Today network infrastructure is just too complicated.

Enclave uses **Zero Trust** principles to simplify and automate network infrastructure.

Enclave saves organisations time and money, increasing agility and improving security.

https://enclave.io/

ENCLAVE

Examples of Enclave Users

Rabobank

NEXOR®

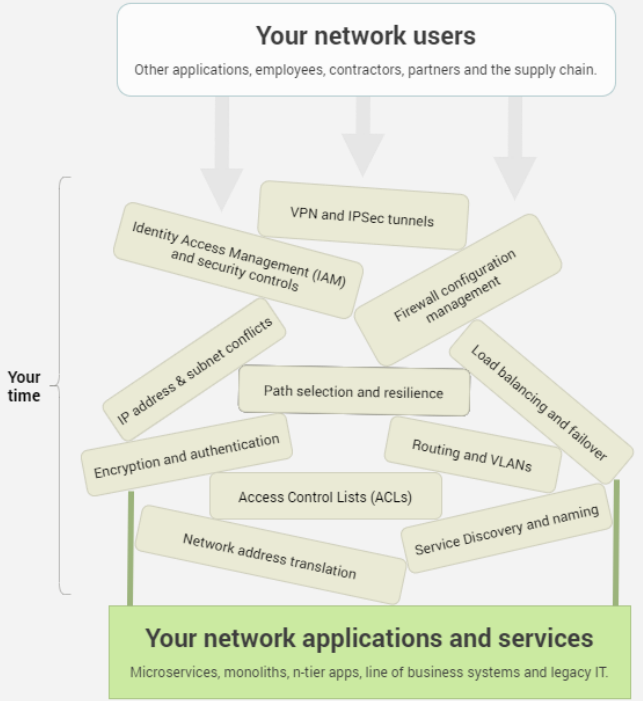
THALES

The problems the Enclave SaaS platform solves.

You need to get something done but the network just gets in the way:

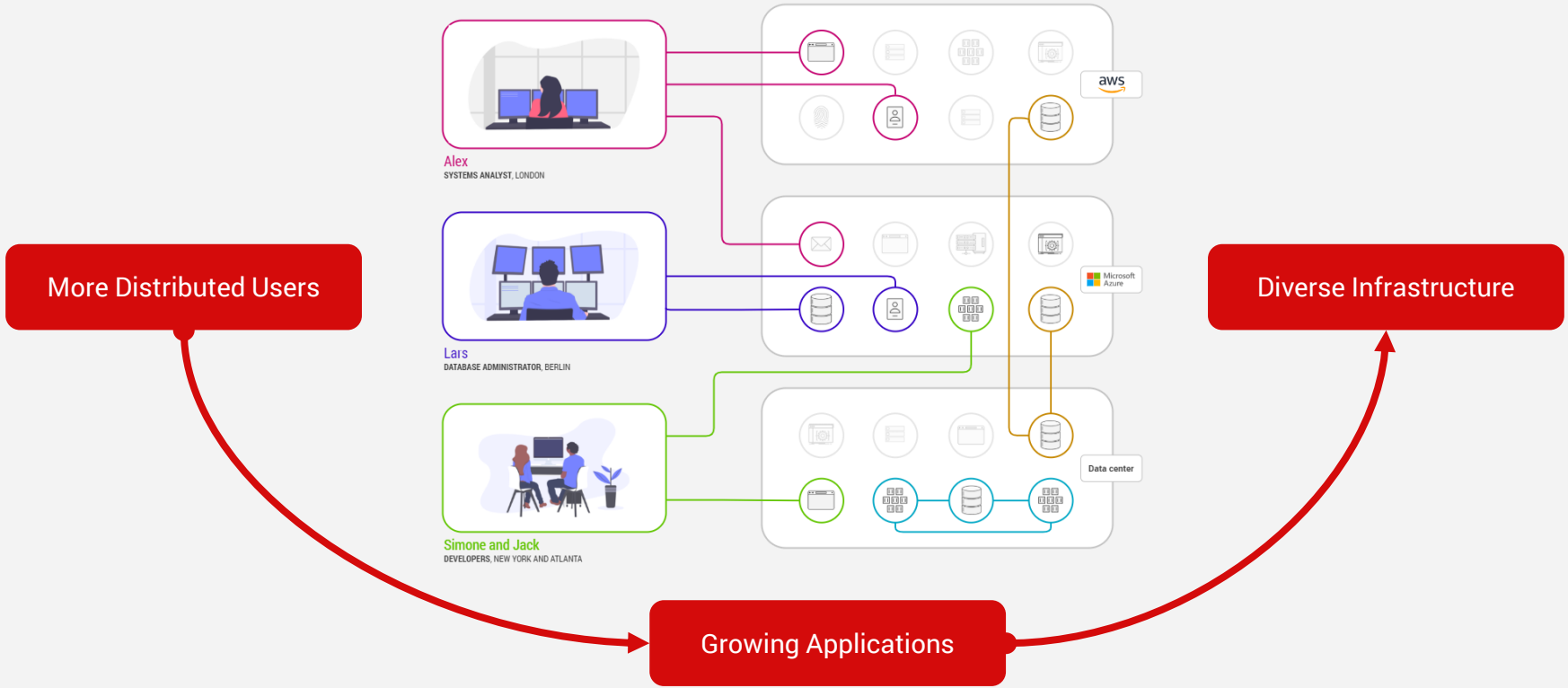
- *Configuring firewalls and VPNs.*
- *Managing IP addresses, subnets, ACLs, NAT.*
- *Routing tables, certificates and secret keys.*
- *VMware, containers, cloud and on prem systems.*
- *Hardware and middleware.*
- *Security planning and review.*

