Pelion

Architecture & Infrastructure

A guide to the infrastructure behind Pelion's reliable global connectivity

Pelion.com

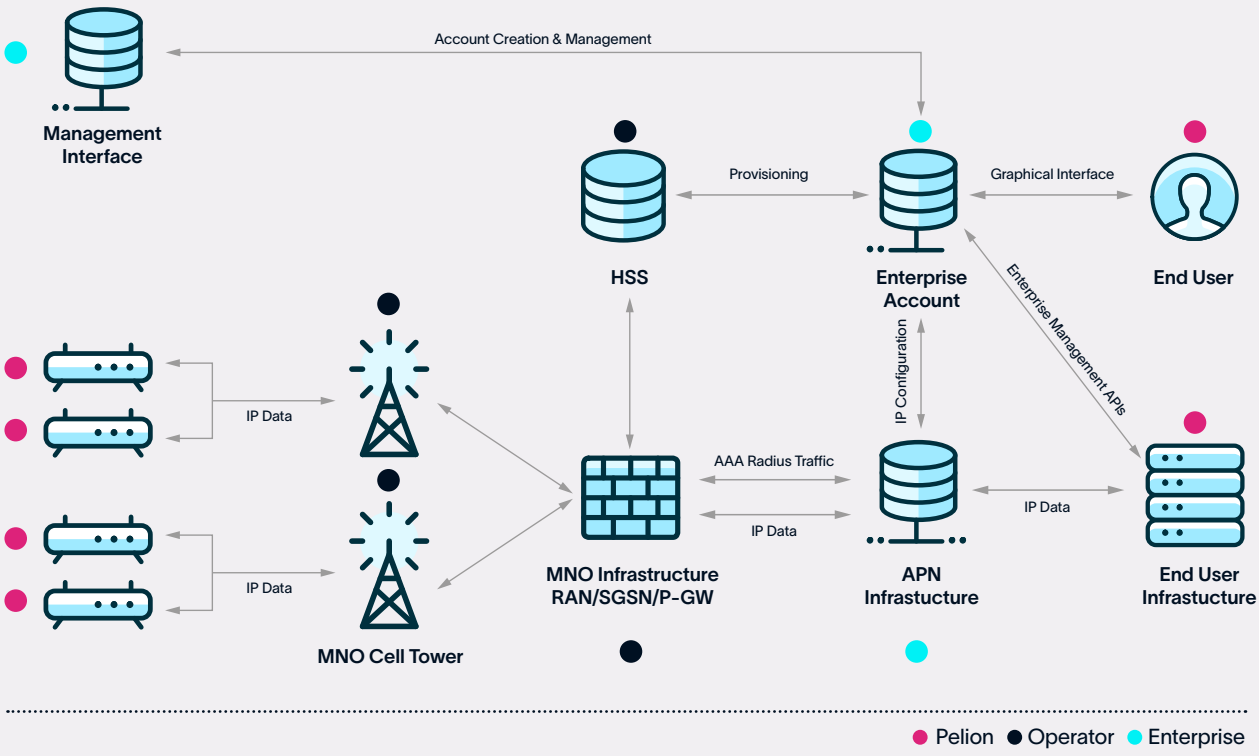
Pelion

ARCHITECTURE & INFRASTRUCTURE

Connected from the Ground Up

Pelion makes it easy to connect and manage devices all over the world.

Behind the scenes, it's built on a solid on-premise, modern infrastructure designed to keep your data secure, your devices connected, and your operations running smoothly – no matter how big you grow.



Cellular Connectivity and Operator Integration

Devices such as smart meters, sensors, and embedded modules connect using Pelion SIMs or eSIMs across multiple mobile network operators (MNOs) worldwide.

Pelion integrates with each operator at both the network level and the API level, allowing all subscriptions – regardless of operator – to be managed centrally through the Pelion Portal. This enables consistent service behaviour, unified provisioning, and global visibility from a single platform.

All operator traffic is terminated directly into Pelion's datacentres, where it enters Pelion's private network environment.

Why It Matters: Your devices stay connected worldwide with one simple system, giving you easy control and visibility from a single platform.

Pelion's Secure Network

All traffic entering Pelion's infrastructure passes through dynamically managed firewalls before reaching the secure core. This is where all critical network functions are executed and protected.

