STEALTH
SOLUTION

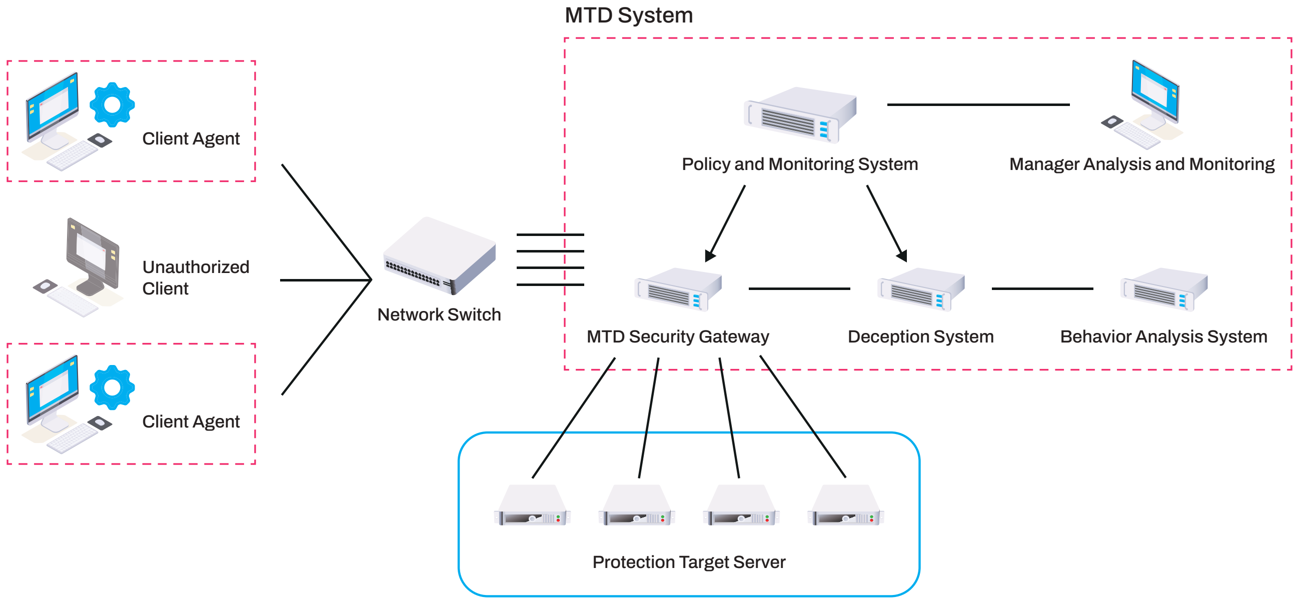
Moving Target Defense

STEALTH MTD

SOLUTION BRIEF

SOLUTION OVERVIEW

MTD Gateway + Deception, Analysis system + Policy system + Agent for clients



- - - - - - MTD Security Zones and Systems

⚙ MTD Agent for Clients

KEY CHALLENGE

The network environment is getting more complex each day under the name of the 4th Industrial Revolution as advanced technologies such as artificial intelligence, autonomous driving, and meta-bus develop into a new era. As networks grow, the attack surface is expanding, and the attacker's influence in attack-defense is increasing day by day due to the Defense in Depth system and signature-based passive type of information protection technology and the static characteristics of the network and configuration.
In order to eliminate the attacker's advantage of this asymmetric structure, it is necessary to adopt a strategy and develop technology that continuously and actively changes the main properties of the object to be protected.
Moving Target Defense (MTD) is a proactive defense strategy that can prevent various cyber attacks in advance by actively changing the main properties of the object to be protected, resolving the asymmetric attack-defense relationship under the attacker's dominance in a static network environment.

