City of Kitchener

Zero Trust with Genian NAC

Agenda

- ❑ City of Kitchener Network Security Challenges
- ❑ Genian NAC Overview
- ❑ City of Kitchener Use Case Examples

Key Technologies: Cloud, Virtualization, Zero Trust / Least Privileged Access

City of Kitchener
Network Cybersecurity Challenges

KITCHENER

- ❑ How do we gain network visibility rapidly and accurately?
- ❑ How do we detect rogue devices connected to our network?
- ❑ How do we manage access for authorized devices?
- ❑ How do we manage network security remotely?

Company Overview

Business Name

Genians, Inc.

Main Products

Genian NAC, Genian DPI,
Genian Insights E EDR

Established

2005

Publicly Traded

263860:KS Listed on KOSDAQ

Employee

140 (70% are engineers)

Customers

Over 1,600

16 Years
Providing Solutions

#1
S.Korean Market

30+
Global Partners

1,600
Happy Customers

Genians Named a Representative Vendor in

FROST & SULLIVAN

Global NAC Market Forecast to 2024

Gartner

Market Guide for NAC 2018, 2020

Genian Next-Gen NAC

1. Illuminate Your Network
NETWORK SENSOR
2. Tidy Up Your Network
3. Control Network Access
4. Log All Activities and Events

Discover → Categorize → Enforce → Monitor

Genian Device Platform Intelligence (GDPI)

Visibility 2.0

Beyond Device Fingerprinting

Platform Identity, Context and Risk

Cloud Database with API

Available as Subscription Service

Over 6000 New Platforms in 2020

https://www.genians.com/dpi-list/

IDENTITY

Specific Platform

- Manufacturer
- Connection Types
- Actual image of each the device

CONTEXT

Business Information

- End of Sale (EOS)
- End of Life (EOL)
- Country of Origin

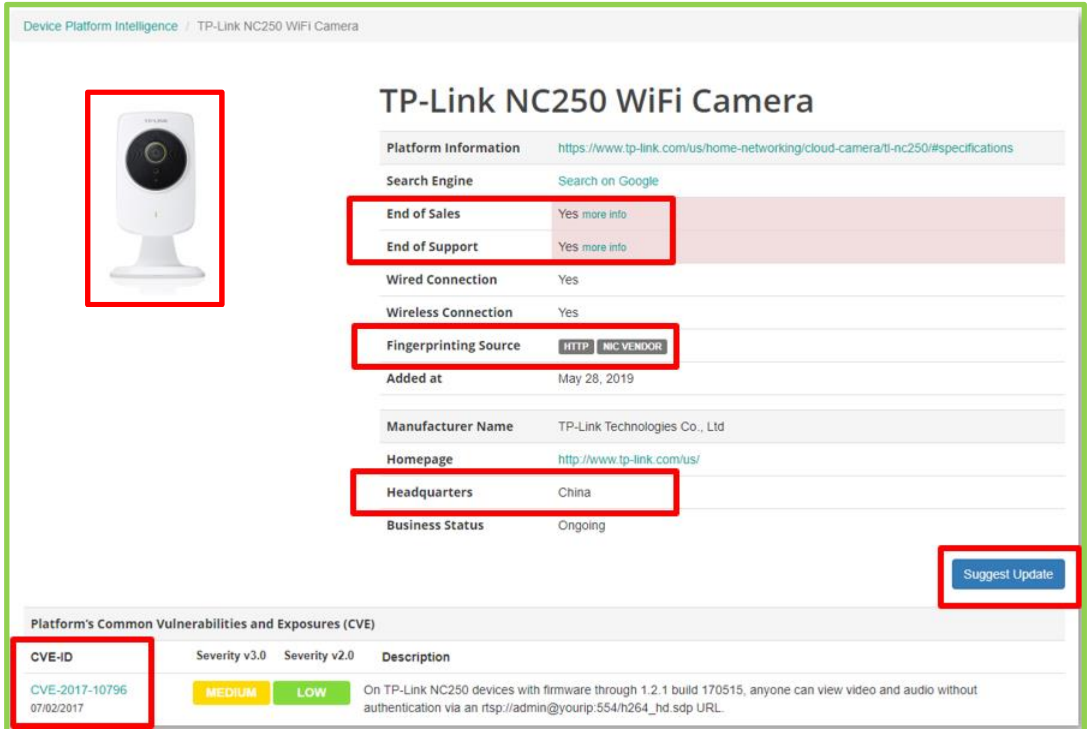
RISK

Technology Vulnerability

- List of CVEs

Business Vulnerability

- Out of Business
- Acquisitions



Device Platform Intelligence / TP-Link NC250 WiFi Camera

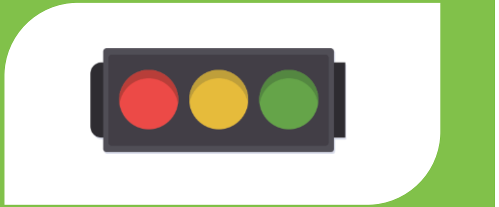
TP-Link NC250 WiFi Camera

Platform Information	https://www.tp-link.com/us/home-networking/cloud-camera/tl-nc250/#specifications
Search Engine	Search on Google
End of Sales	Yes more info
End of Support	Yes more info
Wired Connection	Yes
Wireless Connection	Yes
Fingerprinting Source	HTTP NIC VENDOR
Added at	May 28, 2019
Manufacturer Name	TP-Link Technologies Co., Ltd
Homepage	http://www.tp-link.com/us/
Headquarters	China
Business Status	Ongoing

Platform's Common Vulnerabilities and Exposures (CVE)

CVE-ID	Severity v3.0	Severity v2.0	Description
CVE-2017-10796 07/02/2017	MEDIUM	LOW	On TP-Link NC250 devices with firmware through 1.2.1 build 170515, anyone can view video and audio without authentication via an rtsp://admin@yourip:554/h264_hd.sdp URL.

Network Access Control



Step 1

Dynamic Node Grouping

Step 2

Granular Policy Enforcement

Step 3

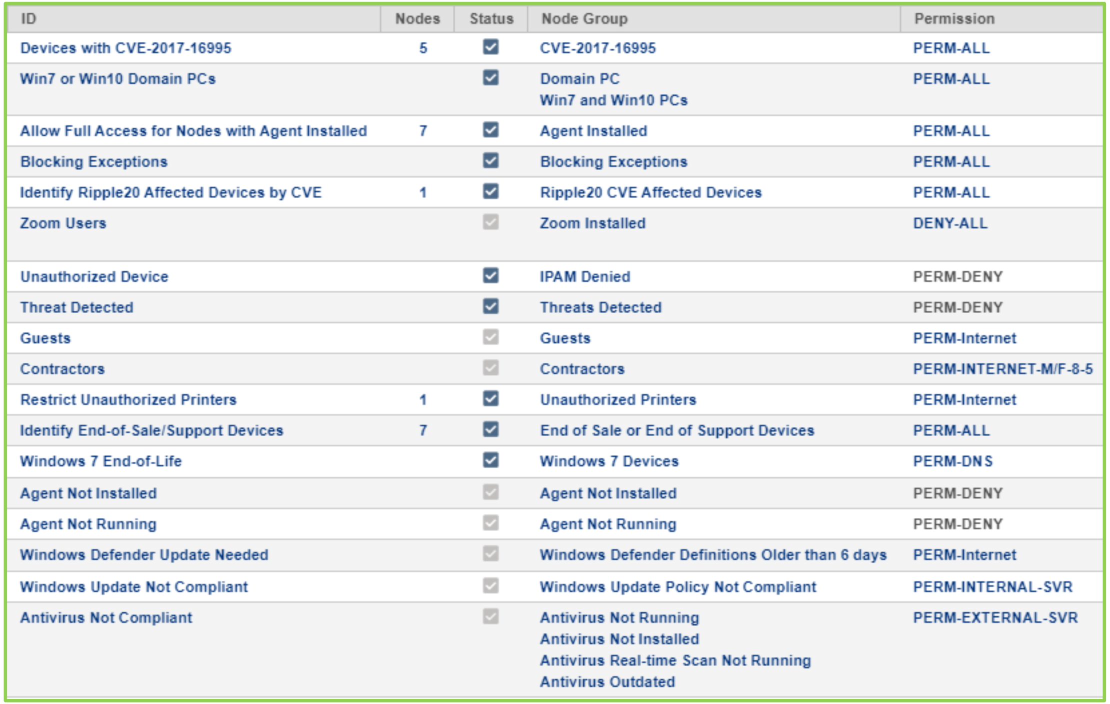
Choose Enforcement Method(s)

