BUILD THE CORE
SECURE ANY IP-ENABLED DEVICES, NO MATTER WHAT.

- Actionable Device Platform Intelligence
- Dynamic Network Access Control
- Seamless IT Security Automation

RUN EASY
YOU CHOOSE, WE DELIVER!

- On-Premises NAC (Get the software for your business needs)
- Cloud-Managed NAC (Run your Policy Server in the cloud)
- MSP-Ready (Deliver NAC as a Service)

HASSLE-FREE
TRY FIRST, GENIANS SUPPORTS.

- Start Anytime
- Upgrade Anytime
- Slack-speed Support
THE KEY TO CYBERSECURITY

DEVICE PLATFORM INTELLIGENCE

Discover all IP-enabled devices that exist in your network and find out which Device Platform has been used for the device along with contextual information about function, network connectivity, EOL/EOS status, manufacturer viability, and Common Vulnerabilities and Exposures (CVE) for both Device Platform and its manufacturer.

SHARING INTELLIGENCE

- Contextual access info (Who, What, Where, When, How)
- Business context (e.g. EOL, EOS, Manufacturer Info)
- Common Vulnerabilities and Exposures (CVE) for each detected device

CORRELATION OF ALL EVENTS

- Analysis of the security posture of applications, users, and data
- User and Entity anomalous behavior
- Cyber threats detection for IoT devices

ACTIONABLE INTELLIGENCE

- Zero Trust Security with auto-isolation and remediation of IoT devices

SECURING THE EDGE

NEXT-GEN NETWORK ACCESS CONTROL

Ensure full network surveillance for all IP-enabled devices and provides dynamic access control to maintain compliance with IT security policies. It then leverages automation to orchestrate an organization’s entire security portfolio in concert with NAC to achieve an optimally secure network access environment.

COMPREHENSIVE MANAGEMENT

- Mobile, BYOD, Guest
- IP Address Management (IPAM)
- Switch Port Management
- WLAN Security
- Endpoint Configuration Management
- Built-in Services (DHCP, RADIUS, Syslog)

IT SECURITY AUTOMATION

Orchestrate an organization's security products by integrating them with a wide range of IT security solutions (NGFW, IDS/IPS, EMM, SIEM, APT, DLP, etc.) to ensure unified policy enforcement via Syslog, Webhook, REST API, and Syslog.
FOUNDATIONAL CYBERSECURITY FRAMEWORK

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.

CORE REQUIREMENTS

<table>
<thead>
<tr>
<th>CORE REQUIREMENTS</th>
<th>PCI</th>
<th>HIPAA</th>
<th>ISO 27002</th>
<th>NIST</th>
<th>NSA</th>
<th>NERC CIP</th>
<th>SAMA</th>
<th>GENIAN NAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Inventory and Control of Hardware Assets</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Detect all IP-enabled devices on the network and identify their specific platform information</td>
</tr>
<tr>
<td>2. Inventory and Control of Software Assets</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Collect installed software information on all devices.</td>
</tr>
<tr>
<td>3. Continuous Vulnerability Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Check the status of IT security policy compliance and remediate non-compliant devices.</td>
</tr>
<tr>
<td>4. Controlled Use of Administrative Privileges</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Authorize devices/users based on users' roles and responsibilities.</td>
</tr>
<tr>
<td>5. Secure Configuration for HW/WS on Mobile devices, Laptops, Workstations and Servers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Inspect detected devices' configuration and security settings and maintain security baseline.</td>
</tr>
<tr>
<td>6. Maintenance, Monitoring and Analysis of Audit Logs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Monitor every single access event by devices and log all access history as part of the audit trail.</td>
</tr>
</tbody>
</table>

DYNAMIC NETWORK ACCESS CONTROL

Genian NAC leverages multiple techniques to enforce IT security policies dynamically to quarantine any non-compliant devices. Then, it remediates them to be compliant through automated processes.

CONSIDERATIONS

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

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

Genians delivers an enterprise-grade NAC solution by leveraging Cloud technology for businesses of all sizes, including SME's that struggle with technical challenges and budget issues.
IN GENIANS WE TRUST

Over the last 15 years, Genians has supported more than 1,600 customers around the world and secured millions of endpoint connections in organizations of all sizes and industries, including global Fortune 500 companies, the government, the military, energy, finance, healthcare, education, and beyond.

“Thanks to Genians’ non-disruptive sensing technology powered by its Device Platform Intelligence, we can see what, who, when, where, and how is connected to our network. It’s ‘Crystal Clear’! This real-time visibility enables us to manage and enforce various types of endpoint devices more precisely and just in time. Yes, we are ready for the IoT era!”

Genians Named a Representative Vendor in Gartner Market Guide for Network Access Control

TOGETHER, MORE SECURE.

Genians (KOSDAQ: 263860) reimagines Network Access Control by using Device Platform Intelligence to monitor the entire lifecycle of all network-connected devices to ensure the highest levels of IT security, availability, resilience, and agility. Genians is working to build a better security culture in the connected world by teaming up with global communities and industry leaders around the world.