Use case

Securing third-party access

Reemo Containers

How to Secure Third-Party Access with Reemo

Reemo

Use case | Securing third-party access

Reemo Containers

How to Secure Third-Party Access with Reemo

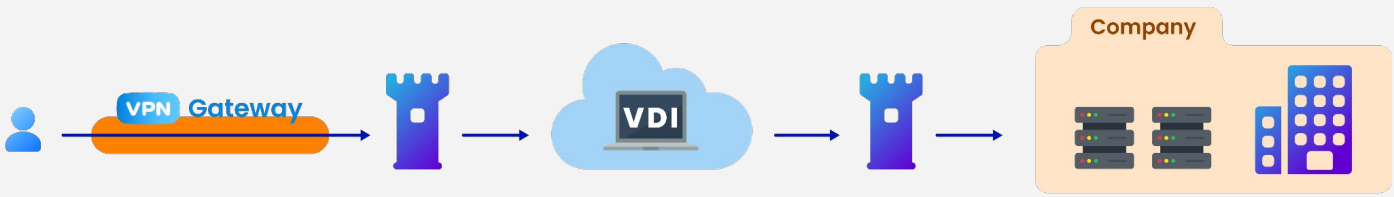
With Reemo Containers, securely grant access to third parties via a simple browser.

Challenges

The common challenge for large organizations : how to allow external providers to securely access specific business applications and necessary resources, while fully protecting the internal infrastructure?

Traditional VPN or VDI solutions are no longer suited : forcing subcontractors to install slow or complex software to access internal servers is no longer realistic in the era of Zero Trust security.

Challenge : Provide subcontractors with smooth and secure access, only to the necessary applications, without compromising the internal infrastructure.

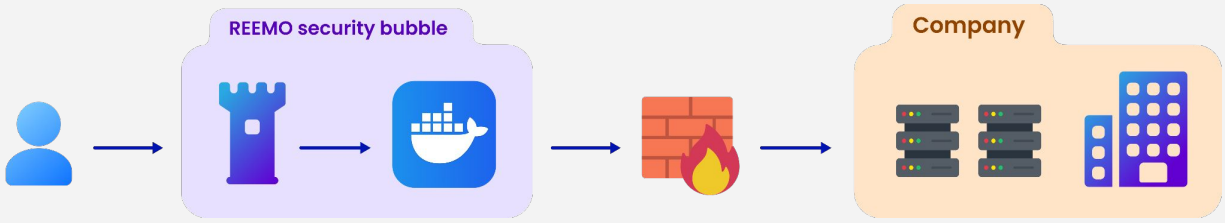


Today, third-party access often relies on a traditional architecture combining **VPNs**, **bastions**, and **virtualized desktops**.

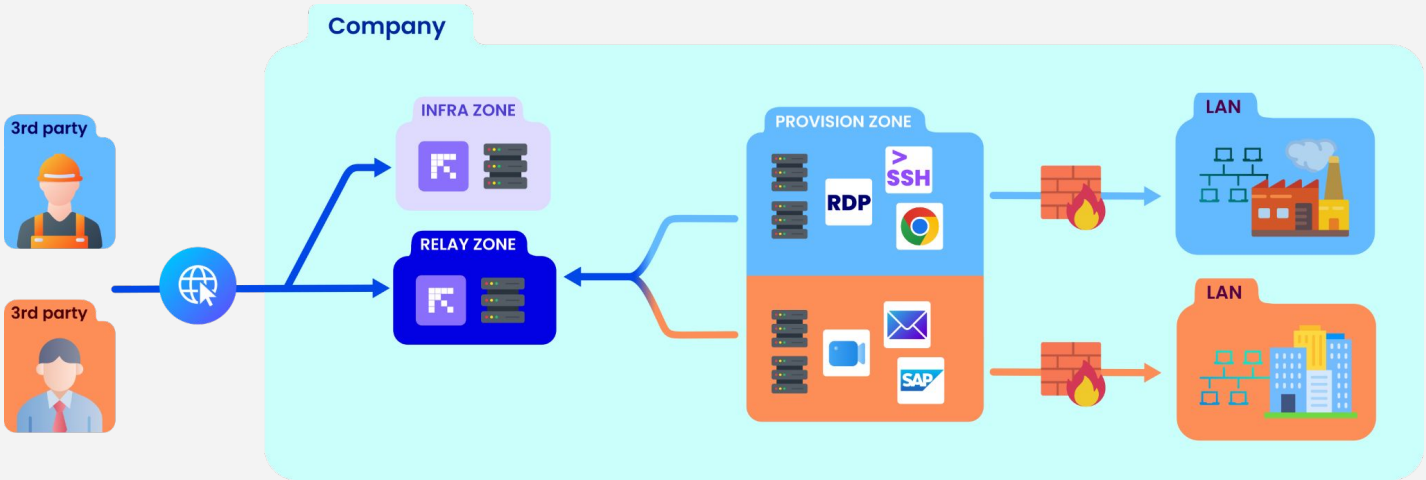
A **costly**, **complex** model, **difficult to maintain**, and increasingly inadequate to meet today's performance and compliance requirements.

