DUAL-USE CAPABILITIES:

Sitehop's Crypto-Agile, Ultra-Low-Latency Platform

Sitehop's hardware-enforced encryption platform delivers a unique blend of dual-use capabilities, addressing both today's and tomorrow's secure communication needs across commercial, government, and defence sectors. At the core, we remove the traditional performance penalties of security - latency, throughput bottlenecks, and operational cost, unlocking deployment opportunities that were previously out of reach.

Commercial and CNI Impact

In the commercial space, especially telecoms, financial services, and critical national infrastructure (CNI), the historical blockers to security adoption remain:

- Increased latency from encryption
- Throughput reductions
- High total cost of ownership and operational friction

Sitehop's fully FPGA-based data path enables line-rate encryption with sub-microsecond latency, allowing security to be deployed without compromising network performance. This is especially critical in environments such as:

- High-speed backbones
- Customer-premises edge deployments
- Cloud interconnects

Moreover, our crypto-agile architecture allows for rapid integration of evolving cryptographic standards, including PQC, ensuring long-term resilience.

Government and Defence Value

For defence and national security, priorities extend beyond performance and cost:

Attack surface reduction
Entire symmetrical encryption operation occurs within an FPGA, avoiding the vulnerabilities of general-purpose processors.

Custom algorithm support
Governments can deploy sovereign or classified encryption mechanisms at high throughput and ultra-low latency.

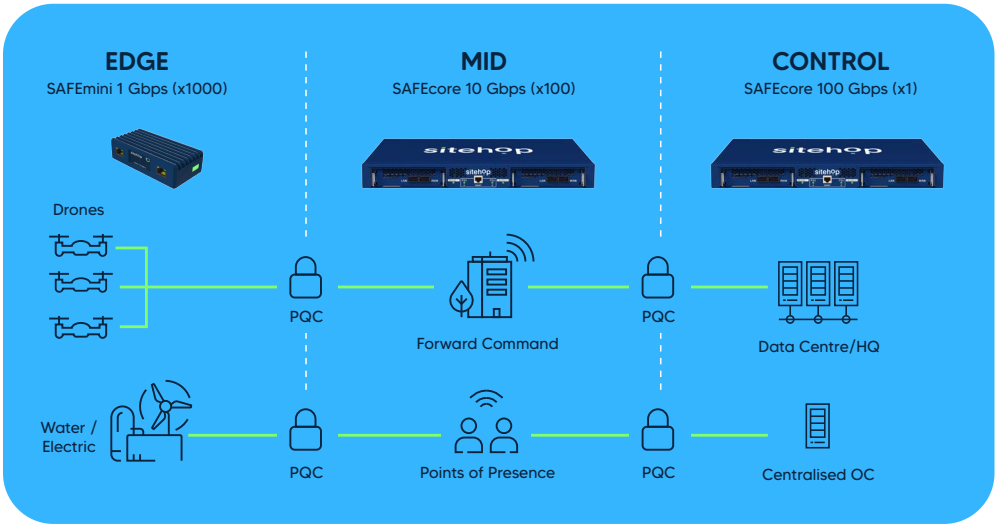
Secure mesh and point-to-multipoint (P2MP) support
Sitehop integrates seamlessly into complex topologies and with existing crypto infrastructure.

On-premises management
Our solution supports full deployment in isolated environments.

sitehop

Multi-Domain, PQC Security

Core to edge hardware-based security.



Quantum Resilience:
Solving Tomorrow's Threats Today

The quantum threat is no longer theoretical. Nation-states and enterprises must prepare for a future where today's encryption can be broken by quantum computers. Sitehop addresses this head-on with:

- **Built-in PQC support:** Leveraging NIST-aligned post-quantum algorithms, we provide quantum-safe encryption options ready for deployment now.
- **Crypto agility by design:** Our architecture allows cryptographic schemes to be updated as standards evolve whether quantum-safe or hybrid classical/ PQC modes.
- **No latency trade-off:** Sitehop delivers PQC-enabled security without the performance hit normally associated with post-quantum algorithms.

This makes Sitehop ideal for organisations planning long-lived or high-sensitivity communications, where forward secrecy and quantum resistance are paramount.

Unified Advantage:
Real-Time Security Without Compromise

From commercial CNI to classified defence systems, the problem is the same: securing real-time communication links without performance degradation. Sitehop delivers the world's lowest-latency, FPGA-based encryption, with future-proof crypto agility and PQC-readiness built in.

Whether protecting today's telco data flows or tomorrow's sovereign secrets, Sitehop enables security without compromise.

Sitehop.
Engineered for resilience. Built for the future.

Sitehop Limited

63 Napier Street, Sheffield S11 8HA | 0114 478 2366 | info@sitehop.com | **sitehop.com**