Genian NAC

HIGHLIGHTS

Challenges

Today's IT managers and network operators face a daunting challenge: how best to maintain effective network security while simultaneously supporting business productivity. Cybersecurity challenges caused by incomplete network visibility, which fails to identify all devices accessing the network, where they are located, who owns them, and the details of their security posture.

Gartner "Expects to see **20 billion** IoT devices and more than 65% of enterprises adopt IoT by 2020. Unfortunately, most of these devices have little or no protection at the software and infrastructure levels."

CISCO "Companies have up to **70 different security vendors installed** and in their company to solve problems."

ESG "62% of companies are **actively consolidating** their cybersecurity vendors and looking for **enterprise class** providers"

CSO "69% of companies see **compliance** mandates driving **spending**."

Symantec "43 percent of cyber attacks target **small business**."

NATIONAL CYBERSECURITY ALLIANCE "60 percent of small companies go out of business **within six months** of a cyber attack."

Common Requirements For Regulatory Compliances

These 6 core requirements are designed to ensure comprehensive network and endpoint visibility and to maintain full, ongoing intelligence of all connected devices' activities.

REQUIREMENTS	PCI	HIPAA	ISO 27002	CSA	NIST	NSA	NERC CIP	SAUDI AMS
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	•	•	•	•	•	•	•	•

Genian NAC supports practical security compliance by providing real-time network surveillance for all the assets in your network and ensures that are all compliant with your IT security policies. Without disturbing existing IT infrastructure or impacting systems availability, Genian NAC gathers and monitors the hardware and software asset information of all IP-enabled devices. It then leverages its Device Platform Intelligence capability to determine each device's technical and business contextual details, identifies all known or potential device vulnerabilities, establishes the level of user access to be provided, and ensures that all detected devices are being compliant.

REQUIREMENTS	GENIAN NAC
1. Inventory and Control of Hardware Assets	Detect all IP-enabled devices on the network and identify their specific platform information
2. Inventory and Control of Software Assets	Collect installed software information on all devices.
3. Continuous Vulnerability Management	Check the status of IT security policy compliance and remediate non-compliant devices.
4. Controlled Use of Administrative Privileges	Authorize devices/users based on users' roles and responsibilities.
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	Inspect detected devices' configuration and security settings and maintain security baseline.
6. Maintenance, Monitoring and Analysis of Audit Logs	Monitor every single access event by devices and log all access history as part of the audit trail.

NAC Architecture Comparison

Without disturbing existing IT infrastructure or impacting systems availability, Genian NAC gathers and monitors the hardware and software asset information of all IP-enabled devices. It then leverages its Device Platform Intelligence capability to determine each device's technical and business contextual details, identifies all known or potential device vulnerabilities, establishes the level of user access to be provided, and ensures that all detected devices are being compliant. Additionally, Genians NAC can integrate with security solutions such as NGFW, SIEM, and EMM to share intelligence to respond to cyber threats on time.

CONSIDERATIONS	RADIUS	SNMP	MIRROR/SPAN	IN-LINE	SENSOR
Update Every Switch Configuration?	Yes	Yes	No	No	No
Add Every Switch to System?	Yes	Yes	No	No	No
Single Point of Failure	Yes	Yes	Yes	Yes	No
High Availability Required?	Yes	Yes	Yes	Yes	No
Truly Vendor Agnostic?	No	No	No	Yes	Yes
Minimum Switch Features Required?	Yes	Yes	Yes	No	No
Downtime Required?	Yes (High Risk)	Yes (High Risk)	No	Yes	No
Reconfigure After Network Refresh	Yes	Yes	Yes	No	No
Throughput/Capacity Concerns?	Potentially	No	Potentially	Yes	No
Cloud Managed?	Potentially	No	No	No	Yes
Zero/Low Touch Provisioning	No	No	Potentially	No	Yes
System at Every Location?	No	No	Potentially	Yes	Yes
Affordable Small Form Factor	No	No	No	No	Yes

Genian NAC Enforcement Methods

Genians promotes ARP Enforcement because of advantages. However, All legacy Enforcement Methods are also supported

- RADIUS Server *included* for centralized RADIUS Enforcement
- DHCP Server *included* for DHCP Enforcement
- SPAN/Mirror Enforcement supported
- SNMP Enforcement supported for switch port shutdown/management
- In-Line Appliance Enforcement option available
- Agent Based Enforcement

Genian NAC Editions

Choose the edition that best meets your business requirements. Upgrade between editions as your network evolves without losing your original investment. The editions can be delivered in 3 different ways:

<table>
<tr><th></th><th>BASIC
Network Surveillance</th><th>PROFESSIONAL
Network Access Control</th><th>ENTERPRISE
Automation</th></tr>
<tr><td>On-Premises</td><td>Free up to 300 devices*</td><td>30 days free trial</td><td rowspan="2">Contact
a Genians Partner</td></tr>
<tr><td>Cloud-Managed
Policy Server in the Cloud</td><td colspan="2">30 days free trial (Support up to 3,000 devices*)</td></tr>
<tr><td>MSP-Ready
NAC as a service</td><td colspan="3">Contact Genians</td></tr>
</table>

** Only count the number of active devices*

Genians

Get Started For Free

www.genians.com