Identity, Visibility and Enforcement

Stop the bad guys immediately

György Ács
Cisco Systems

ISE Champion

CISCOSEC

Agenda

- ISE 2.0 and 2.1 introduction
- Threat Centric NAC
- pxGrid update
- Device Admin (TACACS+)

Agenda

- **ISE 2.0 and 2.1 introduction**
- Threat Centric NAC
- pxGrid update
- Device Admin (TACACS+)

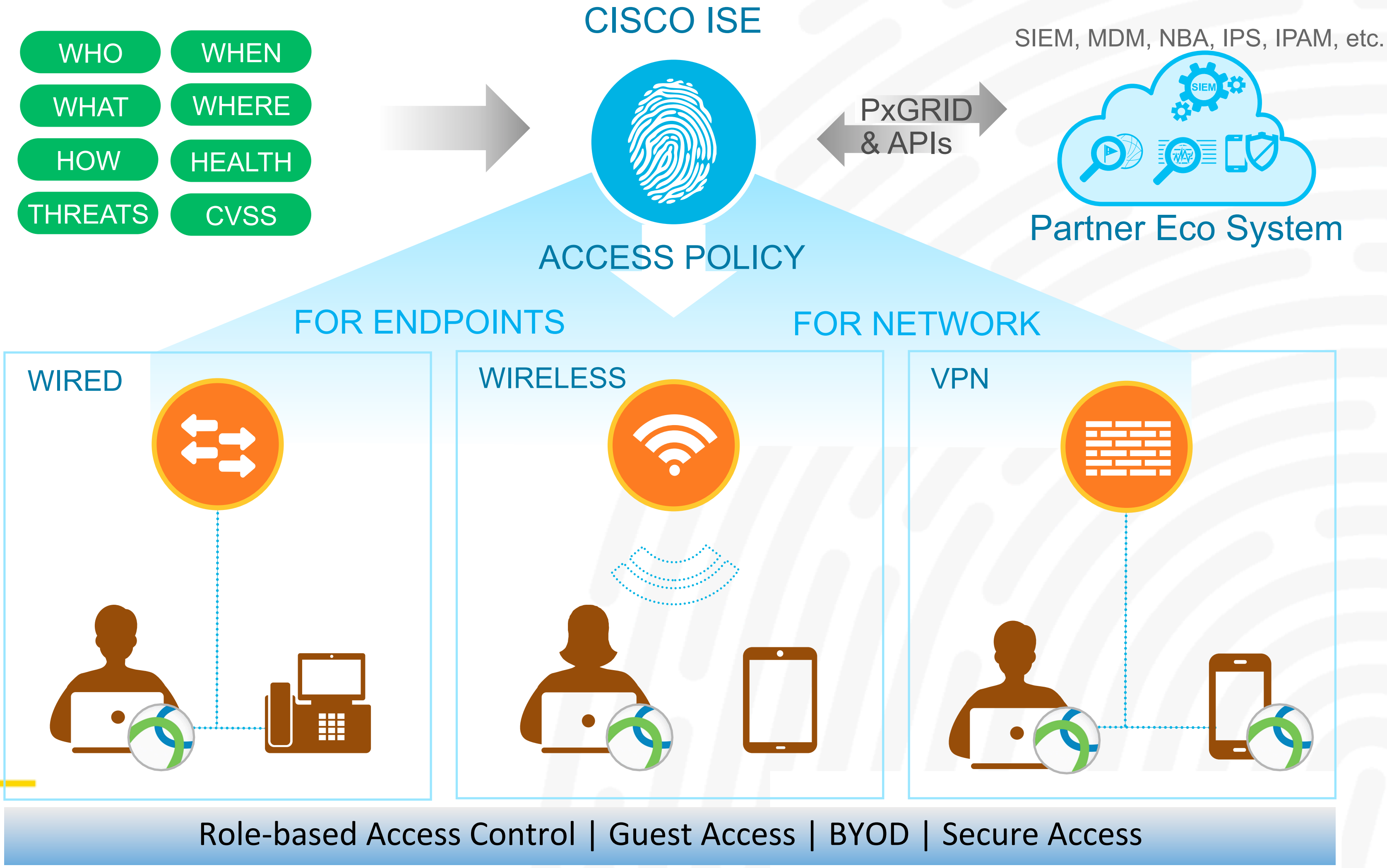
Cisco ISE and AnyConnect

Cisco ISE

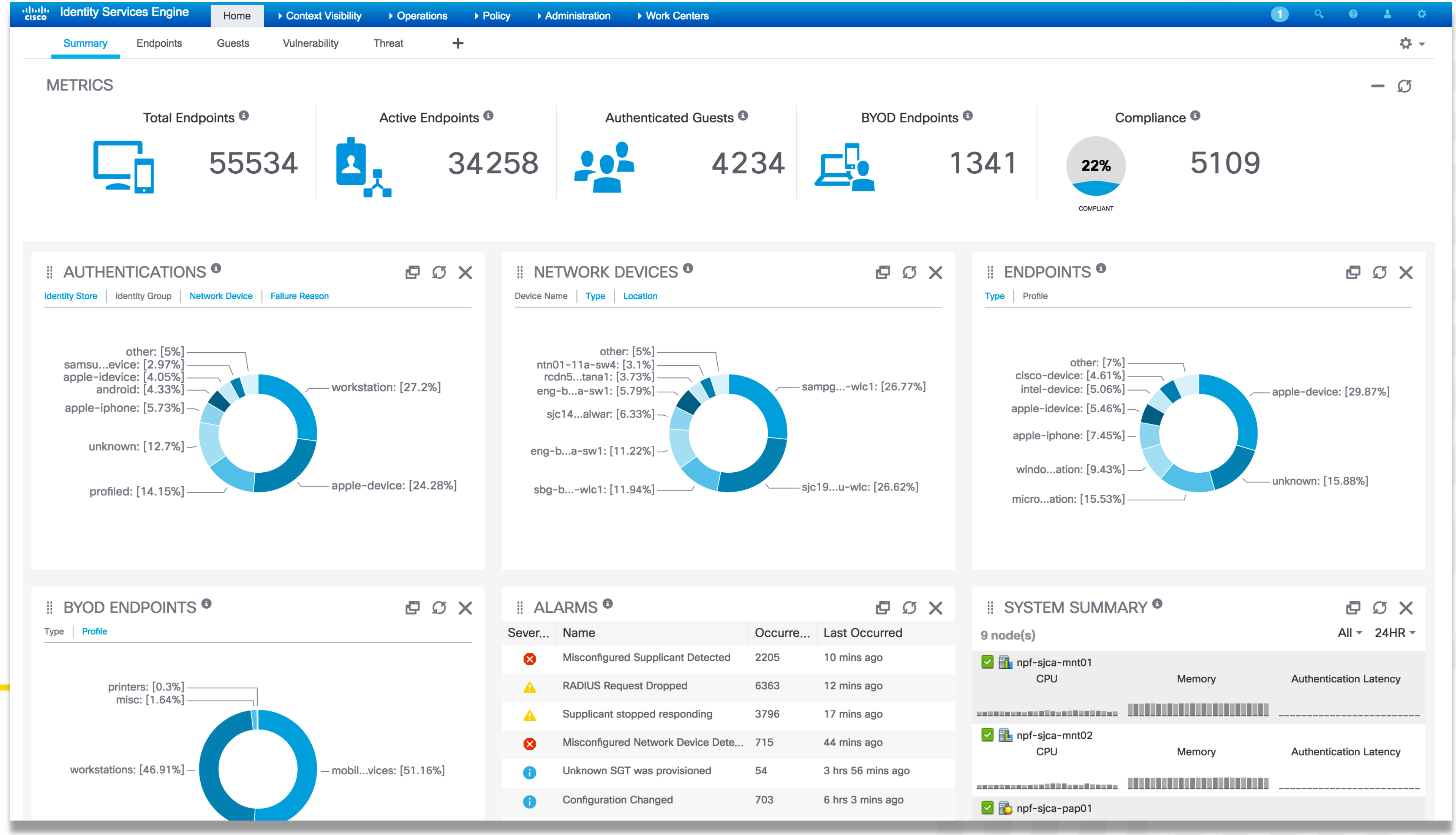
Context aware policy service, to control access and threat across wired, wireless and VPN networks

Cisco Anyconnect

Supplicant for wired, wireless and VPN access. Services include: Posture assessment, Malware protection, Web security, MAC Security, Network visibility and more.



Security starts with ‘Visibility’



Total Endpoints	Active Endpoints	Authenticated Guests	BYOD Endpoints	Compliance
55534	34258	4234	1341	22% 5109

ALARMS

Sever...	Name	Occurre...	Last Occurred
☒	Misconfigured Supplicant Detected	2205	10 mins ago
⚠	RADIUS Request Dropped	6363	12 mins ago
⚠	Supplicant stopped responding	3796	17 mins ago
☒	Misconfigured Network Device Dete...	715	44 mins ago
ⓘ	Unknown SGT was provisioned	54	3 hrs 56 mins ago
ⓘ	Configuration Changed	703	6 hrs 3 mins ago

Asset Visibility

Cisco ISE Profiling

1.5 million

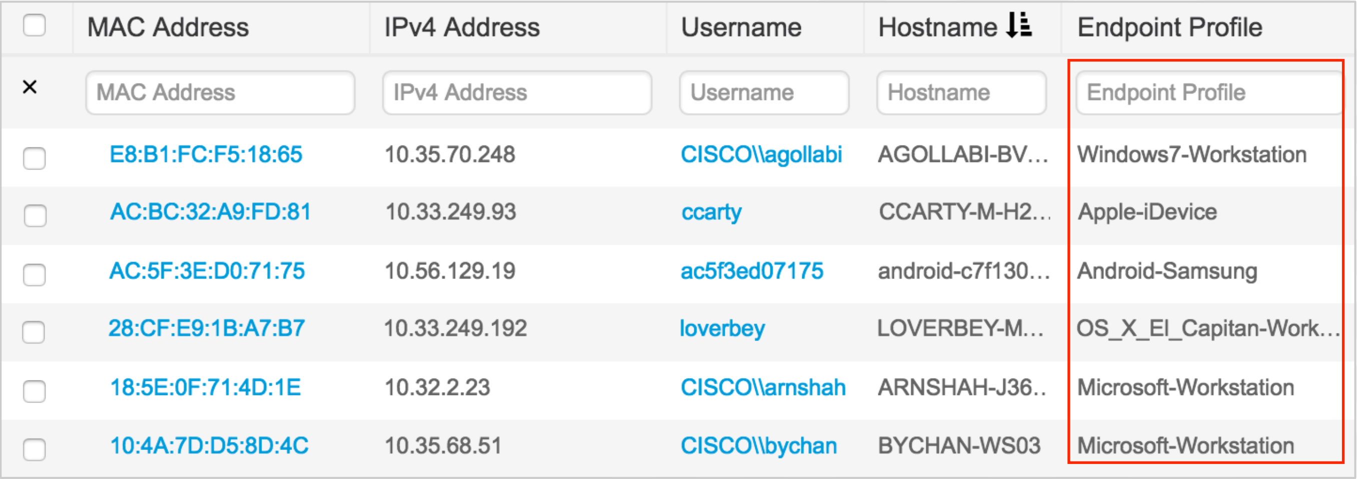
devices with ‘50’ attributes each can be stored

550+

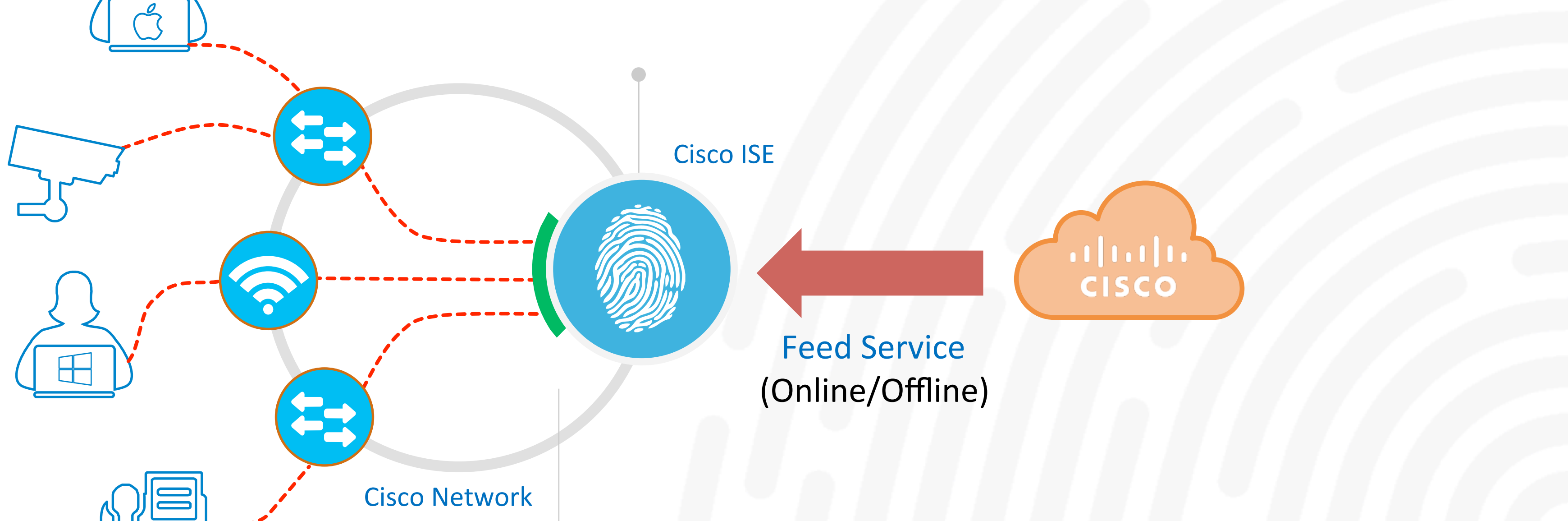
High-level canned profiles. +Periodic feeds

250+

Medical device profiles



□	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
✕	MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
□	E8:B1:FC:F5:18:65	10.35.70.248	CISCO\\agollabi	AGOLLABI-BV…	Windows7-Workstation
□	AC:BC:32:A9:FD:81	10.33.249.93	ccarty	CCARTY-M-H2…	Apple-iDevice
□	AC:5F:3E:D0:71:75	10.56.129.19	ac5f3ed07175	android-c7f130…	Android-Samsung
□	28:CF:E9:1B:A7:B7	10.33.249.192	loverbey	LOVERBEY-M…	OS_X_El_Capitan-Work…
□	18:5E:0F:71:4D:1E	10.32.2.23	CISCO\\arnshah	ARNSHAH-J36..	Microsoft-Workstation
□	10:4A:7D:D5:8D:4C	10.35.68.51	CISCO\\bychan	BYCHAN-WS03	Microsoft-Workstation



