DEFENCE CHEAT SHEET

Building Bulletproof Network Encryption for Defence

A one-page field guide: the mission, the challenges, and how Sitehop closes the gap.

Every mission depends on trust in a connection nobody sees, until the moment it fails. Sitehop protects that connection, hardware-enforced, deployed inline, and built to keep working when conditions are jammed, degraded or denied.

On the Radar: Key Defence Challenges

STRATEGIC DEFENCE

- Fragmented forces and coalition partners
- Rising mission complexity and data volume
- Growing exposure across supply chains

COMMS + NETWORKING

- Disconnected, tactical-edge operations
- Contested, jammed or denied connectivity
- Secure data sharing across coalitions

ENCRYPTION + PQC

- Cryptographic debt in legacy platforms
- PQC readiness without added latency
- Crypto agility without rip-and-replace

Three Critical Pillars of Defence Encryption

Interoperability

Cross-domain microsegmentation shares exactly what's needed, without flattening trust boundaries.

Mission Outcomes

Hardware-assured, sub-millisecond encryption keeps missions intact under contested conditions.

Risk Assurance

A crypto-agile overlay protects legacy platforms and supply chains.

How Sitehop Delivers on the Mission: The Technical Approach

High-level capabilities behind the three pillars:

Hardware-Enforced Encryption
FPGA-based, not software

Inline Overlay Deployment
No rip-and-replace required

Multi-Gigabit Performance
1, 10 and 100 Gbps options

Low, Predictable Latency
Sub-millisecond under load

Crypto-Agile, Hybrid-Ready
Built for the PQC transition

Centralised Management
Configure and monitor from one place

Ready to close the gap in your network encryption? Talk to Sitehop.