

Use case

Network Microsegmentation

Reemo Workspaces

Advanced security through Network
Microsegmentation



SI DR Compliant

Reemo Workspaces

Advanced security through Network Microsegmentation

With Reemo Workspaces, create an ultra-secure collaborative environment.



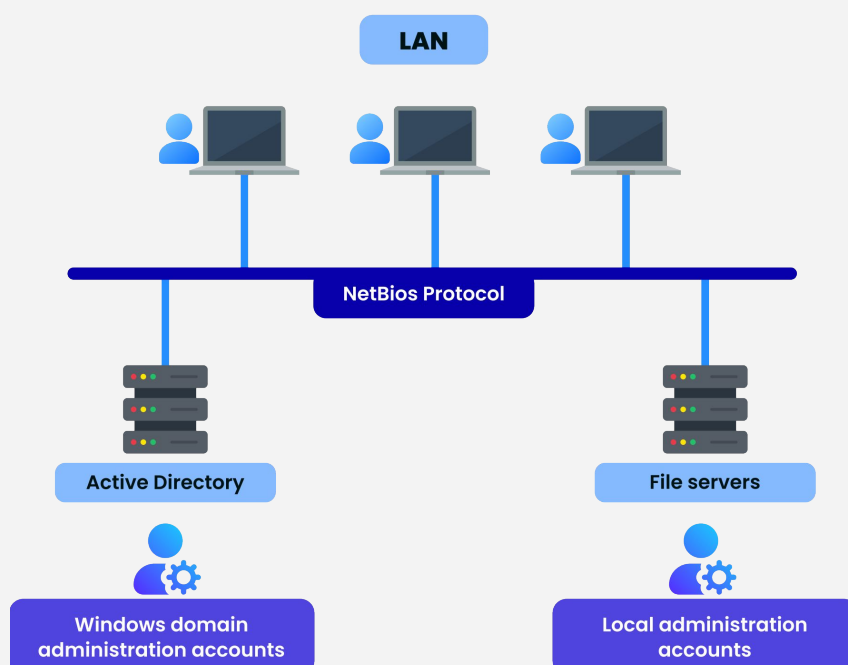
Challenges

Many companies need to collaborate on sensitive projects with external partners or mixed internal/external teams. This situation exposes their infrastructure to an increased risk of compromise, particularly through shared network access.

Traditionally, remote access is managed through a standard client-server VPN, offering a direct entry point into the infrastructure. This leads to several critical issues :

- Excessive access to sensitive resources
- Lack of fine-grained control over user interactions
- No isolation between user environments
- Risk of lateral threat propagation in case of a breach

Traditional architecture



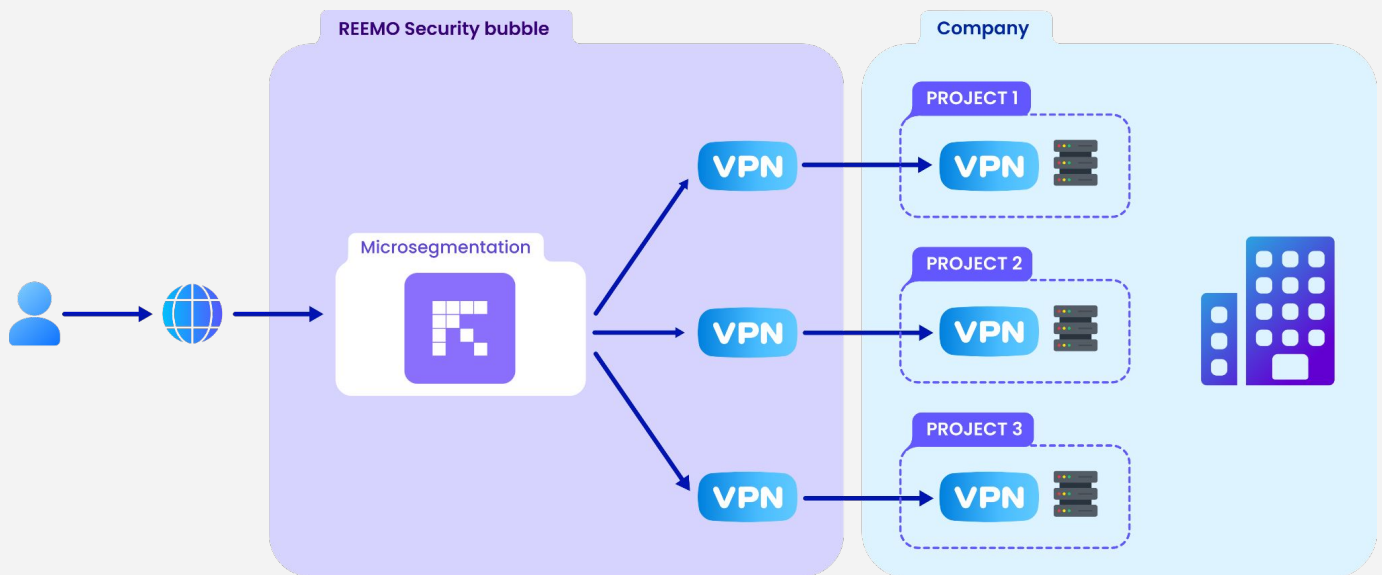
In traditional network architectures, **collaboration tools** (video conferencing, messaging, file sharing) further **expand the attack surface** if not properly isolated.