Solutions

To meet these demands, Reemo offers a **simplified**, **secure**, **all-in-one** infrastructure — adapted to the challenges faced by all types of organizations.



Example #1 Third-party securing through isolation in the Provision Zone



KEY STEPS

Step 1 : From their device, providers connect to the Internet and access a centralized Reemo platform to authenticate.

Step 2 : Once authenticated, they are directed to a shared Relay Zone acting as a secure buffer. A dedicated relay container is created for the user for the duration of their session.

Step 3 : The application container is created in the Provision Zone matching the user's profile.

Step 4 : The user and the container meet within the Relay Zone to establish the session.

GOOD TO KNOW

Containerization gives you full control :

- Peripheral device filtering
- Copy-paste permissions
- Download permissions

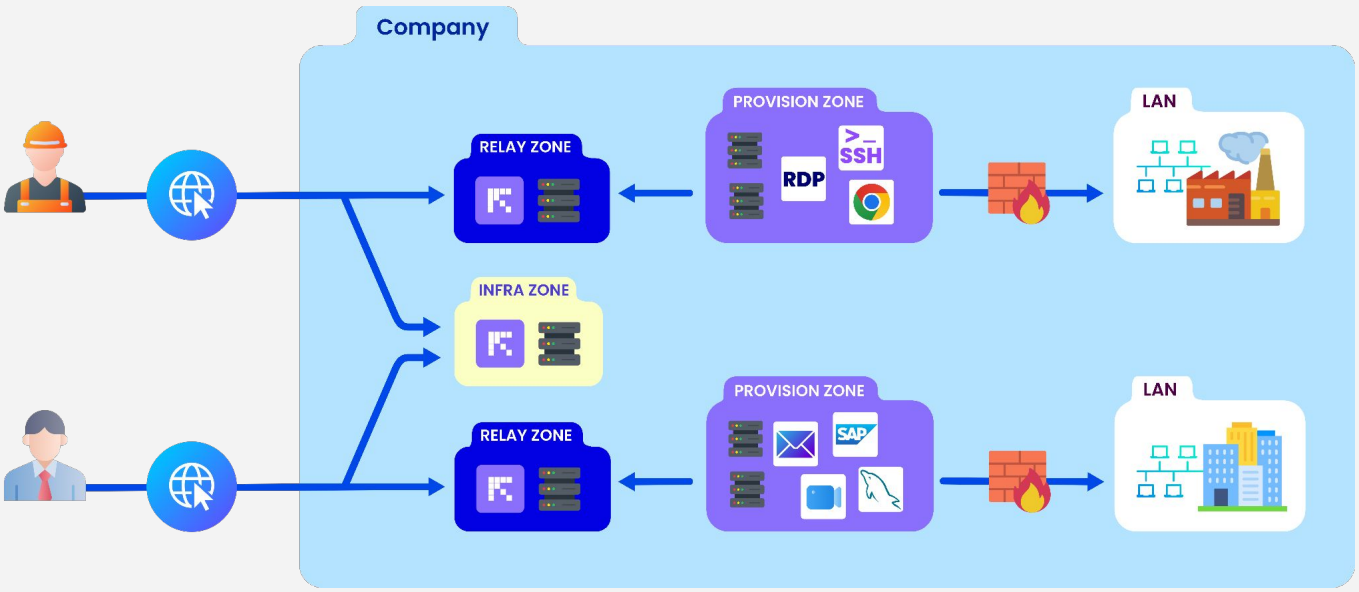
Solutions

Each third-party has **its own Relay Zone** and **Provision Zone**, ensuring complete isolation of access and traffic.

Each Provision Zone is connected to its **dedicated LAN** through a firewall, ensuring strict segmentation, fine-grained traceability, and **total permission control**.

This model is ideal for high-stakes, multi-partner environments.

Example #2 Dedicated On-Premise Architecture Per Provider



Modularity & Scalability : customizable architecture

- ➡️ Ability to create dedicated access portals
- ➡️ Option to unify or separate Provision Zones
- ➡️ Deployment on-prem or in a hybrid cloud according to needs

Results

Enhanced Security

Containerized sessions and **strict ZTNA** ensure third parties access **only necessary resources**, eliminating unauthorized access risks.

Simplified Access

Browser-based access reduces integration complexity for subcontractors, with **no need for configuration or updates** on their local machines.

Optimal Performance

External providers can access critical applications with **near-zero additional latency**, allowing them to work effectively even remotely.