Genians

# Securing the Edge

# Quickly and Accurately

## Genians Cybersecurity Platform Overview

# Why is Securing The Edge Important for Your Business?

- ❑ The Focal Point Of IT Investments And Business Productivity
- ❑ Critical Data Being Generated Via Various Devices At The Edge
- ❑ Major Cybersecurity Challenges And Lucrative Targets By Hackers
- ❑ Cybersecurity Compliance and Risk Assessments

# 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


Genians Named a Representative Vendor in

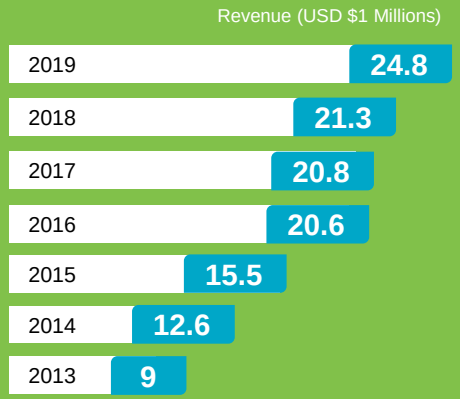
FROST & SULLIVAN

Global NAC Market Forecast to 2024

Gartner

Market Guide for NAC 2018, 2020

# Growing with customers




| Enterprise | Financial | Gov/Military | Infra/Energy | Healthcare | Education |
|---|---|---|---|---|---|
| HYUNDAI | ING LIFE INSURANCE | Ministry of the Interior and Safety | KEPCO KHNP | SAMSUNG Samsung Medical Center | |
| BMW | Prudential | | K water KR | | |
| | MG Community Credit Cooperatives | Supreme Prosecutors' Office Republic of Korea | GS Caltex | | |
| SAMSUNG | BCcard | KCCI Korea Chamber of Commerce and Industry | KNOC | | |
| | Mitsui Sumitomo Insurance | | ex 한국도로공사 | | |
| THAI | Cigna | Ministry of National Defense Republic of Korea | KOGAS | | |
| ebay | | USPK | 5678 SMRT | HEALTH SYSTEMS | |
| LG | MIZUHO Mizuho Financial Group みずほ銀行 | KOREA POST | KORAIL 한국철도공사 | | |

# Common Requirements for Regulatory Compliances

| CIS BASIC Controls | PCI DSS | HIPAA | ISO 27002 | Cloud Security Alliance | NIST | NSA | NERC CIP | PIPEDA |
|---|---|---|---|---|---|---|---|---|
| 1. Inventory and Control of Hardware Assets | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2. Inventory and Control of Software Assets | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3. Continuous Vulnerability Management | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4. Controlled Use of Administrative Privileges | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 6. Maintenance, Monitoring and Analysis of Audit Logs | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

**By implementing Center for Internet Security (CIS) BASIC Controls, your organization can defeat over 85% of common attacks.**

| Core Cybersecurity Requirements | | Genians Cybersecurity Platform Can |
|---|---|---|
| Inventory and Control of Hardware Assets | 1 | Detect all IP-enabled devices on the network and correlate them to a sepcific platform |
| Inventory and Control of Software Assets | 2 | Inventory installed software and version on all devices |
| Continuous Vulnerability Management | 3 | Provide an integrated CVE Dashboard for all devices on the network and provide real-time quarantine |
| Controlled Use of Administrative Privileges | 4 | Authorize devices/users based on users' roles and responsibilities, providing least privilege access |
| Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers | 5 | Inspect detected devices' configuration and security settings and maintain security baseline |
| Maintenance, Monitoring and Analysis of Audit Logs | 6 | Monitor access and security events, maintain logs for audit trail, send notifications to admins and external systems |

# The Building Blocks for Cybersecurity

## SURVEILLANCE

Find out what is exists and what is happening on your network

Genian Device Platform Intelligence (GDPI)

## CONTROL

Access policy compliance, control network access and assign privileges

Genian NAC and Genians Insights E EDR Real-Time Enforcement

## AUTOMATION

Enable Security Automation by integrating with Cybersecury Ecostystem

Genian REST API for GDPI and NAC

# Genians 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

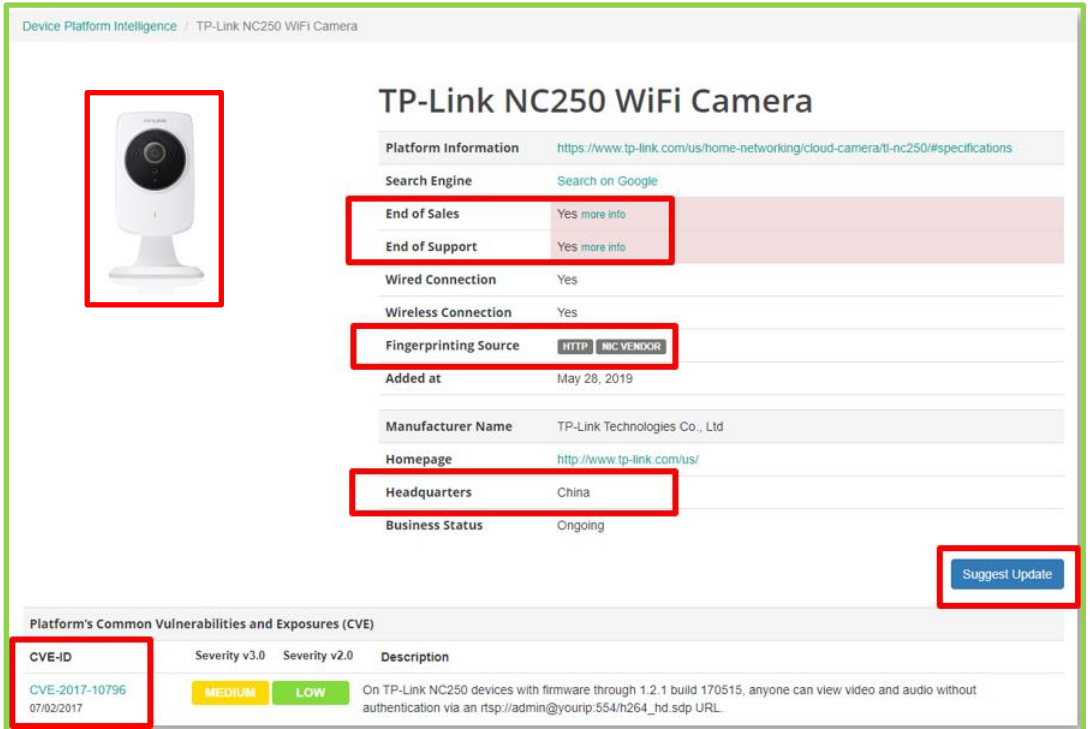
## RISK

Technology Vulnerability

- List of CVEs

Business Vulnerability

- Out of Business
- Acquisitions



# Restrict Access for EOL/EOS Platforms

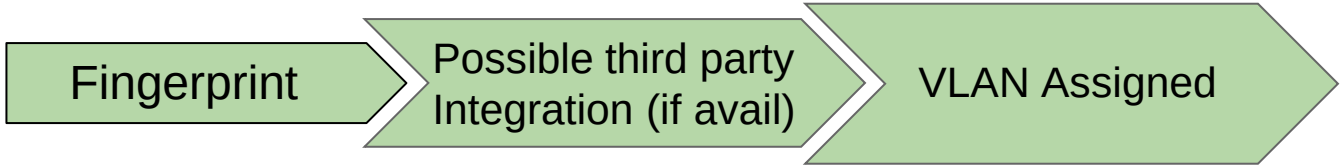
**Step 1**
GDPI Provides End-of-Sale and End-of-Life Information

