InovaMesh®

The Agile Cyber Security Solution by

CyberInova®

Use Cases

CyberInova Ltd

July 2025

Inovamesh Use Cases - Index

InovaMesh Use Cases OverView

InovaMesh® is a standards-based, software-defined solution for identity-managed endpoint segmentation and isolation. It enables microsegmentation, encrypted traffic, obfuscation from adversaries, and threat remediation across both tactical and enterprise-wide deployments, independent of the underlying network or infrastructure control. InovaMesh creates cryptographically isolated overlay networks that can span on-premises, multi-site, public, private, and hybrid cloud environments, allowing a single security policy to govern all operational contexts.

Case: Internet of Things (IoT Devices)

Use Case

Secure the integration, isolation, and management of a fleet of remote IoT and headless devices within enterprise networks.

Scenario

IoT devices, often isolated, are connected to networks for monitoring and control but can be vulnerable to compromise. Additionally, a fleet of remote IoT devices, due to evolving connectivity technologies, operates over time with multiple and non-uniform connection types."

Solution

InovaMesh manages fleets of IoT devices, governing their remote control and protecting both endpoints from intrusions and malware. Additionally, InovaMesh manages and ensures connectivity to remote IoT devices regardless of the communication technology, addressing issues such as the inability to reach individual IoT devices directly from the central hub or the variability of their IP addresses.

Case: Application Architecture Isolation

Use Case

Microsegment the layers of a software/system architecture — front-end, data tiers, remote API services — to contain security breaches.

Scenario

Web servers in the presentation tier, exposed to the public internet, risk being compromised, which could endanger other applications and database tiers through unrestricted network connections.

Solution

InovaMesh establishes communication rules that restrict interactions between different local and remote tiers of applications. Additional filters limit lateral traffic among hosts within the same tier to contain potential breaches.

Case: Secure Remote Application Architecture

Use Case

Establish secure and obfuscated communication between remote, distributed application systems, including those located in private environments without direct exposure to the Internet.

Scenario

With distributed software architectures, often spanning different cloud providers, it becomes extremely difficult, if not impossible, due to networking policies, for a non-public service on one cloud provider to access APIs and similar services hosted on a different cloud provider.

Solution

InovaMesh creates a virtual overlay network, built on top of the existing networking architecture, bypassing its routing limitations. It enables connectivity between endpoints, even if they are in private networks of cloud providers, without requiring explicit exposure to the Internet.

Case: Unsupported/Obsolete Operating System

Use Case

Protect legacy operating systems, no longer supported or economically maintainable, by limiting their network exposure.

Scenario

Organizations, in some case, must maintain outdated servers incompatible with upgrades due to internal software dependencies and lacking manufacturer support.

Solution

InovaMesh creates microsegments that allow legacy systems to access only local resources. Endpoints use ZTNA functions to establish authorized connections, managed through InovaMesh’s centralized control. Unauthorized clients remain invisible, preserving security integrity across the environment.

Case: Legacy Systems Isolation

Use Case

Protect legacy systems (POS, PLC etc..) where no software modifications or installations are possible, ensuring both protection and traffic anonymization.

Scenario

In sectors such as banking, healthcare, or industrial, there are systems in which, by their nature, no modifications are allowed, either on the software or hardware side

Solution

InovaMesh allows installation on various types of modems, routers, and network controllers based on Linux microkernels. In this way, simple devices—referred to by us as Hardware Gateways—can be deployed upstream of the legacy system to be protected, enabling its connection to the InovaMesh ZTNA

without any interaction with the legacy systems being managed.

Case: Zero Trust Secure Remote Access

Use Case

Isolate and manage remote access to enterprise networks and services using strict least-privilege policies.

Scenario

Organizations need to manage and control remote access to internal resources without exposing the network to increased risk from excessive access rights.

Solution

InovaMesh establishes segregated remote access demilitarized zones (DMZs) with specific rules and filters, enforcing controlled access privileges aligned with Zero Trust principles, without the limitations of traditional VPN systems.

Case: Secure Internal Private Cloud

Use Case

Protect and limit internal private cloud environments from threats originating both internally and externally.

Scenario

Private clouds deliver virtualization and cloud services managed within enterprise boundaries, requiring strong access controls.

Solution

InovaMesh acts as network gateways within data center environments, enforcing least-privilege access while maintaining application security protocols.

Case: Secure External Public Cloud

Use Case

Control and safeguard network access to external and public cloud resources by adding obfuscation capabilities.

Scenario

Public clouds offer scalable resources but introduce security concerns due to shared infrastructure and external control.

Solution

InovaMesh provides microsegmentation, encryption, and obfuscation capabilities for cloud platforms, mitigating risks through consistent security policies across both cloud and on-premises deployments. The obfuscation capability is such that the protected cloud service remains invisible to sources outside the InovaMesh ZTNA.

Case: BYOD Devices

Use Case

Safeguard corporate resources accessed via employees' personal devices.

Scenario

Users utilize personal smartphones or laptops for work tasks, introducing risks related to device security and management.

Solution

InovaMesh enables secure remote access for containerized or wrapped applications on personal devices, securely provisioning corporate resources through InovaMesh appliance gateways in the corporate DMZ.