MTD Security Gateway

- Generation of server address randomly through Network Address Mutation
- Block and hide the address exposure of the server for protection

Deception system, Analysis system

- Decoy system configuration
- Response to unauthorized/unauthenticated clients and behavior analysis

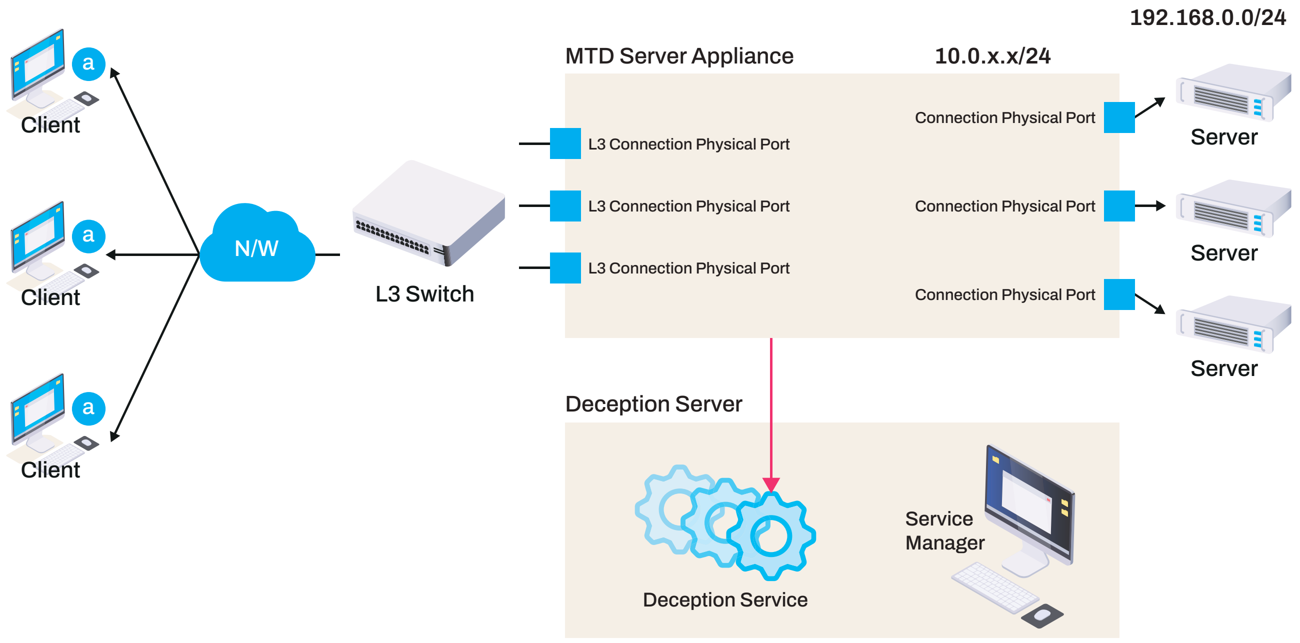
Policy system

- Period setting for random generation and change of network address
- Client authentication and zero trust policy management between client and server

Agent for clients

- Server address tracking algorithm
- Implementation of zero-trust-based authentication policy

HOW IT WORKS



The Stealth MTD Server Appliance is a hardware appliance for protecting a server, which sends a response on behalf of the server when a client requests a service from the server. The client is a PC equipped with an agent and is allowed to access the server only when authentication is completed according to the zero trust policy through the equipment. The East Bank of the server IP mapping card is a physical area that physically connects to the server one-on-one. In the case of West Bank, it serves as a gateway to the connected server, and protects the server from being exposed to the outside by changing the server address randomly through a virtual network driver. The randomly changing server address shall be changed periodically or non-periodically, and one virtual driver is allocated per server port to correspond to the server. The Virtual Routing Module operates as an internal module that handles traffic routing so that the client's request to the MTD within the MTD server can be sent to the server normally. Also, when a client's request occurs, it does not route the unauthorized client's packet to the East bank, but changes the traffic route to the Deception Server, playing a role in changing the traffic so that the deception equipment can analyze the hacker's movements. Deception Server operates a user-defined decoy service and responds to the cyber attacker's request, creating an illusion that the services are operating normally inside the attack. After that, it plays the role of Advanced Honey Pot that operates a virtual environment to understand the behavior, strategy, and technology(TTPS, Tactics, Techniques, Procedures) of hackers.

BENEFITS

01 Hide major server addresses

The main server information can be hidden by continuously changing the properties of the attack surface (IP, Port, Protocol, Application, etc.).

02 Secure client communication

The client that needs to connect according to the hiding of the server address guarantee a secure communication channel (Hidden Tunneling) that is similar to VPN communication by creating separate hidden tunneling to continuously track the server address.