DYNAMIC CLASSIFICATION

- Condition-based Grouping (Over 500 predefined conditions)
- Policy Enforcement Based on Endpoint Compliance Status
- Granular Permissions Assigned

MULTI-LAYERED SECURITY / ENFORCEMENT

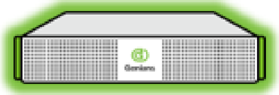
- **Layer 2: ARP Enforcement (Preferred)**
- Layer 2: 802.1x: Built-in RADIUS server
- Layer 3: TCP reset (SPAN/Mirror Port)
- Layer 3: Inline enforcer (Dual-homed Gateway)
- Agent: Quarantine at NIC Level or with Firewall
- DHCP: Built-in DHCP server



ID	Nodes	Status	Node Group	Permission
Devices with CVE-2017-16995	5	☑	CVE-2017-16995	PERM-ALL
Win7 or Win10 Domain PCs		☑	Domain PC Win7 and Win10 PCs	PERM-ALL
Allow Full Access for Nodes with Agent Installed	7	☑	Agent Installed	PERM-ALL
Blocking Exceptions		☑	Blocking Exceptions	PERM-ALL
Identify Ripple20 Affected Devices by CVE	1	☑	Ripple20 CVE Affected Devices	PERM-ALL
Zoom Users		☑	Zoom Installed	DENY-ALL
Unauthorized Device		☑	IPAM Denied	PERM-DENY
Threat Detected		☑	Threats Detected	PERM-DENY
Guests		☑	Guests	PERM-Internet
Contractors		☑	Contractors	PERM-INTERNET-M/F-8-5
Restrict Unauthorized Printers	1	☑	Unauthorized Printers	PERM-Internet
Identify End-of-Sale/Support Devices	7	☑	End of Sale or End of Support Devices	PERM-ALL
Windows 7 End-of-Life		☑	Windows 7 Devices	PERM-DNS
Agent Not Installed		☑	Agent Not Installed	PERM-DENY
Agent Not Running		☑	Agent Not Running	PERM-DENY
Windows Defender Update Needed		☑	Windows Defender Definitions Older than 6 days	PERM-Internet
Windows Update Not Compliant		☑	Windows Update Policy Not Compliant	PERM-INTERNAL-SVR
Antivirus Not Compliant		☑	Antivirus Not Running Antivirus Not Installed Antivirus Real-time Scan Not Running Antivirus Outdated	PERM-EXTERNAL-SVR

Genian NAC System Components

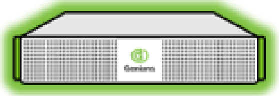
Policy Server



Management

- Cloud Managed in Public, Private or Hybrid Environments
- On-Prem Option Delivered as ISO Image, Install as VM or on H/W
- Correlates Data from All Network Sensors
- Policy Configuration, Distribution and Centralized Logging/Reporting

Network Sensor



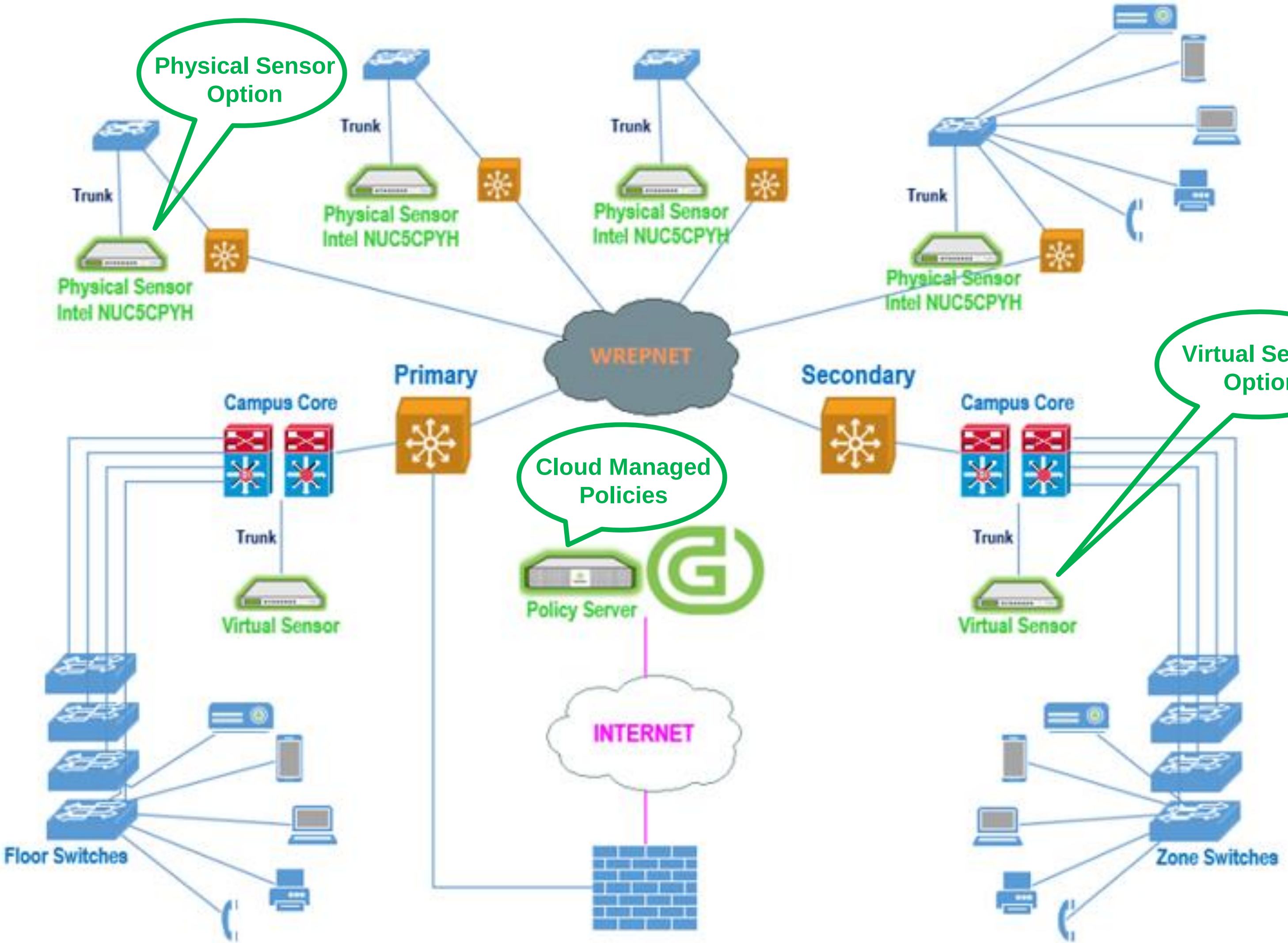
Network Visibility and Control

- Delivered as ISO Image
- Install as a VM or on H/W
- Small Form Factor H/W Supported (Intel NUC, Mini PC, Raspberry Pi)
- No Integration Required, Non-Intrusive, Fail-Safe Option