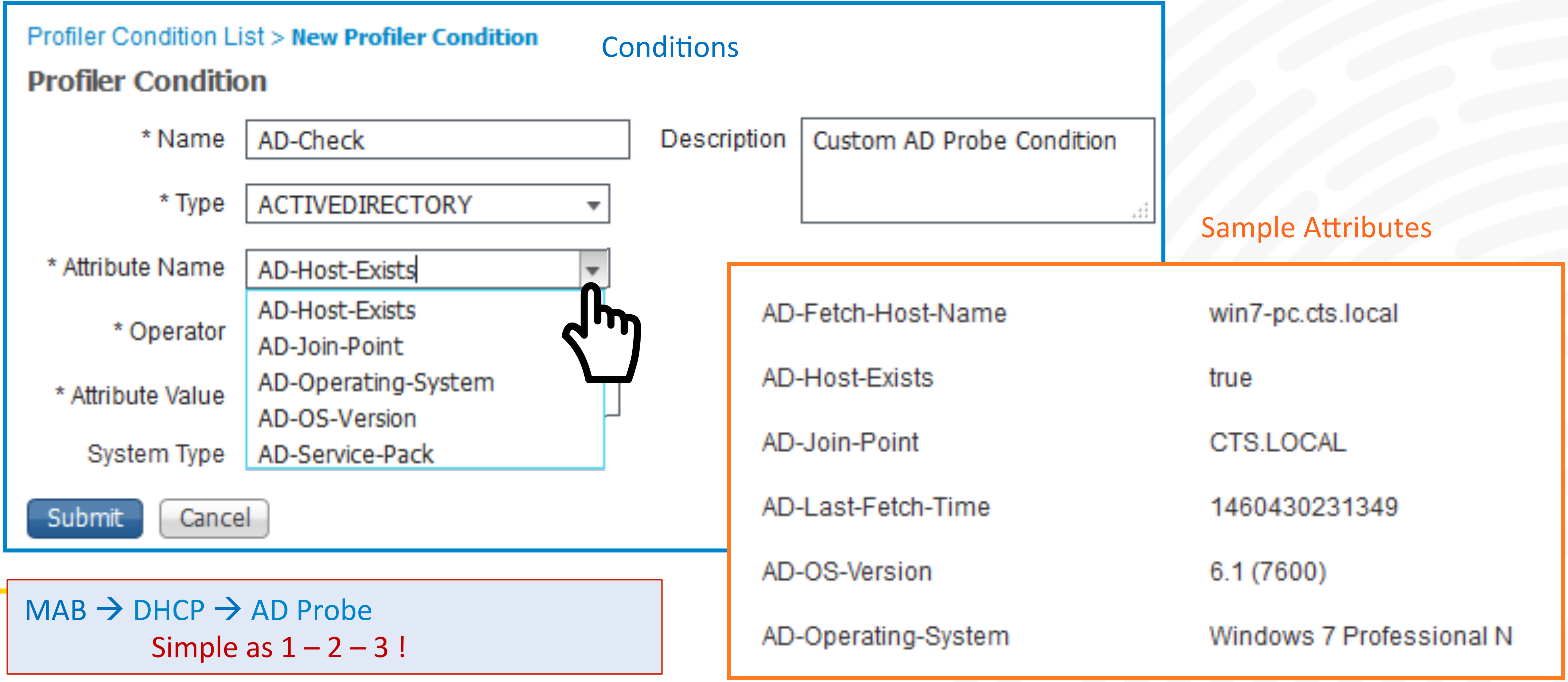
ACTIVE PROBES	Netflow	DHCP	DNS	HTTP	RADIUS	NMAP	SNMP
DEVICE SENSOR	CDP	LLDP	DHCP	HTTP	H323	SIP	MDNS

Profiling : AD Probe

Conditions and Attributes

Match on the following:

- AD Computer?
- Join Point Domain
- OS, Version, and Service Pack



Conditions

Profiler Condition List > **New Profiler Condition**

Profiler Condition

* Name: AD-Check

Description: Custom AD Probe Condition

* Type: ACTIVEDIRECTORY

* Attribute Name: AD-Host-Exists

* Operator

* Attribute Value

System Type

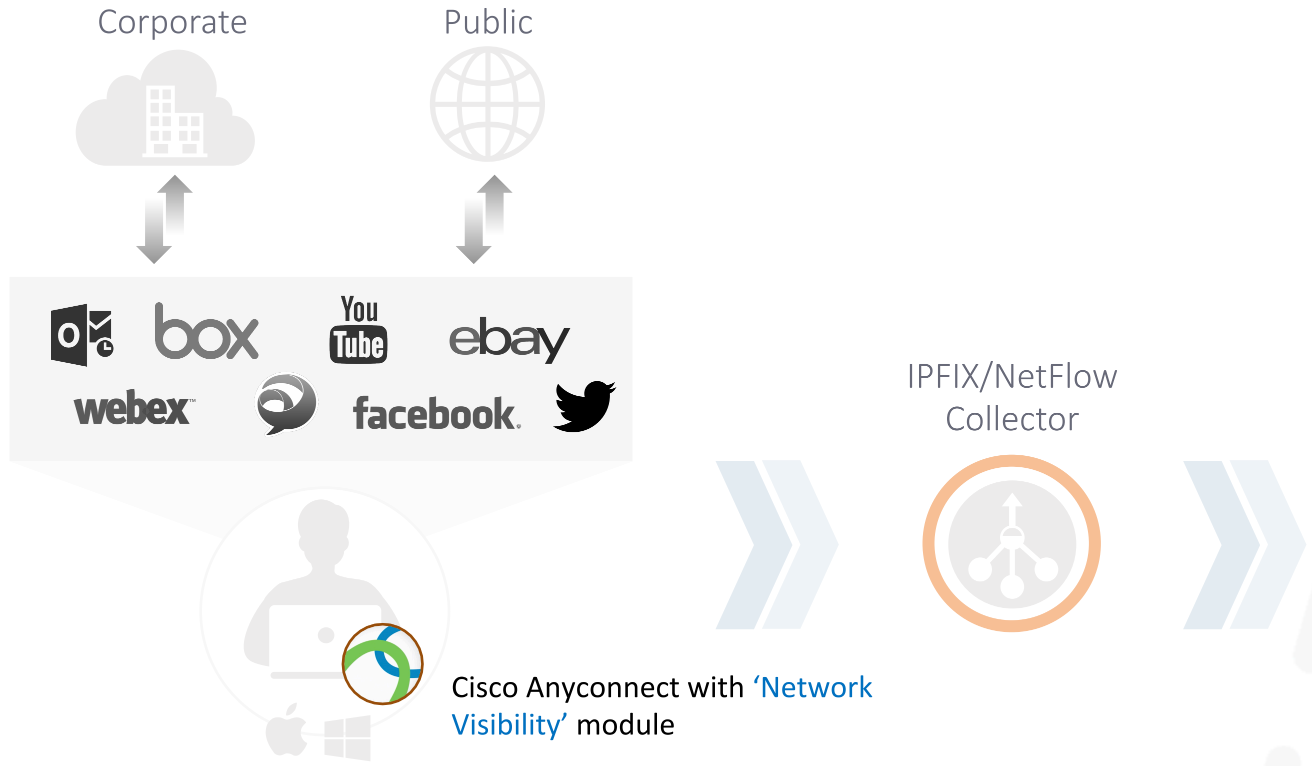
Sample Attributes

AD-Fetch-Host-Name	win7-pc.cts.local
AD-Host-Exists	true
AD-Join-Point	CTS.LOCAL
AD-Last-Fetch-Time	1460430231349
AD-OS-Version	6.1 (7600)
AD-Operating-System	Windows 7 Professional N

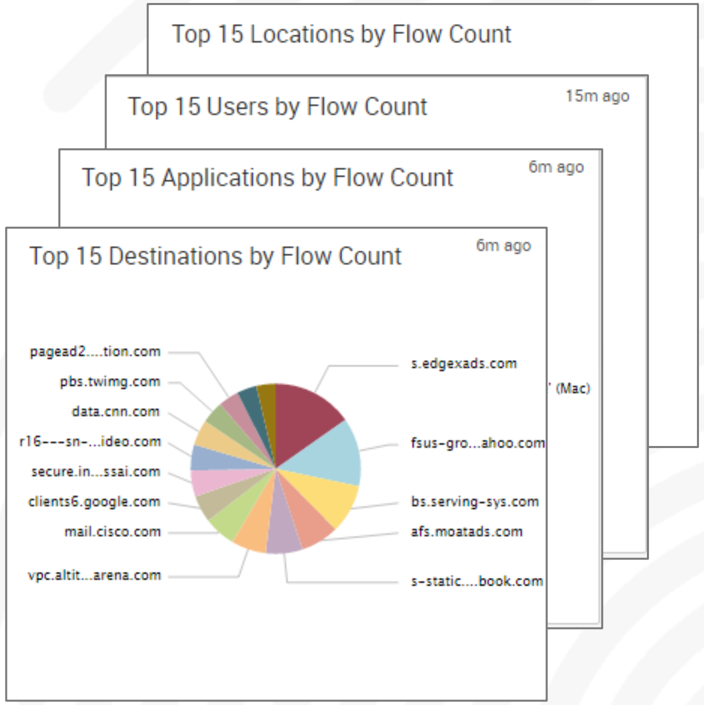
MAB → DHCP → AD Probe

Simple as 1 – 2 – 3 !

Application ‘Visibility’ via Anyconnect



Cisco Anyconnect with ‘Network Visibility’ module


Top 15 Locations by Flow Count

Top 15 Users by Flow Count 15m ago

Top 15 Applications by Flow Count 6m ago

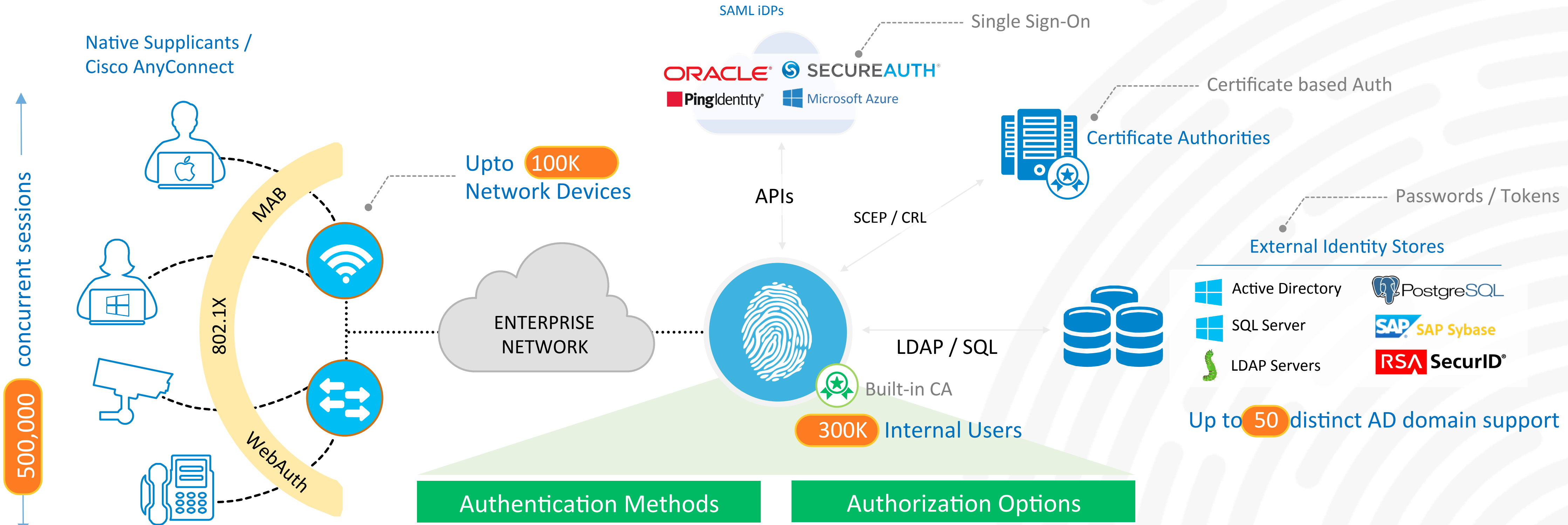
Top 15 Destinations by Flow Count 6m ago

Visibility
in to process, process hash, URLs, and more

Context
for Network Behavioral Analysis

Control
run-time applications via ’Posture Policies’

Authentications and Authorizations



Authentication Methods

PASSIVE IDENTITY

- MAC Authentication Bypass
- **Easy Connect ®**

ACTIVE IDENTITY

- IEEE 802.1X
- Web Authentication
  - Central WebAuth
  - Local WebAuth

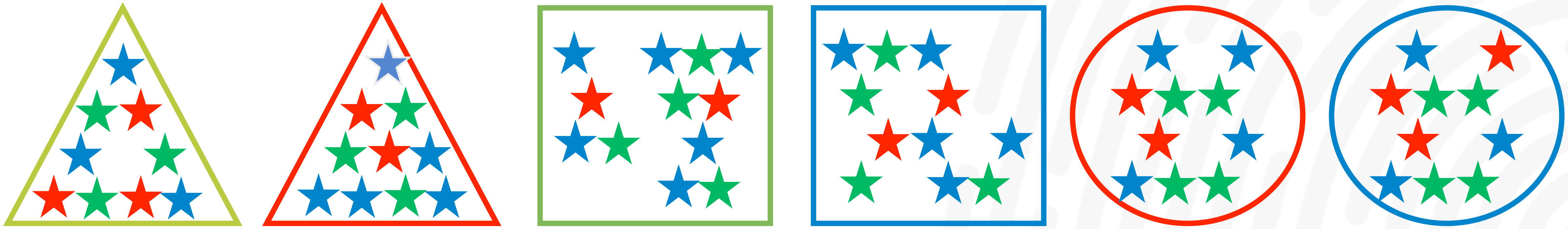
Authorization Options

- **Downloadable / Named ACL**
- Air Space ACL
- VLAN Assignment
- **Security Group Tags**
- URL-Redirection
- Port Configuration
  (ASP Macro / Interface-Template)

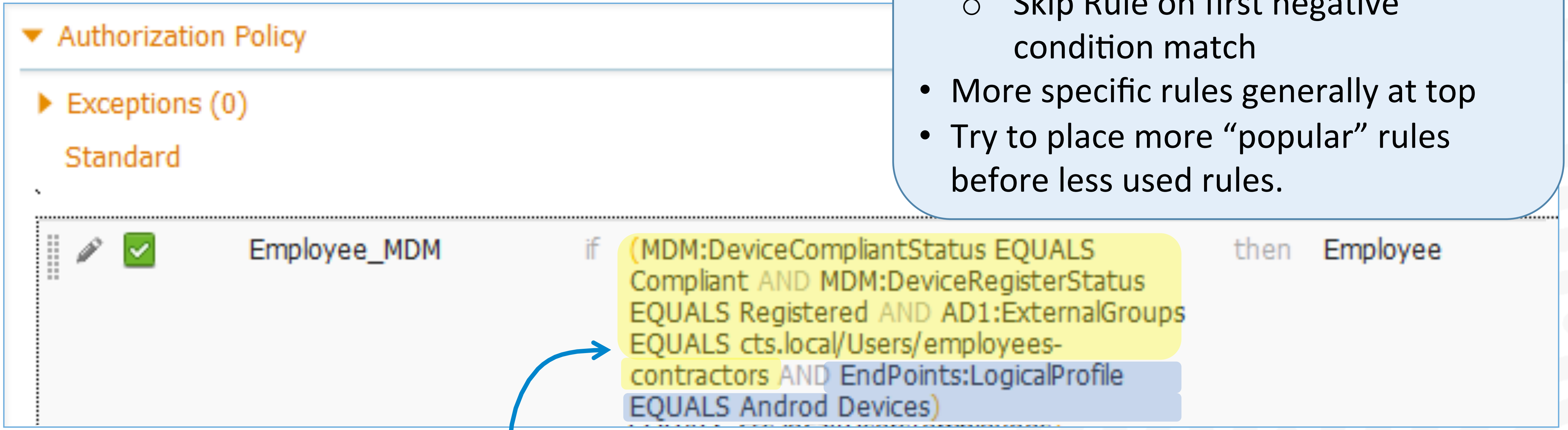
ASP: Auto Smart Port

Search Speed Test

- Find the object where…
  - Total stars = 10
  - Total green stars = 4
  - Total red stars = 2
  - Outer shape = Red Circle



AuthZ Policy Optimization



▼ Authorization Policy

▶ Exceptions (0)

Standard

☑ Employee_MDM if (MDM:DeviceCompliantStatus EQUALS Compliant AND MDM:DeviceRegisterStatus EQUALS Registered AND AD1:ExternalGroups EQUALS cts.local/Users/employees-contractors AND EndPoints:LogicalProfile EQUALS Androd Devices) then Employee

- Policy Logic:
  - First Match, Top Down
  - Skip Rule on first negative condition match
- More specific rules generally at top
- Try to place more “popular” rules before less used rules.

Example of a Poor Rule: Employee_MDM

- All lookups to External Policy and ID Stores performed first, then local profile match!