**Step 2**
EOS/EOL information is tied to specific Platform

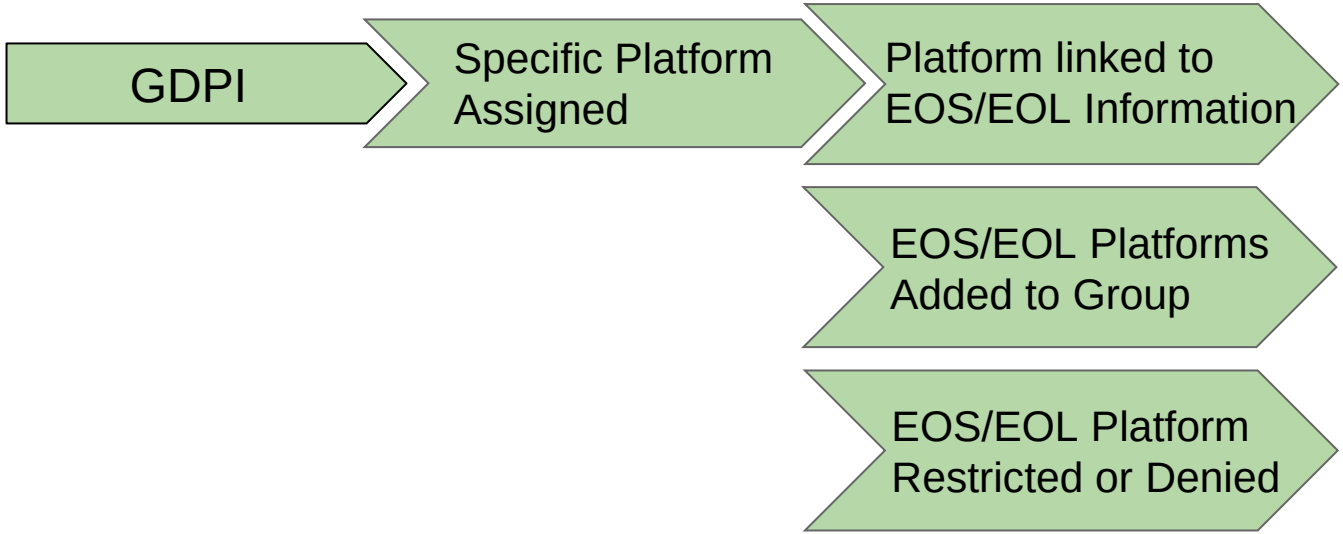
**Step 3**
EOS/EOL Platforms added to Group

**Step 4**
Policy Restricts or Denies network access

## Legacy Fingerprinting Approach




## GDPI with Genian NAC



# Restrict Platforms by Related CVEs

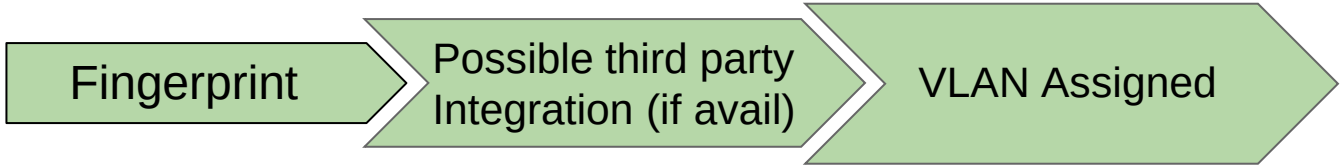
**Step 1**
GDPI Provides CVE Information

**Step 2**
CVE information is tied to specific Platform

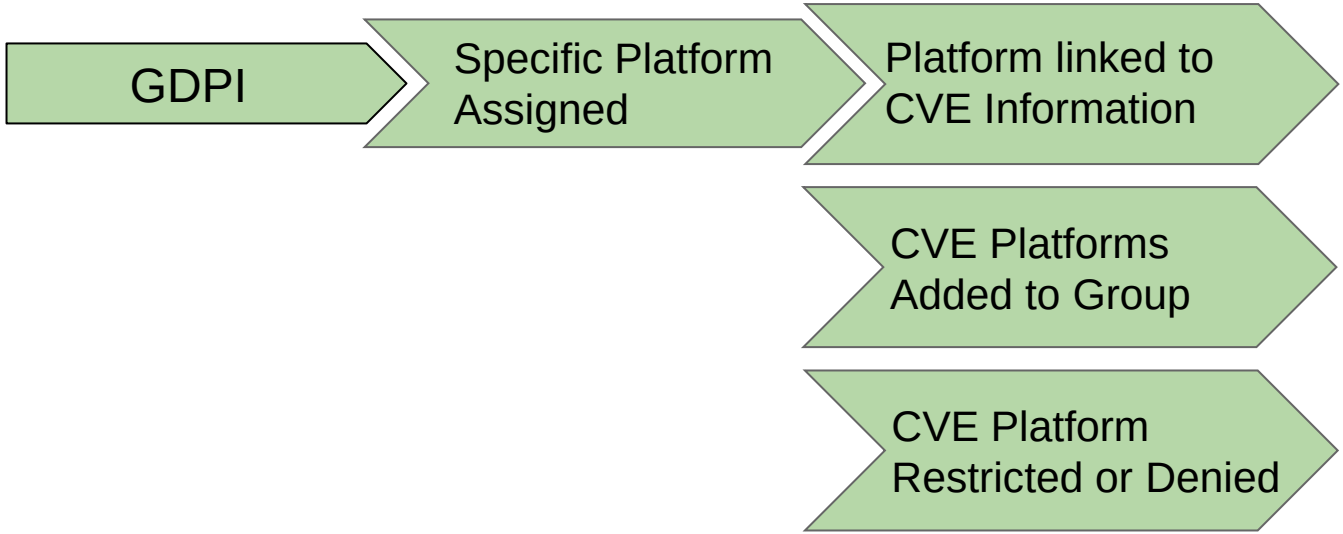
**Step 3**
Platforms with specific CVEs added to Group