Agent (Optional)

Endpoint Visibility And Control

- Endpoint Visibility, Security Policies and Control
- Collect Hardware, Software and User Information
- 802.1X/WPA2E Auto-Provisioning
- Monitor/Prohibit Ports and Applications, Sensor Option Available



Physical Sensor Option

Cloud Managed Policies

Virtual Sensor Option

Small Form Factor device pre-staged at Central Location

Connect to pre-configured port at branch office

Sensor automatically registers with Cloud Policy Server

All Nodes automatically detected and policies enforced

Zero Trust Model – What is It?

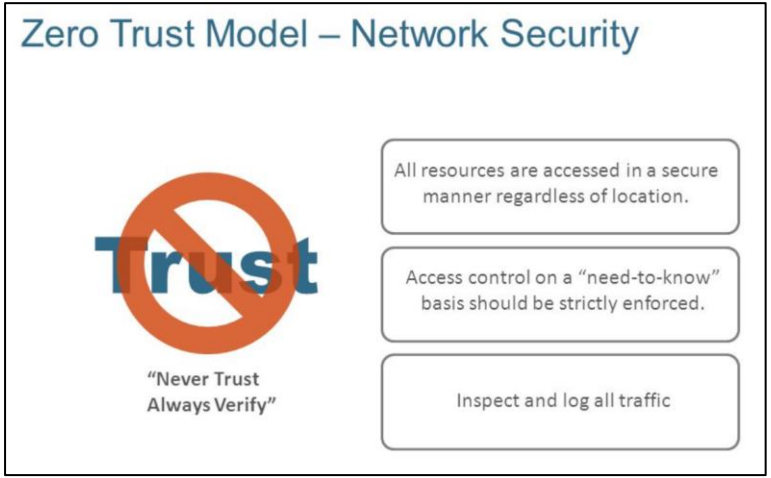
At the most basic level, Zero Trust means exactly what it sounds like, plus a little more. Don’t trust anything/anyone and even when you do, allow as little access as possible. Also, be sure you monitor and adapt if needed.

ZERO TRUST PRINCIPLES

Require secure and authenticated access to all resources

Adopt a least privilege model and enforce access control

Inspect and log all activities using data security analytics



Zero Trust Model – Network Security

“Never Trust Always Verify”

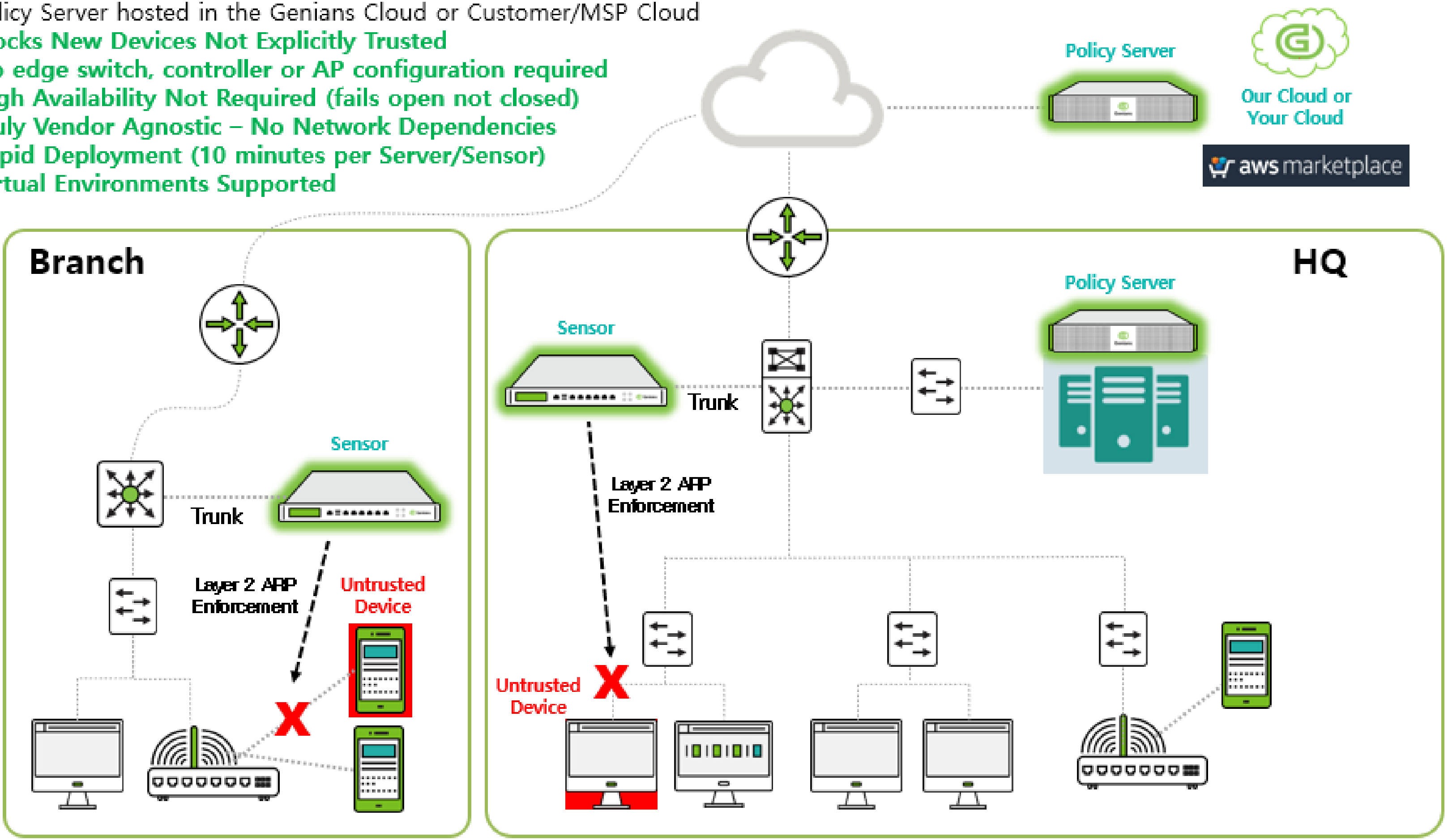
All resources are accessed in a secure manner regardless of location.

Access control on a “need-to-know” basis should be strictly enforced.