Within the secure network, Pelion provides:

- RADIUS-based AAA services (Authentication, Authorisation, Accounting)
- Private IP address allocation and management
- Traffic routing, segmentation, and policy enforcement
- Live usage monitoring and network visibility

The network (including RADIUS and routing services) operates independently from the Pelion Connectivity Management Portal. This separation ensures that network connectivity and authentication services continue to function even if management or API services are unavailable.

Pelion's secure network is deployed using an N+1 resilience model in geographically separate datacentres. Both UK and US datacentres contain at least two independent sites, enabling full cross-site failover for customers who require geographic redundancy.

Within each datacentre, firewalls, routers, and VPN concentrators operate in redundant pairs. This design removes single points of failure and ensures that even customers using a single standard VPN connection remain protected from localized hardware or software issues.

The Pelion network operates as an integrated software defined firewall ensuring traffic segregation and policy enforcement across the traffic path. Each required element is dynamically updated as customer routing, device subnets, or policies change – maintaining segmentation and security without manual intervention.

Why It Matters: Your IoT traffic is always safe, and your devices stay online, even if parts of the system have issues.

Optimized Switching and Traffic Flow

Pelion's network is designed to handle your data quickly, reliably, and securely. Once traffic enters the secure network, it passes through the switching layer, which controls how data moves between devices, operators, and core services.

This layer is built for high performance and resiliency, ensuring traffic is monitored continuously, segregated by customer, and routed efficiently.

By isolating different types of traffic – such as authentication versus data flows – Pelion can quickly identify and resolve issues while maintaining uninterrupted service.

By implementing redundant switching and connectivity across all datacentre sites, Pelion ensures that in the event of a component or site failure, traffic automatically continues through an alternative path, ensuring seamless operation.

Why It Matters: Your device data moves quickly and reliably, keeping everything running smoothly without interruptions.

Pelion's Datacentres

Pelion designs, builds, and operates its network infrastructure in-house, giving us full control over performance, security, and scalability.

By owning both the architecture and the equipment, we ensure a highly efficient, modern connectivity solution that can evolve quickly as technology and customer needs change.

We maintain a physical datacentre presence across diverse geographic regions in the UK and the US, with primary sites in London, Manchester, Austin TX, and Las Vegas NV.

This distributed footprint provides resilience, low-latency access, and regional proximity for customer deployments.

Our UK and US datacentre deployments each follow an N+1 resilience model. While the design and operational processes are consistent across regions, the networks are managed independently.

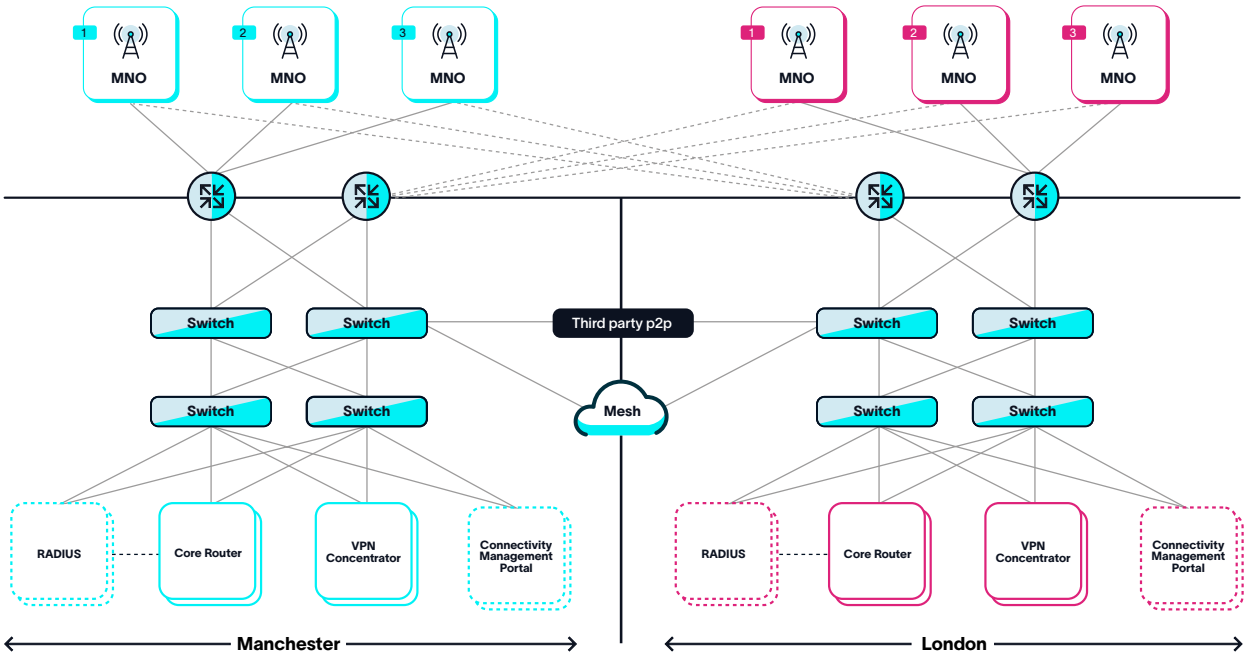
This separation ensures that UK and US data remains safely and legally segregated and allows us to manage relationships with different mobile network operators on a regional basis.

