ARQIT

The Hidden Gap: How IoT and the Military Can Achieve Post-Quantum Security

Connor Spangler
Quantum Security Solutions Architect

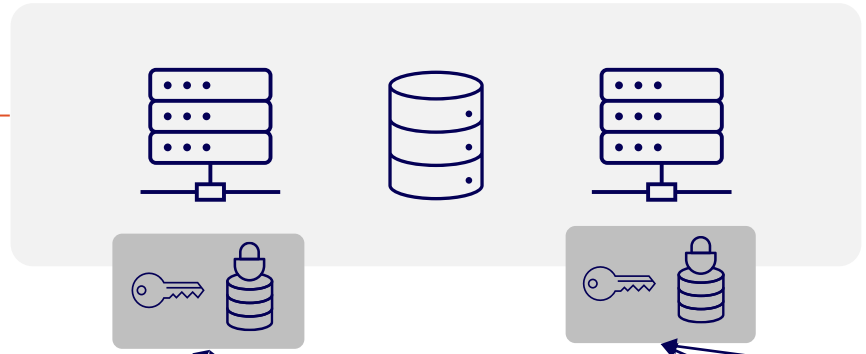
Scaling at the edge – cybersecurity challenges in constrained environments

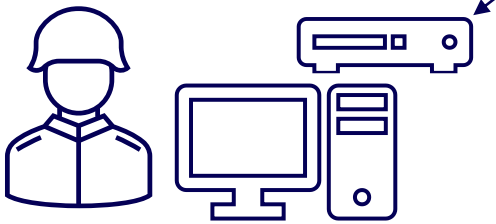
Static hardware:
- presents a single point of failure
- requires significant resource to power

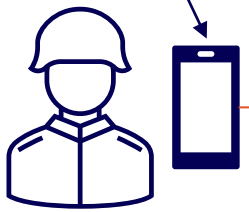
Expensive cryptographic hardware and wired connections required

PKI used at risk due to SWaP requirements of UxVs (not future-proof against quantum attack)

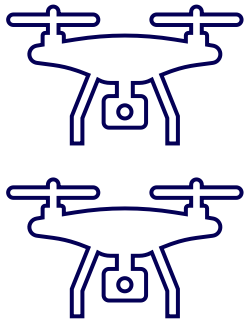
Lack of continuous endpoint authentication reduces anti-spoofing capability and dynamic access control.







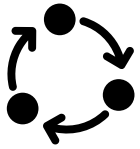
Limited bearer options due to weak encryption



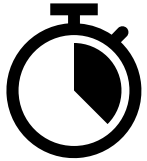
Group keys introduce risk in the case of compromise and device loss.

Bandwidth and Connection Overhead

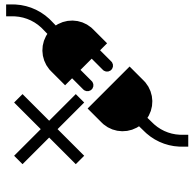
Post-quantum keys are 10–50× larger, creating 2–3× larger connection handshakes.



Larger messages often don’t fit in one transmission, causing retries and slow starts.

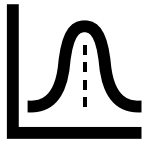


Each retry adds hundreds of ms to seconds on satellite or radio links.



In unstable networks, this can mean failed or delayed initial connections.

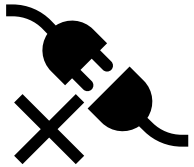
Authentication and Certificate Growth



Digital signatures jump from tens of bytes to several kilobytes each.

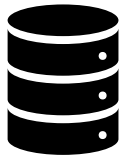
Certificate files expand by multiple kilobytes per device, multiplying network load.

More data = higher packet loss and handshake failure rates in poor links.

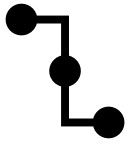


Legacy radios and gateways often drop oversized security messages entirely.

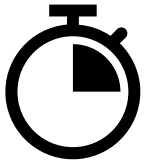
Device and Mission Impact



Small or battery devices can handle PQ math, but struggle with memory and data volume.



