Pelion

Reliability

An overview of how Pelion's architecture ensures reliable global connectivity

Pelion.com

Pelion

RELIABILITY

Connectivity You Can Count On

When it comes to your IoT partner, connectivity should be a given – not a gamble.

That's why we offer an industry leading 99.995% reliability, so you can stress less and sleep easier.

We back this up with global coverage and multi-operator support, so your devices stay online even when one network struggles.

Plus, we provide support designed for your needs, backed by rapid response and reliable incident handling.

Architecture for Resilience

Pelion's network is designed with reliability at its core.

Every critical component is architected with N+1 redundancy (a design approach where one extra component is always available to mitigate any failures), so nothing depends on a single component.

High-availability network design

- **Multiple datacentres:** Pelion runs more than one datacentre per region, so services never depend on a single site.
- **Resilient network entry points:** All connections into the core network use dual paths (primary and backup), automatically switching if one fails.
- **Resilient core systems:** Routers and VPN concentrators are paired using high-availability technologies (e.g. CARP), enabling automatic failover if one device goes down.
- **Active-active operation across sites:** Switching, routing, and firewall layers run simultaneously across both datacentres, ensuring multiple traffic paths without rerouting.
- **Local high availability:** Components use local redundancy (e.g. RAID, virtualization clusters) to provide additional resilience within systems.

This means that if one element fails, another is already running and ready to take over instantly – keeping traffic flowing without interruption.

Why It Matters: Pelion's architecture is designed to ensure failures don't stop your devices from staying connected.

Dual Power as Standard

- Each datacentre rack is equipped with two independent power circuits and Power Distribution Units (PDUs).
- Every device has two power supplies connected to independent power circuits.
- Power utilization is maintained at less than 80% to ensure adequate capacity during any times of increased load.

Why It Matters: Your devices and systems keep running even if one power source fails.

Operator Redundancy

- Every operator is integrated using geographically resilient network paths, employing automatic failover controlled with BGP.
- All RADIUS (the service which controls access to the Pelion network) is hosted at each network entry location and uses local load balancing to ensure high performance in standard operation and high load scenarios.
- Pelion integrates with Operators in the most appropriate way for each solution:
  1. A Leased Line into each regional data centre, carrying both data and RADIUS traffic
  2. IPSec into each regional data centre, carrying both data and RADIUS traffic
  3. L2TP integration including data over one of the above and RADIUS from 4x load balanced LACs across the sites.
- Supplier diversity is employed at all possible levels, avoiding dependency on any single vendor or network path.

Why It Matters: Your connections are resilient so devices can always communicate even if one operator fails.

Load Balancing

- Operators are available in geographically resilient data centre sites.
- RADIUS is load balanced locally within a data centre and geographically between sites; no matter which site services data traffic, RADIUS is available.
- Pelion provide high-capacity links between our data centre locations, ensuring that there is no degradation in performance should the preferred path be unavailable.

Why It Matters: Traffic is shared evenly so performance stays consistent no matter what.

Cross-Site Resiliency

If one datacentre becomes unavailable, the second site automatically takes the full load.