Despite this deliberate segregation, data can still be delivered wherever it is needed. This simplifies policy management for customers while preserving bandwidth and performance.

Operating our own physical infrastructure means we take direct responsibility for outages, upgrades, and capacity scaling.

This ownership keeps our hardware and platforms to a consistently high standard and enables rapid changes without reliance on third-party providers.

We continuously enhance our technology, routing, and hardware, trialling new architectures at small scale before systematically rolling them out across all four primary sites.



Why It Matters: You benefit from predictable performance, strong data governance, and a network that can adapt quickly – without the delays or compromises of third-party infrastructure.

Global Connectivity That Just Works: Pelion's Connectivity, Network & Routing Logic

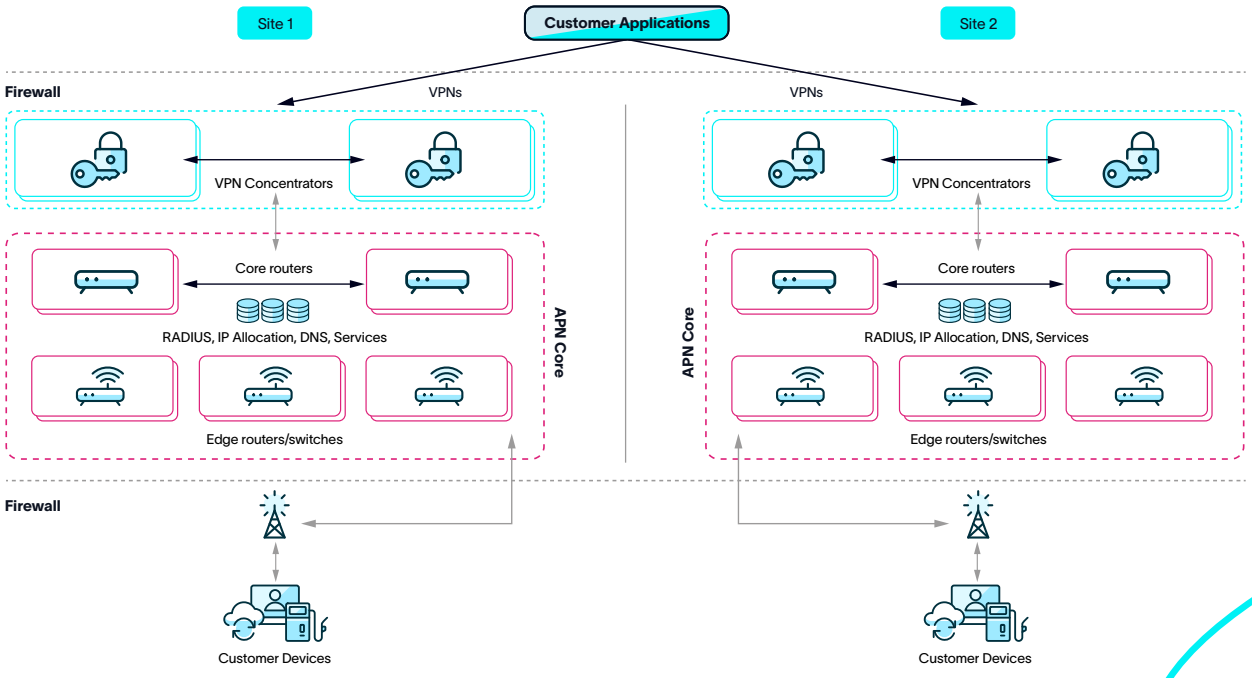
Pelion gives you access to over 600 networks in more than 150 countries, all through one global SIM and a single global APN.