Inspect and log all traffic

Genian NAC ARP Enforcement For Zero Trust

- Policy Server hosted in the Genians Cloud or Customer/MSP Cloud
- Blocks New Devices Not Explicitly Trusted
- No edge switch, controller or AP configuration required
- High Availability Not Required (fails open not closed)
- Truly Vendor Agnostic – No Network Dependencies
- Rapid Deployment (10 minutes per Server/Sensor)
- Virtual Environments Supported

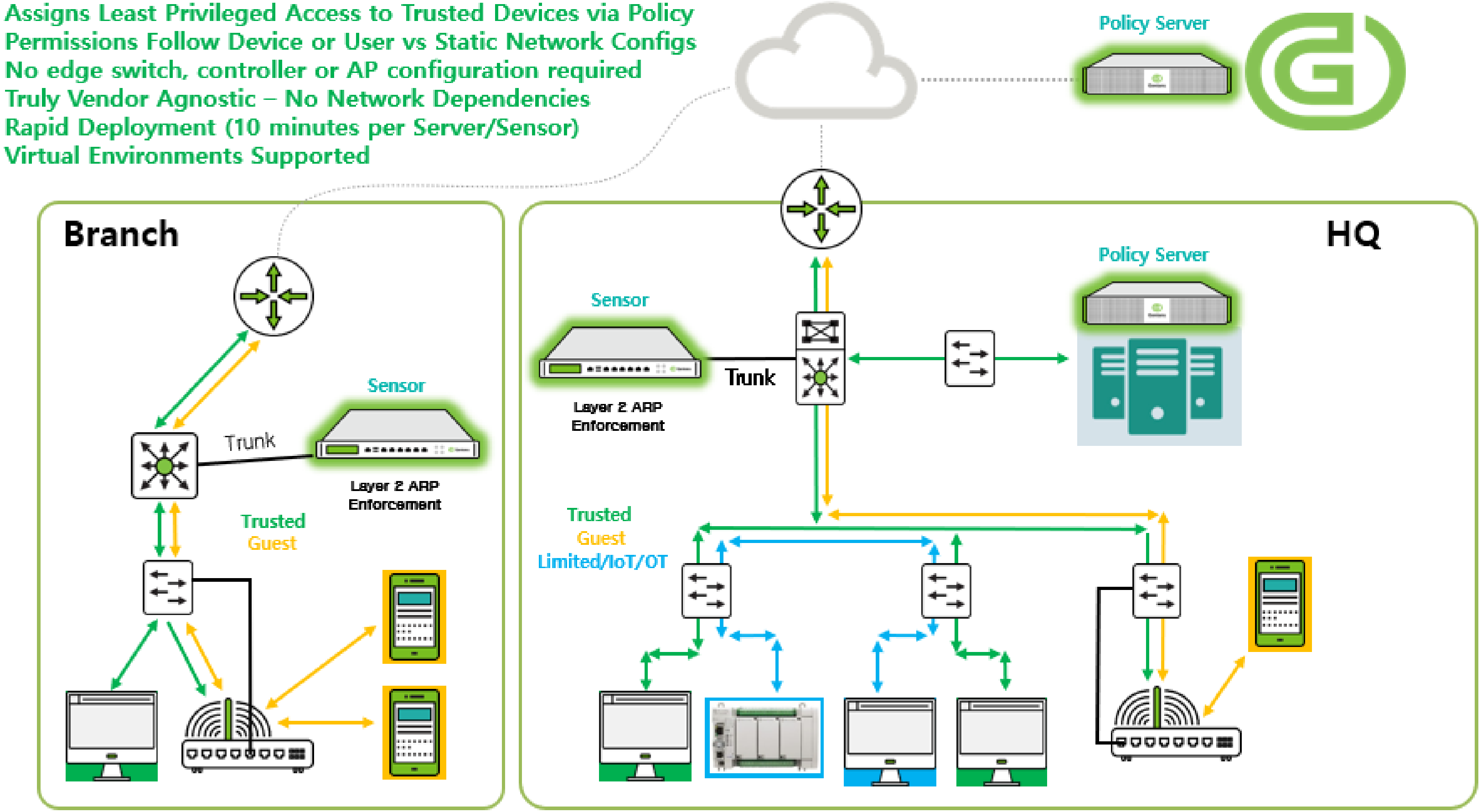


Segmentation with Genian NAC

- ❑ Identify Devices with Device Platform Intelligence
- ❑ Create Security Tags and Permissions
- ❑ Configure Node Groups based on Conditions
- ❑ Assign Least Privileges Required via Enforcement Policy
- ❑ Permissions Follow Node, Not Tied to Network Configuration

Genians ARP Enforcement For Segmentation

- Policy Server hosted in customer Data Center or Genians Cloud
- Assigns Least Privileged Access to Trusted Devices via Policy
- Permissions Follow Device or User vs Static Network Configs
- No edge switch, controller or AP configuration required
- Truly Vendor Agnostic – No Network Dependencies
- Rapid Deployment (10 minutes per Server/Sensor)
- Virtual Environments Supported



Logical Segmentation in Minutes

Step 1

Define Node Tags

Step 2

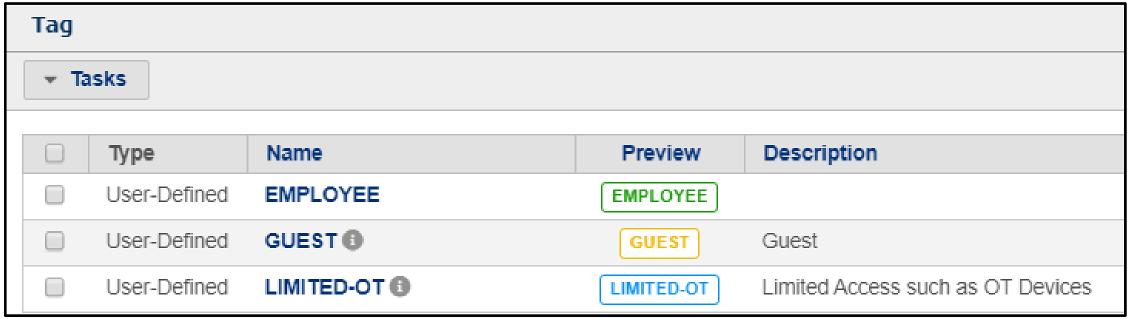
Define Node Groups

Step 3

Create Policies and Permissions

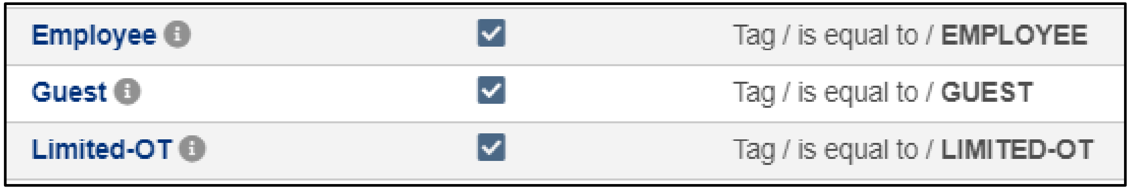
Step 4

Test and Validate

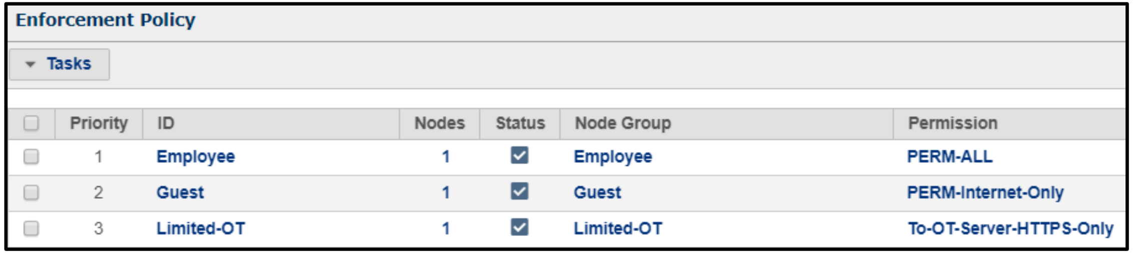


Tag

□	Type	Name	Preview	Description
□	User-Defined	EMPLOYEE	EMPLOYEE	
□	User-Defined	GUEST ℹ	GUEST	Guest
□	User-Defined	LIMITED-OT ℹ	LIMITED-OT	Limited Access such as OT Devices

