Genians

Your Trusted Path To Secure Access

ZERO TRUST NETWORK ACCESS

ZTNA Anywhere Powered by Genians #1 Proven NAC

Accelerate Non-disruptive Zero Trust Implementation

Zero Trust can be complicated and not easy to implement, but not so with Genians, as Genians' ZTNA can guide you with a foundational approach to securing every single connecting point in various networking environments such as VPN, xDSL, and 5G, while ensuring secure users, devices, applications, data, and services.

- Device Platform Intelligence
- Zero Trust Segmentation
- Biometric (FIDO) Network Access Control
- ARP, 802.1X (RADIUS), Cloud Gateway, Agent Enforcement
- Application Visibility and Control
- Actionable Compliance (PCI, HIPAA, NIST, ISO 27002)
- Secure Remote Access from Home and Branch Offices
- Security Service Edge (SSE)
- White-labeled SASE Solution for MSSP

Genians has consolidated the complexity of all essential Zero Trust features into a single platform, Genian ZTNA. Genian ZTNA can ensure full network observability for all network-enabled devices and provides context-based access control to maintain compliance with IT security policies. It then leverages automation to orchestrate an organization's entire security portfolio in concert with Genian ZTNA to achieve an optimally secure network access environment

ZTNA Anywhere

With a Single Touch, Securely Access IT Resources.

- Remote Workers
- Campus Workers
- Campus Devices
- Cloud Security Groups

Get Started Anytime

Less Touch, Greater Results.

- Get Comprehensive Network Visibility in Less Than 10 mins
- Pragmatic Implementation: Visibility, Control, Automation
- Endpoint-initiated and Service-initiated ZTNA
- As-a-Service and Self-hosted ZTNA

THE KEY TO CYBERSECURITY SUCCESS

DEVICE PLATFORM INTELLIGENCE / Genian DPI

Genian DPI provides next-gen device fingerprinting for the IoT era, combining technology info with business context to understand where vulnerabilities may exist. This demands not only a more comprehensive view of the devices themselves, but also better understanding of risk indicators.

Layer-2 based Network Sensing Technology

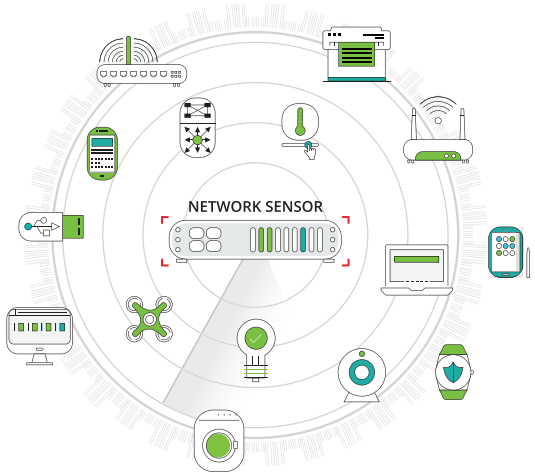
- No network configuration changes needed. Real-time data
- Expand visibility into IT/OT convergence

Manage the Entire Lifecycle of All IP-enabled Devices

- The most accurate detection of the device platform
  (e.g. Not just "Android phone" but "Samsung Galaxy S6 mobile phone")
- Contextual access information (Who, What, Where, When, How)
- Business context (e.g. EOL, EOS, Manufacturer Info)
- Common Vulnerabilities and Exposures (CVE)

Actionable Intelligence

- Auto-isolation and remediation of non-compliant devices with Genian ZTNA



ZTNA Anywhere

ZERO TRUST NETWORK ACCESS / Genian ZTNA

In this perimeter-less world, where do you currently stand, as network environments continue to evolve dramatically and cyber threat surfaces continue to change and expand? Expedite securing network edges by adopting Genian ZTNA. These three essential steps will help you solve the puzzle of how to achieve Zero Trust Security:

1

Get the Most Contextual Digital Attributes Empowered by Genian DPI

"Never trust, always verify" – but never trust what? Define the specifics of devices accessing your network by correlating them with both their technical and business contexts in real-time.