**Step 4**
Policy Restricts or Denies network access

## Legacy Fingerprinting Approach




## GDPI with Genian NAC



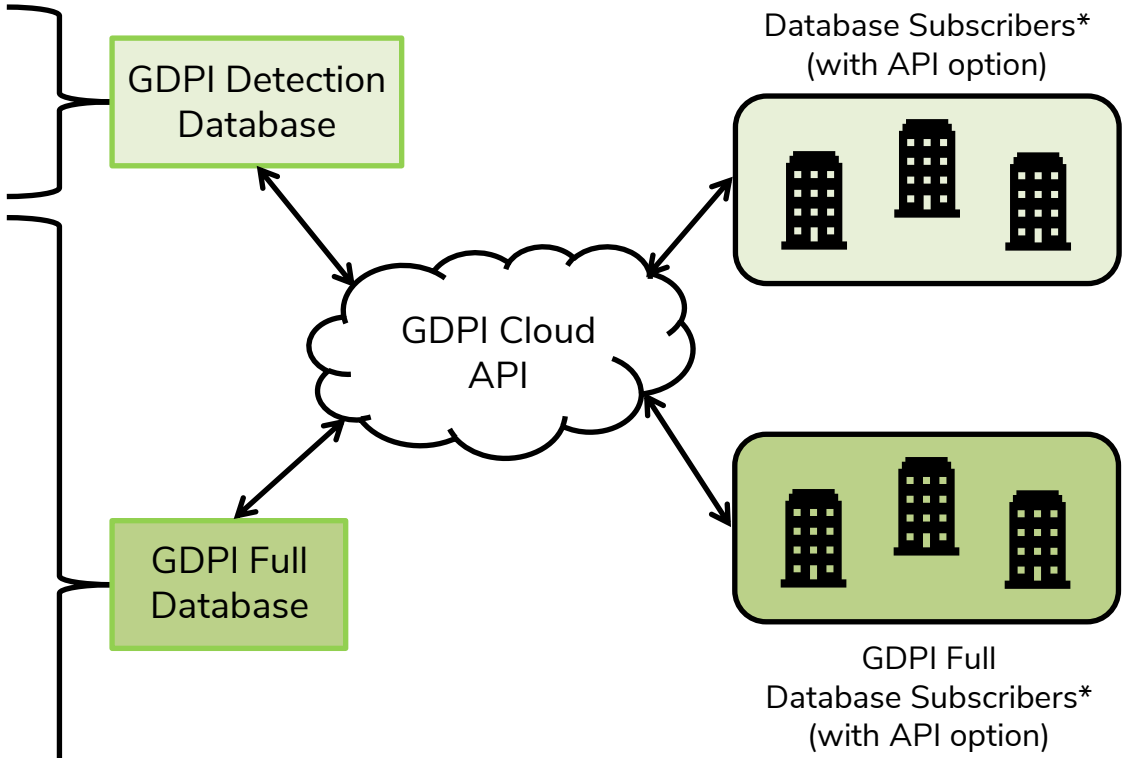
## GDPI

Regex-based Detection Rules (Support 20+ Standard Protocols)

- **Platform***
  - Name, Type
- **Manufacturer***
  - Name

Platform Detection Database plus

- **Platform***:
  - Official Product Information URL
  - Product Image (Large and Small Size)
  - Operating System
  - Connection Type (Wired, Wireless)
  - End-of-Sales (EoS): Date and associated web URL
  - End-of-Life Date(EoL): and associated web URL
  - Common Platform Enumeration (CPE) mapping
  - Common Vulnerabilities and Exposures (CVE) mapping
- **Manufacturer***
  - Name, Logo, Homepage URL, HQ Country
  - Business Status (Ongoing/Closed, Acquisition Company)
  - MAC Address OUI
  - Common Platform Enumeration (CPE) mapping




**Empowering MSPs with GDPI**

**Flexible Subscription Options**
**Co-branding Options**
**White-label Options**

# 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

**Enforcement Policy**

Tasks

| Priority | ID | Nodes | Status | Node Group | Permission | Agent Action |
|---|---|---|---|---|---|---|
| 1 | Blocking Exceptions | 1 | ☑ | Blocking Exceptions | PERM-ALL | |
| 2 | Zoom Users | | ☑ | Zoom Installed | DENY-ALL | Notify Zoom Prohibited macOS.<br>Notify Zoom Prohibited Windows. |
| 3 | Unauthorized Device | 1 | ☑ | IPAM Denied | PERM-DENY | |
| 4 | Threat Detected | | ☑ | Threats Detected | PERM-DENY | |
| 5 | User Not Authenticated | | ☑ | User Not Authenticated | PERM-DENY | |
| 6 | Guests | | ☑ | Guests | PERM-Internet | |
| 7 | Contractors | | ☑ | Contractors | PERM-INTERNET-M/F-8-5 | |
| 8 | Restrict Unauthorized Printers | 2 | ☑ | Unauthorized Printers | PERM-Internet | |
| 9 | Block CVE-2017-10796 devices | 1 | ☑ | CVE-2017-10796 | PERM-ALL | |
| 10 | Identify End-of-Sale/Support Devices | 5 | ☑ | End of Sale or End of Support Devices | PERM-ALL | |
| 11 | Windows 7 End-of-Life | | ☑ | Windows 7 Devices | PERM-DNS | Agent Popup |
| 12 | Devices with Any CVE | | ☑ | Devices with any CVE | PERM-ALL | |
| 13 | Block CVE-2016-2105 devices | 1 | ☑ | CVE-2016-2105 | PERM-DENY | |
| 14 | RADIUS Attribute Assignment Policy Example | | ☑ | VoIP Phones | PERM-ALL | |
| 15 | Agent Not Installed | | ☑ | Agent Not Installed | PERM-DENY | |
| 16 | Agent Not Running | | ☑ | Agent Not Running | PERM-DENY | |
| 17 | Windows Defender Update Needed | | ☑ | Windows Defender Definitions Older than 6 days | PERM-Internet | Network Control via Windows Firewall |
| 18 | Windows Update Not Compliant | | ☑ | Windows Update Policy Not Compliant | PERM-INTERNAL-SVR | |
| 19 | Antivirus Not Compliant | | ☑ | Antivirus Not Running<br>Antivirus Not Installed<br>Antivirus Real-time Scan Not Running<br>Antivirus Outdated | PERM-EXTERNAL-SVR | |
| 20 | VLAN Assignment Based on AD Group | | ☑ | Brett Testing VLAN Assignment | PERM-ALL | |
| 21 | DLP noncompliant | | ☑ | DLP requirement | PERM-Internet | |
| 22 | Default Policy | 49 | ☑ | All Nodes | PERM-ALL | |