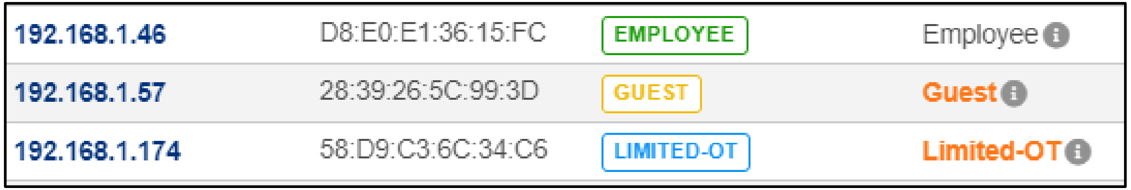


Employee ℹ	☑	Tag / is equal to / **EMPLOYEE**
Guest ℹ	☑	Tag / is equal to / **GUEST**
Limited-OT ℹ	☑	Tag / is equal to / **LIMITED-OT**

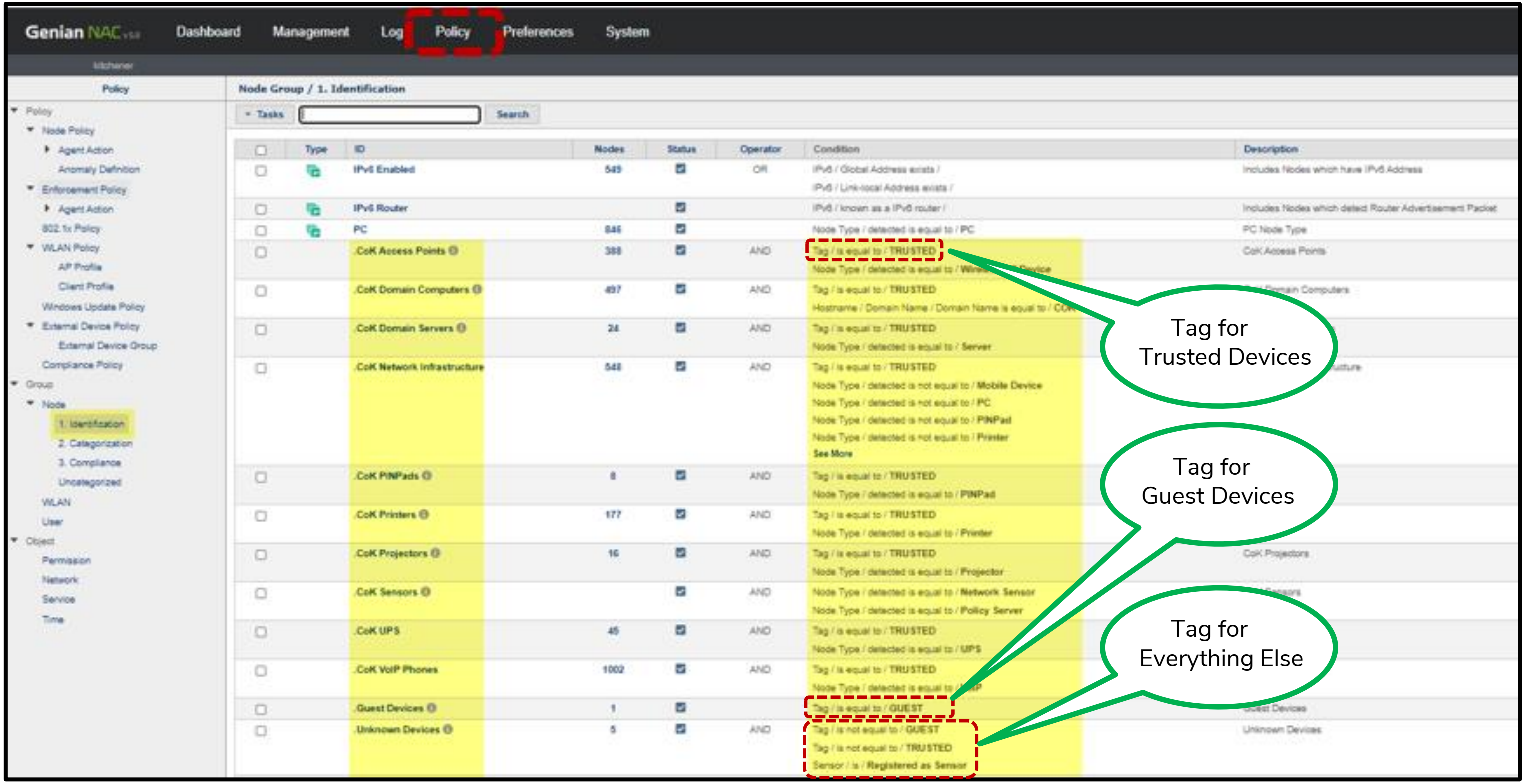


Enforcement Policy

□	Priority	ID	Nodes	Status	Node Group	Permission
□	1	Employee	1	☑	Employee	PERM-ALL
□	2	Guest	1	☑	Guest	PERM-Internet-Only
□	3	Limited-OT	1	☑	Limited-OT	To-OT-Server-HTTPS-Only



192.168.1.46	D8:E0:E1:36:15:FC	EMPLOYEE	Employee ℹ
192.168.1.57	28:39:26:5C:99:3D	GUEST	Guest ℹ
192.168.1.174	58:D9:C3:6C:34:C6	LIMITED-OT	Limited-OT ℹ