That means your devices can connect wherever they are, without the hassle of switching SIM cards or managing multiple network providers.

Key features include:

- **Network redundancy:** Critical network systems such as routers and VPN concentrators (VPNCs) run in redundant pairs and are active at the same time. They use high-availability technologies like CARP (a protocol that allows devices to share addresses and take over instantly) to balance traffic and ensure seamless failover.
- **Dual-site and multi-site resilience:** Operator connections are delivered into multiple, geographically separate datacentres. Traffic is automatically routed between sites using BGP (the protocol that selects the best available network path) if a site or link becomes unavailable.
- **Operator redundancy:** Resilience is built into all operator connection types, including leased lines, encrypted VPNs (IPSec), and virtual tunnel integrations. Traffic is load-balanced across these connections to maximize uptime and stability.

This ensures that Pelion handles all routing, backhaul, and failover, letting you focus on your devices rather than network management.



Why It Matters: Your devices connect anywhere in the world, with built-in backups that prevent downtime and let you focus on your business.

Pelion

Streamlined and Secure: Data Flow, Monitoring, and Control

Pelion separates how you manage connections from how your devices send data.

Through the Pelion Portal and its APIs, you can activate SIMs, set up alerts, monitor data usage, and link everything to your existing business systems.

Meanwhile, your device data flows securely via private network to wherever you need it: a cloud platform, data warehouse, or on-premise systems.

Continuous end-to-end monitoring and alerting ensures that if any component or link experiences degradation, Pelion's automation instantly recovers internal service while notifying internal teams for triage and action.

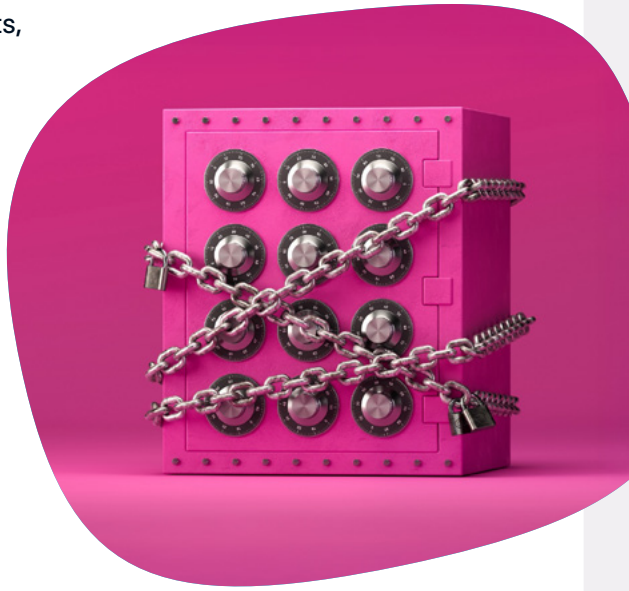
So, you can stay in full control of your connectivity, while your devices send data quickly and securely wherever it's needed.

Why It Matters: You can see and manage your device activity while your data flows safely to where it's needed, with automatic problem recovery.

Security You Can Trust: Multi-Layer Protection for Devices, Data & Networks

Pelion provides multiple secure connectivity methods to suit different deployment requirements:

- **Policy-Based IPSec:** Encrypts traffic between defined subnets, ideal for simple site-to-site connections.
- **VTI IPSec:** Route-based tunnels that support overlapping subnets and dynamic BGP routing – perfect for cloud-based services or complex networks.
- **OpenVPN:** Certificate-based, ad-hoc secure access for engineers or service visits, with self-service management of profiles.
- **Direct Inbound Network Access (DINA):** Authenticated, temporary access to subscribers without exposing public IPs.
- **Data Centre Connect:** Direct private links from datacentres to customer infrastructure for low-latency, high-performance applications.



Each connectivity option can be configured for varying levels of resiliency – from basic single-tunnel failover to advanced multi-tunnel, multi-site configurations – depending on the customer's infrastructure and requirements.

Why It Matters: Your devices and data are protected with multiple options, so your IoT network stays secure no matter the setup.

Built to Grow with You: Scalability & Capacity Planning

Pelion is built for growth – whether you're managing a small test deployment or millions of connected devices across the globe. Our platform is designed to scale seamlessly with your needs, ensuring you can expand without friction.

The Pelion Portal gives you full visibility and control over your IoT ecosystem. From activating SIMs and managing data plans to monitoring usage in real time, everything is automated and accessible from a single interface.