# 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

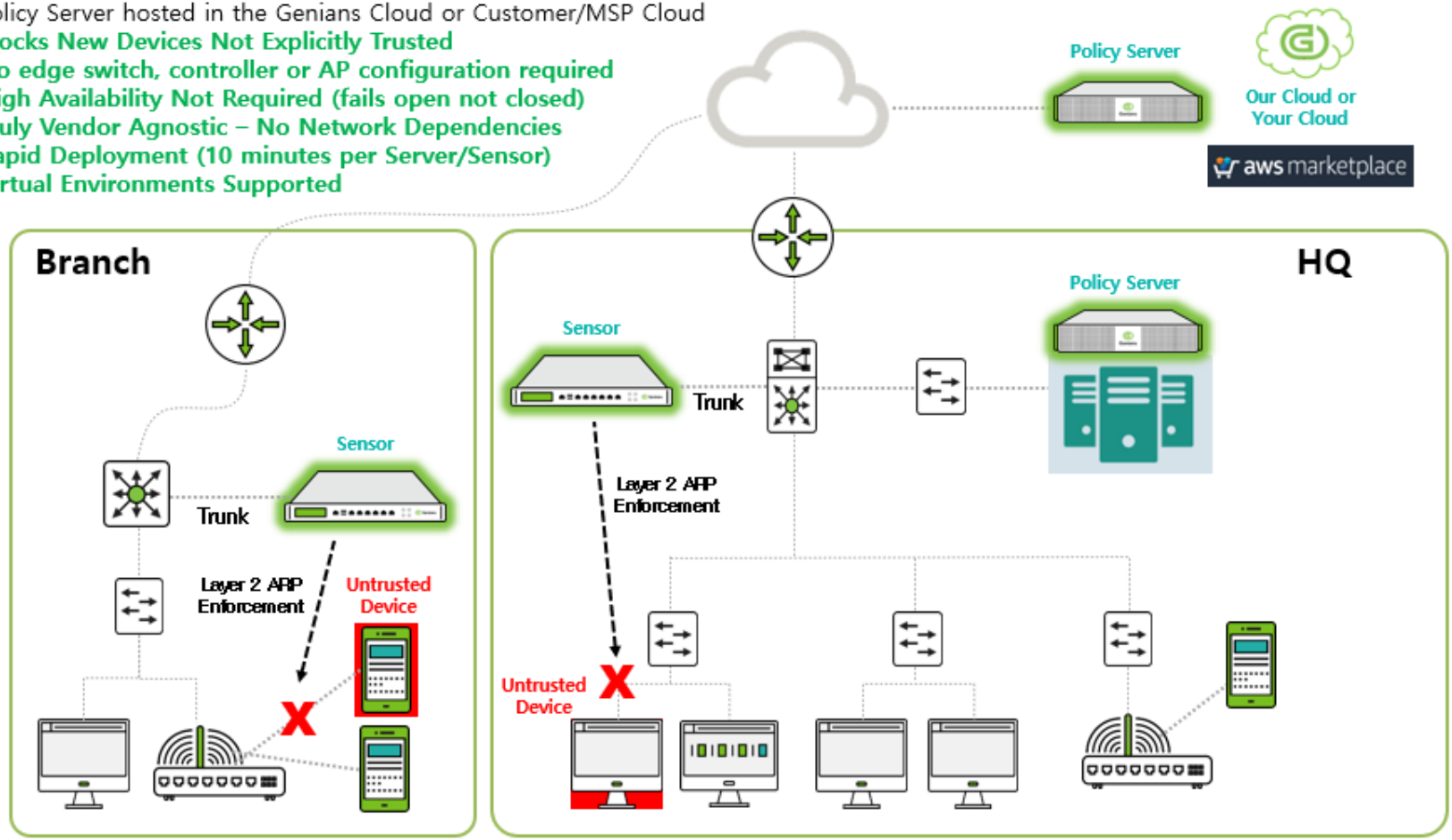
## Agent (Optional)

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

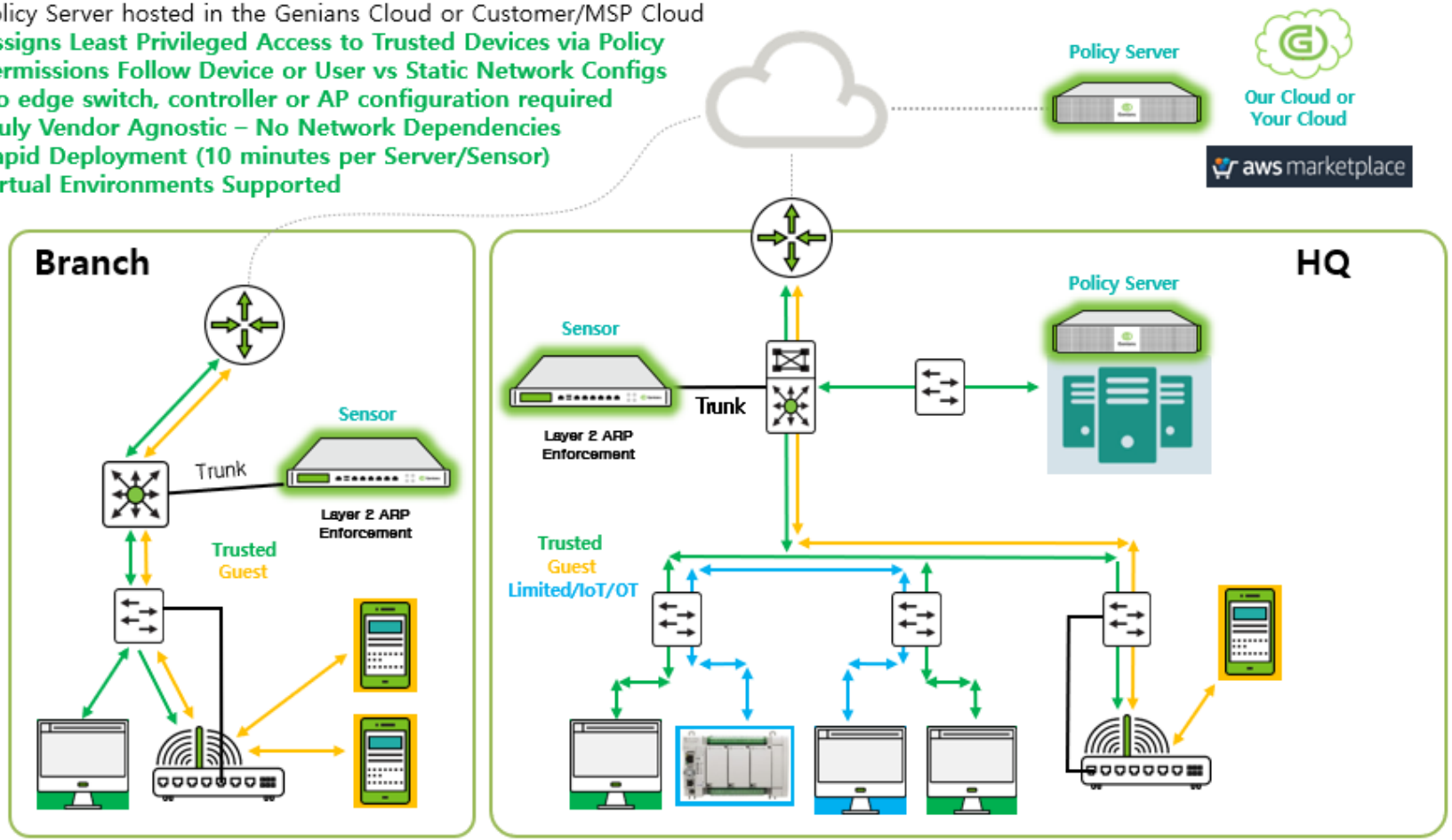
# Genian NAC ARP Enforcement For Zero Trust

- 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**



# Genian NAC ARP Enforcement For Segmentation

- Policy Server hosted in the Genians Cloud or Customer/MSP 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**