Added handshake traffic uses bandwidth meant for sensor or command data.

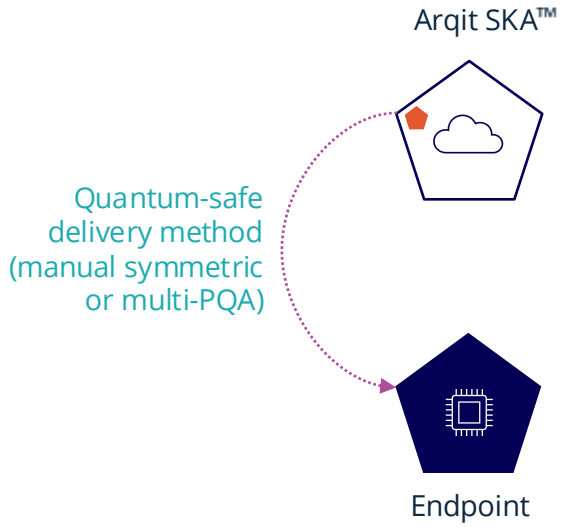


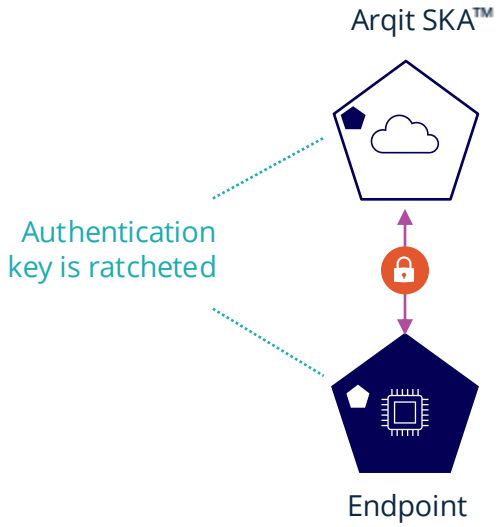
In field conditions, connection delays can exceed operational tolerance.

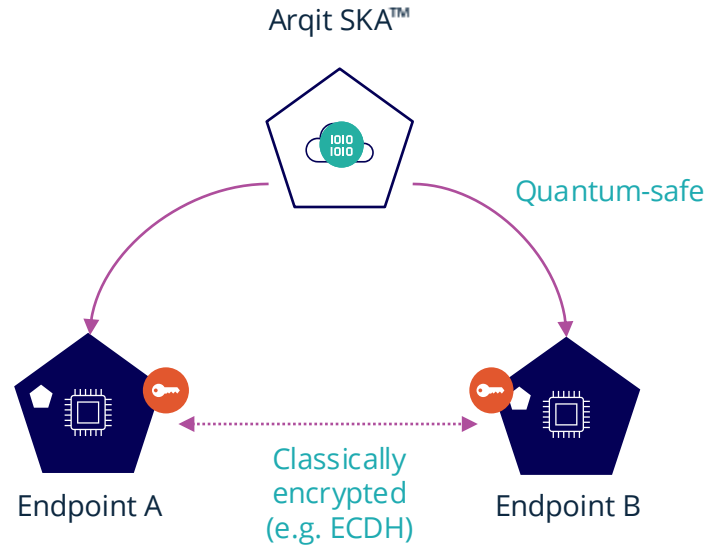
PQC is secure but heavy and brittle in disconnected or tactical networks — driving the need for lightweight yet still secure alternatives