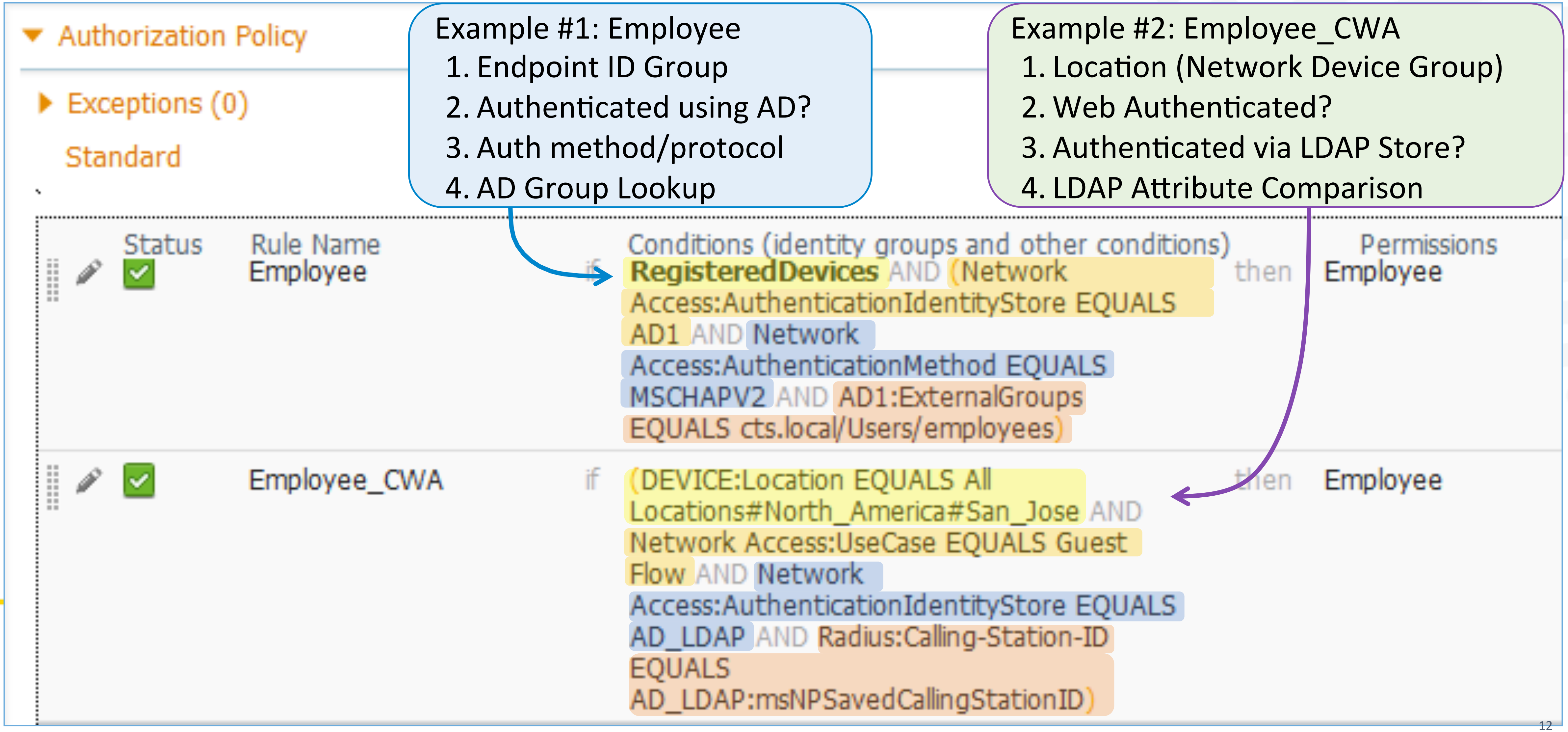
AuthZ Policy Optimization (Good Examples)

Example #1: Employee

1. Endpoint ID Group
2. Authenticated using AD?
3. Auth method/protocol
4. AD Group Lookup

Example #2: Employee_CWA

1. Location (Network Device Group)
2. Web Authenticated?
3. Authenticated via LDAP Store?
4. LDAP Attribute Comparison



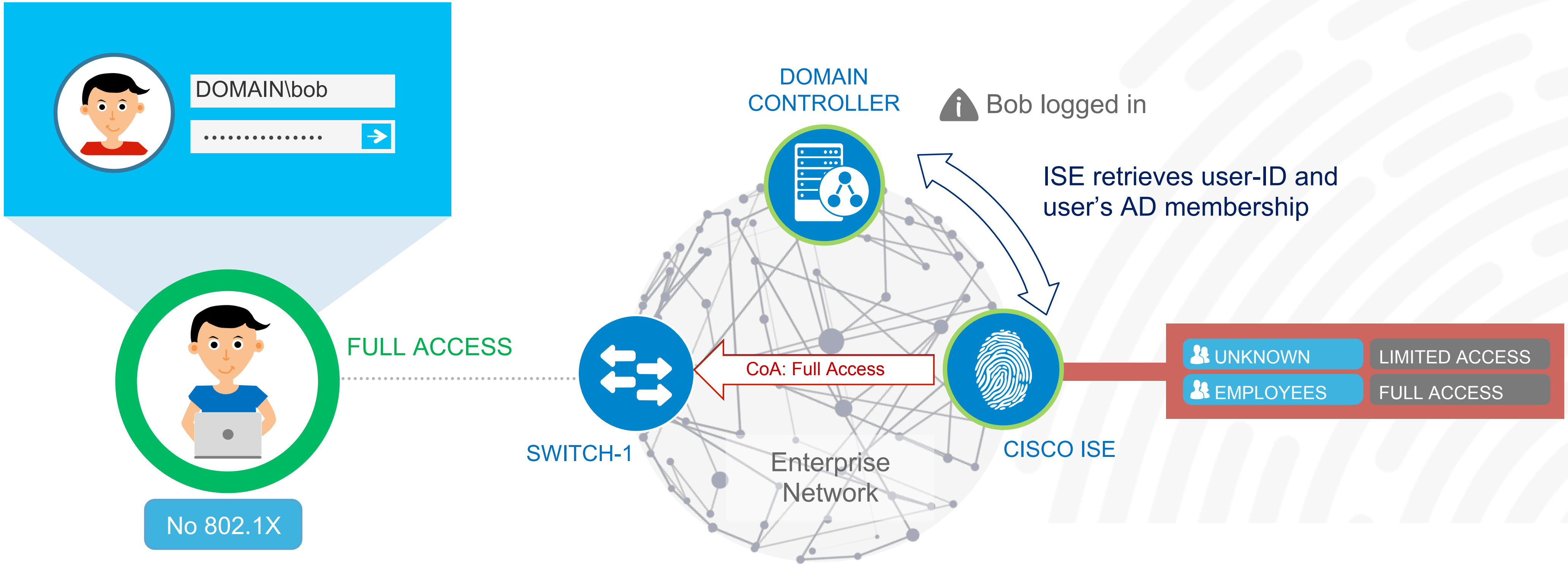
▼ Authorization Policy

▶ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Employee	if	RegisteredDevices AND (Network Access:AuthenticationIdentityStore EQUALS AD1 AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND AD1:ExternalGroups EQUALS cts.local/Users/employees)	then	Employee
☑	Employee_CWA	if	(DEVICE:Location EQUALS All Locations#North_America#San_Jose AND Network Access:UseCase EQUALS Guest Flow AND Network Access:AuthenticationIdentityStore EQUALS AD_LDAP AND Radius:Calling-Station-ID EQUALS AD_LDAP:msNPSavedCallingStationID)	then	Employee

Quickly see value with ‘Easy Connect’



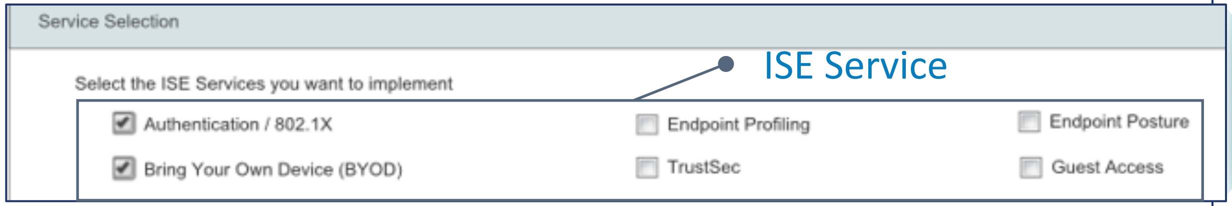
Immediate value
Leverage existing infrastructure

Increased visibility
into active network sessions

Flexible deployment
co-operates with other auth methods

ISE Deployment Assistant (IDA)

to simplify Cisco ‘Network Device’ configurations



Service Selection

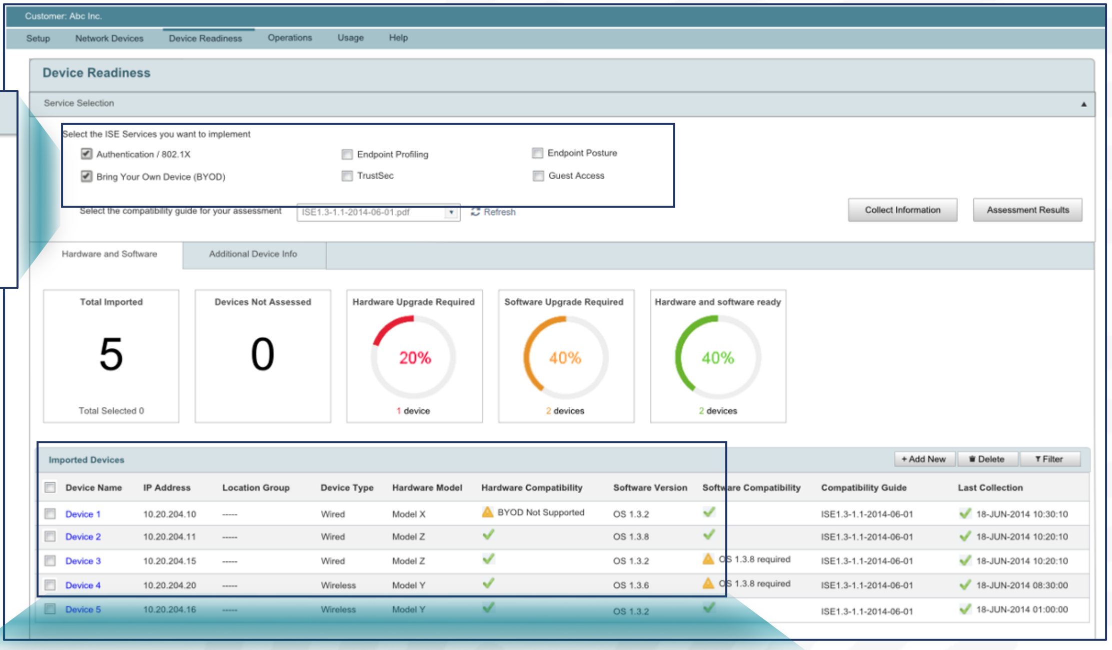
Select the ISE Services you want to implement

☑ Authentication / 802.1X　　□ Endpoint Profiling　　□ Endpoint Posture

☑ Bring Your Own Device (BYOD)　　□ TrustSec　　□ Guest Access

ISE Service

- freely downloadable Windows tool
- Network Assessment
- Configuration of NADs (Network Access Devices)
- Ability to Troubleshoot failed authentications



Customer: Abc Inc.

Device Readiness

Service Selection

Select the ISE Services you want to implement

☑ Authentication / 802.1X　　□ Endpoint Profiling　　□ Endpoint Posture

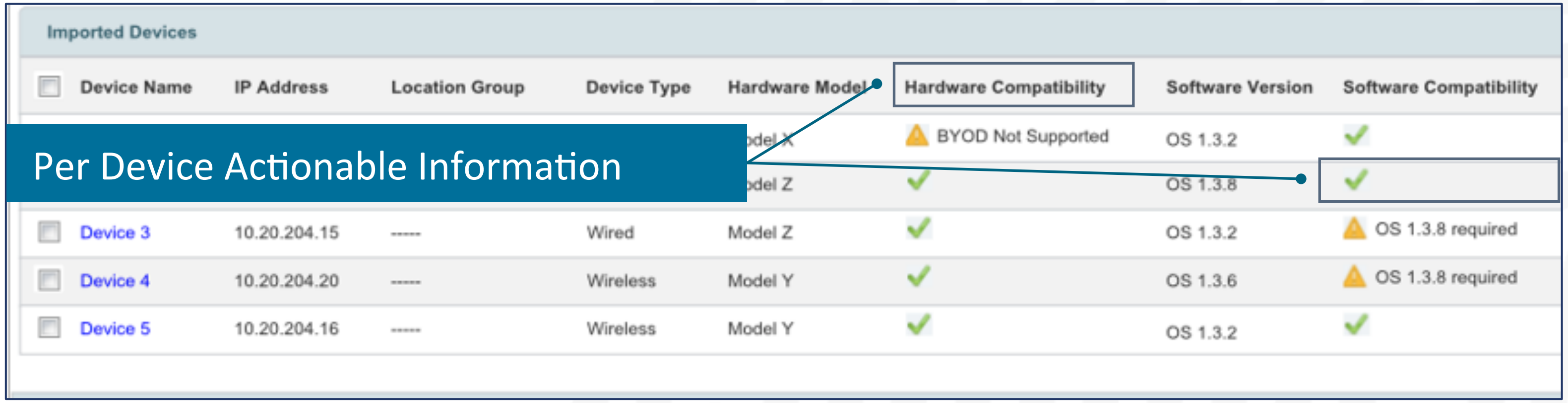
☑ Bring Your Own Device (BYOD)　　□ TrustSec　　□ Guest Access

Select the compatibility guide for your assessment: ISE1.3-1.1-2014-06-01.pdf

Total Imported	Devices Not Assessed	Hardware Upgrade Required	Software Upgrade Required	Hardware and software ready
5	0	20%	40%	40%
Total Selected 0		1 device	2 devices	2 devices

Imported Devices

□	Device Name	IP Address	Location Group	Device Type	Hardware Model	Hardware Compatibility	Software Version	Software Compatibility	Compatibility Guide	Last Collection
□	Device 1	10.20.204.10	-----	Wired	Model X	⚠ BYOD Not Supported	OS 1.3.2	✓	ISE1.3-1.1-2014-06-01	✓ 18-JUN-2014 10:30:10
□	Device 2	10.20.204.11	-----	Wired	Model Z	✓	OS 1.3.8	✓	ISE1.3-1.1-2014-06-01	✓ 18-JUN-2014 10:20:10
□	Device 3	10.20.204.15	-----	Wired	Model Z	✓	OS 1.3.2	⚠ OS 1.3.8 required	ISE1.3-1.1-2014-06-01	✓ 18-JUN-2014 10:20:10
□	Device 4	10.20.204.20	-----	Wireless	Model Y	✓	OS 1.3.6	⚠ OS 1.3.8 required	ISE1.3-1.1-2014-06-01	✓ 18-JUN-2014 08:30:00
□	Device 5	10.20.204.16	-----	Wireless	Model Y	✓	OS 1.3.2	✓	ISE1.3-1.1-2014-06-01	✓ 18-JUN-2014 01:00:00



Imported Devices

□	Device Name	IP Address	Location Group	Device Type	Hardware Model	Hardware Compatibility	Software Version	Software Compatibility
					odel X	⚠ BYOD Not Supported	OS 1.3.2	✓
					odel Z	✓	OS 1.3.8	✓
□	Device 3	10.20.204.15	-----	Wired	Model Z	✓	OS 1.3.2	⚠ OS 1.3.8 required
□	Device 4	10.20.204.20	-----	Wireless	Model Y	✓	OS 1.3.6	⚠ OS 1.3.8 required
□	Device 5	10.20.204.16	-----	Wireless	Model Y	✓	OS 1.3.2	✓

Per Device Actionable Information

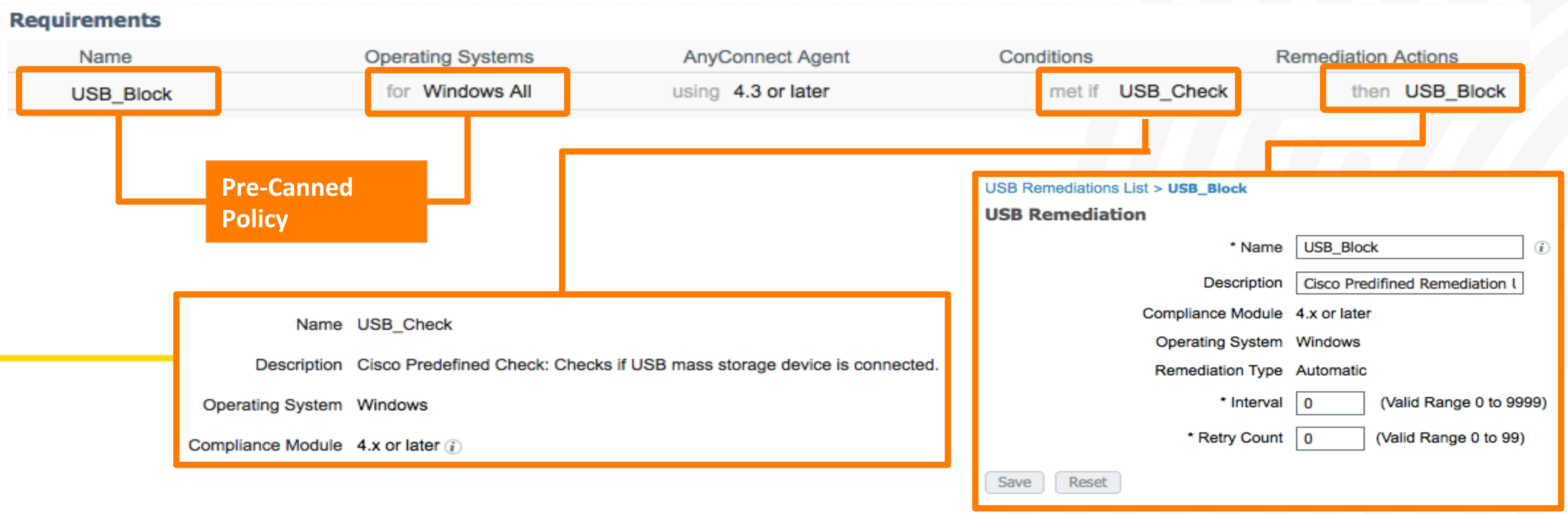
http://www.securview.com/products/cisco-ise-deployment-assistant/

Posture : USB Condition and Remediation

USB Checks are "Dynamic" a.k.a real time enforced, although USB check could be configured at initial posture check or Passive Reassessment checks (PRA).