Solutions

Reemo introduces a radically different approach based on **Zero Trust architecture** and a **multi-layered network microsegmentation system**, fully aligned with the "need-to-know" principle.

Deployment of a secure bubble upstream of the company's infrastructure

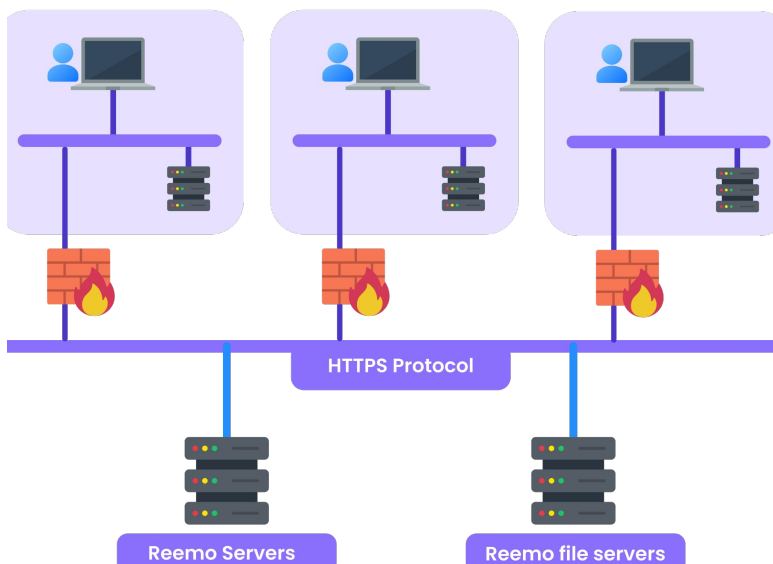
This secure bubble is connected via a site-to-site VPN. Unlike a traditional VPN, this bubble acts as a secured gateway: **the user does not transit directly into the infrastructure** but is automatically redirected to an isolated environment.



 reemo.io

Reemo architecture with micro-segmentation

LAN



Isolated user environments

Each user operates in a stand-alone, single-session **Windows environment** integrated within the Reemo bubble. These are not just remote accesses — they are fully isolated environments at every level.

The administrator configures **access externally** through the Reemo console, directing each user only to the part of the infrastructure they are authorized to reach. **Users cannot modify this configuration in any way.**

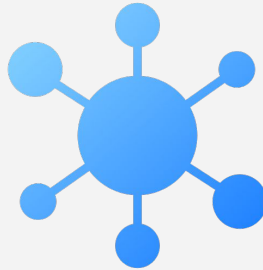
Solutions

Three-Layer Microsegmentation

- **Network level** : Blocks all network communication between users, preventing lateral attacks.
- **Virtualization level** : Eliminates risks of Virtual Machine Hyper Jumping.
- **User level** : Prevents any unauthorized privilege escalation.



 No Active Directory



 No Corporate Network



 No Administrator

An Ultra-Secure Collaborative Environment **designed for sensitive projects involving multiple internal or external stakeholders** — such as R&D environments, public tenders, or investigations (legal, OSINT, or cybersecurity) — where each user only accesses **strictly assigned resources**. No lateral communication is possible, ensuring **total session isolation**, fine-grained access traceability, and a level of security fully **compliant with the highest regulatory standards**.

Results

Total isolation

Each user operates in **total isolation**: even within the same project, an attack cannot spread between users.

Seamless Admin

Access management is centralized **through a single console**, with no action required from users or changes to the core infrastructure.

User experience

The experience remains seamless and intuitive: users instantly access **only the resources they need** — securely and efficiently.