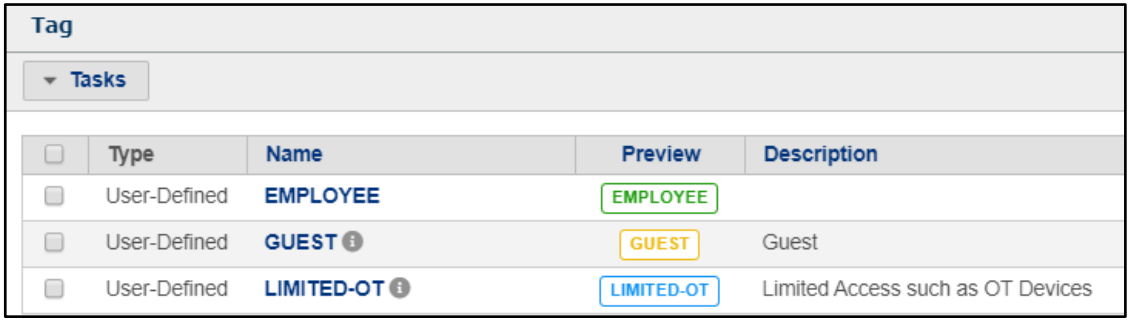
**Define Node Groups**

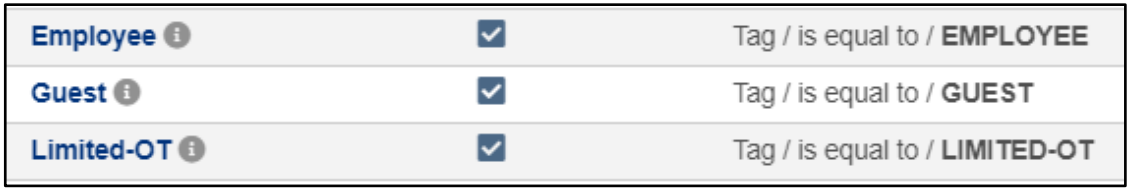
**Step 3**

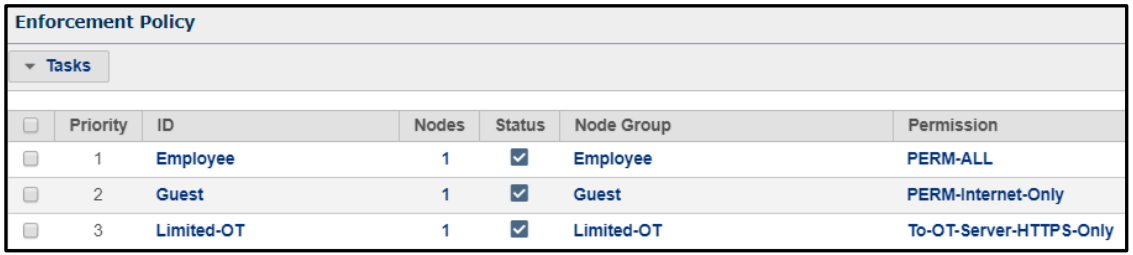
**Create Policies and Permissions**

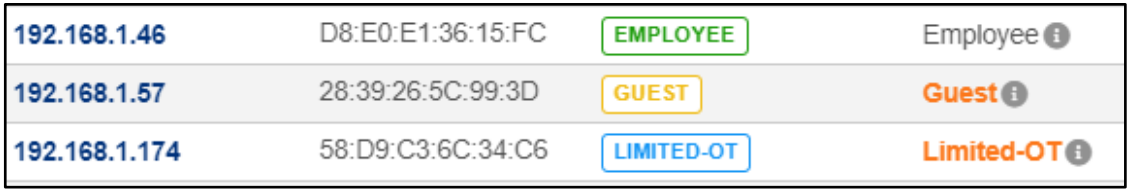