Any Connect 4.3 enforces the Disk Encryption Policy

ISE 2.1 only supports it for Windows



Requirements

Name	Operating Systems	AnyConnect Agent	Conditions	Remediation Actions
USB_Block	for Windows All	using 4.3 or later	met if USB_Check	then USB_Block

Pre-Canned Policy

Name	USB_Check
Description	Cisco Predefined Check: Checks if USB mass storage device is connected.
Operating System	Windows
Compliance Module	4.x or later

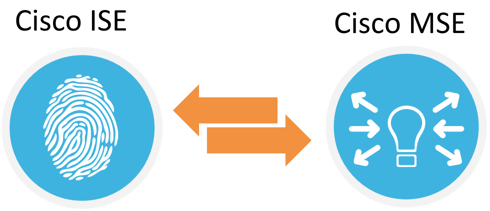
USB Remediations List > **USB_Block**

USB Remediation

* Name	USB_Block
Description	Cisco Predifined Remediation
Compliance Module	4.x or later
Operating System	Windows
Remediation Type	Automatic
* Interval	0 (Valid Range 0 to 9999)
* Retry Count	0 (Valid Range 0 to 99)

Location based authorization

with the integration of Mobility Services Engine (MSE)



The integration of Cisco Mobility Services Engine (MSE) adds the physical location of a user and/or endpoint to the context by which access is authorized.

Granular control of network access with location-based authorization for individual users

Enhanced policy enforcement with automated location check and reauthorization

Simplified management by configuring authorization with ISE management tools

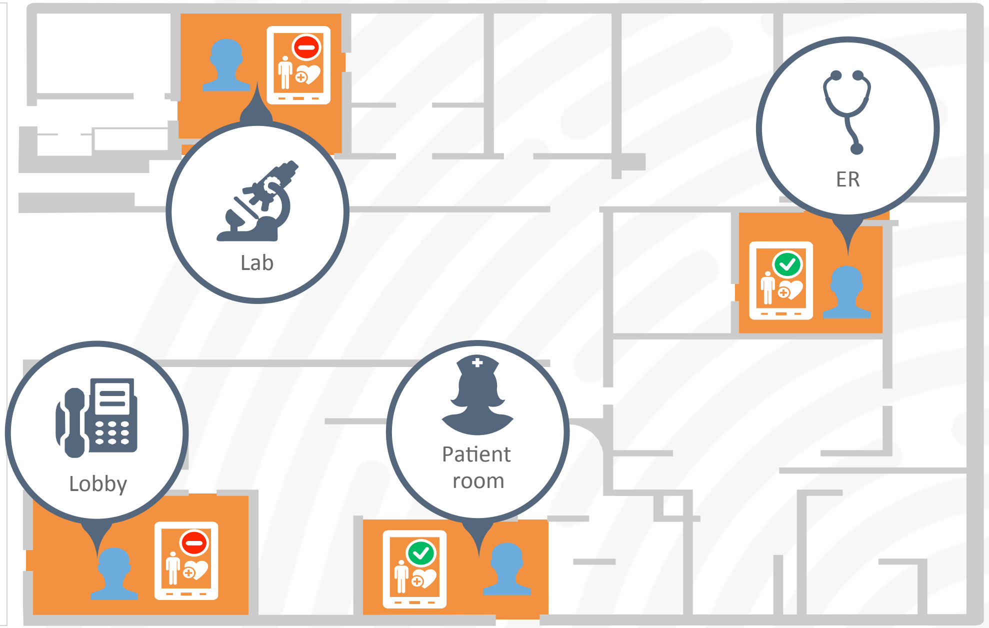
Location-based authorization

Admin defines location hierarchy and grants users specific access rights based on their location.

Patient data access locations

Patient data

	Lobby	Patient room	Lab	ER
Doctor	No access to patient data ⛔	Access to patient data ✓	No access to patient data ⛔	Access to patient data ✓



Authorization changes on location change

Agenda

- ISE 2.0 and 2.1 introduction
- **Threat Centric NAC**
- pxGrid update
- Device Admin (TACACS+)

Threat Centric NAC

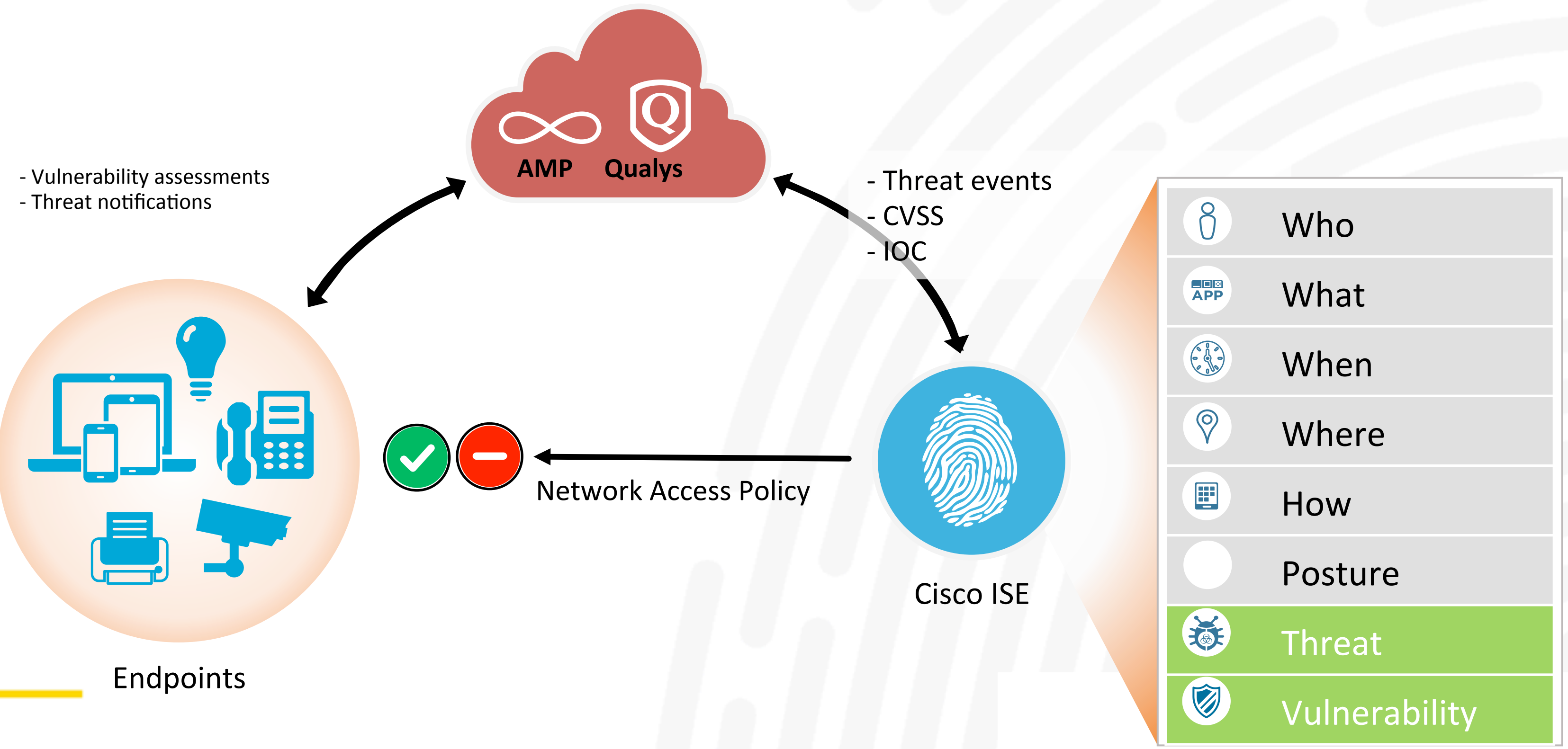
Cisco ISE protects your network from data breaches by segmenting compromised and vulnerable endpoints for remediation.

Compliments Posture
Vulnerability data tells endpoint's posture from the outside

Expanded control
driven by threat intelligence and vulnerability assessment data

Faster response
with automated, real-time policy updates based on vulnerability data and threat metrics

Create ISE authorization policies based on the threat and vulnerability attributes



AMP Qualys

- Vulnerability assessments
- Threat notifications

- Threat events
- CVSS
- IOC

Endpoints

Network Access Policy

Cisco ISE

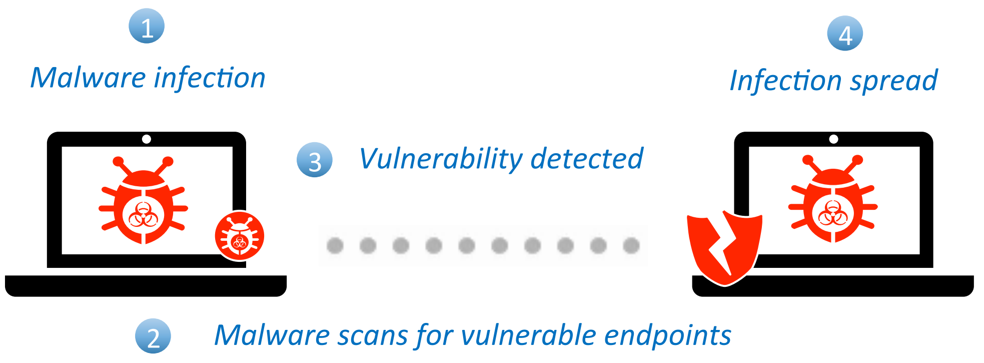
Who
What
When
Where
How
Posture
Threat
Vulnerability

Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC)

Threat Centric NAC explained

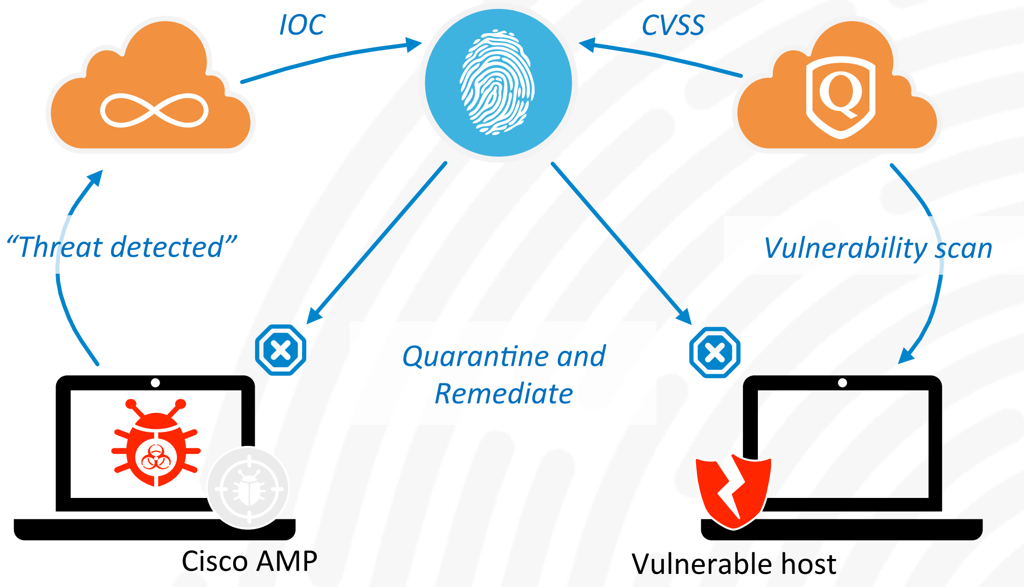
Reduce vulnerabilities, contain threats

Problem



Compromised endpoints spread malware by exploiting known vulnerabilities in the network

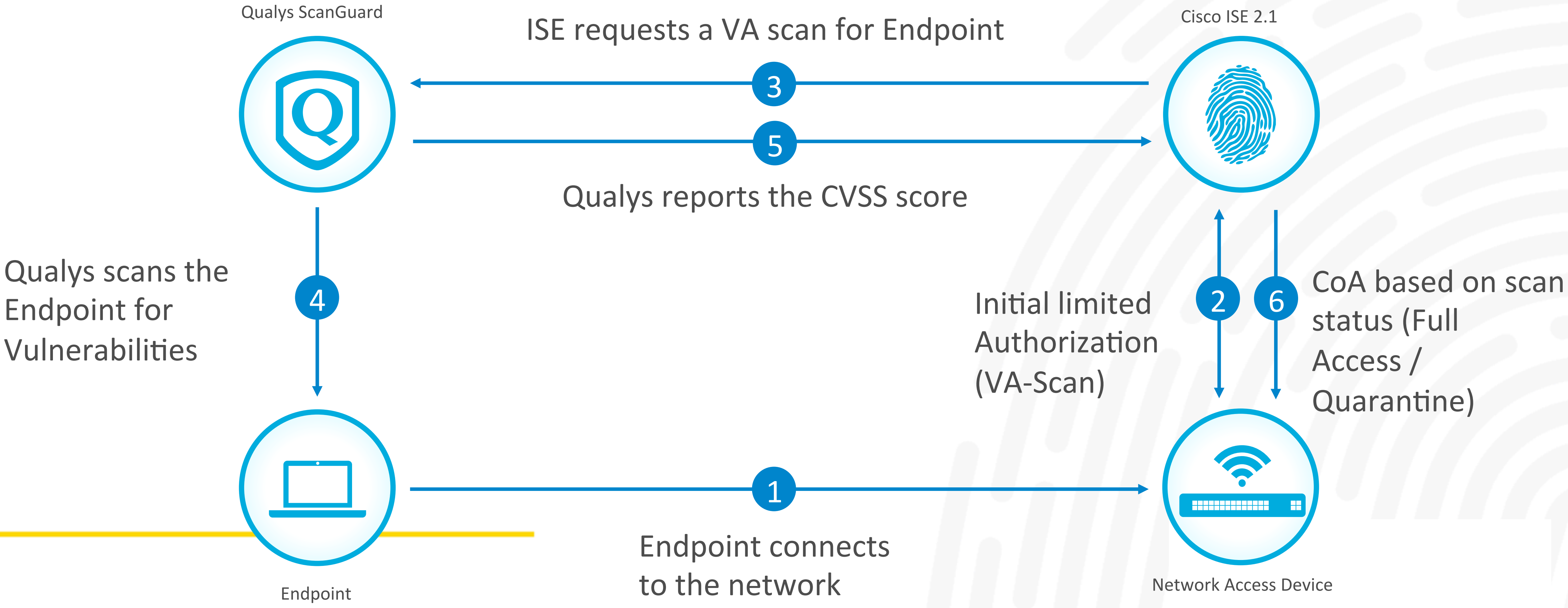
Solution



Flag compromised and vulnerable hosts and limit access to remediation Segment

Common Vulnerability Scoring System (CVSS) | Indicators of Compromise (IOC) | Advanced Malware Protection (AMP)