Designed for total failover

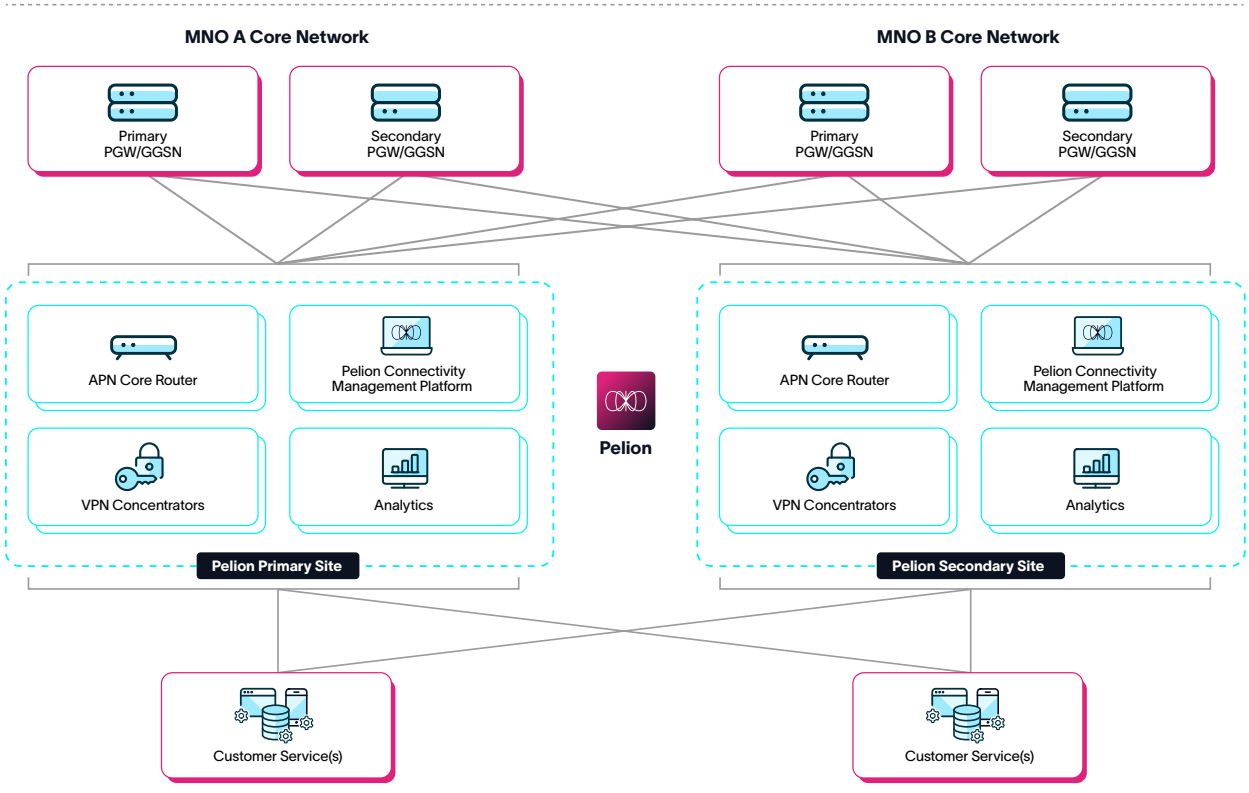
- Each site has capacity to handle 100% of traffic during an emergency.
- Edge ports run at 10 or 25Gb (appropriate for the connected service), with equivalent cross-site bandwidth.
- All core services are duplicated like-for-like in each site, with configuration management in place to ensure consistency of performance and availability.

Geographically-Redundant Data

All collected data is stored across Pelion's datacentres, ensuring consistency and availability even during regional disruptions.

Resilient cross-site mesh

- All sites are interconnected through a mesh network.
- Links are delivered by multiple separate network suppliers for true provider diversity.
- If any provider's link fails, the alternate link carries all traffic automatically.



Why It Matters: Your data and devices stay fully operational even if a site goes down or a connection fails, because traffic automatically switches to other locations and your data is safely stored in multiple places.

Pelion

Platform and Virtualization Resiliency

Virtualized Services

In addition to dedicated physical systems being used in the critical network path, Pelion leverages virtualization and containerization technologies to provide resilient, scalable infrastructure to support key services.

In addition to application-level high availability, hypervisor clusters are used to allow seamless recovery in the event of a hardware failure.

Why It Matters: If part of the system fails, your IoT platform recovers automatically so operations continue without interruption.

Benefits of Cellular Fallback & Resiliency with Pelion

1

Operational Continuity

In business-critical IoT applications, fallback and resiliency ensure services remain operational without downtime.

2

Scalability

Ensures continuous connectivity, allowing businesses to scale with confidence while maintaining reliable performance.

3

Enhanced Reliability

Multi-network connectivity improves IoT reliability by leveraging multiple carriers and network technologies.