03 Hacking Prevention

It can effectively defend against attacks in the reconnaissance and detection phases of the cyber kill chain. It is particularly effective against active and passive scanning attacks.

04 Zero trust

Block unauthorized client server access and deal with insider threats through zero trust policy.

05 Ensure server stability

Adopting a secure gateway method of physical card type, which does not require installation of server agent, ensures server stability and installation of legacy solutions without compromise.

06 Construction of an advanced deception system

Construction of an advanced deception system that provides improved functions such as behavior analysis and abnormal behavior detection of unauthorized/unauthenticated clients along with network address changing technology.

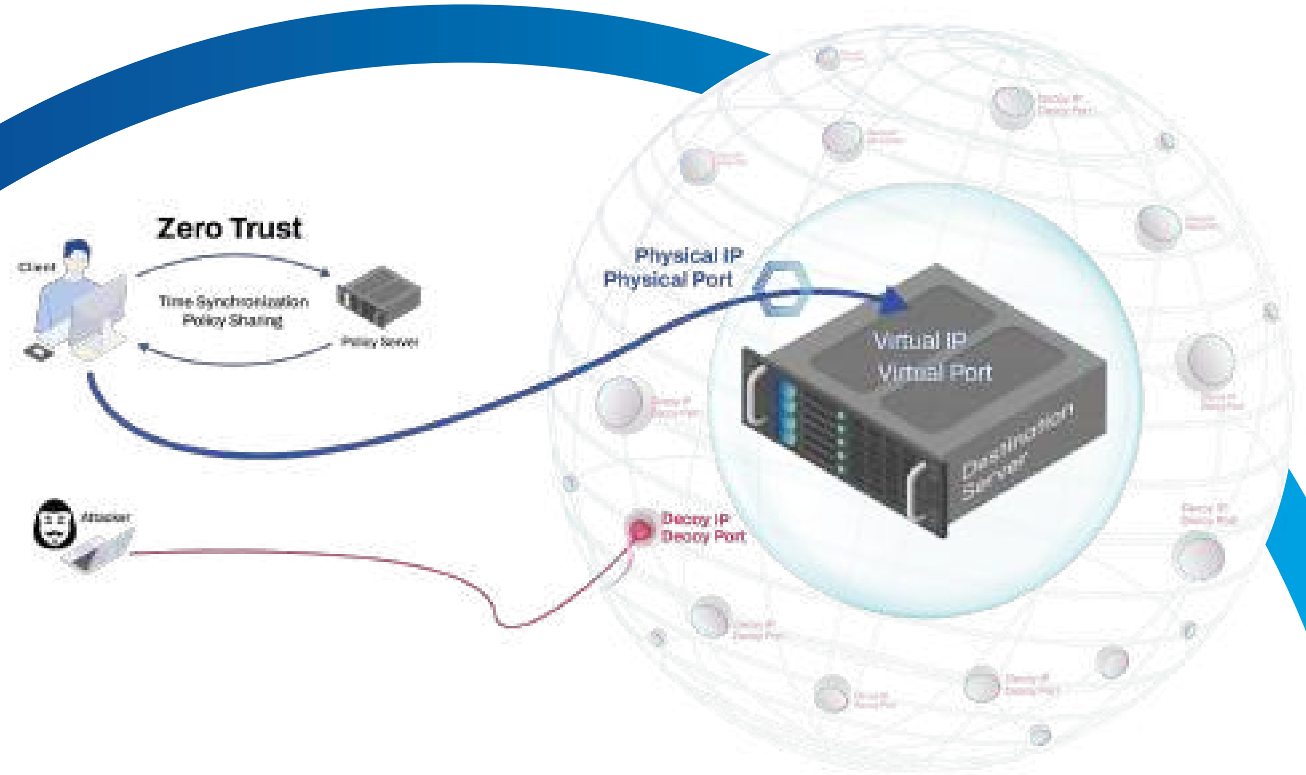
ABOUT STEALTHSOLUTION

The transformation and settlement of the non-face-to-face era and the cloud transformation of business and service environments are explosively increasing the amount of network usage.
As a result, the attack surface of the network is also widely spread, and the probability of being exposed to risks such as hacking is also rapidly increasing.
Stealth Solution, located in Seoul, South Korea, is a startup that provides an intelligent security platform for a new security paradigm to help companies continuously invest in security infrastructure, build a cyber-threat response environment and eliminate risk factors.
Stealth Solution actively respond to cyberattacks by applying next-generation MTD strategies to detect and block malicious attacks.