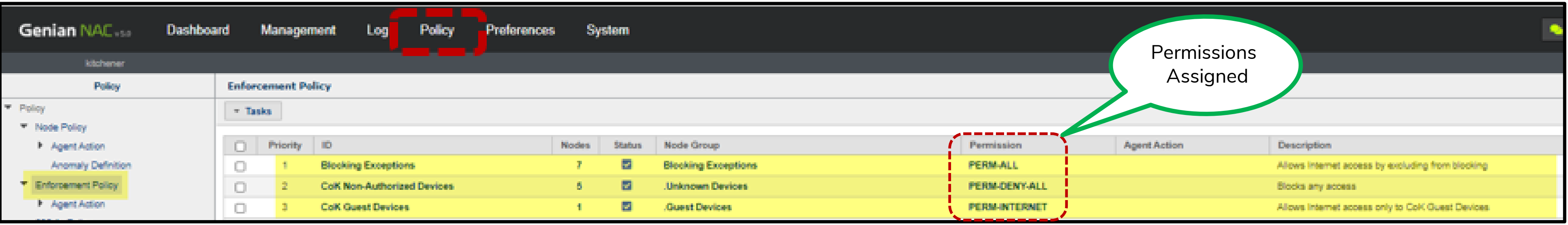
Node Group / 1. Identification

☐	Type	ID	Nodes	Status	Operator	Condition	Description
☐		IPv6 Enabled	549	☑	OR	IPv6 / Global Address exists / IPv6 / Link-local Address exists /	Includes Nodes which have IPv6 Address
☐		IPv6 Router		☑		IPv6 / known as a IPv6 router /	Includes Nodes which detect Router Advertisement Packet
☐		PC	846	☑		Node Type / detected is equal to / PC	PC Node Type
☐		.CoK Access Points	388	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / Wire… Device	CoK Access Points
☐		.CoK Domain Computers	497	☑	AND	Tag / is equal to / TRUSTED Hostname / Domain Name / Domain Name is equal to / COK	…main Computers
☐		.CoK Domain Servers	24	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / Server	
☐		.CoK Network Infrastructure	548	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is not equal to / Mobile Device Node Type / detected is not equal to / PC Node Type / detected is not equal to / PINPad Node Type / detected is not equal to / Printer See More	…ucture
☐		.CoK PINPads	8	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / PINPad	
☐		.CoK Printers	177	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / Printer	
☐		.CoK Projectors	16	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / Projector	CoK Projectors
☐		.CoK Sensors		☑	AND	Node Type / detected is equal to / Network Sensor Node Type / detected is equal to / Policy Server	…Sensors
☐		.CoK UPS	45	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / UPS	
☐		.CoK VoIP Phones	1002	☑	AND	Tag / is equal to / TRUSTED Node Type / detected is equal to / …P	
☐		.Guest Devices	1	☑		Tag / is equal to / GUEST	…uest Devices
☐		.Unknown Devices	5	☑	AND	Tag / is not equal to / GUEST Tag / is not equal to / TRUSTED Sensor / is / Registered as Sensor	Unknown Devices

Tag for Trusted Devices

Tag for Guest Devices

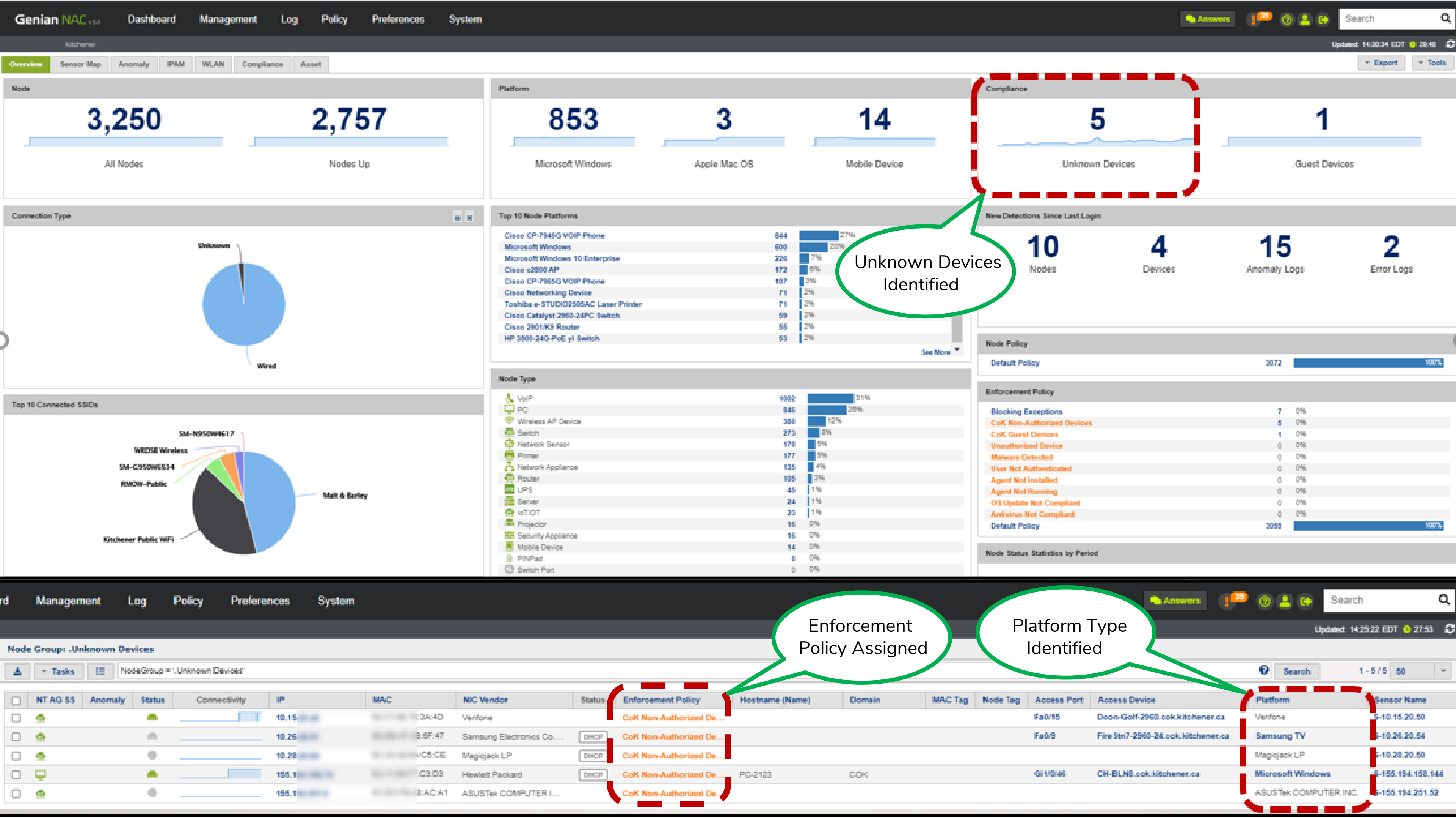
Tag for Everything Else



Enforcement Policy

☐	Priority	ID	Nodes	Status	Node Group	Permission	Agent Action	Description
☐	1	Blocking Exceptions	7	☑	Blocking Exceptions	PERM-ALL		Allows Internet access by excluding from blocking
☐	2	CoK Non-Authorized Devices	5	☑	.Unknown Devices	PERM-DENY-ALL		Blocks any access
☐	3	CoK Guest Devices	1	☑	.Guest Devices	PERM-INTERNET		Allows Internet access only to CoK Guest Devices

Permissions Assigned



Node

3,250	2,757
All Nodes	Nodes Up

Platform

853	3	14
Microsoft Windows	Apple Mac OS	Mobile Device

Compliance

5	1
Unknown Devices	Guest Devices

Unknown Devices Identified

Connection Type

Top 10 Connected SSIDs

Top 10 Node Platforms

Cisco CP-7945G VOIP Phone	844	27%
Microsoft Windows	600	20%
Microsoft Windows 10 Enterprise	226	7%
Cisco c2800 AP	172	6%
Cisco CP-7965G VOIP Phone	107	3%
Cisco Networking Device	71	2%
Toshiba e-STUDIO2505AC Laser Printer	71	2%
Cisco Catalyst 2960-24PC Switch	59	2%
Cisco 2901/K9 Router	55	2%
HP 3500-24G-PoE yl Switch	53	2%

Node Type

VoIP	1002	31%
PC	846	26%
Wireless AP Device	388	12%
Switch	273	8%
Network Sensor	178	5%
Printer	177	5%
Network Appliance	135	4%
Router	105	3%
UPS	45	1%
Server	24	1%
IoT/OT	23	1%
Projector	16	0%
Security Appliance	16	0%
Mobile Device	14	0%
PINPad	8	0%
Switch Port	0	0%

New Detections Since Last Login

10	4	15	2
Nodes	Devices	Anomaly Logs	Error Logs

Node Policy

Default Policy	3072	100%

Enforcement Policy

Blocking Exceptions	7	0%
CoK Non-Authorized Devices	5	0%
CoK Guest Devices	1	0%
Unauthorized Device	0	0%
Malware Detected	0	0%
User Not Authenticated	0	0%
Agent Not Installed	0	0%
Agent Not Running	0	0%
OS Update Not Compliant	0	0%
Antivirus Not Compliant	0	0%
Default Policy	3059	100%