Enclave gets the network out of the way ,so you can focus on creating business value.



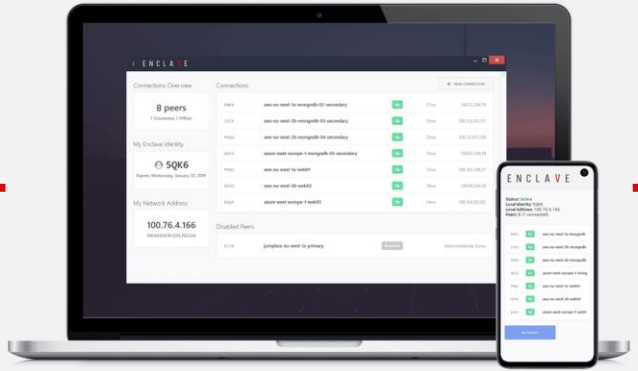
DevOps for your network.

The future will require better solutions...



DevOps for your network with Enclave.

Zero Trust, invisible network infrastructure.



Easy to Deploy

Enclave allows you to effortlessly connect your assets without ever needing to think about network configuration or firewalls.

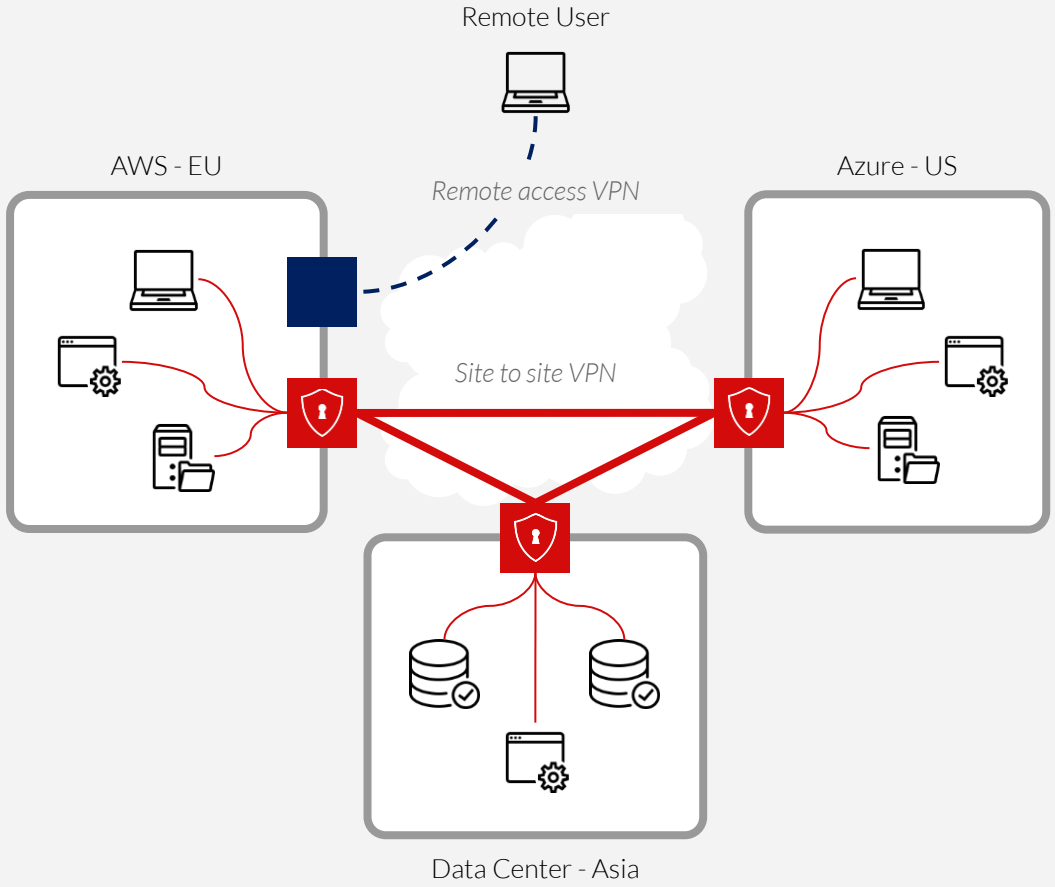
Secure by Design

With Enclave's Authenticate-then-Connect technology, your infrastructure is invisible, protecting you from attack.

