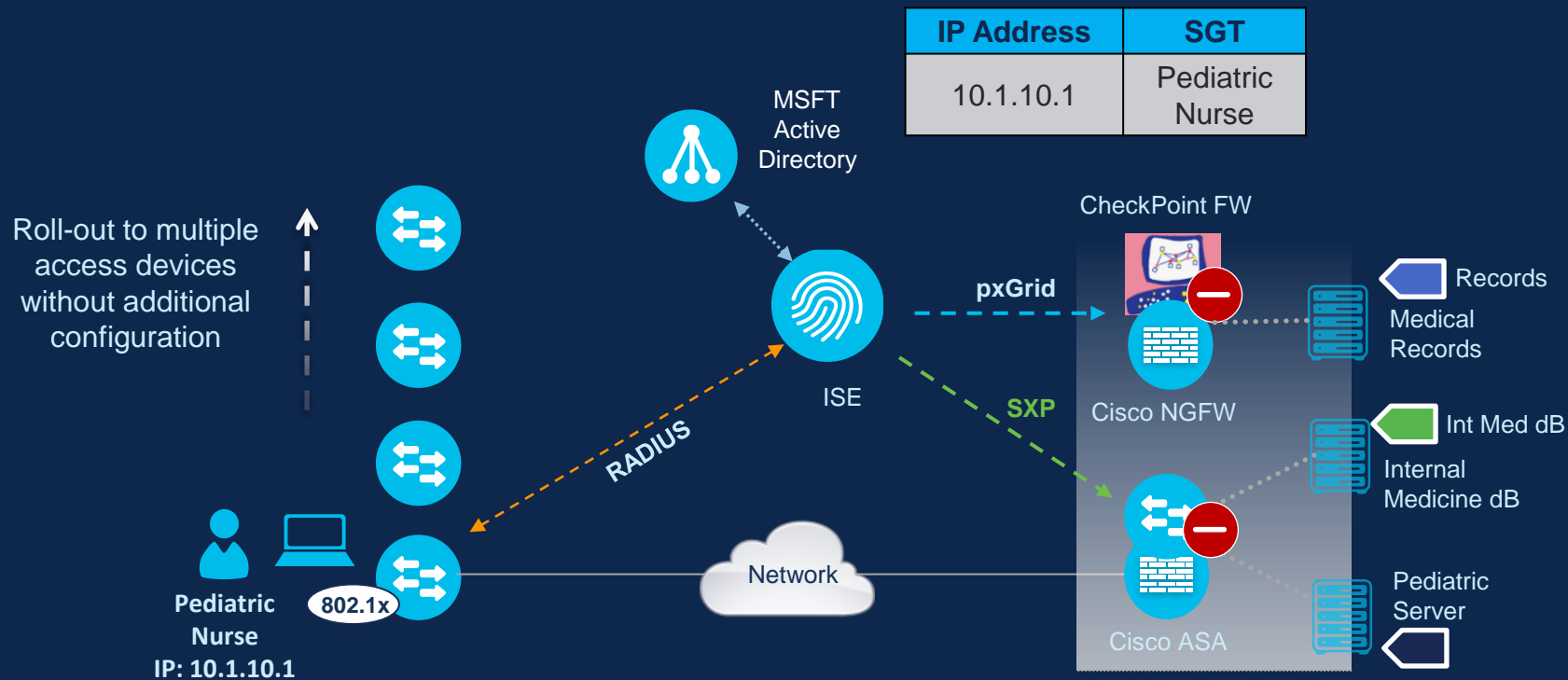


Propagation
Carry VN and Group context
across the network



Enforcement
Group Based Policies
ACLs, Firewall Rules

SGT Propagation using ISE (SXP and pxGrid)