**Step 4**

**Test and Validate**



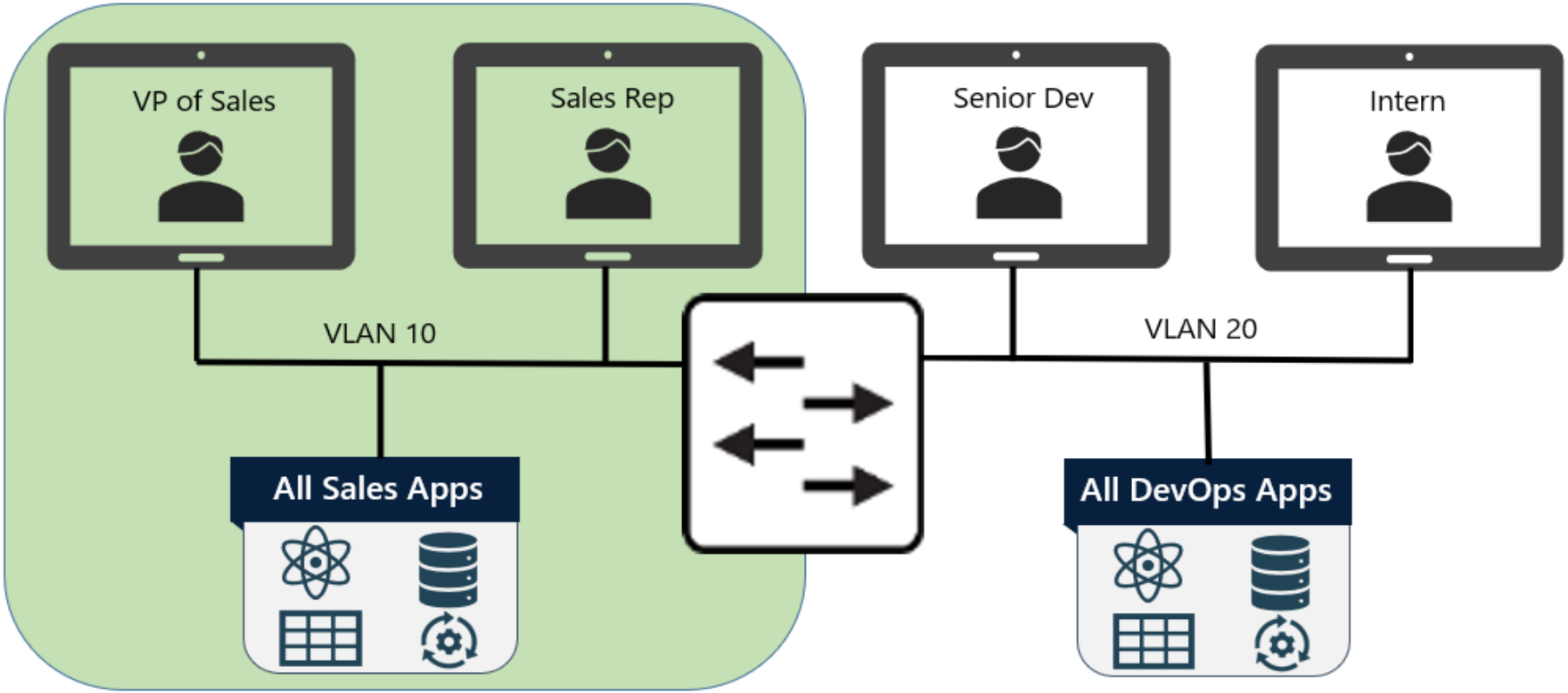



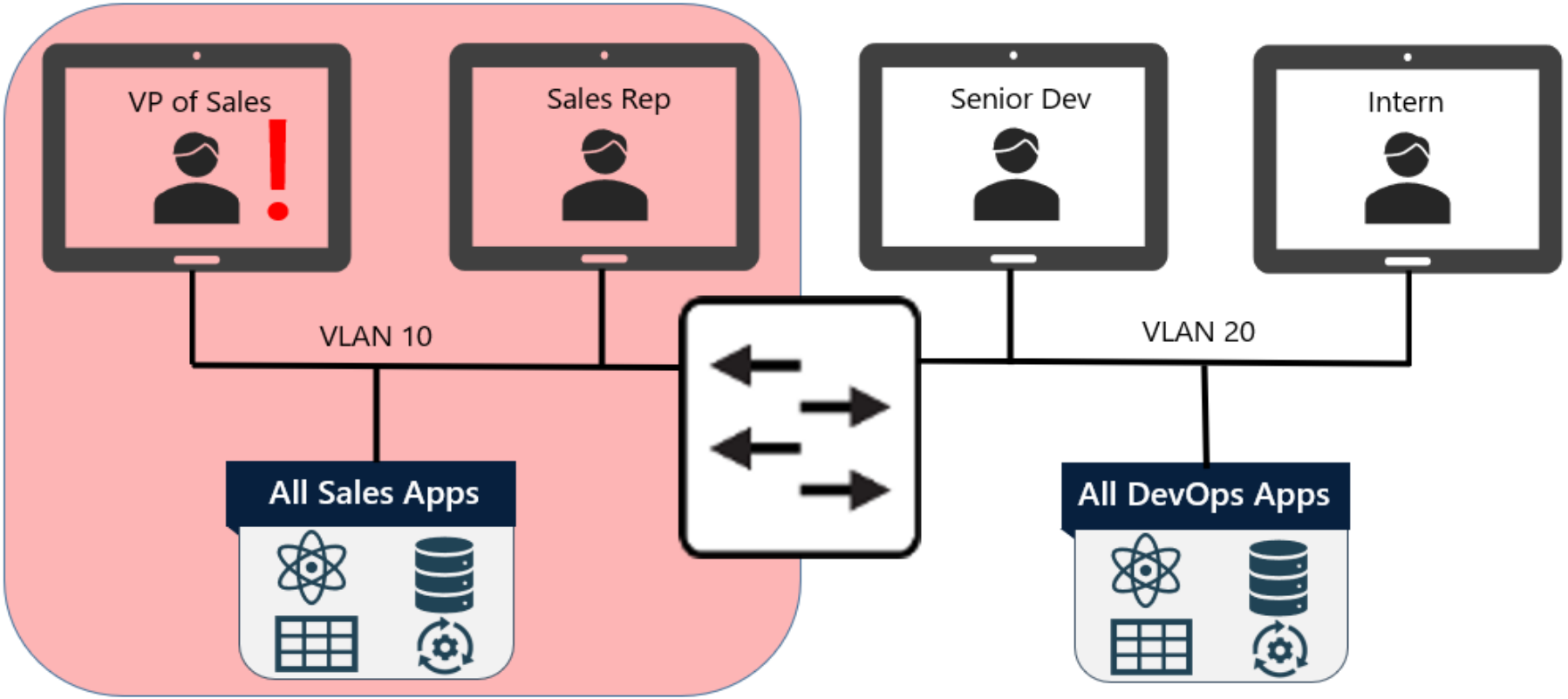
# Legacy Privilege Access

## Static Segregation at Network Level, By Department/Unit



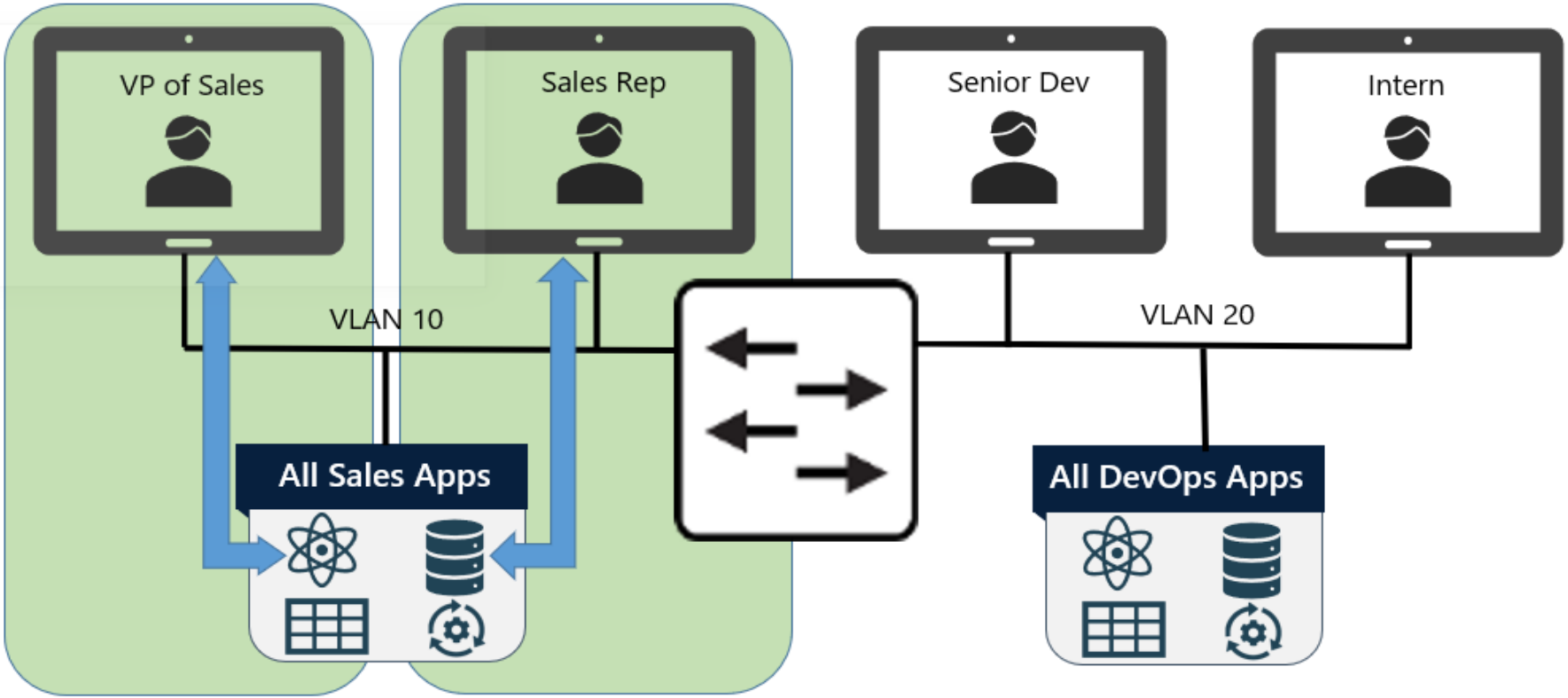
# Legacy Privilege Access – Increased Exposure/Risk

