Next-Gen NAC with AI-Based SIEM for Managed Security Service Providers

Genians' Next-Gen Network Access Control (NAC) powered by Seceon's AI-based SIEM delivers an enhanced cybersecurity stack to provide actionable intelligence for Enterprise IT infrastructure and mitigate cybersecurity threats in real-time.

This stack empowers Enterprises and Managed Service Providers (MSP, MSSP, MDR) to secure users, hosts, applications, Network & IT Infrastructure, ensuring a baseline for security and risk compliance.

Sharing Intelligence for Endpoints, Networks, and Threats

Genians' Device Platform Intelligence (DPI) with Seceon's aiSIEM™ Threat Intelligence encompass a spectrum of network activities from Layers 2 to 7 holistically. The resulting intelligence encompasses the following information:

- The most accurate device platform identity
- Contextual access information (Who, What, Where, When, How)
- Business context related to device (e.g. EOL, EOS, Manufacturer Info)
- Common Vulnerabilities and Exposures (CVE) for each detected device
- User and Entity anomalous behavior
- Analysis of the security posture of applications, users, and data
- Zero Trust Security with auto-remediation

Actionable Intelligence

With shared intelligence, Genians' Node Grouping feature classifies and profiles all devices associated with users, data, applications, and services before malicious threats are able to cause damage.

Seceon's aiSIEM helps bolster cybersecurity by generating meaningful alerts with improved accuracy from scores of threat indicators otherwise analyzed by security professionals and produces actionable intelligence for threat containment and elimination in real-time.

Genians NAC consumes this threat intelligence and responds immediately to cybersecurity alerts by enforcing security policies in order to block, isolate, and remediate non-compliant and compromised devices.

Threat Response Automation

The stack runs the process for compliance and security posture checks without requiring administrator attention.

- Monitor every individual network access attempt by devices associated with users, applications, data, and services
- Detect status changes for security and compliance
- Enforce unified policies with Seceon's aiSIEM
- Log all activities as part of the audit trail
- Log and events are shareable via RESTful API

HIGHLIGHTS

The cybersecurity stack by Genians and Seceon combines intelligence of device platforms and threats, which become actionable to control non-compliant devices and mitigate threats. For MSPs, the stack can provide the technology required to manage compliance and security threats more effectively.

Network Surveillance

Genians Layer 2-based sensing technology illuminates your entire network (Wired, Wireless, Virtual). Without disturbing existing network infrastructure and configuration, you can detect all IP-enabled devices (including legacy, industrial devices like SCADA, ICS, and IoT devices) with their technology, business, and risk-related contextual information.

Threat Detection & Response

Seceon's AI driven platform analyses network, identity, host & application data and offers:

- Proactive threat detection
- Automated Real-time threat containment & elimination
- Comprehensive visibility
- User & Entity Behavioral Analytics
- SIEM with no SIEM complexity
- Continuous Compliance
- Known & zero-day threats
- Multi-tenancy

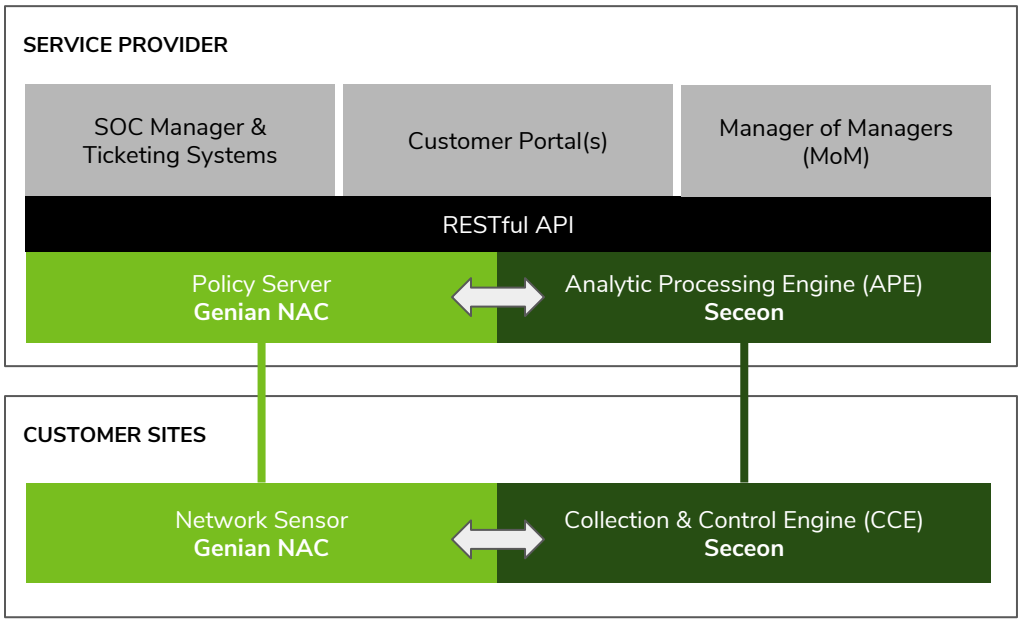
Network Access Control

Unified policies leverage intelligence gathered to precisely locate any compromised devices. Then, Genians can instantly block, limit, or remediate them using various access control methods: ARP-based, 802.1x, Switch Port, and SSID.

Network Security Automation

The stack supports open RESTful API to integrate with other security solution seamlessly.

The Technology Stack from Genians and Seceon



One-stop Services

Supports managing sites, users, licenses, subscriptions, and billing

Multi-tenancy

Use of Docker containers, making it easy to deploy the solution in any public or private cloud on a VM

A Single Box

Universal Customer Premises equipment (uCPE) can be used to combine Network Sensor with CCE

Enhance MSSP Business with NAC+SIEM

Genians and Seceon provide the most essential features for threat detection and response delivering comprehensive security solution as-a-service with various deployment options: On-premises, Cloud-managed, and NAC+SIEM-as-a-Service.

Genian NAC

- Network Surveillance
- Network Access Control
- Mobile, BYOD, Guest Management
- IP Address Management
- Switch Port Management
- WLAN Security
- Desktop Configuration Management
- Network Security Automation

Seceon aiSIEM

- Proactive Threat Detection
- Automated Real-time Threat Containment & Elimination
- Comprehensive Visibility User & Entity Behavioral Analytics
- SIEM with no SIEM Complexity
- Continuous Compliance
- Known & Zero-day Threats
- Multi-tenancy

Genians keeps working to build a better security culture in the connected world by teaming up with community and industry leaders around the world.

About Seceon

Seceon is focused on "Cybersecurity Done RIGHT". We empower organizations of any size to Visualize, Proactively Detect known and unknown Threats, automatically Eliminate/Contain Threats and provide Compliance through continuous Monitoring, Assessment, Policy Enforcement and Reporting.

www.seceon.com

About Genians

Genians (KOSDAQ: 263860) provides the industry's leading Network Access Control solution, which helps maintain full visibility and control of all your network assets and ensures that they are operating at the highest levels of security and compliance. Genians secures millions of endpoint connections in organizations of all sizes and industries, including global Fortune 500 companies, the government, military, energy, finance, healthcare, education, and more.

www.genians.com