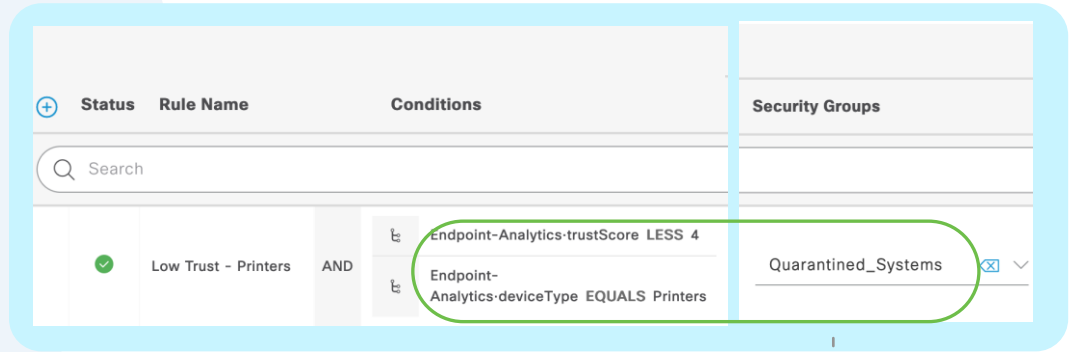


Rapid Threat Control

Trusted access using seamless ISE integration

Use case

ISE admins has to manually create custom profiles per endpoint type creating additional configuration overhead and reclassification



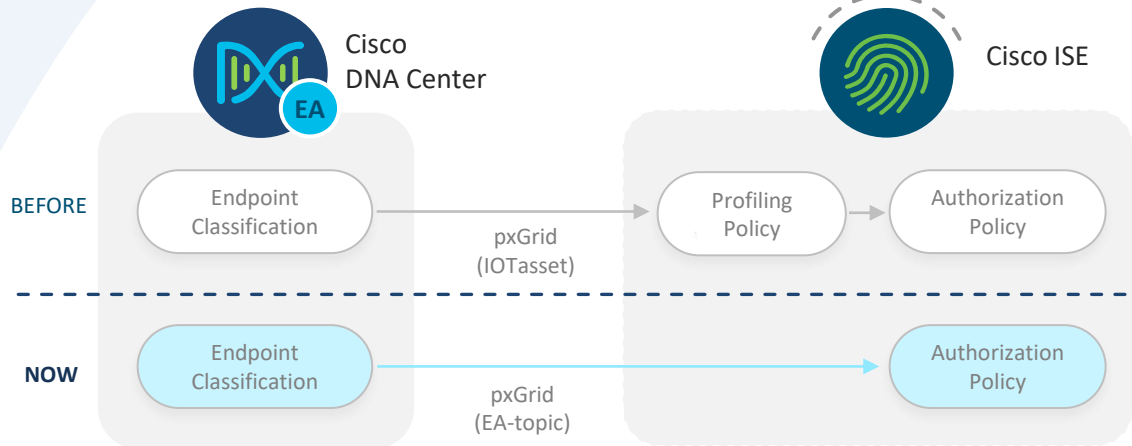
Capability

Sharing endpoint profile labels, scores, CMDB attributes in authorization policy eradicates the need for custom profile and ISE profiler reclassification.

Considerations

DNAC Version: 2.2.3 (Shockwave)