2

Build an Agile and Secure Digital Onboarding Process

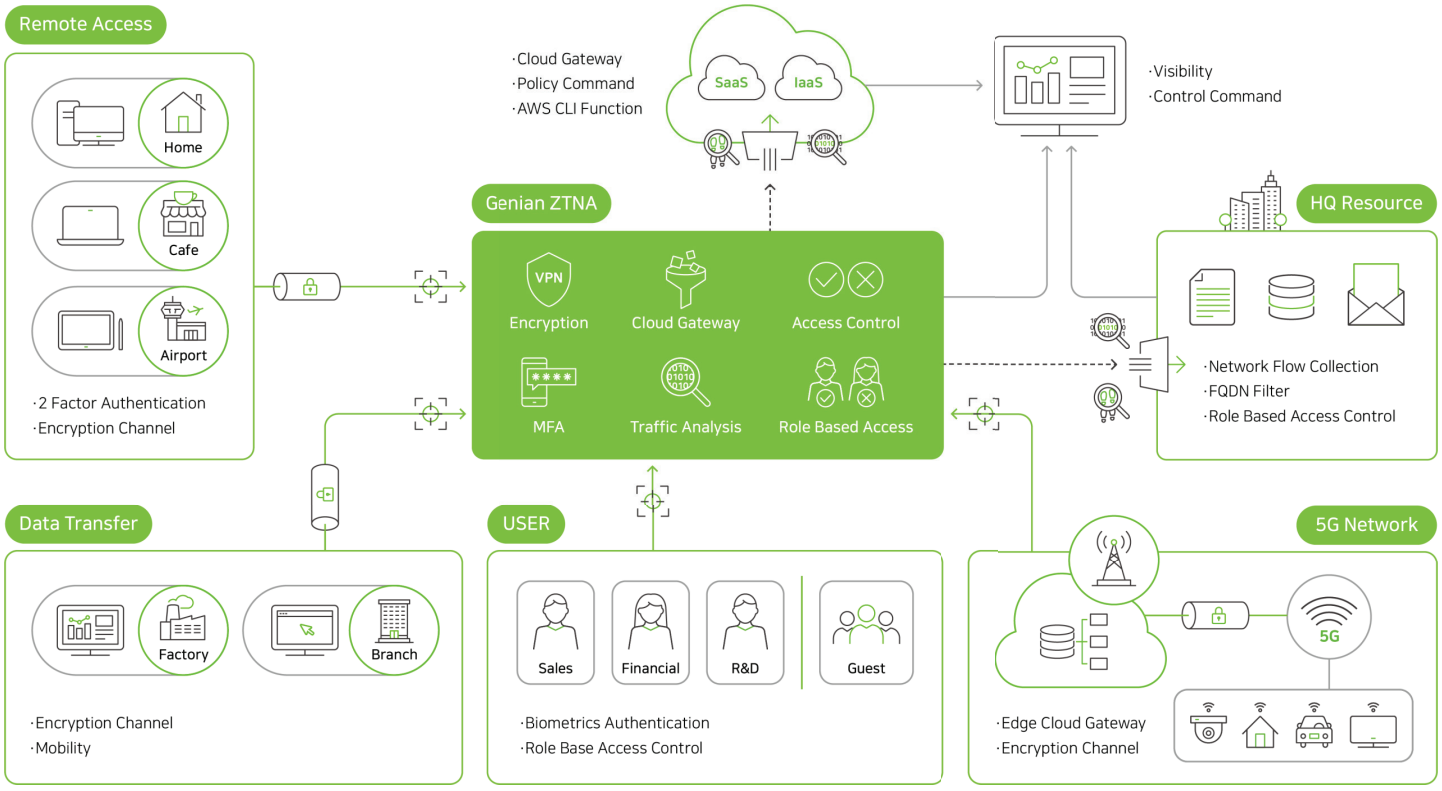
Map device information with users based on their access privileges and provide seamless FIDO authentication, contextual authorization, and actionable audit processing across your evolving network environments.

3

Automate IT Security by Eliminating Cybersecurity Silos

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

Genian ZTNA



Network Observability

- Infrastructure Independent Network Sensor
- Device Platform Intelligence
- IP Address Management
- Switch Port Management (SNMP)
- WLAN Visibility/Security
- Traffic Flow/Analysis (Netflow)

Cloud Security

- Cloud Workload Visibility
- Cloud Security Group Management Automation
- Zero Trust Security Policy for Cloud Workload
- Security Service Edge (SSE) on the Cloud (AWS, Azure, GCP)
- White-labeled SASE solution for MSSP

Endpoint Security

- Endpoint Visibility
- Device Configuration
- Application Management
- Malware Detection
- Compliance and Risk Posture Measurement
- Automated Remediation

