192.158.1.38 10.10.10.1 10.10.10.1 192.158.1.38 192.158.1.38

HACKERS CAN'T ATTACK WHAT THEY CANNOT FIND

Cyber-attack surfaces are growing exponentially... and the existing solutions are reactive.

Be proactive and stop at the first point of attack.

Invisinet's groundbreaking technology enforces Zero Trust identity-based access through First Packet Authentication™ essentially making high-value network segments invisible.

- Cloak Networks and Assets
- Enforce Identity-based Micro-segmentation
- Highly interoperable across IT and OT hybrid networks
- Secure business-critical AI applications

Cloud & Datacenter
INVISINET works in all major cloud and customer datacenter environments.

Cloak Networks & Assets
INVISINET authenticates and enforces identity and shields networks & network-connected assets from unauthorized discovery, shutting down reconnaissance of critical information and infrastructure.
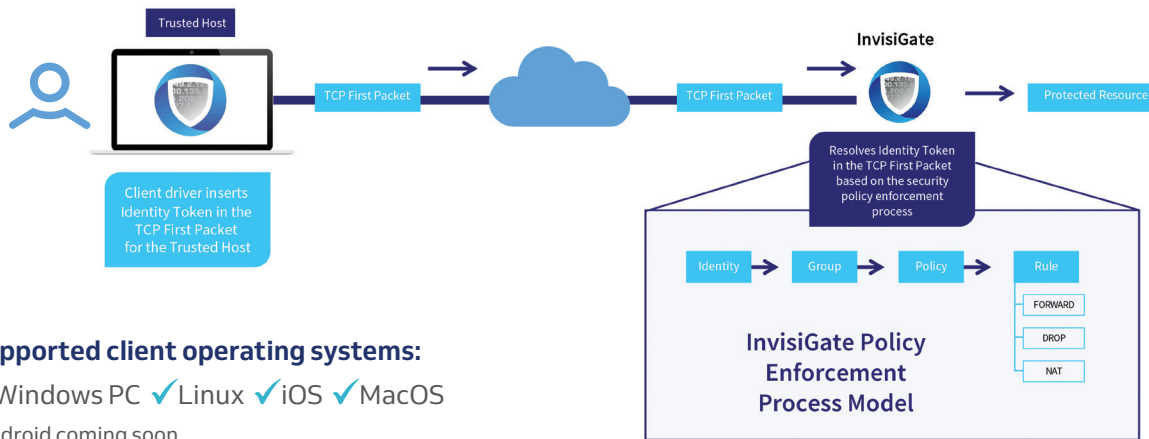
Ease of Deployment
INVISINET fits into your existing network, saving complex and costly infrastructure changes.

TRUE CYBER ATTACK PREVENTION

Software Innovation — Invisinet's Zero Trust Authentication Platform

InvisiPoint Endpoint Protection: Agent to gateway policy enforcement for Enterprises

This model secures endpoint user application traffic to protected resources. Light-weight software agents are installed on users' endpoint devices. These agents insert user identity at the traffic's source to ensure secure communication to and through the protected network.

Trusted Host

InvisiGate

TCP First Packet

TCP First Packet

Protected Resource

Client driver inserts Identity Token in the TCP First Packet for the Trusted Host

Resolves Identity Token in the TCP First Packet based on the security policy enforcement process

Identity → Group → Policy → Rule

FORWARD

DROP

NAT

InvisiGate Policy Enforcement Process Model

Supported client operating systems:

✓Windows PC ✓Linux ✓iOS ✓MacOS

*Android coming soon

InvisiGate Protection: Gateway to gateway policy enforcement for IoT

The Gateway-to-Gateway deployment model excels at offering bidirectional protection. It allows trusted hosts on both ends to access resources on the opposite side while safeguarding resources on both sides.

InvisiGate

InvisiGate

TCP First Packet

TCP First Packet

Protected Resource

Trusted Host

Client driver inserts Identity Token in the TCP First Packet for the Trusted Host

Resolves Identity Token in the TCP First Packet based on the security policy enforcement process

Identity → Group → Policy → Rule

FORWARD

DROP

NAT

InvisiGate Policy Enforcement Process Model