Currently, Site-to-Site VPNs are the norm.

Normal connectivity is client to server with traffic routed through site-to-site VPNs. This creates three challenges:

- **Complex configuration** – Punching holes in firewalls and increased security takes engineering time
- **Visible front door** - VPNs become a point of attack
- **Private network access** - Often, once an attacker is in, they have access to whole network



Zero Trust Network Access (ZTNA)

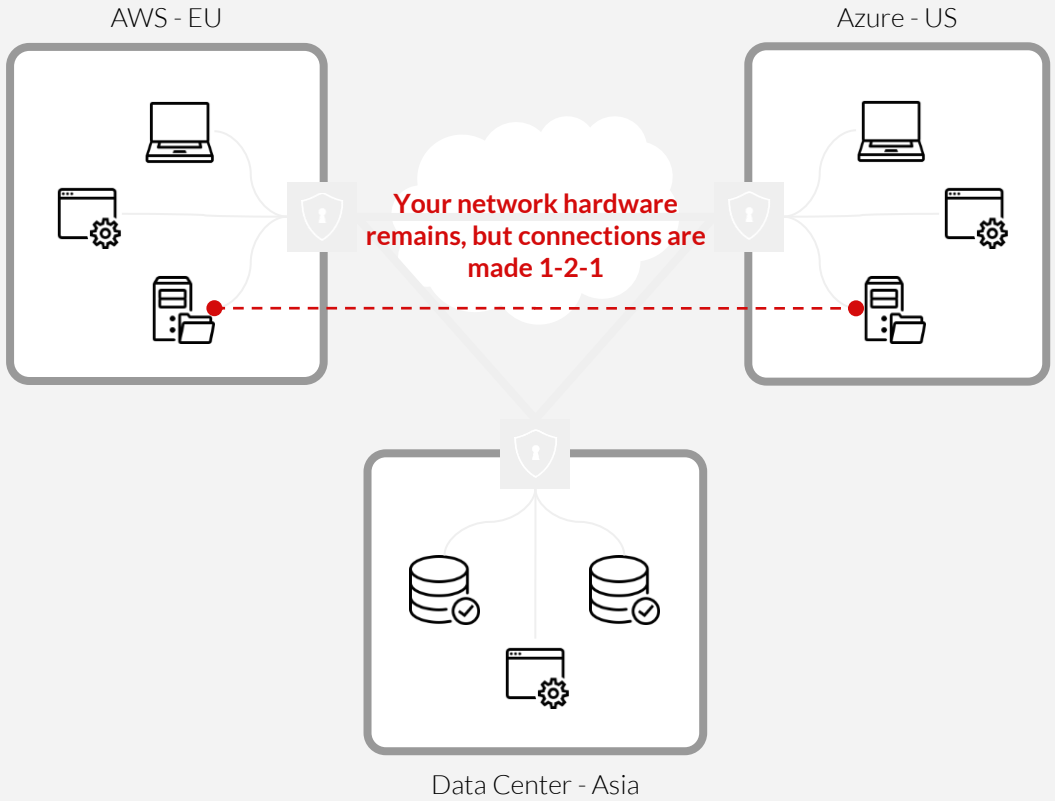
Enclave creates connectivity, with firewalls closed.