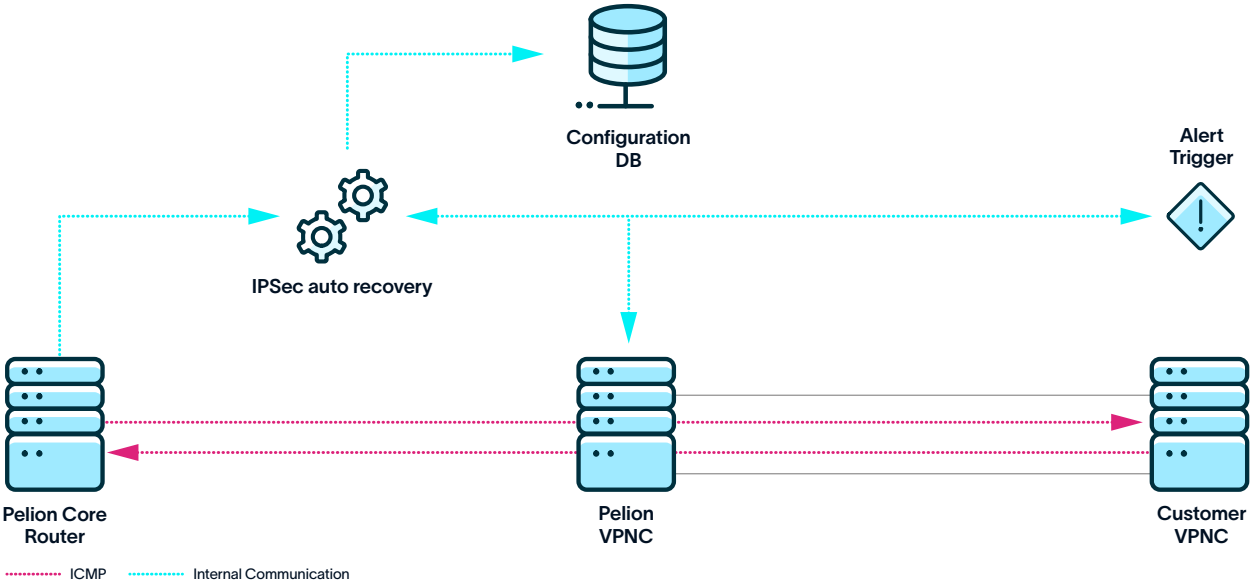
Incident Management & Recovery

Pelion continuously monitors its infrastructure so that if a problem occurs, automated systems react immediately to fix it.

- Automated systems detect and respond to failures instantly.
- Traffic is rerouted, services failover, and redundant components activate without user intervention.
- Internal engineering teams receive immediate alerts for triage and follow-up.

Internally, Pelion operates a robust and streamlined recovery management process, involving key experts from across engineering and support, ensuring a coordinated and efficient resolution.

This combination of automation and real-time visibility minimizes disruption and keeps your IoT operations predictable.



Building for The Future

Connectivity environments change fast – new networks, evolving standards, increasing device counts.

Pelion stays ahead by adopting technologies like eUICC SIMs, higher availability transport layers and adding new networks globally.

You're not only buying today's stability – you're investing in tomorrow's capability.

Whether you scale out across thousands of devices, move into new regions or adopt new standards, Pelion ensures your connectivity foundation stays ready for what's next.

Why It Matters

Pelion's architecture is built for peace of mind.

When reliability, performance and support are all wrapped into one offering, you can focus on building your business – not on firefighting connectivity problems.

With Pelion's architecture, redundancy, monitoring, uptime promise and future ready approach, you get a partner built for IoT at scale.

Your devices stay connected, your data stays safe, and your services keep running – even when unexpected issues arise.

Let your devices do the work you need.

Let Pelion manage the connectivity behind them.

Pelion

Glossary:

Term	Description
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.
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.
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.
IPSec	Internet Protocol Security. A method for securely encrypting data traveling between networks.
L2TP	Layer 2 Tunneling Protocol. A way to create secure connections between networks, often used in VPN setups.
LAC	L2TP Access Concentrator. A network component that receives secure tunnel connections from devices or partners.
MNO	Mobile Network Operator. A company that owns and runs mobile network infrastructure, such as cell towers and radio networks.
N+1 Redundancy	A design approach where one extra system is available as backup to prevent downtime if something fails.
PDU	Power Distribution Unit. A device that safely distributes electrical power to servers and network equipment.
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.
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.

Pelion

Global IoT Connectivity Made Effortless

Contact us today or visit our website

hello@pelion.com | Pelion.com