We support all major IoT network types (4G, 5G) as well as NB-IoT, LTE-M, and Cat-M1, allowing you to optimize coverage, power efficiency, and cost depending on your deployment requirements.

Capacity planning at Pelion is an ongoing, robust process. Taking inputs from across Pelion, our customers and their growth plans we build a roadmap of expansion that meets our network needs today and into the future.

We work collaboratively to ensure that your deployments are supported at every level, including the right IP allocation, geographic coverage, and expected data volumes.

This comprehensive approach helps match your operational needs with the right network configurations and data management strategies, so you can scale confidently as your IoT ecosystem grows.

Why It Matters: Your IoT system can grow as much as you need without delays or complications.

Data on Your Terms: APIs, Data Stores & Flow Management

Pelion's APIs are the backbone of our integration and automation capabilities.

They run on secure, resilient instances that always follow our capacity management process, ensuring consistent performance even as your IoT deployments grow.

These APIs provide programmatic access to every major function of the Pelion Portal, letting you control SIMs, manage data usage, and feed insights directly into other business systems.

On the data side, Pelion's infrastructure is designed to move information seamlessly into your chosen environment. Whether you're using a cloud data lake, real-time streaming tools, or on-premises analytics platforms, Pelion provides connectors and data flow options that balance flexibility and control.

All data stores are secure and segregated by customer to meet privacy and regulatory requirements, such as GDPR. Data is retained only for the appropriate duration, and all data held internally is backed up in real time on its specifically designed, segmented network across dual sites to ensure durability and continuity.

This approach means your IoT data remains fully yours – accessible, secure, and ready to power the insights your business relies on.

See our full Pelion API documentation **here.**

Why It Matters: You always have access to your data, in the way you need it, while it stays safe and private.

Pelion

Glossary:

Term	Description
AAA	Stands for Authentication, Authorisation, and Accounting. This is RADIUS protocol and describes how a network checks a device's identity, decides what it is allowed to do, and records how much it uses the network.
APN	Access Point Name. A setting on a device that tells it which mobile data network to connect to and how to reach private or secure services.
API	Application Programming Interface. A way for software systems to talk to each other automatically, allowing customers to manage devices, data usage, and settings without logging into a website.
BGP	Border Gateway Protocol. A system that helps large networks decide the best path for data to travel across its network or the internet.
CARP	Common Address Redundancy Protocol. A method that ensures network services stay available by switching traffic to a backup system if the main one fails.
Cat-M / LTE-M	A mobile network technology designed for IoT devices that use small amounts of data and need good battery life, such as trackers or sensors.
DINA	Direct Inbound Network Access. A secure way to temporarily access a device without giving it a public internet address.
eSIM	A digital version of a SIM card that allows mobile plans to be added or changed remotely without physically replacing the SIM.
eUICC	The physical chip inside a device that stores one or more eSIM profiles. Often used interchangeably with "eSIM," but technically refers to the hardware.
IP Address	A numerical label given to a device so it can send and receive data on a network. It can change over time and may be private or public. Every device/server/switch/website/router in the world has an IP address.
IPSec	Internet Protocol Security. A method for securely encrypting data traveling between networks.
MNO	Mobile Network Operator. A company that owns and runs mobile network infrastructure, such as cell towers and radio networks.
MVNO	Mobile Virtual Network Operator. A company that sells mobile connectivity using an MNO's network, often adding extra services or security layers.
N+1 Redundancy	A design approach where one extra system is available as backup to prevent downtime if something fails.
NB-IoT	Narrowband IoT. A network technology designed for very low data usage devices like meters and sensors.
RADIUS	A system that controls which devices are allowed on the network, assigns them access, and tracks their usage.
RAID	Redundant Array of Independent Disks. A way of storing data across multiple hard drives to prevent data loss
SIM	A small piece of hardware in a device that identifies it on a mobile network and enables connectivity.

Pelion

Glossary:

Term	Description
VPN	Virtual Private Network. A secure connection that encrypts data between devices and private networks.
VPNCs	Virtual Private Network Concentrators. Devices that manage and terminate large numbers of VPN connections.
VTI	Virtual Tunnel Interface. A logical network interface used to manage secure tunnels more easily.

Pelion

Global IoT Connectivity Made Effortless

Contact us today or visit our website

hello@pelion.com | Pelion.com