Threat Centric NAC with Qualys - Overview



Qualys ScanGuard

Cisco ISE 2.1

Endpoint

Network Access Device

1 Endpoint connects to the network

2 Initial limited Authorization (VA-Scan)

3 ISE requests a VA scan for Endpoint

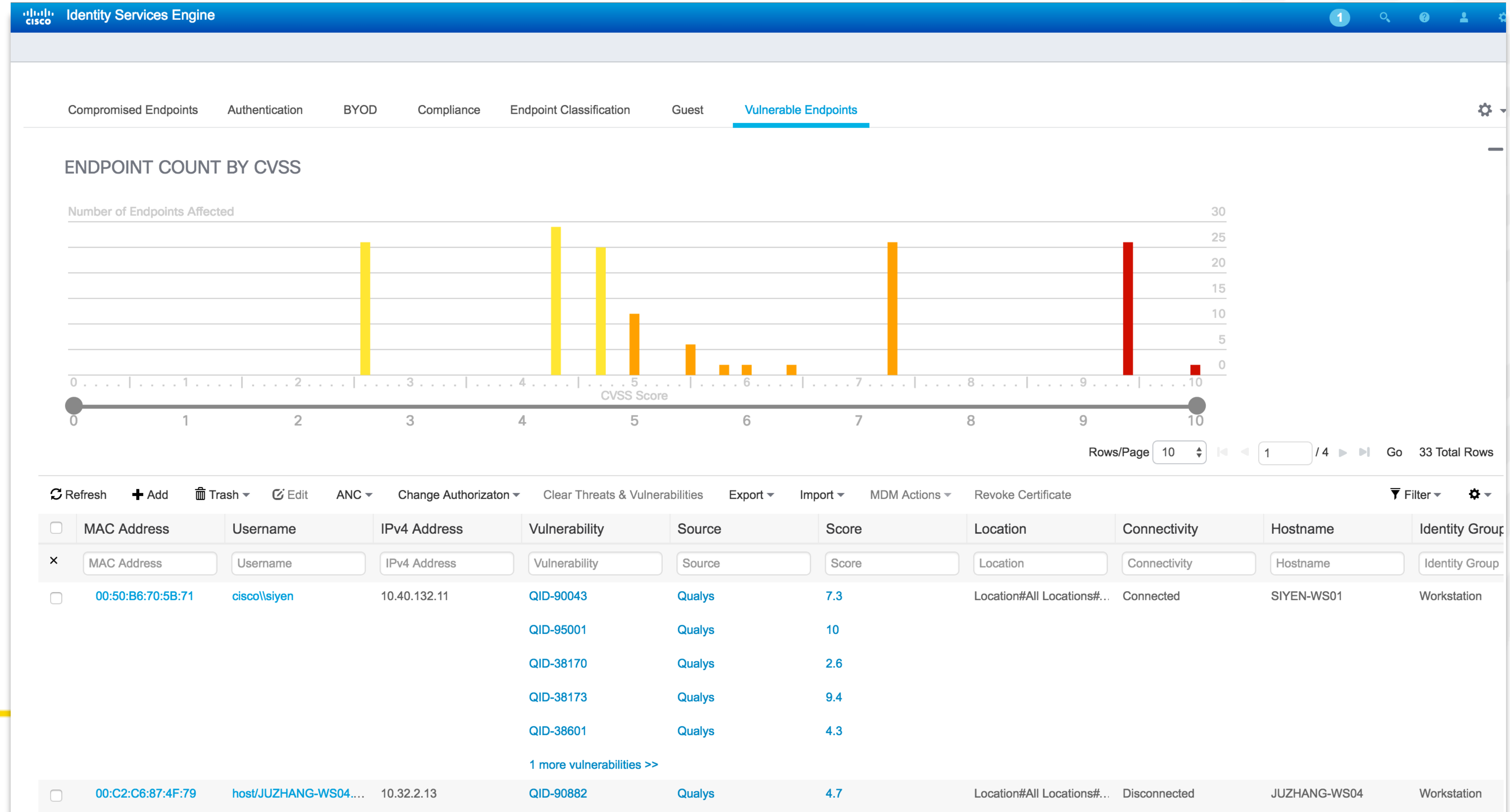
4 Qualys scans the Endpoint for Vulnerabilities

5 Qualys reports the CVSS score

6 CoA based on scan status (Full Access / Quarantine)

‘Vulnerable Endpoints’

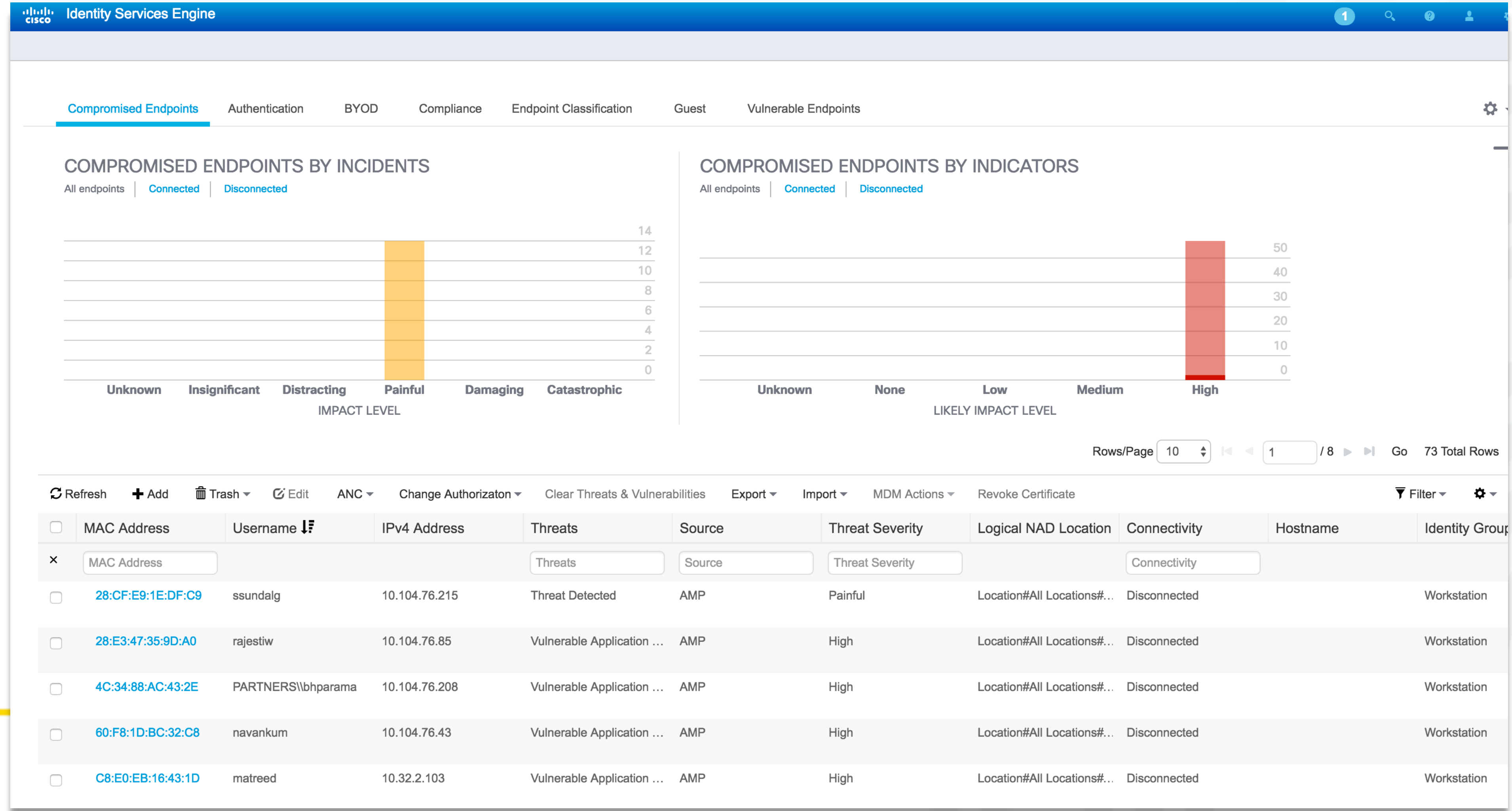
based on Common Vulnerability Scoring System (CVSS)



□	MAC Address	Username	IPv4 Address	Vulnerability	Source	Score	Location	Connectivity	Hostname	Identity Group
□	00:50:B6:70:5B:71	cisco\\siyen	10.40.132.11	QID-90043	Qualys	7.3	Location#All Locations#...	Connected	SIYEN-WS01	Workstation
				QID-95001	Qualys	10				
				QID-38170	Qualys	2.6				
				QID-38173	Qualys	9.4				
				QID-38601	Qualys	4.3				
				1 more vulnerabilities >>						
□	00:C2:C6:87:4F:79	host/JUZHANG-WS04....	10.32.2.13	QID-90882	Qualys	4.7	Location#All Locations#...	Disconnected	JUZHANG-WS04	Workstation

‘Compromised Endpoints’

based on Incidents and Indicators



COMPROMISED ENDPOINTS BY INCIDENTS

All endpoints | Connected | Disconnected

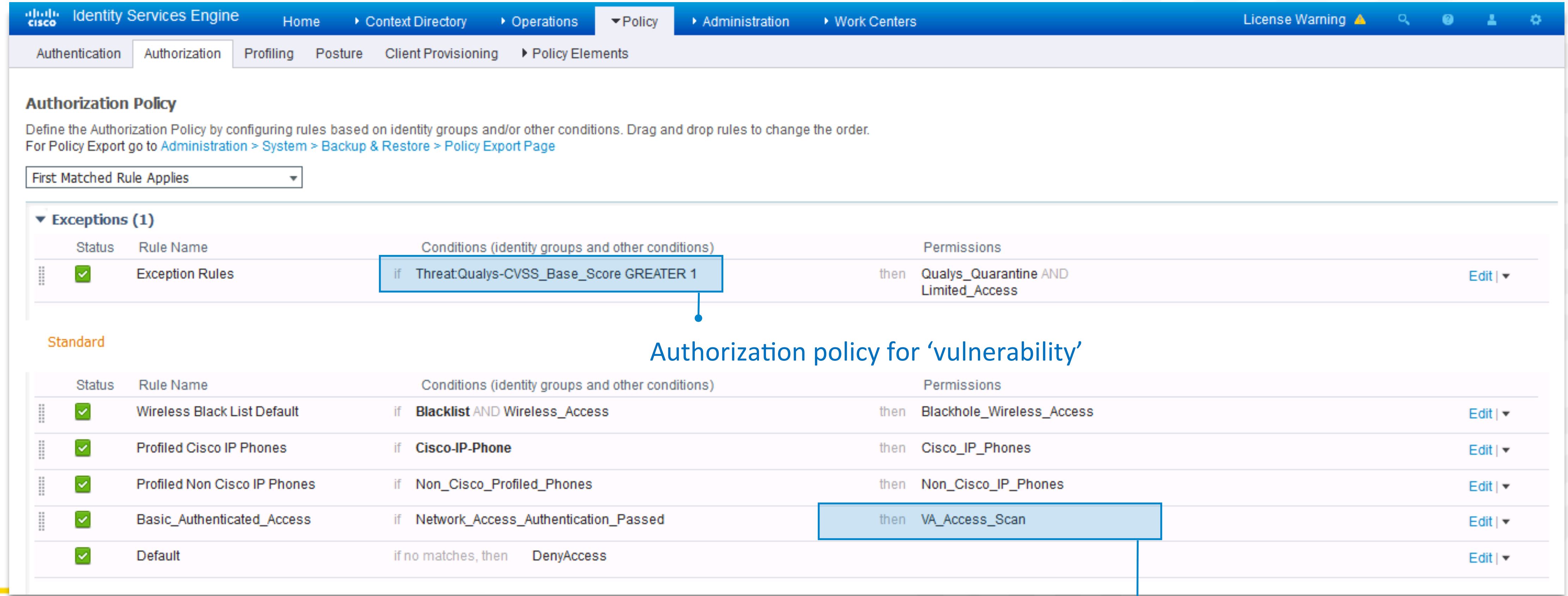
COMPROMISED ENDPOINTS BY INDICATORS

All endpoints | Connected | Disconnected

Rows/Page 10 | 1 / 8 Go 73 Total Rows

	MAC Address	Username	IPv4 Address	Threats	Source	Threat Severity	Logical NAD Location	Connectivity	Hostname	Identity Group
×	MAC Address			Threats	Source	Threat Severity		Connectivity		
□	28:CF:E9:1E:DF:C9	ssundalg	10.104.76.215	Threat Detected	AMP	Painful	Location#All Locations#...	Disconnected		Workstation
□	28:E3:47:35:9D:A0	rajestiw	10.104.76.85	Vulnerable Application ...	AMP	High	Location#All Locations#...	Disconnected		Workstation
□	4C:34:88:AC:43:2E	PARTNERS\\bhparama	10.104.76.208	Vulnerable Application ...	AMP	High	Location#All Locations#...	Disconnected		Workstation
□	60:F8:1D:BC:32:C8	navankum	10.104.76.43	Vulnerable Application ...	AMP	High	Location#All Locations#...	Disconnected		Workstation
□	C8:E0:EB:16:43:1D	matreed	10.32.2.103	Vulnerable Application ...	AMP	High	Location#All Locations#...	Disconnected		Workstation

TC-NAC Policy



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (1)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Exception Rules	if	Threat:Qualys-CVSS_Base_Score GREATER 1	then	Qualys_Quarantine AND Limited_Access	Edit | ▾

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	VA_Access_Scan	Edit | ▾
☑	Default	if no matches, then	DenyAccess			Edit | ▾

Authorization policy for ‘vulnerability’

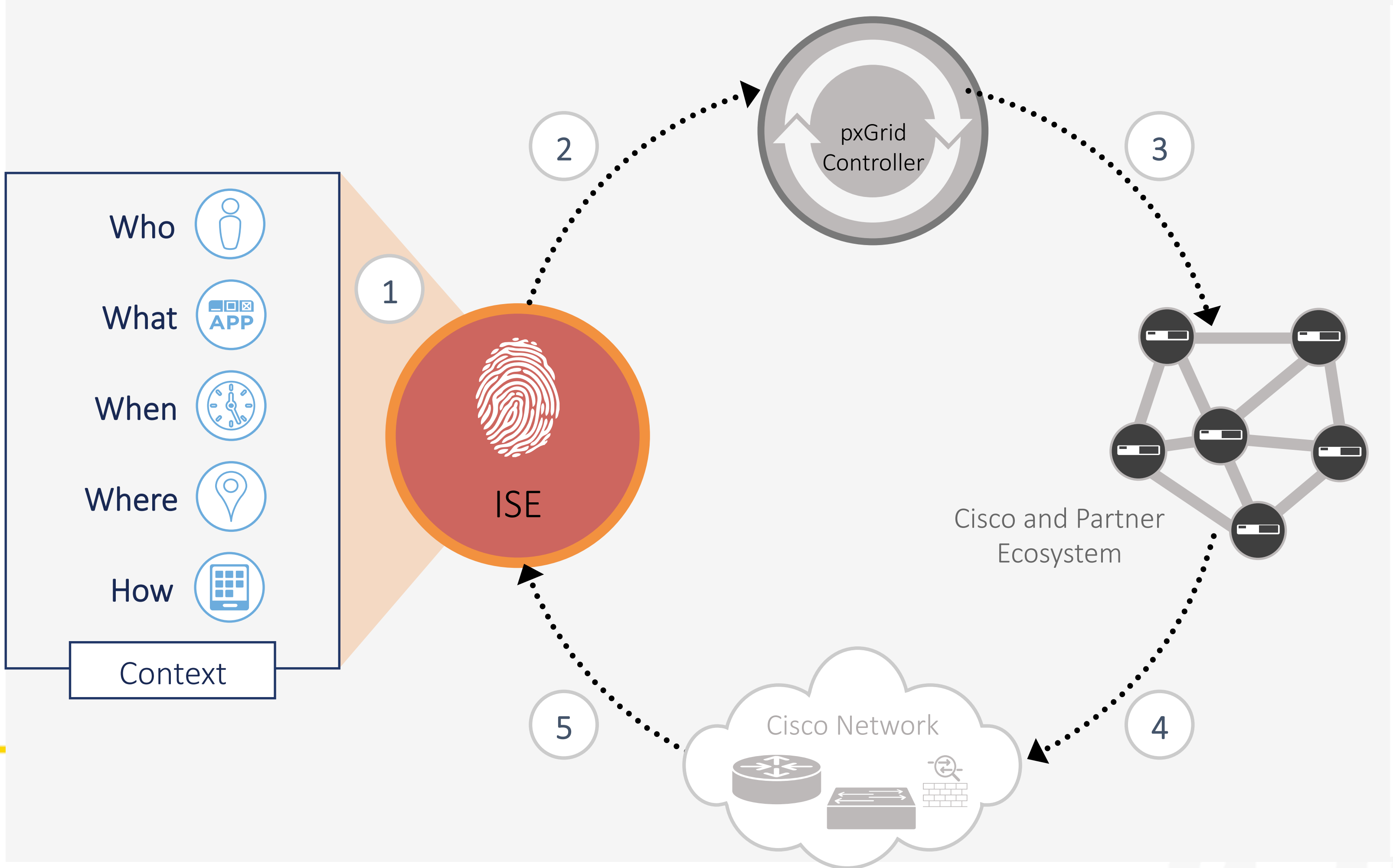
Initial ‘limited access’ + Vulnerability Scan