Node Status Statistics by Period

Enforcement Policy Assigned

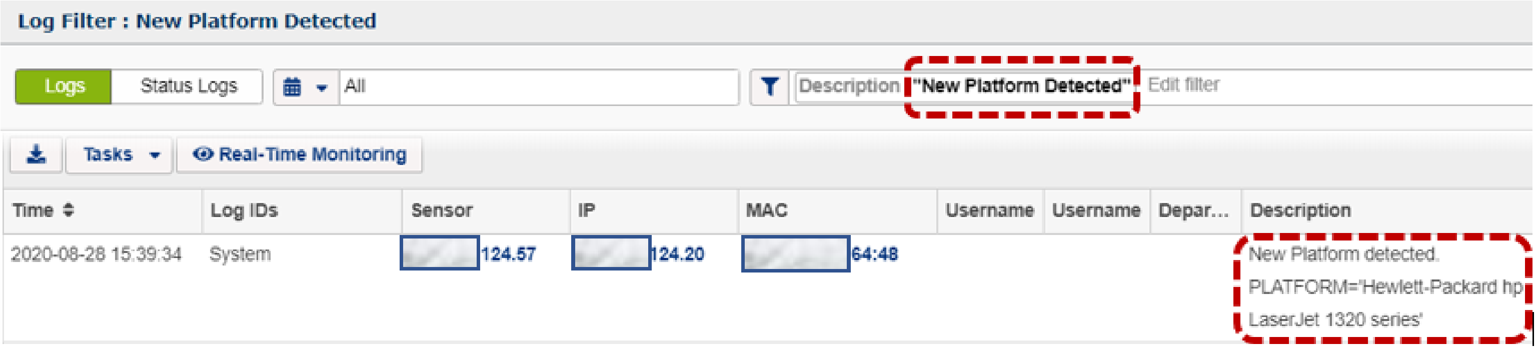
Platform Type Identified

Node Group: .Unknown Devices

NodeGroup = '.Unknown Devices'

□	NT AG SS	Anomaly	Status	Connectivity	IP	MAC	NIC Vendor	Status	Enforcement Policy	Hostname (Name)	Domain	MAC Tag	Node Tag	Access Port	Access Device	Platform	Sensor Name
□					10.15[redacted]	[redacted]:3A:4D	Verifone		CoK Non-Authorized De...					Fa0/15	Doon-Golf-2960.cok.kitchener.ca	Verifone	S-10.15.20.50
□					10.26[redacted]	[redacted]B:6F:47	Samsung Electronics Co....	DHCP	CoK Non-Authorized De...					Fa0/9	Fire Stn7-2960-24.cok.kitchener.ca	Samsung TV	S-10.26.20.54
□					10.28[redacted]	[redacted]:C5:CE	Magicjack LP	DHCP	CoK Non-Authorized De...							Magicjack LP	S-10.28.20.50
□					155.1[redacted]	[redacted]:C3:D3	Hewlett Packard	DHCP	CoK Non-Authorized De...	PC-2123	COK			Gi1/0/46	CH-BLN8.cok.kitchener.ca	Microsoft Windows	S-155.194.158.144
□					155.1[redacted]	[redacted]:AC:A1	ASUSTek COMPUTER I...		CoK Non-Authorized De...							ASUSTek COMPUTER INC.	S-155.194.251.52

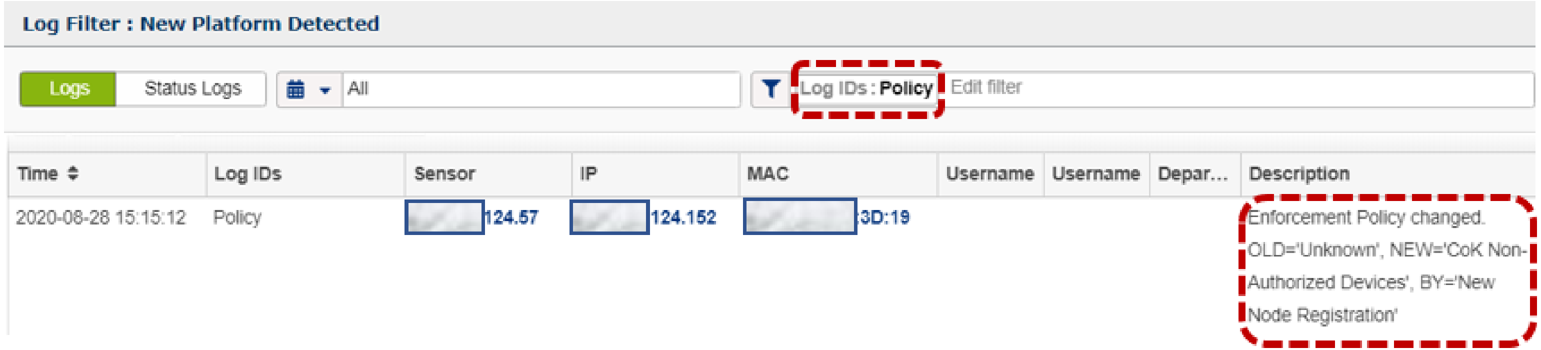
Monitoring - Logs



Log Filter : New Platform Detected

Description "New Platform Detected"

Time	Log IDs	Sensor	IP	MAC	Username	Username	Depar...	Description
2020-08-28 15:39:34	System	[redacted]124.57	[redacted]124.20	[redacted]64:48				New Platform detected. PLATFORM='Hewlett-Packard hp LaserJet 1320 series'

