CyberInova®

Never as today the increasing moving of data and information due to digitalization and remote working requests high protection to the integrity and the access of a system. Threads like data theft, alterations of the structure, impossibility of access, smarter ackers, for a company can mean risk to stop and block entire manufacturing process, work flow, goods delivery, with high costs and losses at different levels.
The Cloud Security Alliance (CSA) delineated new defensive strategies from aggressions on the network with a new, called Software Defined Perimeter (SDP) based on the concept of Zero Trust Network Access (ZTNA), a security framework where access is continuously verified.

Based on the zero trust concept, our aim is to enhance the way people connect, to deliver the most agile, safe and efficient cybersecurity structure.

This is the reason why we designed
InovaMesh.

Agile Security Solution

An innovative cyber security strategy

InovaMesh is an application framework based on the idea that no device or user can be trusted, regardless of whether they are inside or outside the network perimeter.
In the cloud, InovaMesh networking aims to create secure network communications focus on the user as the heart of the entire architecture.

A 1 to 1 relationship between user and the data to access

InovaMesh replaces centralized security controls with distributed software agents that operate under the control of the application manager and provide access to the application infrastructure only after identity verification. These agents create encrypted connections between requesting systems and application infrastructure, with a one to one relationshionship between them.

InovaMesh IoT: an all-in-one device that protects IoT devices by providing microsegmentation, isolation, alert and monitoring.

Benefits

1. Trought micro-segmentation InovaMesh removes implicit trusts and implements micro-perimeters (Software Defined Micro Perimeters) prevents techniques of hacking, as lateral movement which can be possible with traditional VPNs.
2.` It’s a SaaS solution (Software as a Service) accessible by client software agents and/or in version with its hardware client; any apparatus can be connected via LAN/WLAN to InovaMesh (Windows, Linux, macOS, iOS, Android ecc) .
3. Extremely easy installation, requires no changes to existing infrastructure.
4. Replaces traditional VPNs with a superior segmentation solution in terms of security, scalability, ease of installation, management and TCO (Total Cost of Ownership).
5. Uses modern encryption and communication protocols providing superior performance and security.
Integrated Host Firewall with the granular access control (IP, service, ports)
6. Go SDK to build agents for a variety of Operating Systems and hardware architectures.
7. Strong identity control:

- Integration with the customer’s existing Identity Provider
- Standard supported are SAML2, OAuth2 or OpenID Connect
- Integrates 2FA if required

8. Granular access filter based on security groups

9. Captures and organizes the IP traffic that crosses the mesh by recording it locally and at the same time sending it to the ELK (Elasticsearch Logstash Kibana) for auditing and troubleshooting