Arqit's SKA process

Provisioning, authentication, and key agreement







1

Every endpoint is securely provisioned once with a "bootstrap" key

2

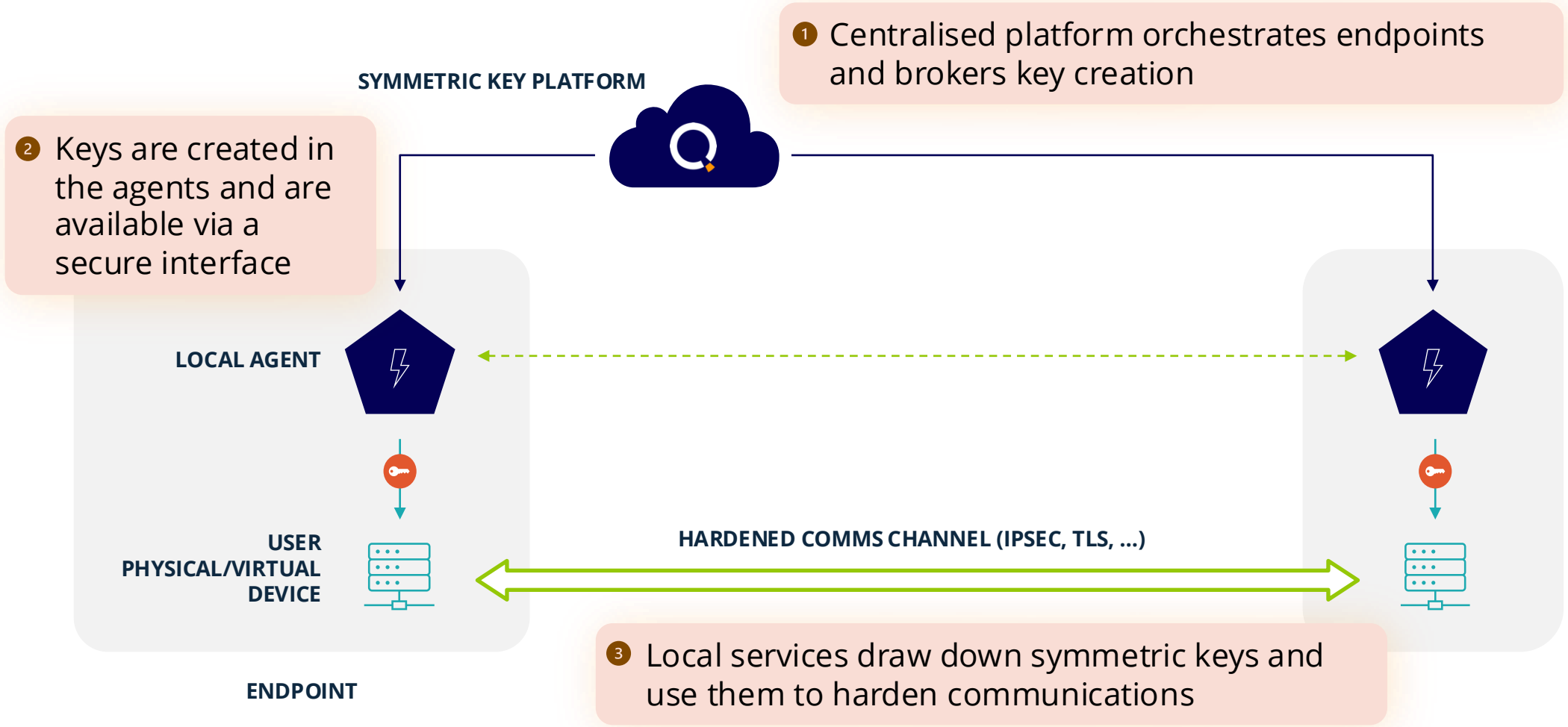
Endpoints strongly, mutually authenticate with perfect forward secrecy

3

Groups of endpoints agree quantum-safe symmetric keys using material provided by Arqit SKA™