ISE Version: 3.1



Machine learning identifies malware



Malware in encrypted traffic



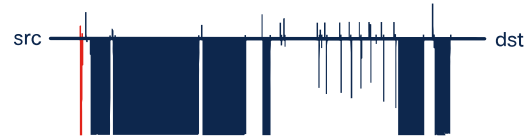
Security AND privacy



Detection: 99.99% accuracy



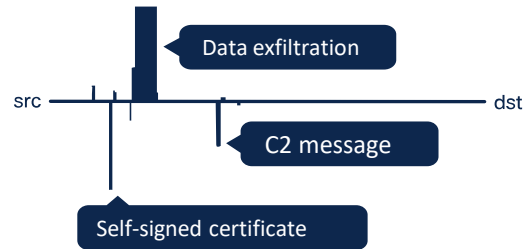
Infrastructure view of the data



Google Search



Firefox self-repair

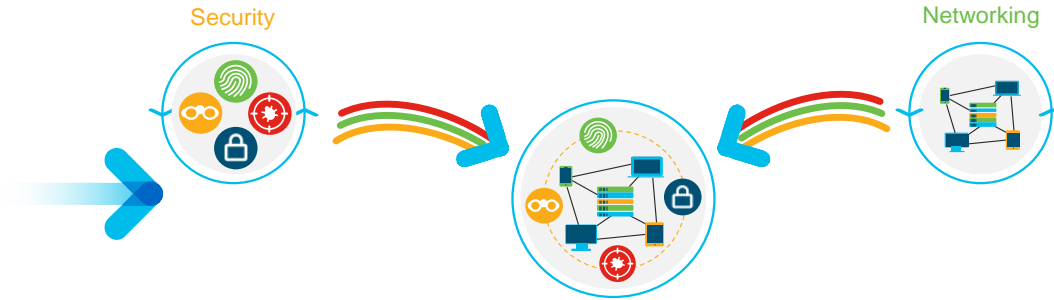
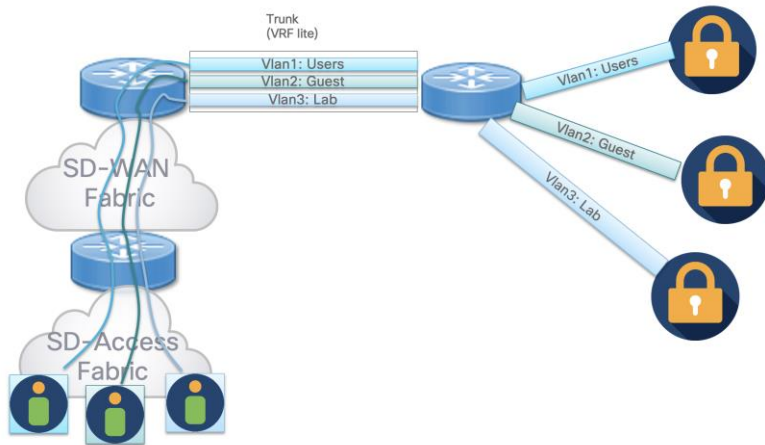


Bestafera malware

Bonus

Secure Service Insertion

Security Service Insertion - Extending Intent to Security Services



Intent-Based Network but Topology-Based Service Insertion

- Intent-Based Security Services delivered as part of the network
- Flexible security services with reusable objects shared between network and security services

Use Cases

- Policy Driven Traffic Steering
- Better Utilization of Firewall Resources
- Secure IoT network
- Secure Guest Network



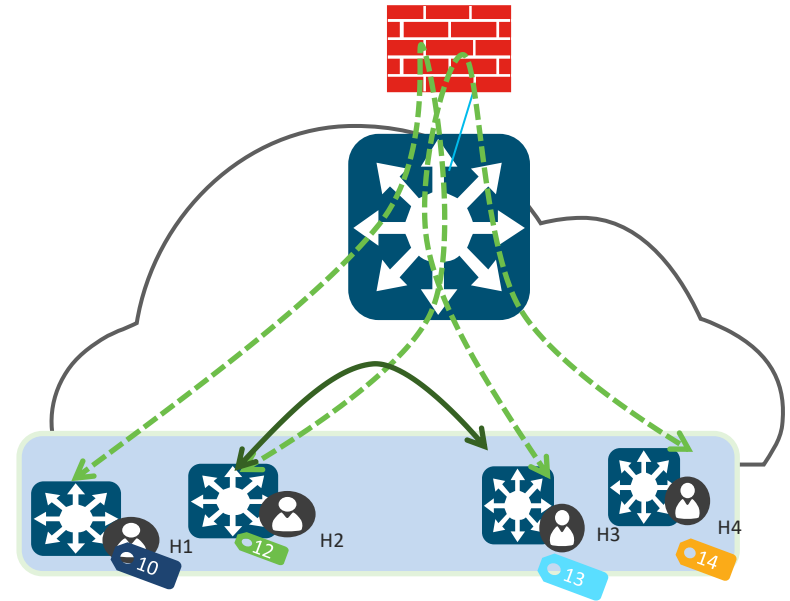
Policy Driven Traffic Steering

Use Case

- Subject traffic from one microsegment to another to specific security functions on the firewall
- Zero day protection with unpatched/end of support Windows devices.