Platform

STEALTH MESSENGER

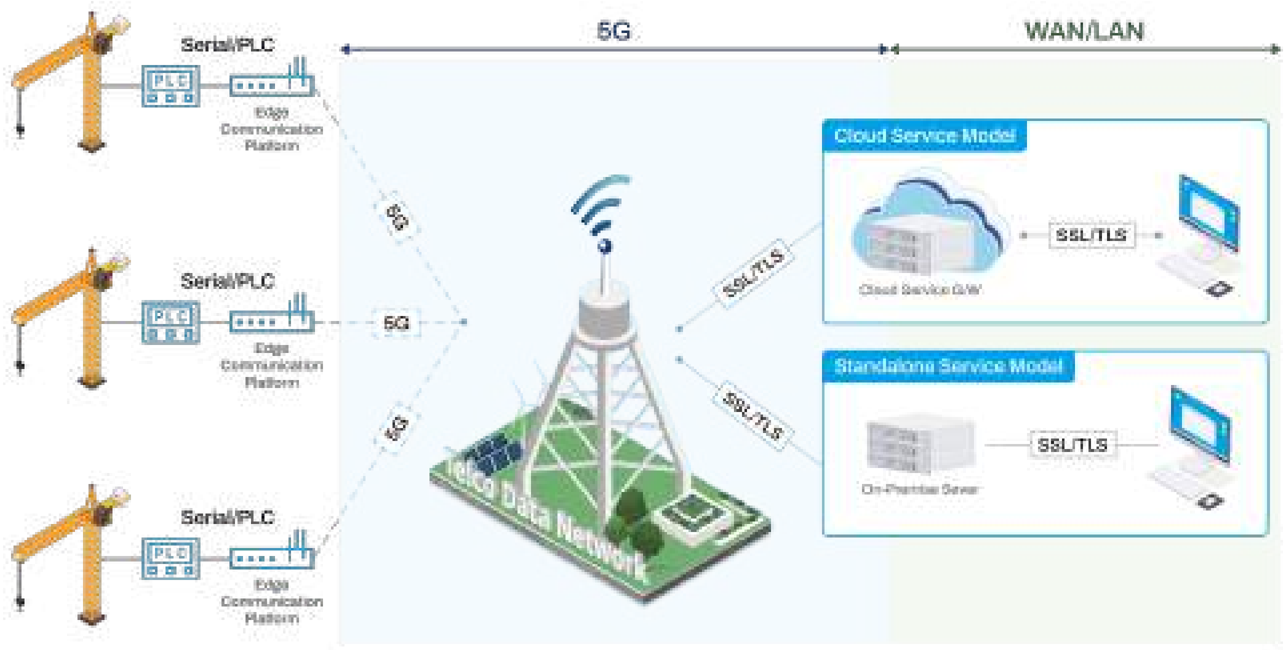
STEALTH MESSENGER is an encryption messaging application that includes the nextgen encryption technology, Secure Multi-Party Computation, and zero-knowledge proof technology.



Information Technology

STEALTH MTD(Moving Target Defense)

STEALTH MTD(Moving Target Defense) is based on network host address mutation technology that mutates IP address and PORT number of network host continuously, network deception technology, and network reflection technology so that it makes impossible for attackers to identify the network host from the first attack stage.



Operation Technology

STEALTH MAVERICK

STEALTH MAVERICK is a smart construction machine remote management platform using 5G, cloud technology, and PLC management technology. This platform enables integrated managemen and control of contruction machines in industrial sites.

STEALTH
SOLUTION

4F, 83, Uisadang-Daero, Yeongdeungpo-gu, Seoul, Republic of Korea
Tel: +82-2-562-1221 E-mail: info@stealths.co.kr
www.stealthsolution.co.kr