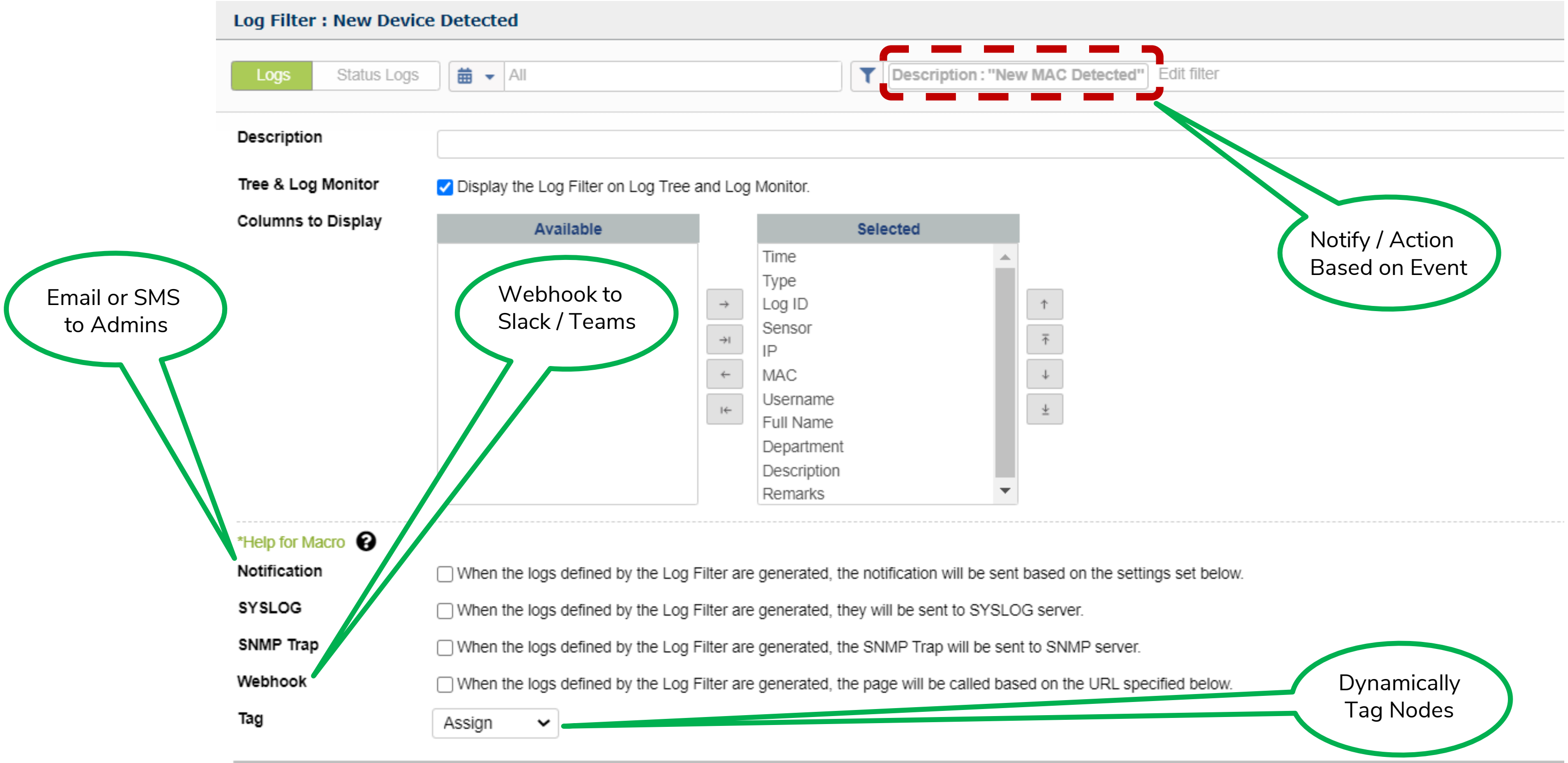


Log Filter : New Platform Detected

Log IDs : Policy

Time	Log IDs	Sensor	IP	MAC	Username	Username	Depar...	Description
2020-08-28 15:15:12	Policy	[redacted]124.57	[redacted]124.152	[redacted]3D:19				Enforcement Policy changed. OLD='Unknown', NEW='CoK Non-Authorized Devices', BY='New Node Registration'

Monitoring – Notifications / Actions



Log Filter : New Device Detected

Description

Tree & Log Monitor: ☑ Display the Log Filter on Log Tree and Log Monitor.

Columns to Display

Available	Selected
	Time Type Log ID Sensor IP MAC Username Full Name Department Description Remarks

*Help for Macro

Notification: □ When the logs defined by the Log Filter are generated, the notification will be sent based on the settings set below.

SYSLOG: □ When the logs defined by the Log Filter are generated, they will be sent to SYSLOG server.

SNMP Trap: □ When the logs defined by the Log Filter are generated, the SNMP Trap will be sent to SNMP server.

Webhook: □ When the logs defined by the Log Filter are generated, the page will be called based on the URL specified below.

Tag: Assign

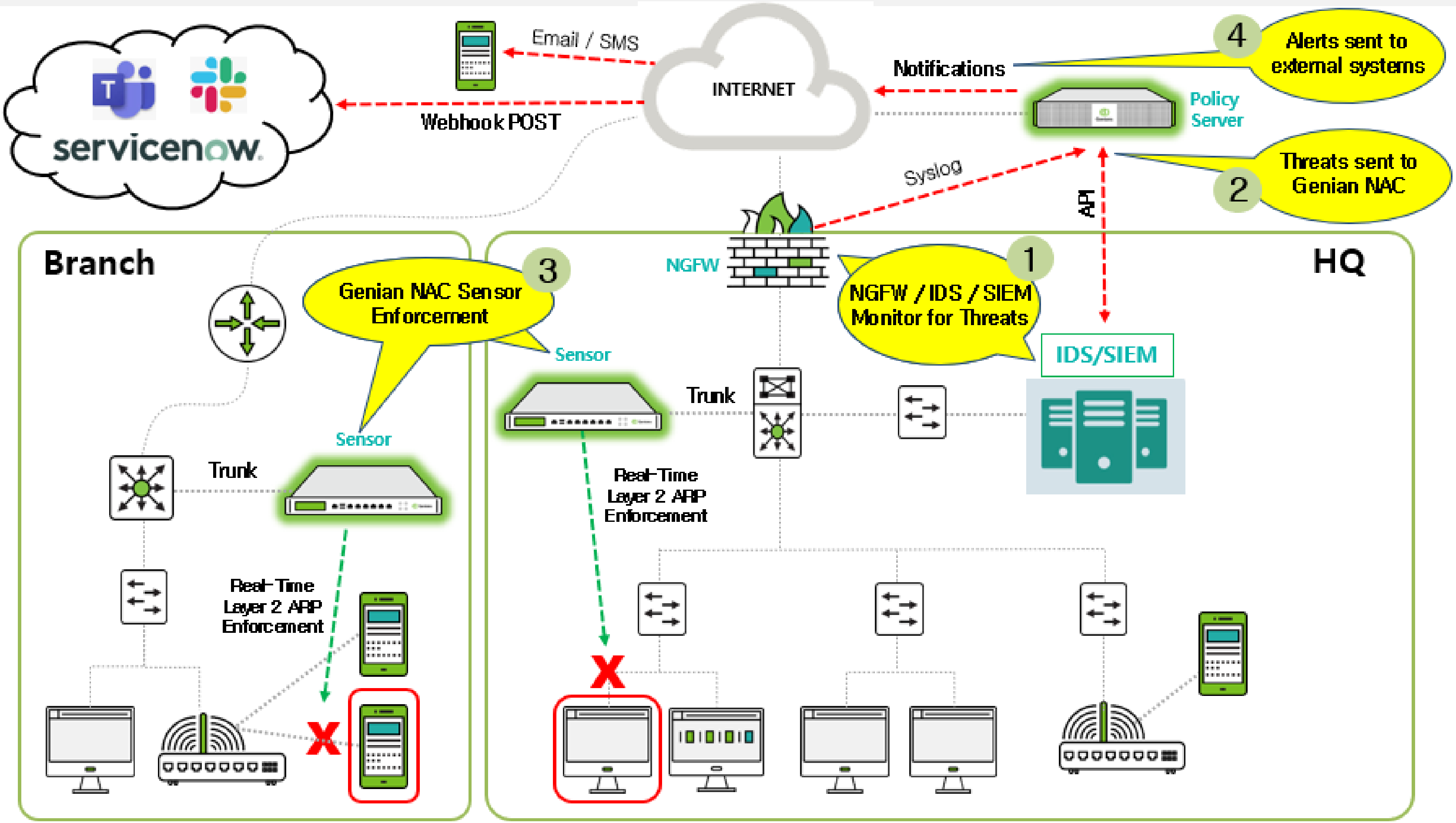
Notify / Action Based on Event

Email or SMS to Admins

Webhook to Slack / Teams

Dynamically Tag Nodes

Genians and IDS/SIEM/NGFW Security Automation



1 NGFW / IDS / SIEM Monitor for Threats

2 Threats sent to Genian NAC

3 Genian NAC Sensor Enforcement

4 Alerts sent to external systems

THANK YOU!

Questions?

petar.lopandic@kitchener.ca

hello@genians.com

Next-Gen Network Access Control

www.genians.com