Agenda

- ISE 2.0 and 2.1 introduction
- Threat Centric NAC
- **pxGrid update**
- Device Admin (TACACS+)

Cisco Platform Exchange Grid (PxGrid)

Enable Unified Threat Response by Sharing Contextual Data



1 Cisco® ISE collects contextual data from network

2 Context is shared via pxGrid technology

3 Partners use context to improve visibility to detect threats

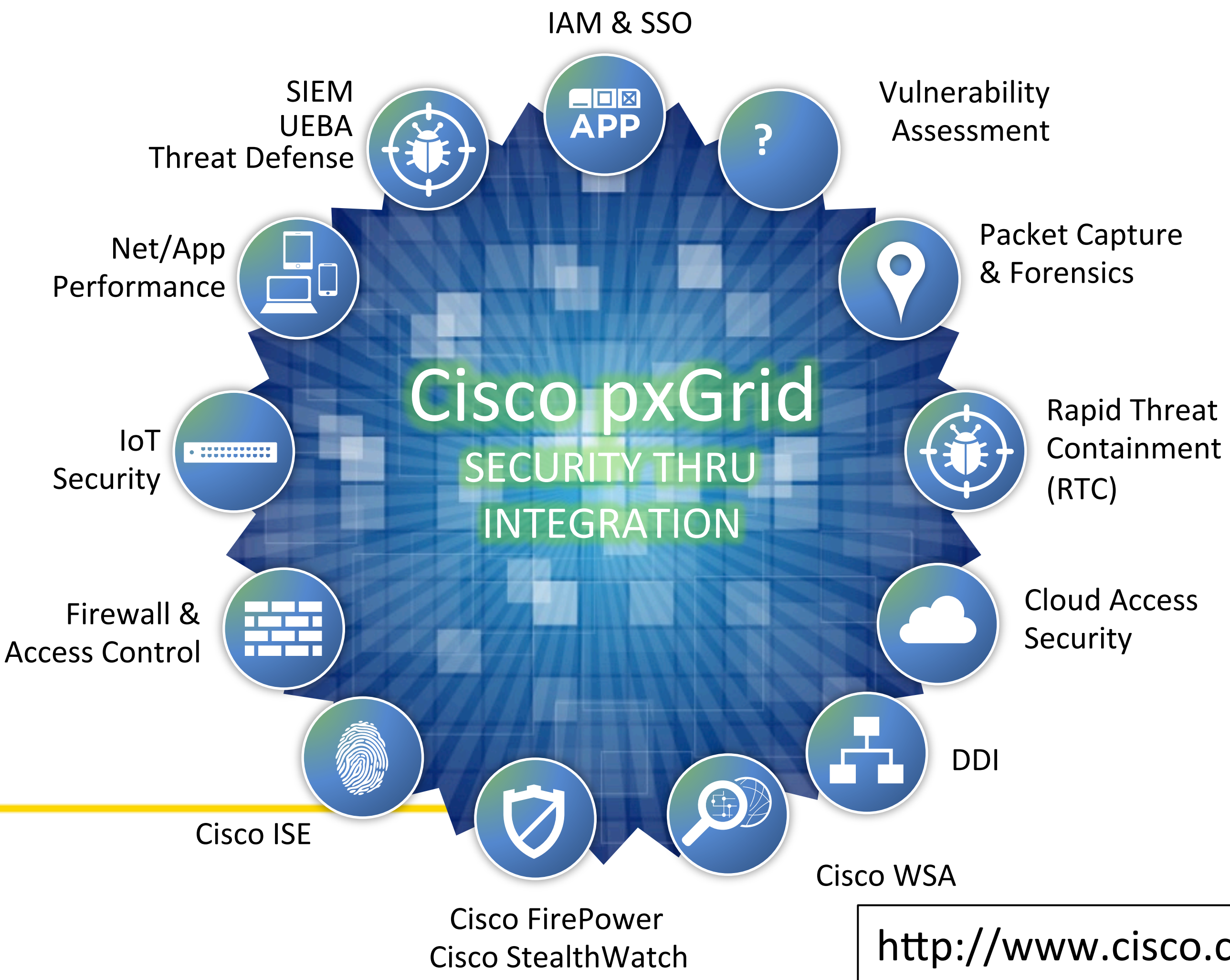
4 Partners can direct ISE to rapidly contain threats

5 ISE uses partner data to update context and refine access policy

https://datatracker.ietf.org/doc/draft-appala-mile-xmpp-grid/

pxGrid – Industry Adoption Critical Mass

40+ Partner Product Integrations and 12 Technology Areas in 18 Months Since Production Release

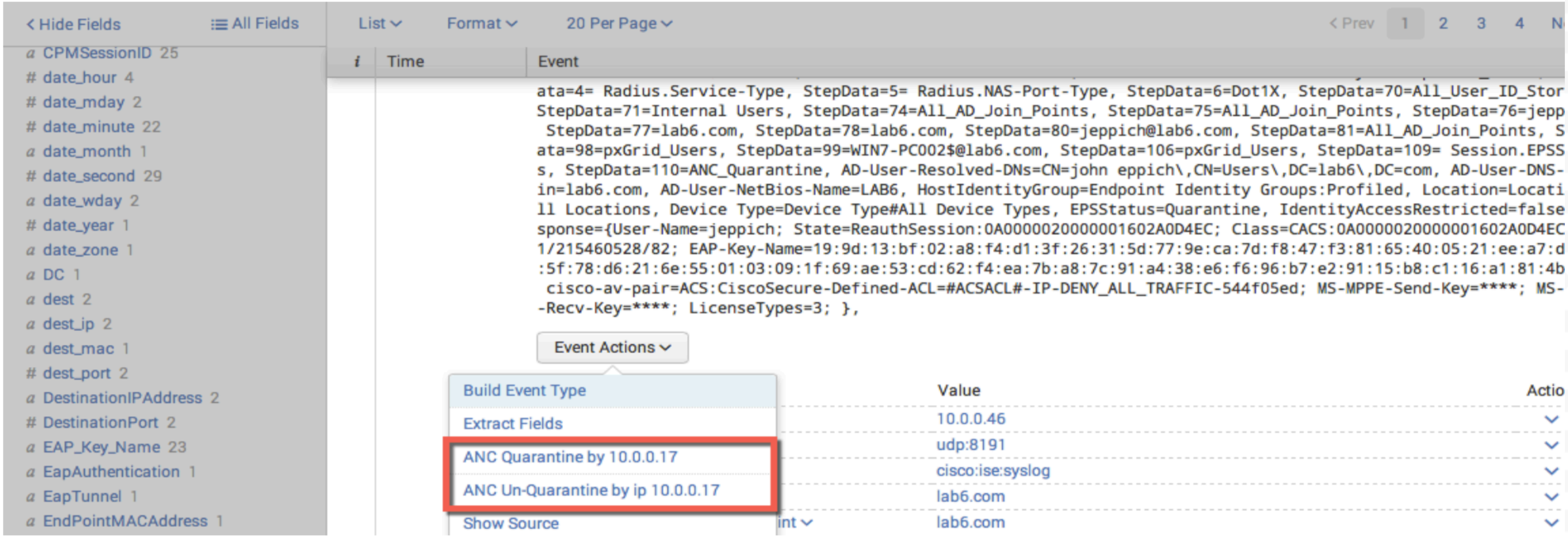


pxGrid-Enabled Partners:

- Cisco: WSA, FirePower, ISE, StealthWatch
- RTC: Cisco FirePower, Cisco StealthWatch, Attivo, Bayshore, E8, Elastica, Hawk, Huntsman, Infoblox, Intelliment, Invincea, Lemonfish, LogRhythm, NetIQ, Rapid7, RedShift, SAINT, Splunk, Tenable, ThreatTrack, TrapX
- Firewall: Check Point, Infoblox, Intelliment, Bayshore
- DDI: Infoblox
- CASB: Elastica, Netskope, SkyHigh
  Net/App: Lumeta, Savvius
- SIEM/TD: LogRhythm, NetIQ, Splunk
  UEBA: E8, FortScale, Niara, Rapid7
- IAM: NetIQ, Ping, SecureAuth, Situational
- Vulnerability: Rapid7, SAINT, Tenable
- IoT Security: Bayshore Networks
- P-Cap/Forensics: Emulex

http://www.cisco.com/c/en/us/products/security/identity-services-engine/technology-partners.html

Splunk use case



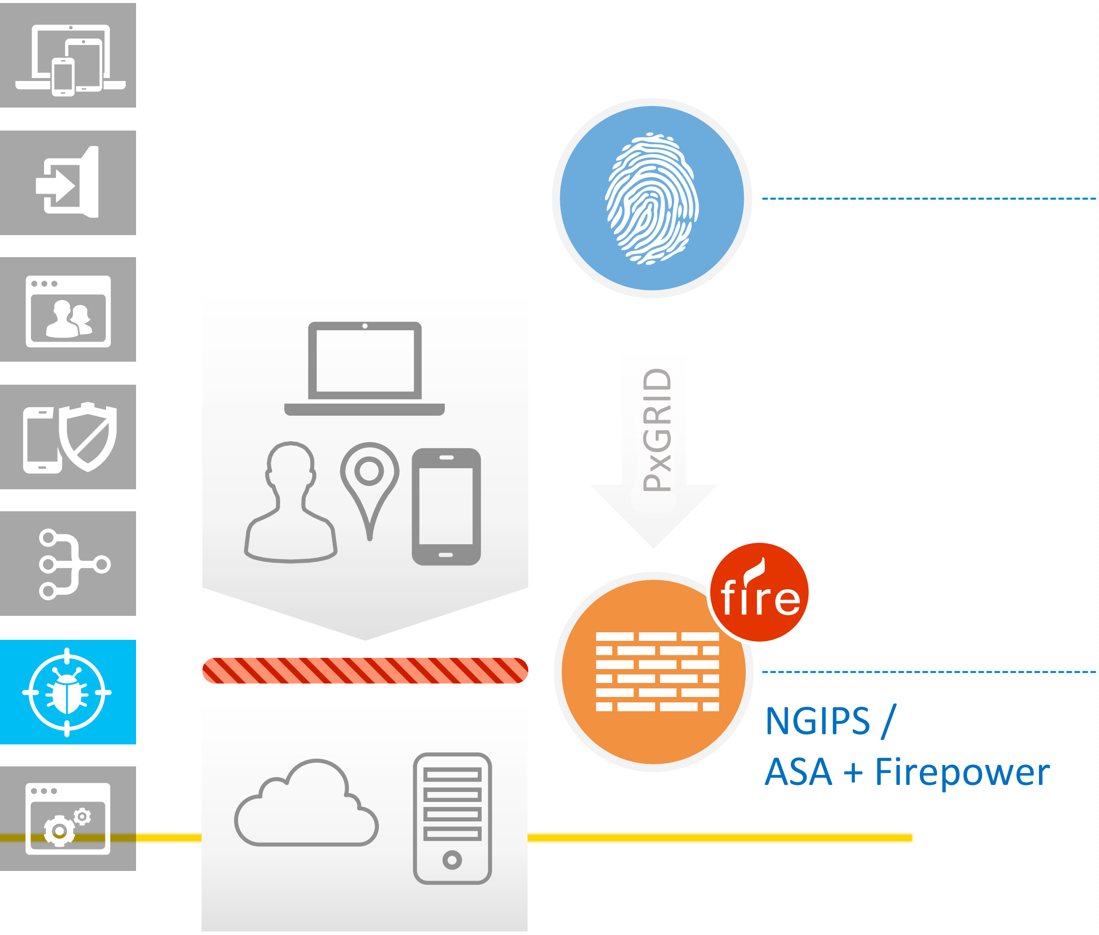
a	CPMSessionID	25
#	date_hour	4
#	date_mday	2
#	date_minute	22
a	date_month	1
#	date_second	29
a	date_wday	2
#	date_year	1
a	date_zone	1
a	DC	1
a	dest	2
a	dest_ip	2
a	dest_mac	1
#	dest_port	2
a	DestinationIPAddress	2
#	DestinationPort	2
a	EAP_Key_Name	23
a	EapAuthentication	1
a	EapTunnel	1
a	EndPointMACAddress	1

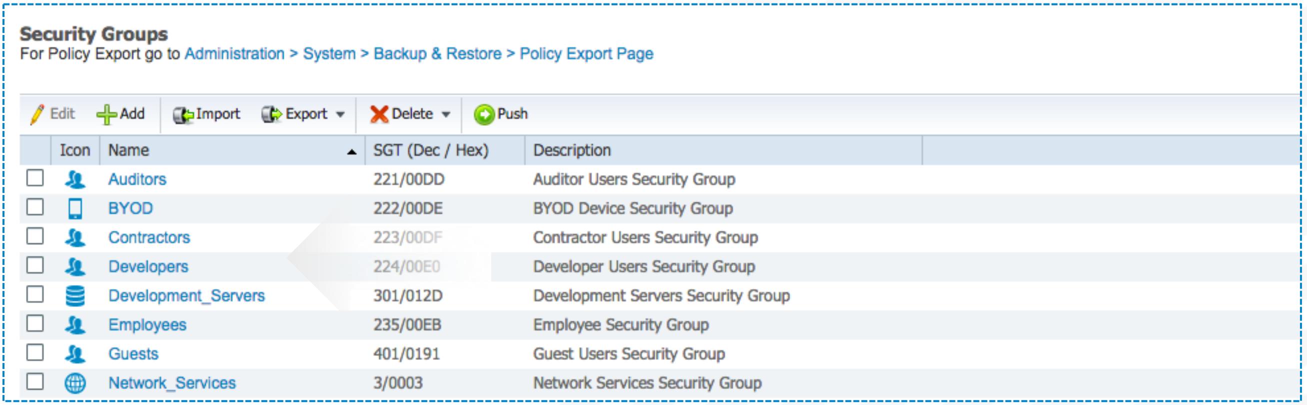
```
ata=4= Radius.Service-Type, StepData=5= Radius.NAS-Port-Type, StepData=6=Dot1X, StepData=70=All_User_ID_Stor
StepData=71=Internal Users, StepData=74=All_AD_Join_Points, StepData=75=All_AD_Join_Points, StepData=76=jepp
 StepData=77=lab6.com, StepData=78=lab6.com, StepData=80=jeppich@lab6.com, StepData=81=All_AD_Join_Points, S
ata=98=pxGrid_Users, StepData=99=WIN7-PC002$@lab6.com, StepData=106=pxGrid_Users, StepData=109= Session.EPSS
s, StepData=110=ANC_Quarantine, AD-User-Resolved-DNs=CN=john eppich\,CN=Users\,DC=lab6\,DC=com, AD-User-DNS-
in=lab6.com, AD-User-NetBios-Name=LAB6, HostIdentityGroup=Endpoint Identity Groups:Profiled, Location=Locati
ll Locations, Device Type=Device Type#All Device Types, EPSStatus=Quarantine, IdentityAccessRestricted=false
sponse={User-Name=jeppich; State=ReauthSession:0A0000020000001602A0D4EC; Class=CACS:0A0000020000001602A0D4EC
1/215460528/82; EAP-Key-Name=19:9d:13:bf:02:a8:f4:d1:3f:26:31:5d:77:9e:ca:7d:f8:47:f3:81:65:40:05:21:ee:a7:d
:5f:78:d6:21:6e:55:01:03:09:1f:69:ae:53:cd:62:f4:ea:7b:a8:7c:91:a4:38:e6:f6:96:b7:e2:91:15:b8:c1:16:a1:81:4b
 cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-DENY_ALL_TRAFFIC-544f05ed; MS-MPPE-Send-Key=****; MS-
-Recv-Key=****; LicenseTypes=3; },
```

Value
10.0.0.46
udp:8191
cisco:ise:syslog
lab6.com
lab6.com

Firepower polices based on ISE attributes

‘Access Control Policies’ based on ISE Attributes **(SGT, Device-type and Endpoint Location)**