Benefit

- Insertion of security services selectivity for specific traffic subsets in the enterprise, in an automated and policy driven manner (OpEx advantage)
- Avoids network-redesign to insert security + maintains network availability and performance
- Visibility and policy for traffic that is typically not subjected to firewall functions (SecOps value)



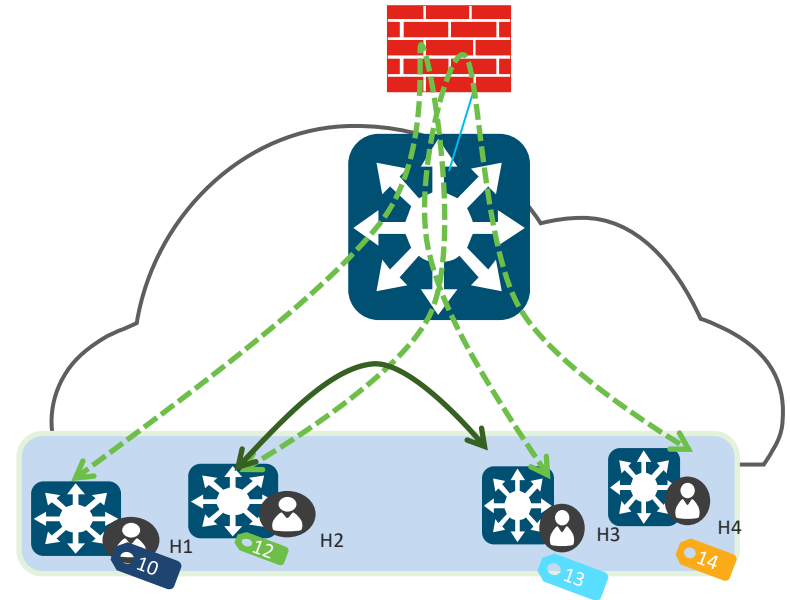
Better Utilization of Firewall Resources

Use Case

- Bypass the FW if redirection not required
- Improve the overall firewall throughput
- Improve the firewall CPU performance for higher bandwidth tasks

Benefit

- Enable higher firewall throughput by redirecting specific part of the network to firewall
- Better firewall performance



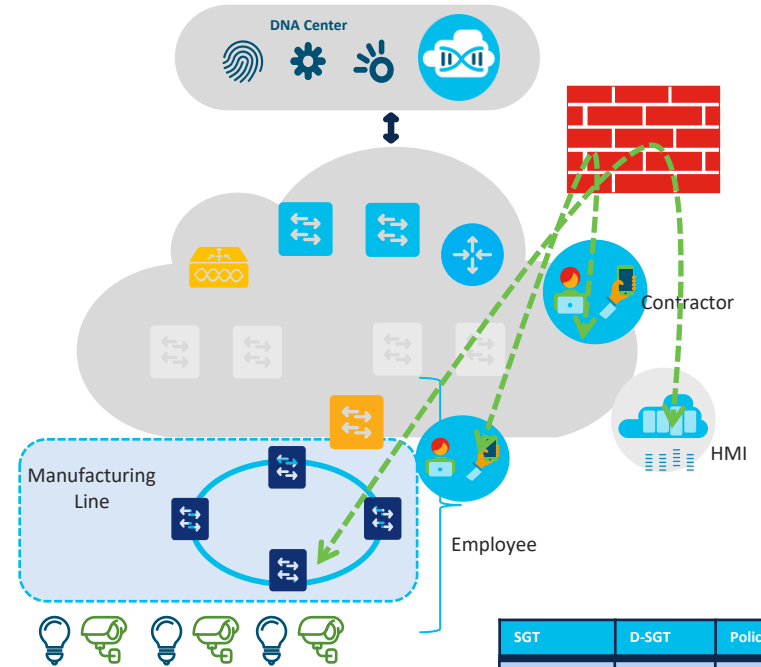
Secure IOT Network

Use Case

- Firewall will be required to inspect traffic between different groups of users and devices in IOT network
- Allow consistent policy and redirection with user mobility without increasing capex and opex

Benefit

- Secure IoT network
- Allow for movement without adding firewalls to multiple places in the factory or manufacturing flow



