DISPEL

Enclave

Flexible, secure networks

What Are Enclaves?

An Enclave is a network of virtual machines provisioned from one or many public and private clouds. Each virtual machine within an Enclave has a specific task—traffic routing, collaboration, a custom application, etc. Through the Dispel Management Console, you decide what you want in each of your Enclaves, where you want them deployed, and who should be given access.

Why Are They Useful?

Roughly half of our customers use Enclaves simply because they need versatile networks that they can readily launch, assign, and maintain from a management console. The other half use Enclaves to proactively defend their devices, datasets, SCADA systems, and unpatched infrastructure.

Why Are They Secure?

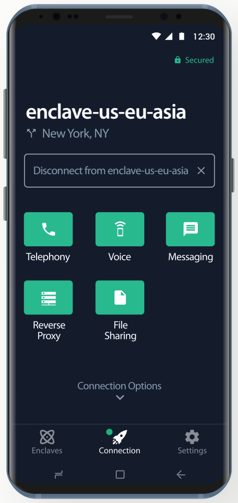
1. Enclaves are cloud agnostic. Virtual machines from your private clouds, as well as the 150+ data centers that belong to the world's 7 major commerical public cloud providers, can be used to build an Enclave.

2. The transmissions between virtual machines within an Enclave are protected with strong end-to-end encryption.

3. Enclaves automatically and unobtrusively swap out their virtual machines with fresh ones over time, meaning an adversary cannot locate and sustain target lock.

Together, these three traits mean that Enclaves both encrypt and cloak the resources contained within them, affording those assets sustained protection from targeted cyber attacks.

Connection Methods



Software

Dispel Application

Enables end-to-end encrypted connections to Enclaves.

Hardware

Dispel Wicket and Gateway

Connects any Internet enabled device (or group of devices) to a specific Enclave or, in the case of Gateways, a set of Enclaves.

Why are Enclaves important?

Protect The Essentials

Defend the things you care about most: data, teams, and equipment.

Sheer Convenience

Build and manage flexible, scalable, networks without adding staff.

Sustain Legacy Systems

Defend the unpatched and unpatchable parts of your infrastructure.

Protect Your People

Keep your people and their actions hidden from electronic detection.

Accelerate Collaboration

Work with people you don't completely trust in environments where they cannot harm you.

Keep Things Self-Contained

Design your networks to fit your workflows, rather than the other way around.

Technical Specifications

Encryption

Each link in an Enclave is protected by two layers of cascade ciphered AES-256 with independent 4096-bit keys used for the initial key exchange.

Polymorphic

Enclaves automatically swap out their constituent components with fresh ones over time, shifting their network topologies in the process.

Performant

70 Mbps throughput over cloaked transmission tunnels.

Self-Contained

Assets inside of an Enclave communicate exclusively over private IP space.

Multi-Factor Authentication

Enclaves are only accessible through at least two stages of authentication.

No Data Leaks

Enclaves are immune to IPv4, IPv6, WebRTC, and DNS leaks.