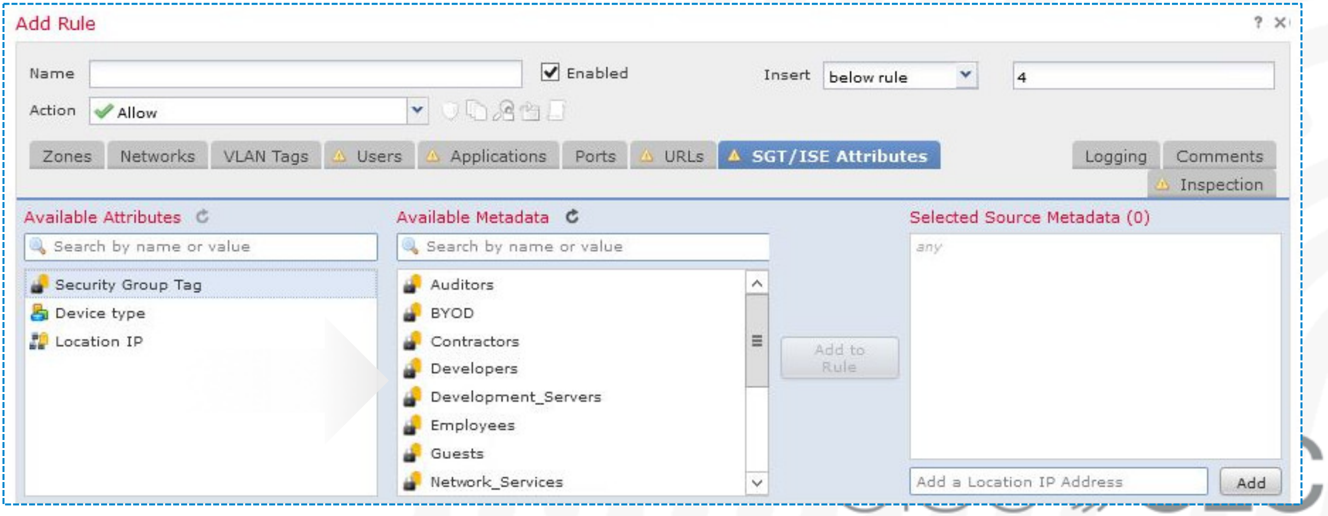




Security Groups

For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

	Icon	Name	SGT (Dec / Hex)	Description
□		Auditors	221/00DD	Auditor Users Security Group
□		BYOD	222/00DE	BYOD Device Security Group
□		Contractors	223/00DF	Contractor Users Security Group
□		Developers	224/00E0	Developer Users Security Group
□		Development_Servers	301/012D	Development Servers Security Group
□		Employees	235/00EB	Employee Security Group
□		Guests	401/0191	Guest Users Security Group
□		Network_Services	3/0003	Network Services Security Group



Add Rule

Name:

☑ Enabled

Insert: below rule 4

Action: Allow

Available Attributes

Search by name or value

- Security Group Tag
- Device type
- Location IP

Available Metadata

Search by name or value

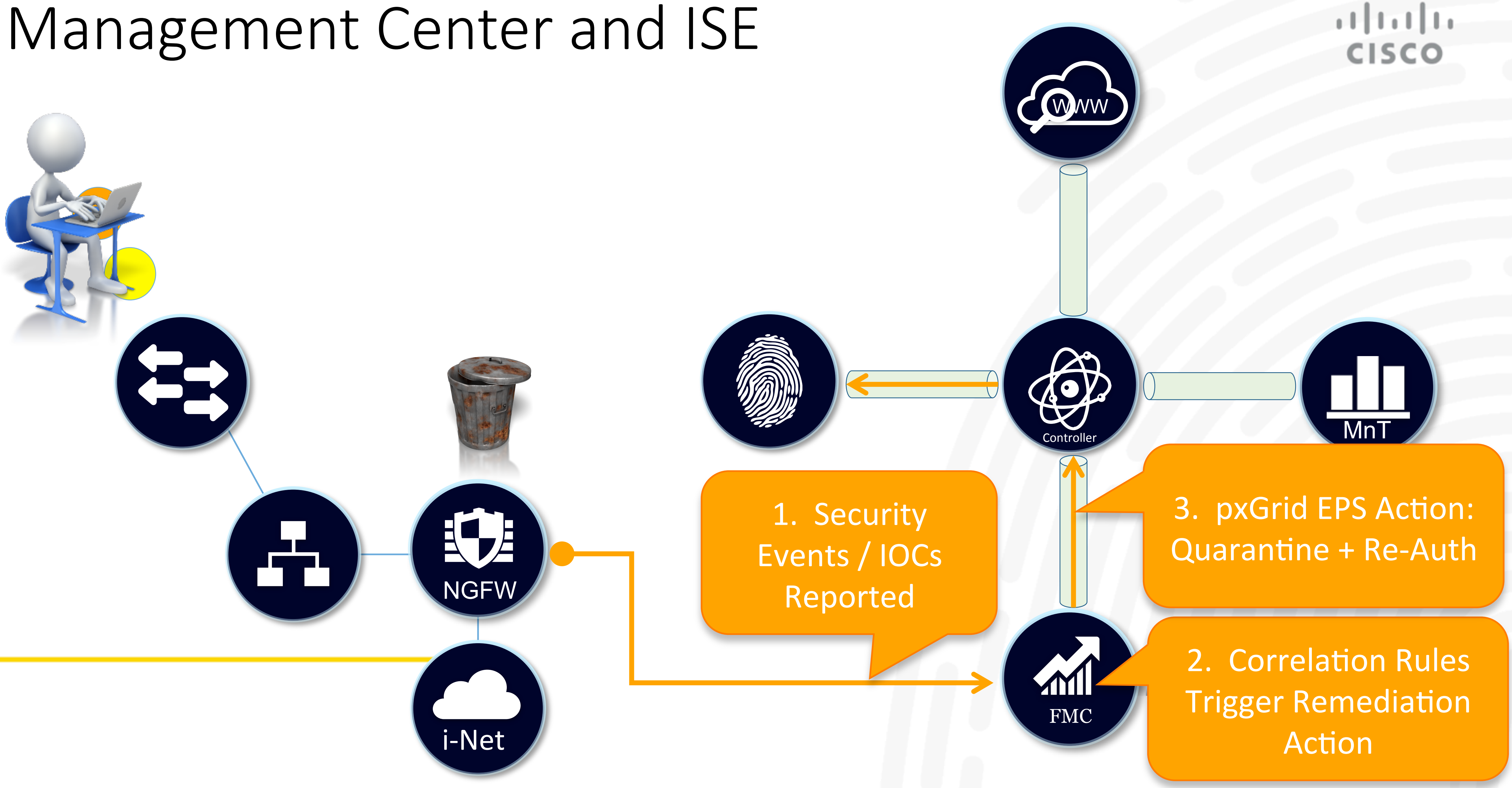
- Auditors
- BYOD
- Contractors
- Developers
- Development_Servers
- Employees
- Guests
- Network_Services

Selected Source Metadata (0)

any

Add a Location IP Address

Rapid Threat Containment with Firepower Management Center and ISE

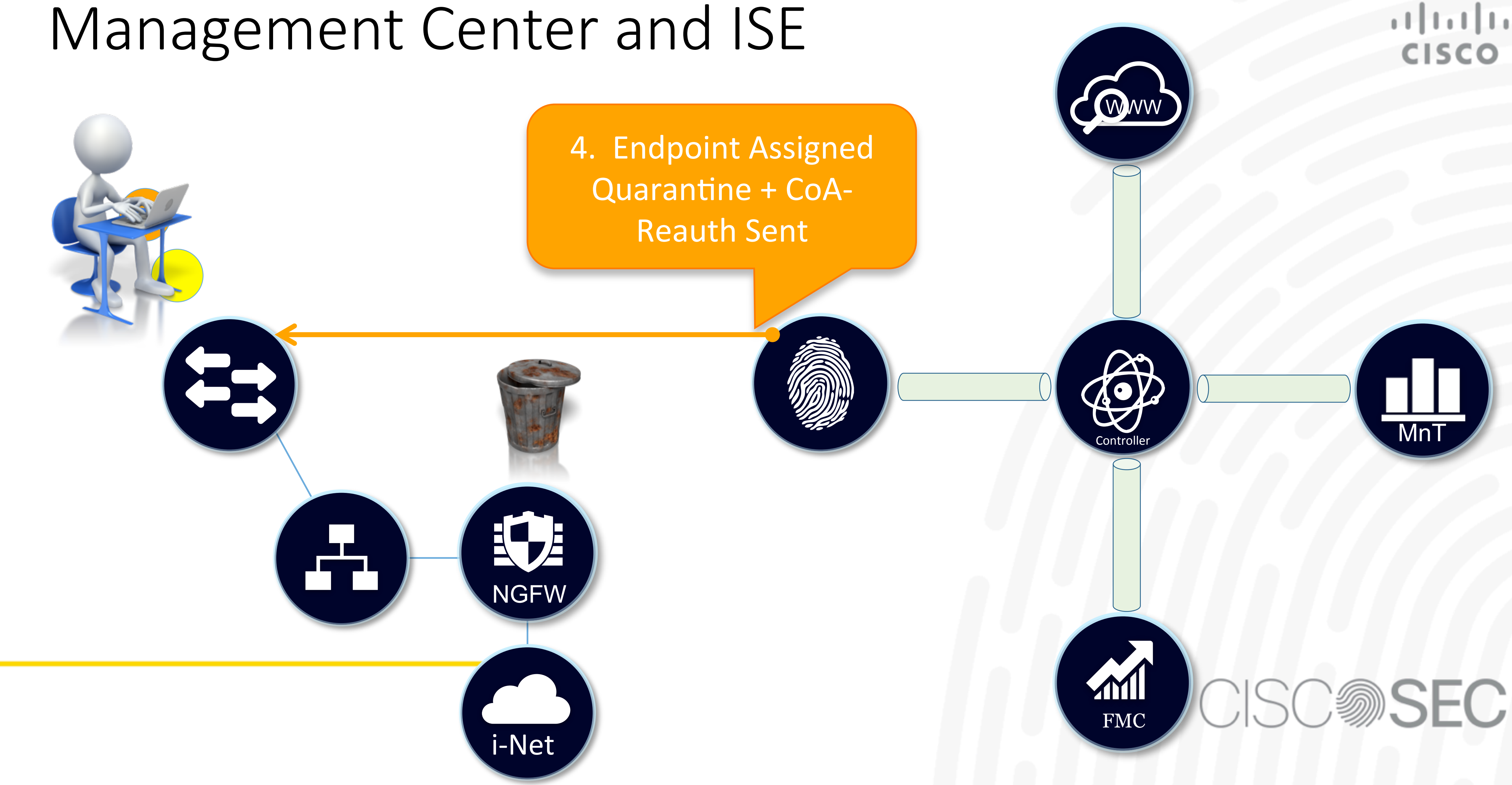


1. Security Events / IOCs Reported

2. Correlation Rules Trigger Remediation Action

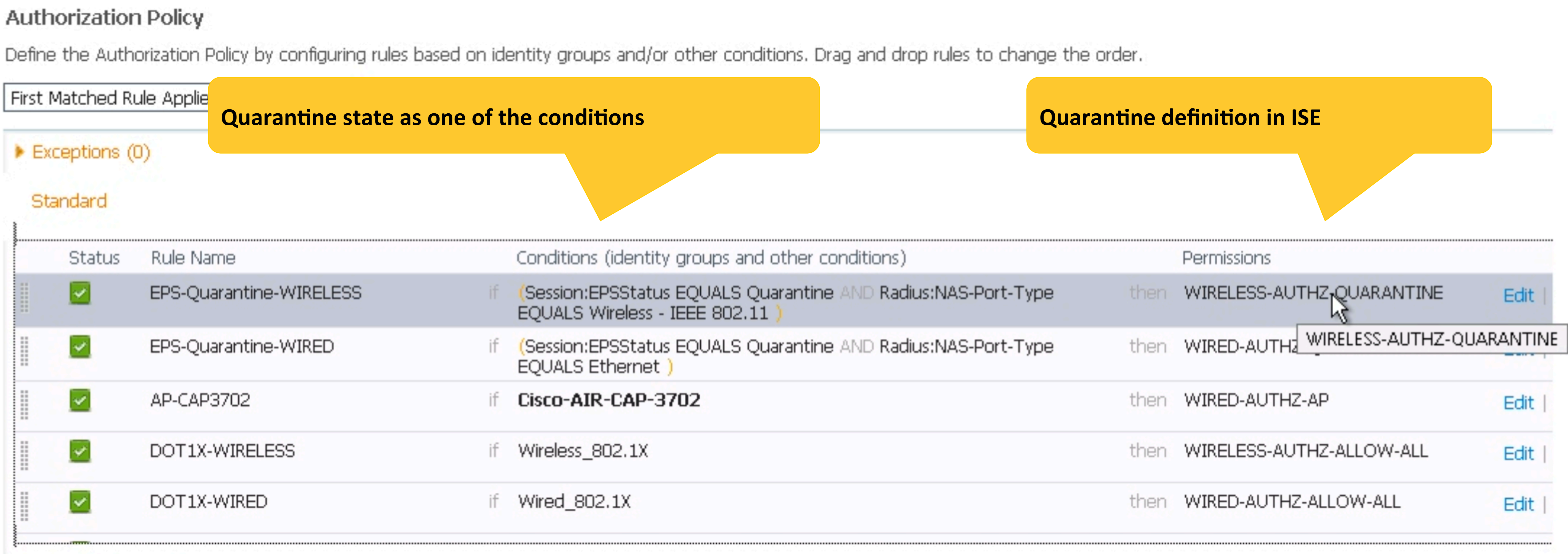
3. pxGrid EPS Action: Quarantine + Re-Auth

Rapid Threat Containment with Firepower Management Center and ISE



4. Endpoint Assigned Quarantine + CoA-Reauth Sent

Authorization Policy in ISE using Quarantine Service



Quarantine state as one of the conditions

Quarantine definition in ISE

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applie

▸ Exceptions (0)

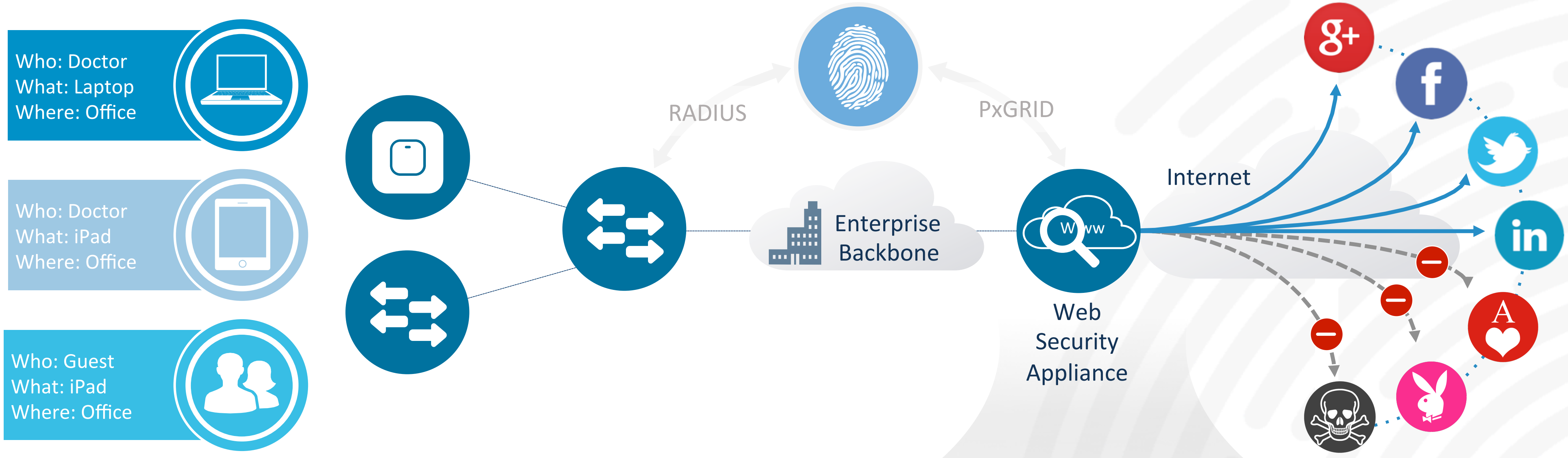
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	EPS-Quarantine-WIRELESS	if	(Session:EPSStatus EQUALS Quarantine AND Radius:NAS-Port-Type EQUALS Wireless - IEEE 802.11)	then	WIRELESS-AUTHZ-QUARANTINE	Edit |
☑	EPS-Quarantine-WIRED	if	(Session:EPSStatus EQUALS Quarantine AND Radius:NAS-Port-Type EQUALS Ethernet)	then	WIRED-AUTHZ	
☑	AP-CAP3702	if	**Cisco-AIR-CAP-3702**	then	WIRED-AUTHZ-AP	Edit |
☑	DOT1X-WIRELESS	if	Wireless_802.1X	then	WIRELESS-AUTHZ-ALLOW-ALL	Edit |
☑	DOT1X-WIRED	if	Wired_802.1X	then	WIRED-AUTHZ-ALLOW-ALL	Edit |

