

AI-Powered Converged NAC, ZTNA, and NaaS for Smart Manufacturing

Security-First Network Infrastructure for Industry 4.0



Genians (KOSDAQ: 263860) delivers a Zero Trust Access Platform designed to protect critical digital assets by securing all users, devices, and network connections with the highest levels of security and compliance. Trusted by 5,000+ clients – From SMEs to Fortune 500.

Ramen Inc. An innovator in AI-powered NaaS, delivering secure, automated wireless infrastructure across industrial environments via private 5G, Wi-Fi 6E/7, and mmWave.

Designed for Industry 4.0, the converged solution combines security and networking in a unified, intelligent architecture—built to secure and simplify industrial network operations at scale.

Operational Fit

IT/OT Network Engineers managing complex, distributed infrastructure

SecOps Teams seeking Zero Trust enforcement without agents

Smart Manufacturing and Logistics Operators needing secure wireless for automation and IoT

Facilities with limited local IT support requiring remote visibility and control

AI-Driven Security Assistants

The platform's multi-agent AI infrastructure automates onboarding, enforcement, and compliance via context-aware conversational control.

AI Agents			
Self-help	Security Compliance	Discovery	
Policy, Config & Data	Operational Telemetry	Density Diversity Growth	Usage Growth
NAC	Wireless		

AI, robotics, and automation are rapidly transforming manufacturing and logistics. To support this shift, enterprises need secure, high-performance connectivity across both IT and OT domains. However, traditional agent-based security tools are often impractical in industrial environments due to system limitations and operational constraints.

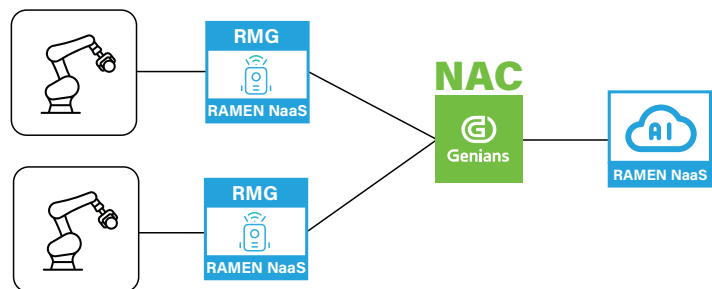
To address this, Genians and Ramen Inc. offer a converged, AI-powered platform combining Network Access Control (NAC), Zero Trust Network Access (ZTNA), and Network-as-a-Service (NaaS)—designed to ensure secure, scalable, and compliant connectivity for both enterprise (carpeted) and industrial (uncarpeted) settings.

Industrial organizations face growing network complexity and security gaps driven by:

- Limited visibility into unmanaged and legacy devices
- Inability to enforce security without disrupting operations
- Disconnected IT, OT, and cloud tools
- Resource-intensive compliance efforts
- Managing secure wireless in harsh environments

NAC-driven Zero Trust Meets AI-Driven Networking

In response, Genians and Ramen offer a unified architecture that aligns Zero Trust principles with scalable, AI-driven network infrastructure.



Network-as-a-Service (Ramen Inc.)

- End-to-end wireless connectivity using Wi-Fi 6E, Wi-Fi 7, Private 4G/5G, mmWave
- Delivered via the Ramen Machine Gateway (RMG), a component of Ramen NaaS, with AI-powered orchestration.
- One-stop service: design, deployment, and maintenance

Network Access Control & Zero Trust Network Access (Genians)

- Agentless, non-disruptive device discovery and platform intelligence
- Dynamic access control with deny-by-default policies
- Micro-segmentation and enforcement from Layer 2 to Layer 7
- Centralized policy authoring with distributed enforcement

Intelligence Fusion & AI Agent Automation

- Self-Help Agent: Automates issue resolution, reducing support load
- Security & Compliance Agent: Audit-ready for ISO, HIPAA, PCI, GDPR
- Growth Discovery Agent: Tracks expansion and recommends network optimization.