## Potential Attack Surface if Single User/Device is Compromised



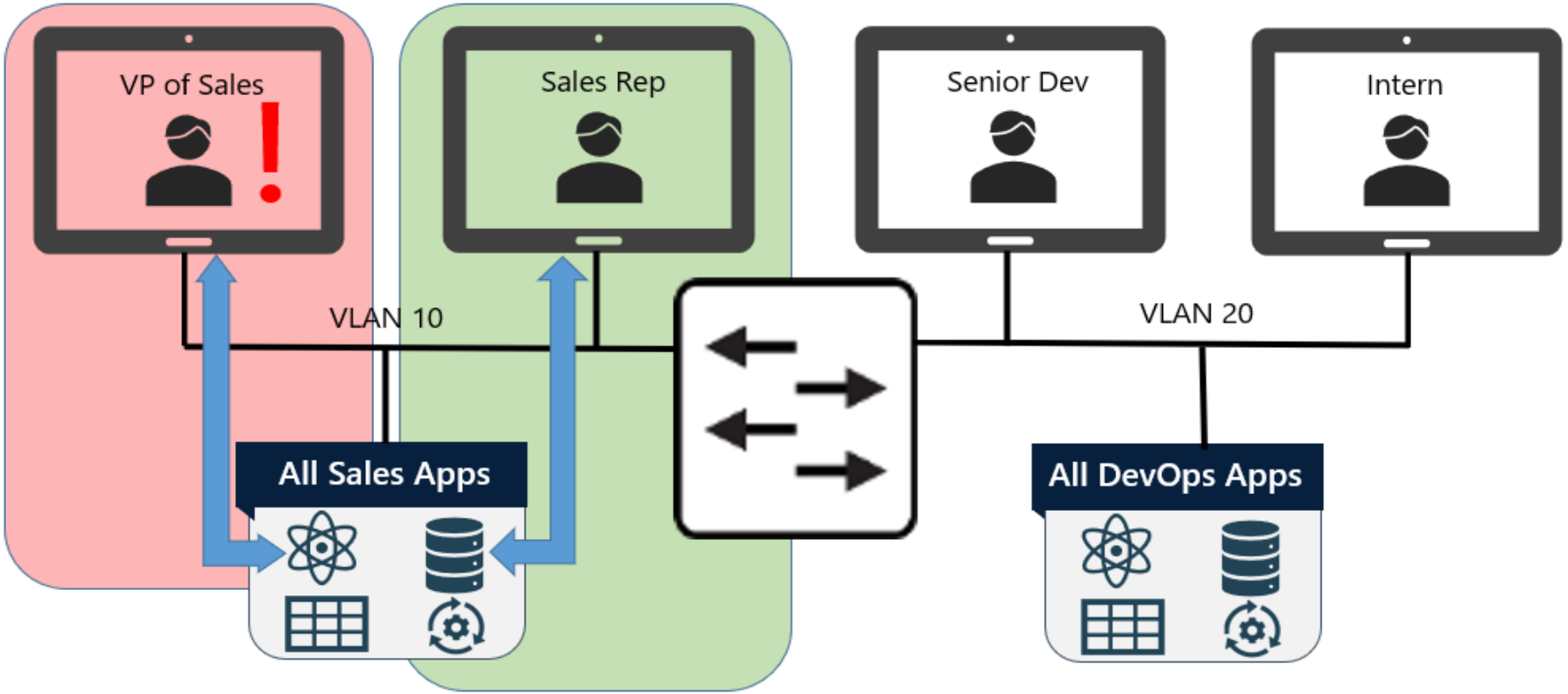
# Least Privilege Access

## Dynamic Segregation by User/Device/Compliance – No Network Dependency

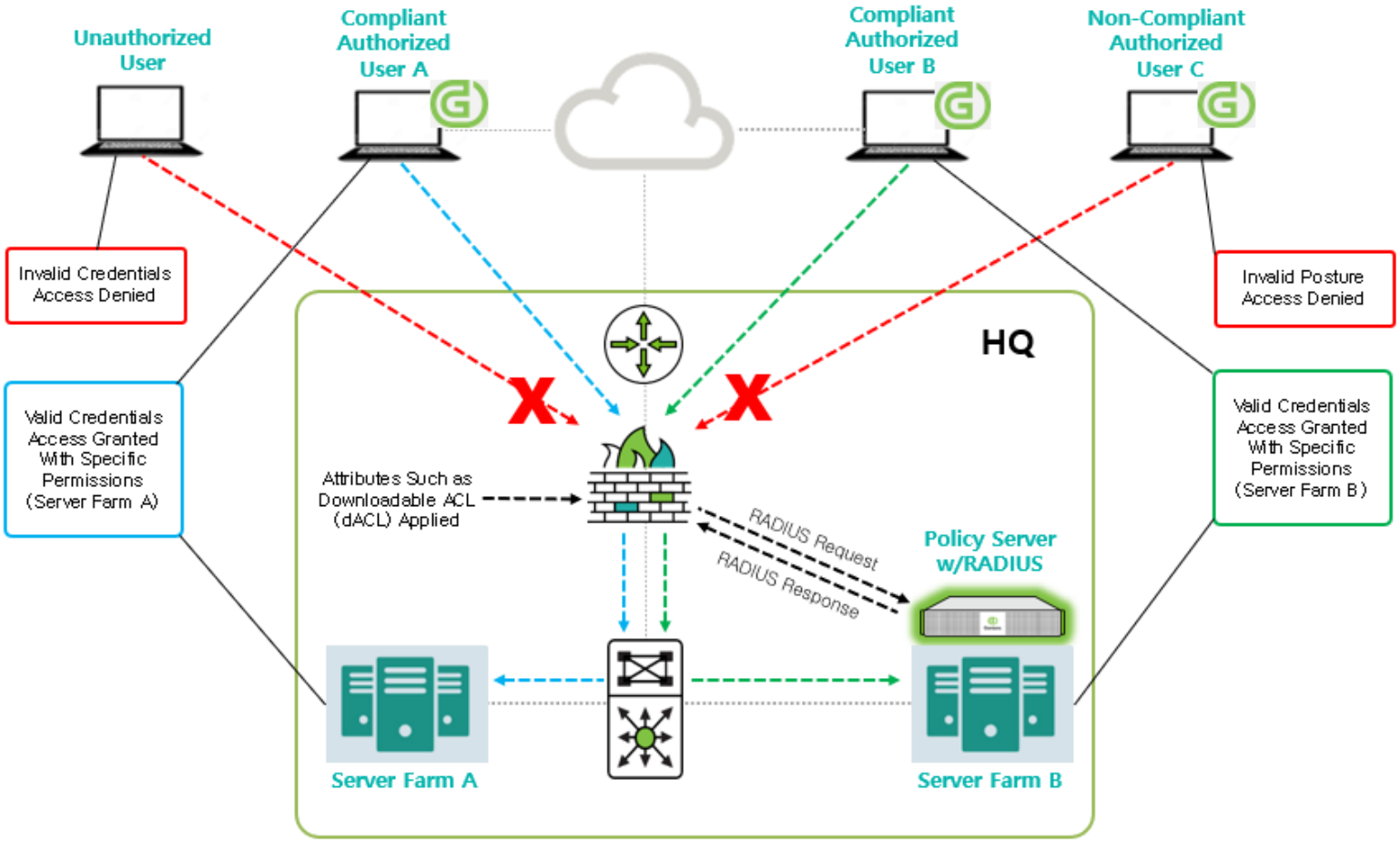


# Least Privilege Access – Reduced Exposure/Risk

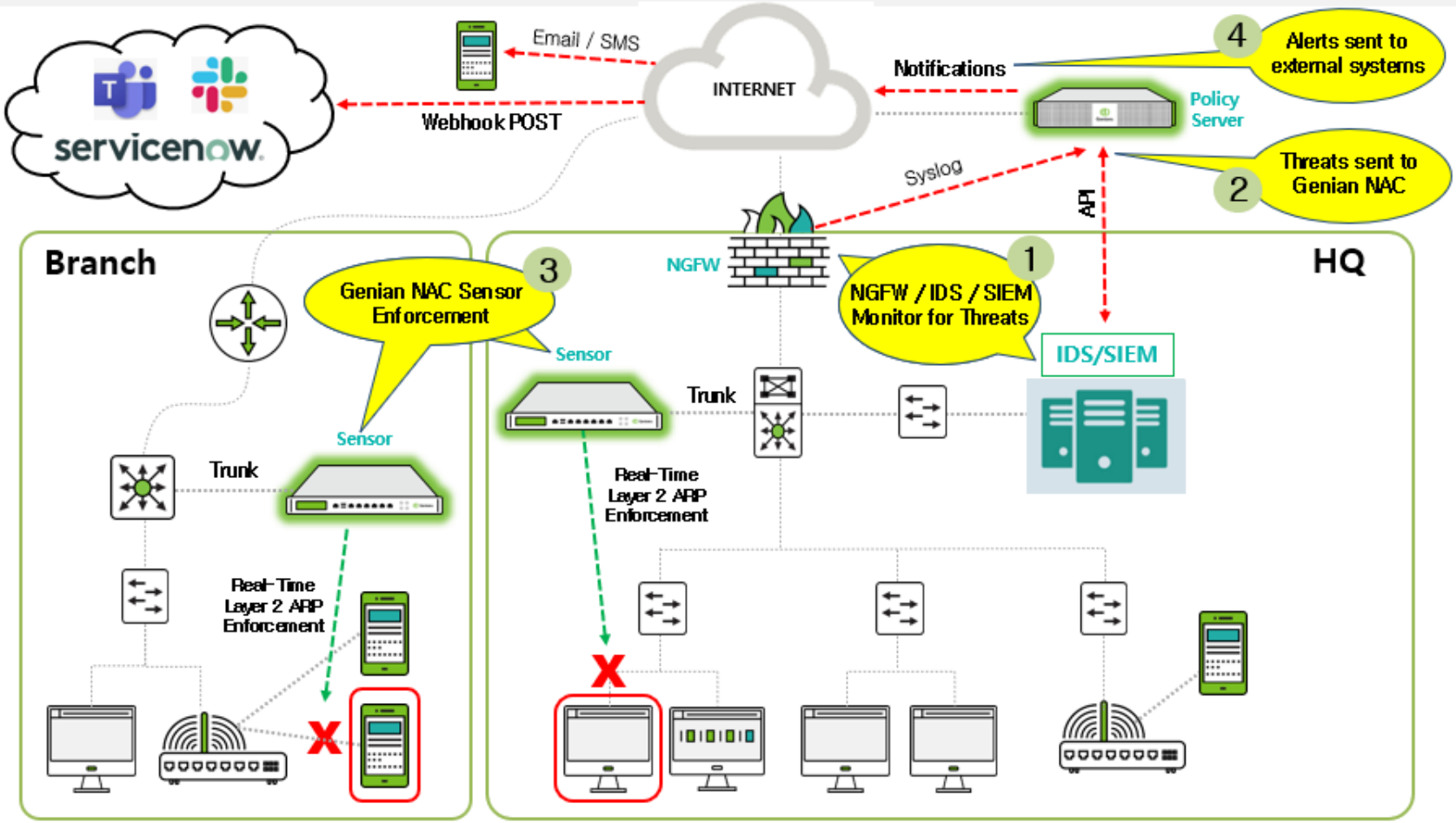
## Potential Attack Surface if Single User/Device is Compromised



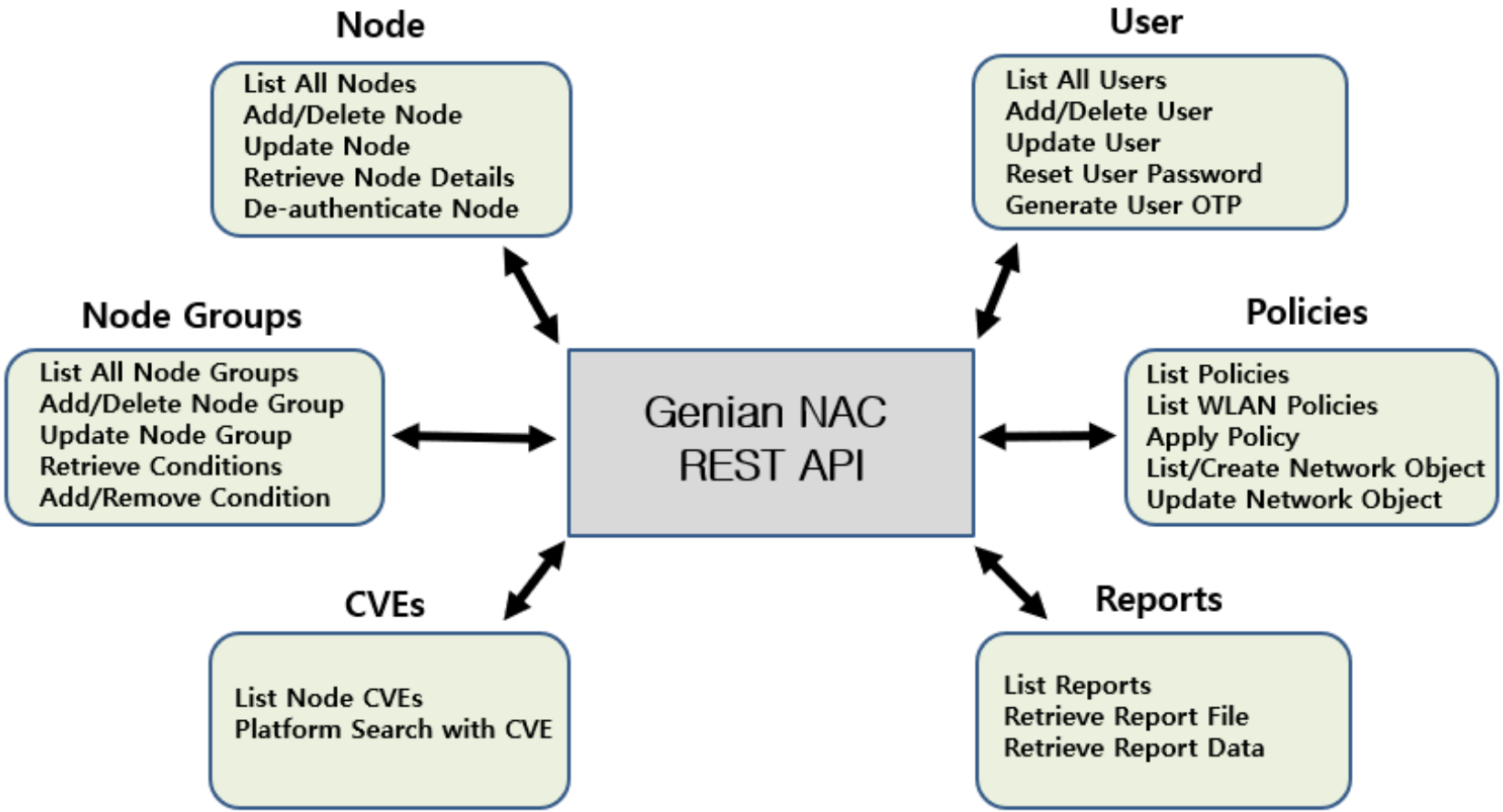
# Genian NAC - Remote Access Enforcement



# Genians and IDS/SIEM/NGFW Security Automation



# Genian NAC REST API Common Use Cases



# Key Features to Secure The Edge

## Critical Features

- ❑ Visibility Of All Ip-enabled Devices Without Disturbing Existing It Operations
- ❑ Contextual Device Platform Intelligence
- ❑ Zero Trust, Segmentation, And Least Privilege Access
- ❑ Abnormal Traffic Detection And Quarantine In Real-time
- ❑ X Behavior Analysis (Xba) To Detect And Mitigate Unknown Threats

## Edge Environment Support

- ❑ Pragmatic Implementation (Visibility, Enforcement, Automation)
- ❑ Contactless Deployment Options
- ❑ Low-complexity And Seamless Integration With 3rd Party Systems
- ❑ Cloud Management In Public, Private, Or Hybrid Environments

Genians Cybersecurity Platform

www.genians.com