WIRELESS-AUTHZ-QUARANTINE

Context based ‘Web filtering’

With Cisco Web Security Appliance (WSA) and Identity Service Engine (ISE)



Who: Doctor
What: Laptop
Where: Office

Who: Doctor
What: iPad
Where: Office

Who: Guest
What: iPad
Where: Office

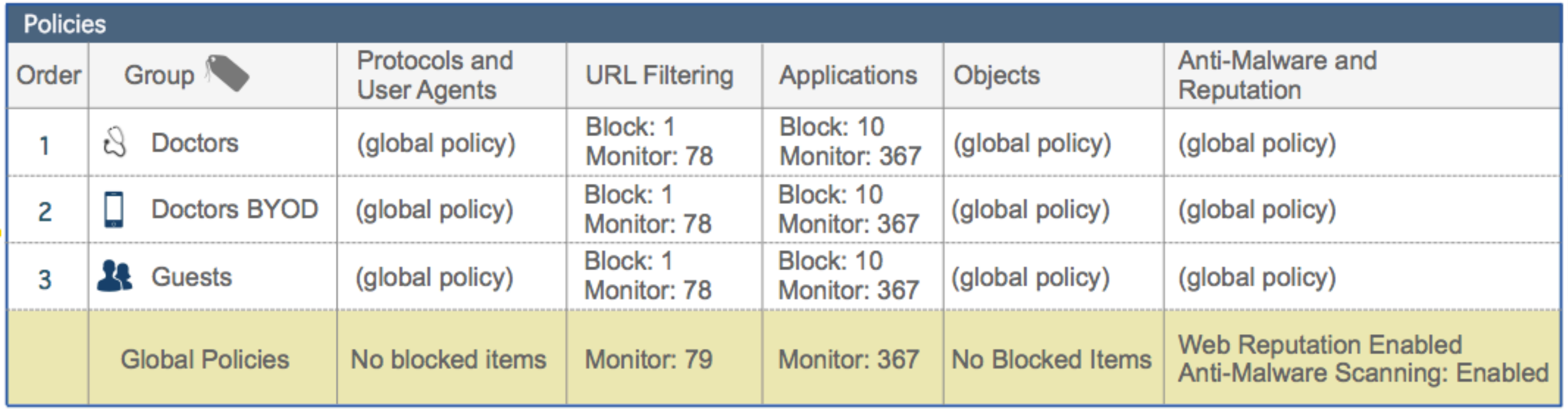
RADIUS

PxGRID

Enterprise Backbone

Internet

Web Security Appliance

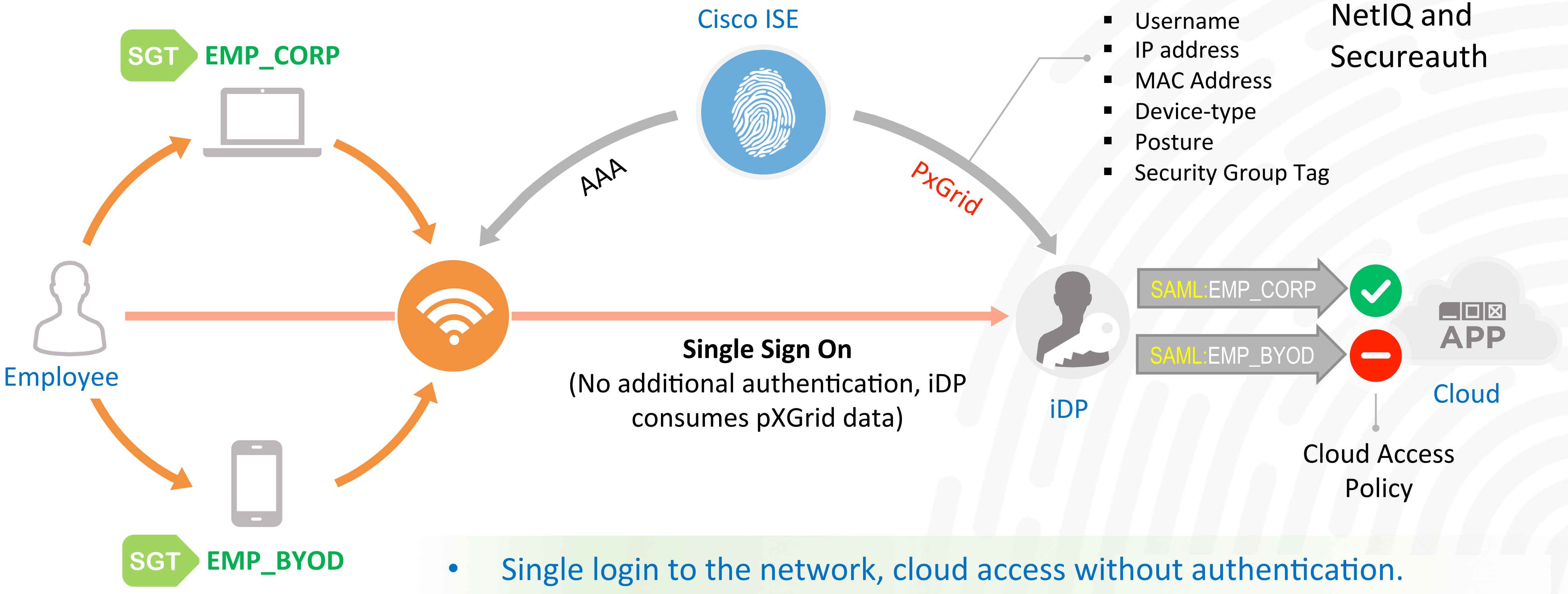


Policies

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation
1	Doctors	(global policy)	Block: 1 Monitor: 78	Block: 10 Monitor: 367	(global policy)	(global policy)
2	Doctors BYOD	(global policy)	Block: 1 Monitor: 78	Block: 10 Monitor: 367	(global policy)	(global policy)
3	Guests	(global policy)	Block: 1 Monitor: 78	Block: 10 Monitor: 367	(global policy)	(global policy)
	Global Policies	No blocked items	Monitor: 79	Monitor: 367	No Blocked Items	Web Reputation Enabled Anti-Malware Scanning: Enabled

Secure cloud access

Context enables Single-Sign-On (SSO) and role-based access



- Username
- IP address
- MAC Address
- Device-type
- Posture
- Security Group Tag

Situational, NetIQ and Secureauth

Single Sign On
(No additional authentication, iDP consumes pXGrid data)

Cloud Access Policy

- Single login to the network, cloud access without authentication.
- Differentiated cloud access, based on contextual data sent over SAML

Agenda

- ISE 2.0 and 2.1 introduction
- Threat Centric NAC
- pxGrid update
- **Device Admin (TACACS+)**

Same ISE for ‘Network Device’ Administration

Feature Highlight

Customers can now use Terminal Access Controller Access Control System (TACACS) with ISE to simplify device administration and enhance security through flexible, granular control of access to network devices.

Benefits

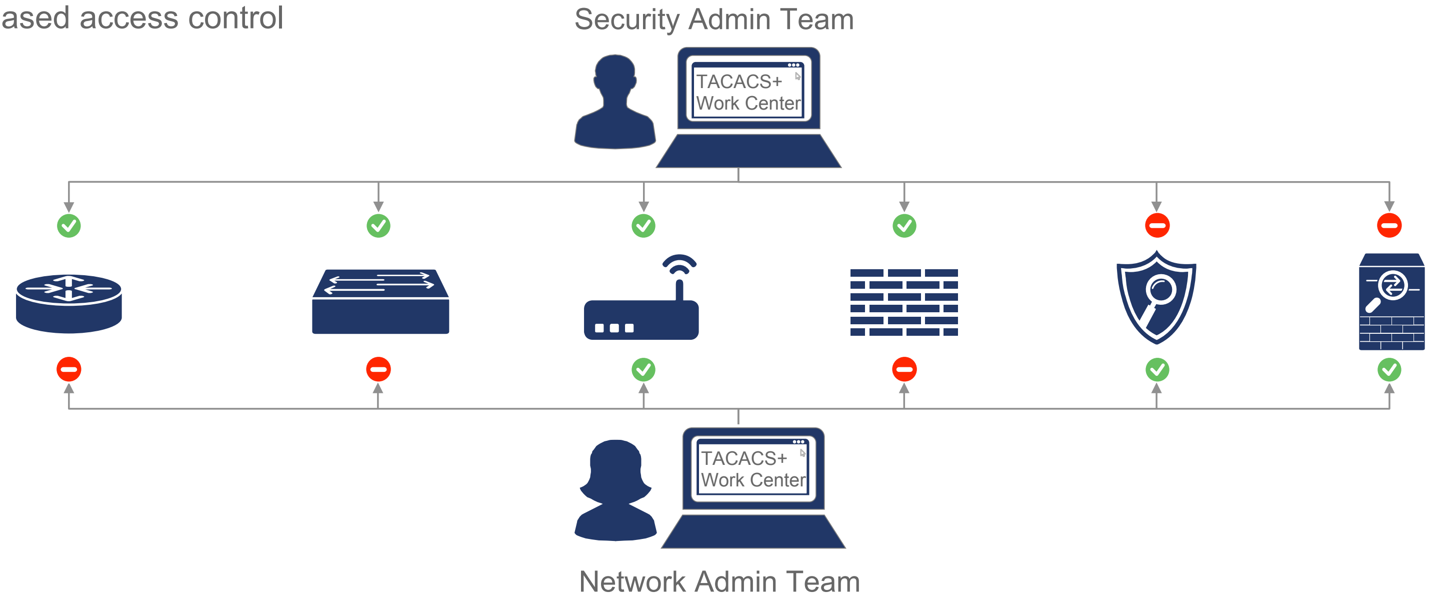
Simplified, centralized device administration
Increase security, compliancy, auditing for a full range of administration use cases

Flexible, granular control
Control and audit the configuration of network devices

Holistic, centralized visibility
Get a comprehensive view of TACACS+ configurations with the TACACS+ administrator work center

TACACS+ Device Administration

Role-based access control

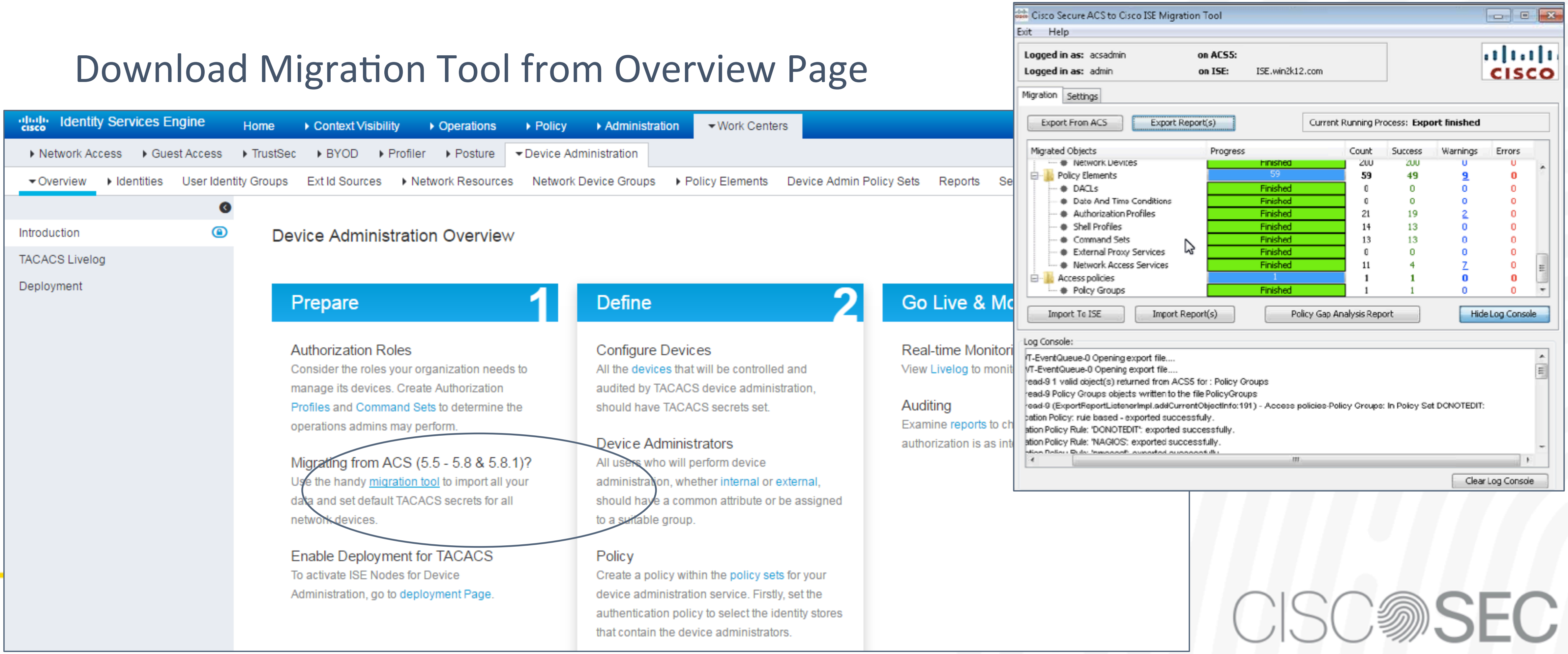


Capabilities

- Role-based access control
- Flow-based user experience
- Command level authorization with detailed logs for auditing
- Dedicated TACACS+ workcenter for network administrators
- Support for core ACS5 features

TACACS+ Migration Tool

Download Migration Tool from Overview Page



Device Administration Overview

Prepare 1

Authorization Roles

Consider the roles your organization needs to manage its devices. Create Authorization Profiles and Command Sets to determine the operations admins may perform.

Migrating from ACS (5.5 - 5.8 & 5.8.1)?

Use the handy migration tool to import all your data and set default TACACS secrets for all network devices.

Enable Deployment for TACACS

To activate ISE Nodes for Device Administration, go to deployment Page.

Define 2

Configure Devices

All the devices that will be controlled and audited by TACACS device administration, should have TACACS secrets set.

Device Administrators

All users who will perform device administration, whether internal or external, should have a common attribute or be assigned to a suitable group.

Policy

Create a policy within the policy sets for your device administration service. Firstly, set the authentication policy to select the identity stores that contain the device administrators.

Go Live & Mo

Real-time Monitori

View Livelog to monit

Auditing

Examine reports to ch

authorization is as int

Cisco Secure ACS to Cisco ISE Migration Tool

Logged in as: acsadmin **on ACS5:**

Logged in as: admin **on ISE:** ISE.win2k12.com

Current Running Process: **Export finished**

Migrated Objects	Progress	Count	Success	Warnings	Errors
Network Devices	Finished	200	200	0	0
Policy Elements	59	59	49	9	0
DACLs	Finished	0	0	0	0
Date And Time Conditions	Finished	0	0	0	0
Authorization Profiles	Finished	21	19	2	0
Shell Profiles	Finished	14	13	0	0
Command Sets	Finished	13	13	0	0
External Proxy Services	Finished	0	0	0	0
Network Access Services	Finished	11	4	7	0
Access policies	1	1	1	0	0
Policy Groups	Finished	1	1	0	0

Log Console:

```
VT-EventQueue-0 Opening export file....
VT-EventQueue-0 Opening export file....
read-9 1 valid object(s) returned from ACS5 for : Policy Groups
read-9 Policy Groups objects written to the file PolicyGroups
read-9 (ExportReportListenerImpl.addCurrentObjectInfo:191) - Access policies-Policy Groups: In Policy Set DONOTEDIT:
cation Policy: rule based - exported successfully.
ation Policy Rule: 'DONOTEDIT': exported successfully.
ation Policy Rule: 'NAGIOS': exported successfully.
```

Thank you

György Ács
Cisco Systems
Gacs [at] cisco [dot] com