SGT	D-SGT	Policy
PLC	HMI	FW
HMI	Historian	FW
Engineer	Historian	FW
Contractor	PLC	FW

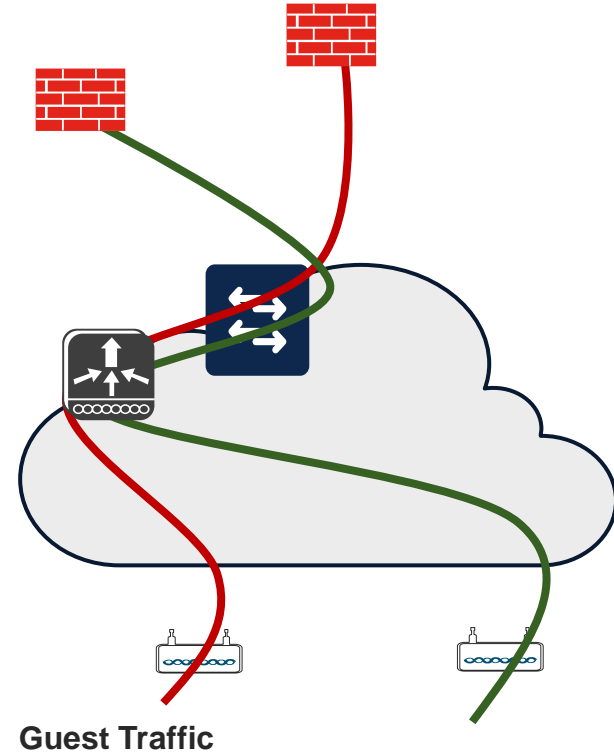
Secure Guest Network

Use Case

- Guest traffic must be segmented from internal network
- Guest traffic need to be redirected to FW

Benefit

- We can use traffic steering mechanism to redirect all the guest traffic to a FW service directly from the WLC
- Remove the requirement for anchor controller

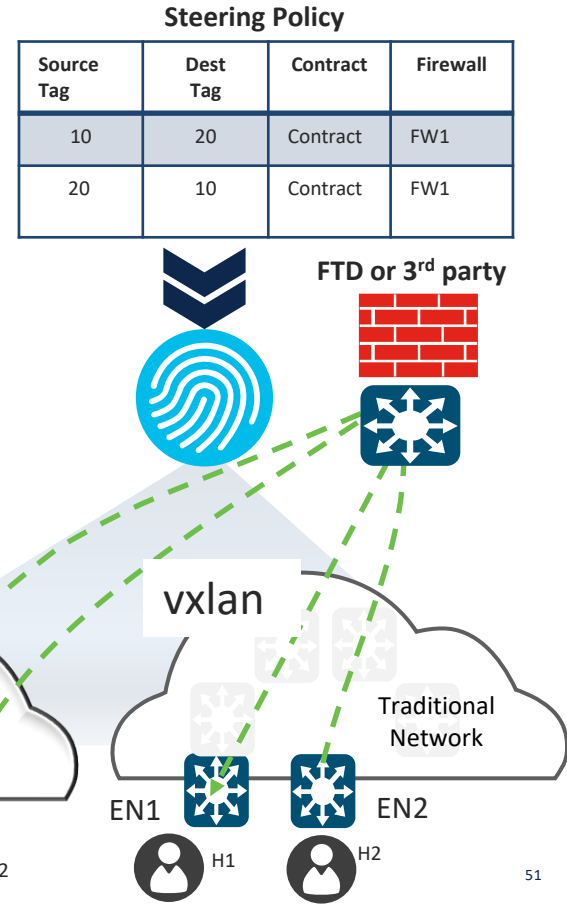


Security Services Insertion-“Hawkeye”

- Policy Based Traffic Steering



- 1) Create traffic steering policy on DNA Center
- 2) DNA Center sends steering policy to ISE (GA)
- 3) Steering policy programmed in the network upon request
- 4) Host's traffic redirected to FW based on the steering policy



Key Takeaways



- Clear picture on Cisco DNA Architecture
- Understand how Cisco DNA with SD-Access can help you to implement Zero Trust Architecture at your Workplace
- Inspired to do some Proof of Concept or Proof of Value activities