Zero Trust NAC

- Micro Segmentation
- Context-based Least Privilege Access
- Multi-layered Enforcement – ARP, DHCP, 802.1x (RADIUS), SPAN (Mirror) Cloud Gateway, Agent
- Application Visibility and Control
- IP Mobility (VxLAN, Always on ZTNA)

Secure Remote Access

- ZTNA Agent for Secure Remote Connection
- Biometric (FIDO) Authentication
- Dynamic Policy Enforcement (RADIUS CoA)
- Always on ZTNA
- IPSec / SSL-VPN Gateway

Flexible Deployment Options

On-Premises ZTNA: Install and run Genian ZTNA on the premises of your organization using the Genian ZTNA software

Cloud-Managed ZTNA: Run Policy Server in the Cloud either managed by Genians or Yourself.

ZTNA as a Service: Deliver Genian ZTNA as a Service for your MSP business or organizations ready for Cloud services

Genian ZTNA Core Principles Map to 7 Tenets of NIST's Zero Trust Architecture

Genian ZTNA supports core industry regulatory requirements, such as PCI, HIPAA, ISO 27002, CSA, NIST, NSA, NERC CIP, and SAMA, by securing a Node – a connection point that can be connected to a network and communicates with other Nodes.

DOMAINS	GOALS	GENIAN ZTNA
Granting Access	All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	All connecting Nodes trying to obtain access are authenticated first with enhanced authentication methods: FIDO, SAML, OAuth, OTP, RADIUS-based, etc. (even if re-authentication is needed); this process ensures the authenticity of users and associated Nodes.
	The enterprise monitors and measures the integrity and security posture of all owned and associated assets.	Maintains Node compliance at the highest levels by continuously monitoring compliance status of all connected Nodes (e.g. OS updates, security patches, required software, etc.)
	Access to resources is determined by dynamic policy.	Provides observable states of every single Node by leveraging their condition-based Node Grouping technology with over 600 predefined conditions. This allows you to monitor and evaluate the characteristics and behavioral attributes of Nodes in real-time before granting access. Dynamic policy assignment is enforced based on the status change of Node compliance.
Controlling Access	All data sources and computing services are considered as 'resources.'	Detects, identifies, and classifies all resources automatically by Node Grouping empowered by Device Platform Intelligence (DPI). This way, it can control access to the minimal resource at the maximum granularity based on your requirements.
	Access to individual enterprise resources is granted on a per-session basis.	Accessing resources is granted on a per-session basis to reduce risks by minimizing access in time.
Monitoring & Securing Access	Collect as much information about the network and infrastructure as possible.	With non-disruptive sensing technology, Genian ZTNA can collect identifiable data from all egress and ingress traffic to establish actionable context by leveraging DPI, which can correlate device fingerprinting data with contextual data regarding function, network connectivity, EOL/EOS status, manufacturer viability, and Common Vulnerabilities and Exposures (CVE). Additionally, relevant Software Bill Of Material (SBOM) patterns and Manufacture Usage Description (MUD) profile are provided.
	All communication is secured regardless of network location.	Supports end-to-end encrypted communication (North-South, East-West) via Genian ZTNA Agent and ZTNA Cloud Gateway. Network traffic aggregations and network security function are delivered as a single service at dispersed SASE points of presence (PoPs).

IN GENIANS WE TRUST

Since 2005, the company has served more than 2,400 customers, in organizations of all sizes and industries, including global Fortune 500 companies, the government, the military, critical infrastructure, finance, healthcare, education, and more.

Genians Is ISO 27001 Certified

Genians Named A Representative Vendor In Gartner and Frost & Sullivan Report

TOGETHER, MORE SECURE.

Genians (KOSDAQ: 263860), the industry pioneer in Zero Trust Network Access (ZTNA), provides a fundamental cybersecurity platform for building a trusted path to secure access for any connecting devices by leveraging its Device Platform Intelligence (DPI), Network Access Control (NAC), and Endpoint Detection and Response (EDR). 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.

Genians

Asia Pacific and Japan

12F A, Pyeongchon HIFIELD Knowledge industrial Center
66 Beolmal-ro, Dongan-gu. Anyang-si
Gyeonggi-do, South Korea

apac@genians.com
+82-31-422-3823

North America / EMEA / LATAM

3003 North 1st St, #210
San Jose, CA, 95134
United States of America

hello@genians.com
+1-617-307-4090