With Enclave, the hardware still exists, but we enable agility on top of it.

Key benefits:

- Authenticate then connect. Connections only after trust policies are met.
- Automated network management; set protocol “guard rails” in Enclave.
- Direct connections configured at a software level.
- No firewall configuration.
- End-end encrypted.
- Microsegmentation – reduce lateral movement risks.

Engineering tasks are massively reduced and security is improved.



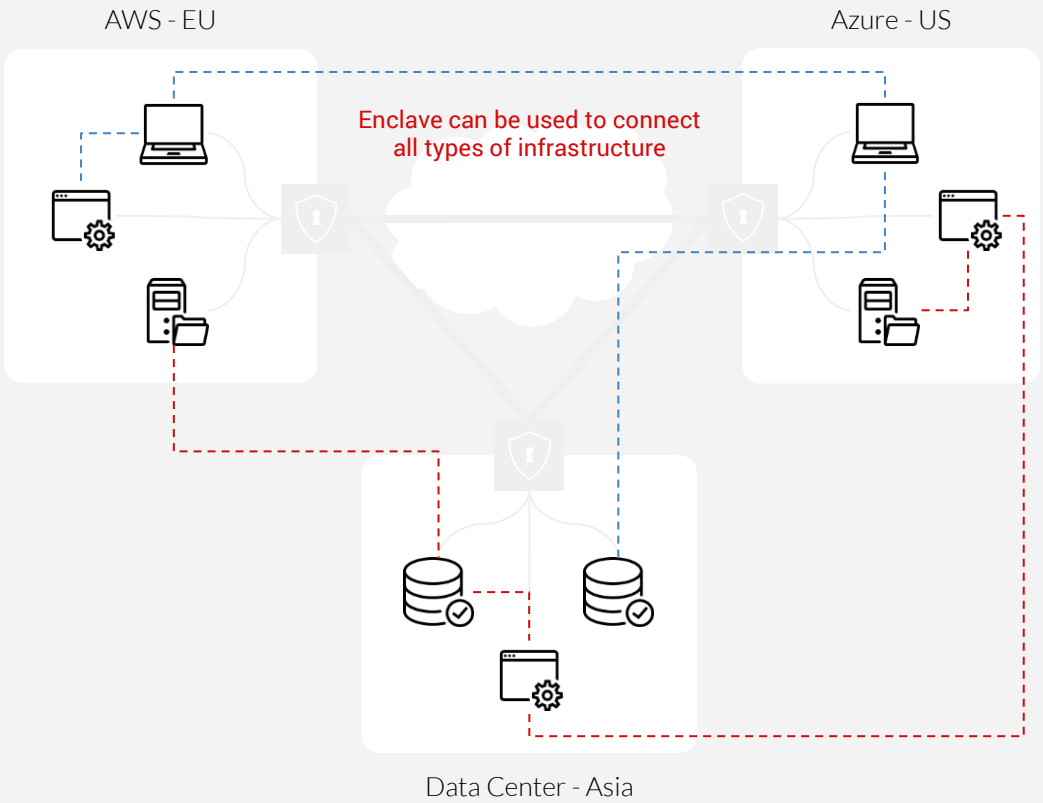
Connect and Microsegment all your infrastructure.