Core Capabilities Across All Environments

Designed to support secure, scalable, and intelligent network operations across IT, OT, and cloud infrastructures.


- 1. Agentless Device Discovery and Platform Intelligence:** Automatically identifies, classifies, and fingerprints all connected devices—including unmanaged, legacy, and headless systems—without requiring endpoint agents.
- 2. Centralized Visibility with Distributed Control (Cloud + Edge):** Provides a unified view of all assets while enabling localized policy enforcement through edge gateways and sensors, ensuring real-time responsiveness at scale.
- 3. Dynamic Zero Trust Policy Enforcement:** Applies deny-by-default access control policies based on real-time context such as user, device type, location, and network behavior.
- 4. Multi-Layer (L2-L7) Access Control and Micro-Segmentation:** Enforces fine-grained, behavior-aware access policies across network layers to contain lateral movement and isolate potential threats.
- 5. AI-Based Anomaly Detection and Compliance Automation:** Continuously monitors traffic patterns to detect behavioral anomalies and automatically generate compliance alerts and logs.
- 6. AI-Driven Self-Healing Infrastructure:** Resolves issues autonomously with policy-based remediation and predictive analytics, reducing manual intervention and downtime.
- 7. Pre-Built Compliance Frameworks:** Supports industry standards such as ISO 27001, HIPAA, PCI-DSS, and GDPR with automated reporting and audit readiness out-of-the-box.

Deployment Scenarios By Industrial Environments


The following deployment scenarios illustrate how the Genians + Ramen platform applies its core capabilities across different operational environments—from factory floors to distributed logistics and hybrid IT/OT networks. Each use case reflects distinct infrastructure requirements and control challenges, addressed through scalable, AI-driven network and security integration.

	Smart Manufacturing Facilities	Logistics and Warehousing Networks	Hybrid IT/OT Environments
Requirements	<ul style="list-style-type: none">• Diverse industrial devices (PLCs, robots, sensors)• Harsh environments with high EMI• No downtime tolerance during security enforcement	<ul style="list-style-type: none">• Limited IT resources at distributed sites• High mobility devices (scanners, tablets)• Rapid deployment and minimal configuration	<ul style="list-style-type: none">• Bridging enterprise IT with industrial control systems• Diverse endpoint types and protocols• Minimize lateral movement risk
Capabilities	<ul style="list-style-type: none">• Plug-and-play RMGs with resilient wireless• Micro-segmentation at machine level• Continuous anomaly detection for OT devices• Non-intrusive policy enforcement	<ul style="list-style-type: none">• Centralized access policy across multiple locations• RMG-enabled wireless deployment in days, not weeks• Auto-onboarding and policy enforcement by AI agents• Roaming-aware access control	<ul style="list-style-type: none">• Unified access policy for IT/OT assets• AD/LDAP integration for role-based segmentation• East-west traffic visibility and micro-isolation• Real-time remediation without disrupting operations


Built for the demands of Industry 4.0, the Genians and Ramen platform unifies security and networking into a single, intelligent architecture—purpose-built to secure and simplify industrial network operations at scale.




- Top 5 NAC Vendors in the Global Market – Recognized by Gartner.
- Zero Disruptions – Visibility & Policy Enforcement without Network Changes.
- Deploy Anywhere – On-Prem, Cloud, or Hybrid.
- All-in-One Security – NAC, BYODZero Trust, IPAM and More, Ready Out of the Box.
- Secure Access, Everywhere – Campus, Remote, and Cloud.



- Instantaneous visibility into factory and warehouse operations; leveraging NVIDIA Jetson platforms and DeepStream SDK.
- SLA-Driven wireless connectivity optimized for warehouses and distribution centers.
- Wireless network tuned to industrial networking demands.
- Built-in protection against cyber-attacks and ransomware.



hello@genians.com



sales@rameninc.com