Connect all of your things across locations, vendors and tech stacks in the same way with a technology that just works.

Engineering tasks are massively simplified.

Example Use Case:

Network attached storage device running on-prem in the datacenter, that can push data to a windows cloud server, which is then accessed by an off-site remote staff using MACs and specific on-site colleagues vis their phones.

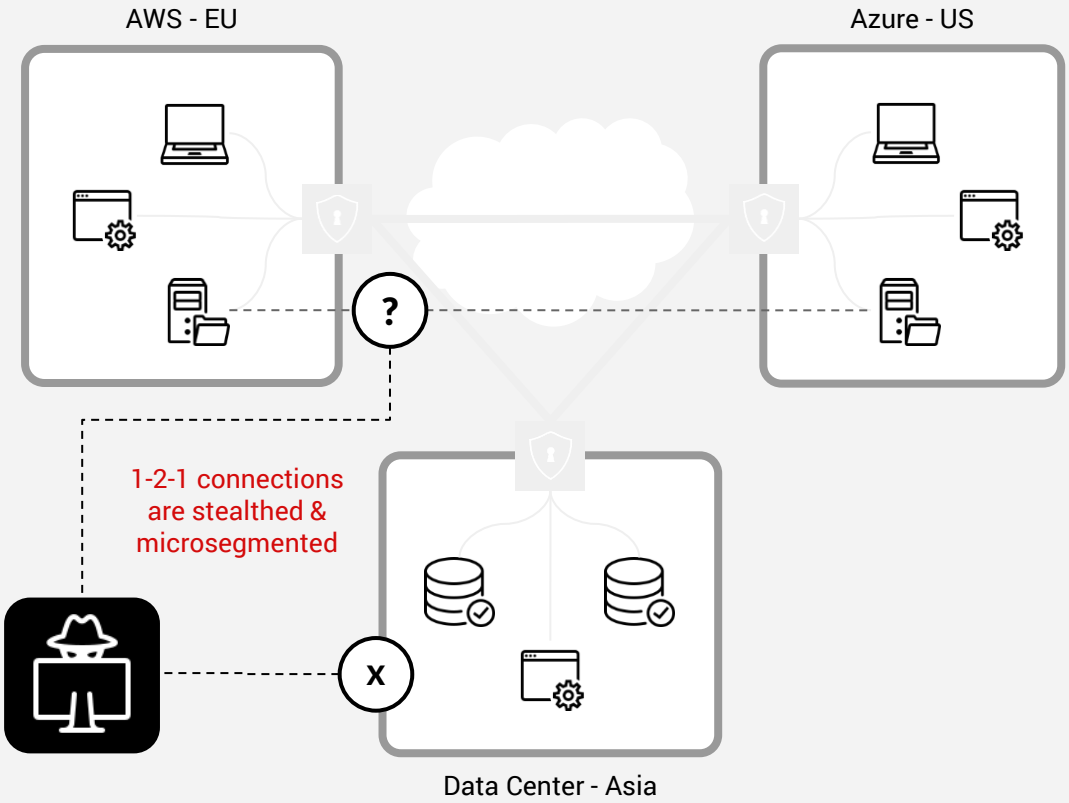


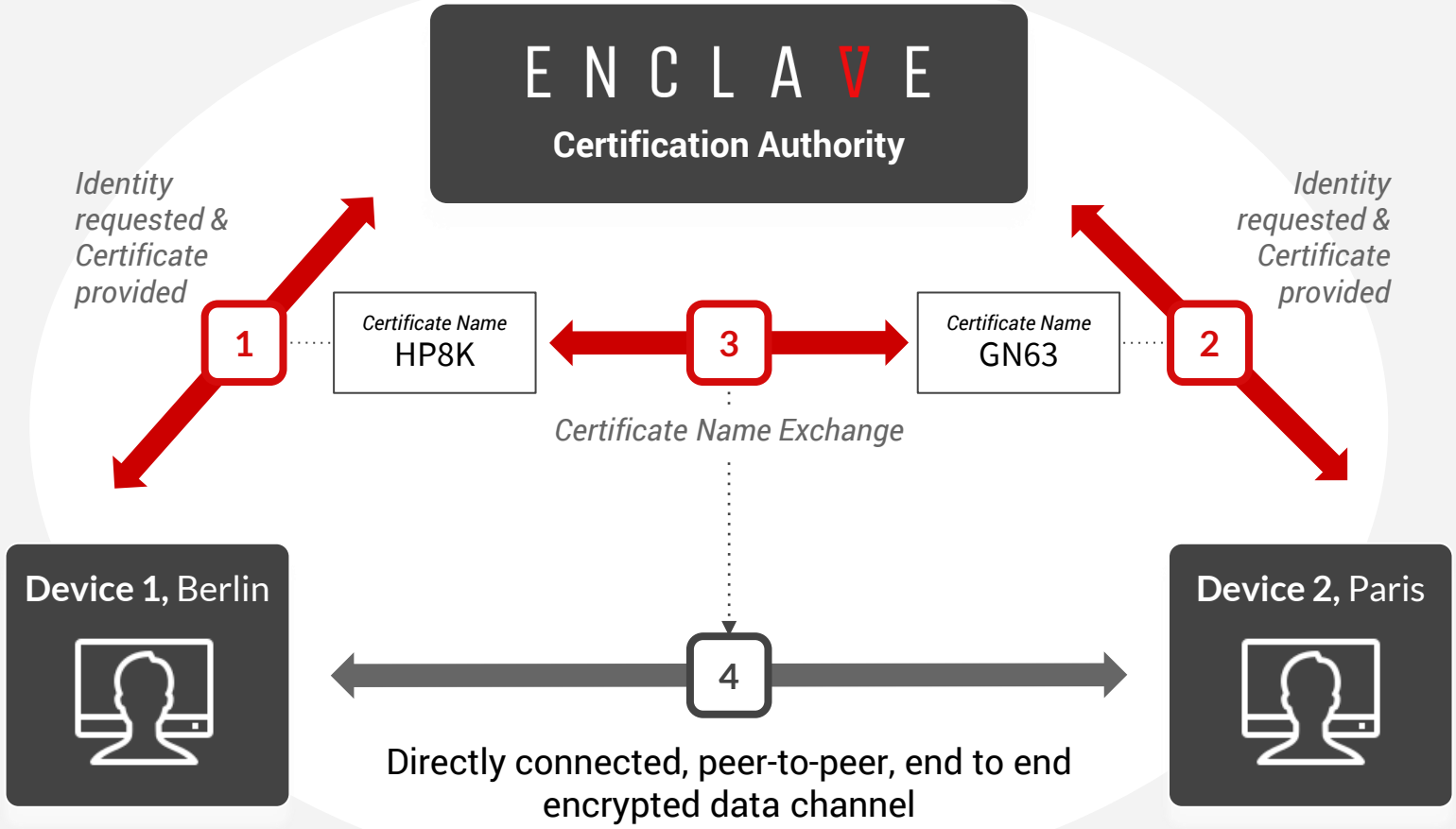
ZTNA - with no “front door” to attack.

Authentictae then connect - Enclave connections are established as client-client connections. Firewalls stay closed, raising the level of security of the network.

Connections are invisible and micro-segmented. Its harder to attack something you don’t know is there.

Reduce the risk and scale of security incidents.




ENCLAVE
Certification Authority
Identity requested & Certificate provided
Identity requested & Certificate provided
1
2
3
Certificate Name
HP8K
Certificate Name
GN63
Certificate Name Exchange
Device 1, Berlin
Device 2, Paris
4
Directly connected, peer-to-peer, end to end encrypted data channel

Deploying Enclave is simple

Install on Devices

Request Certificates

Exchange Certificates

Direct, Peer to Peer Connection

2 minutes to deploy

No need for:

- ➔ Firewall configuration
- ➔ Setup and Teardown
- ➔ Beefed up security

A simple pricing structure...

Core

Free

Up to 10 systems

Great for individuals, small teams and mini-projects. Get Core + for £40/month for up to 100 enrolled systems.

Teams

Starts at £250/month

Sold in packs of 50 systems

Great for teams, centralised management and policy based deployment.

Enterprise

Custom Pricing