Platform for sovereign, quantum-safe networking

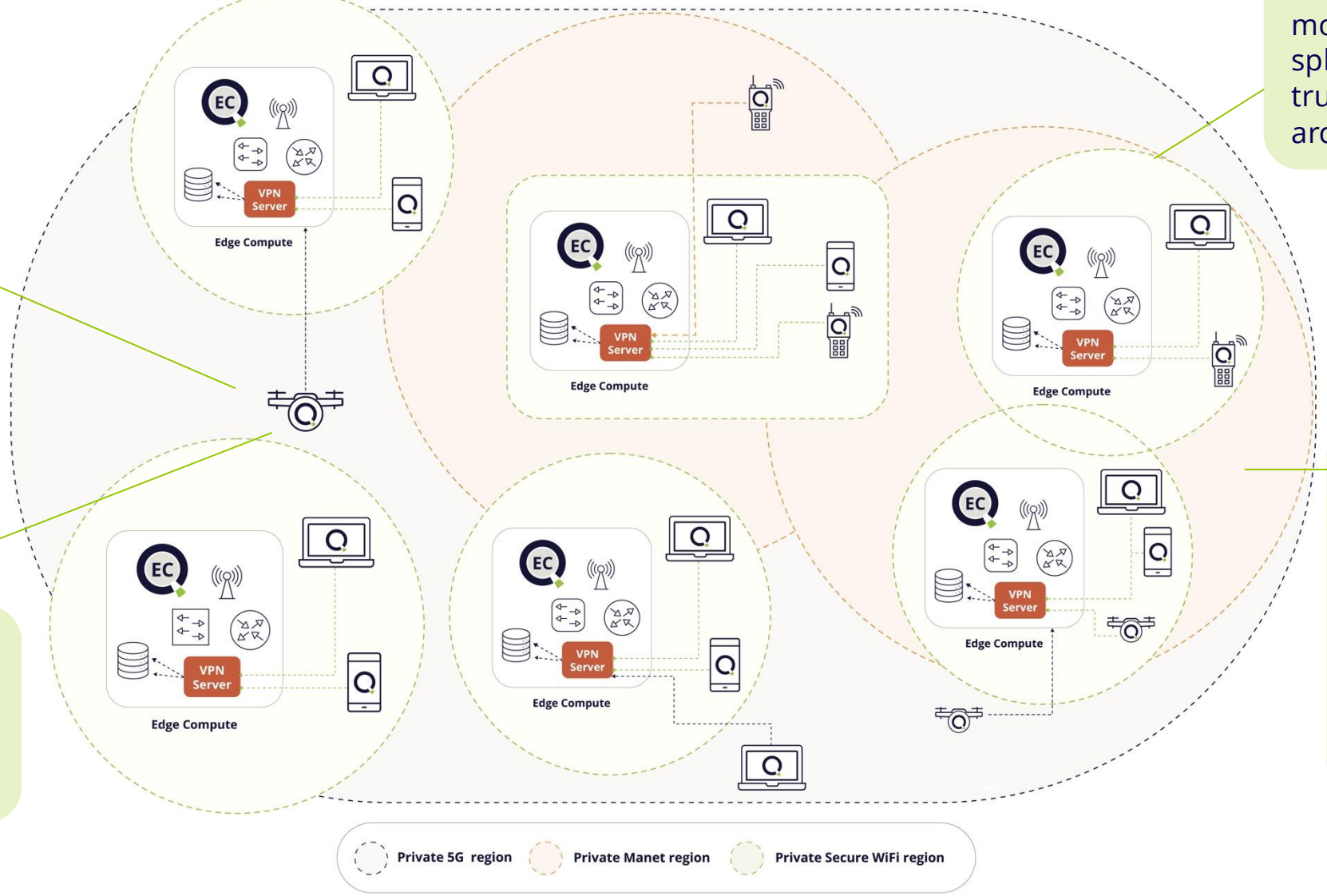
Protect critical communication channels with hardened symmetric keys



Dispersed and distributed modern operations

Edge capability to support a rapidly deployable HQ that is scalable, enhances manoeuvrability, reduces SWaP and supports reduced overheads and a dynamic PACE concept

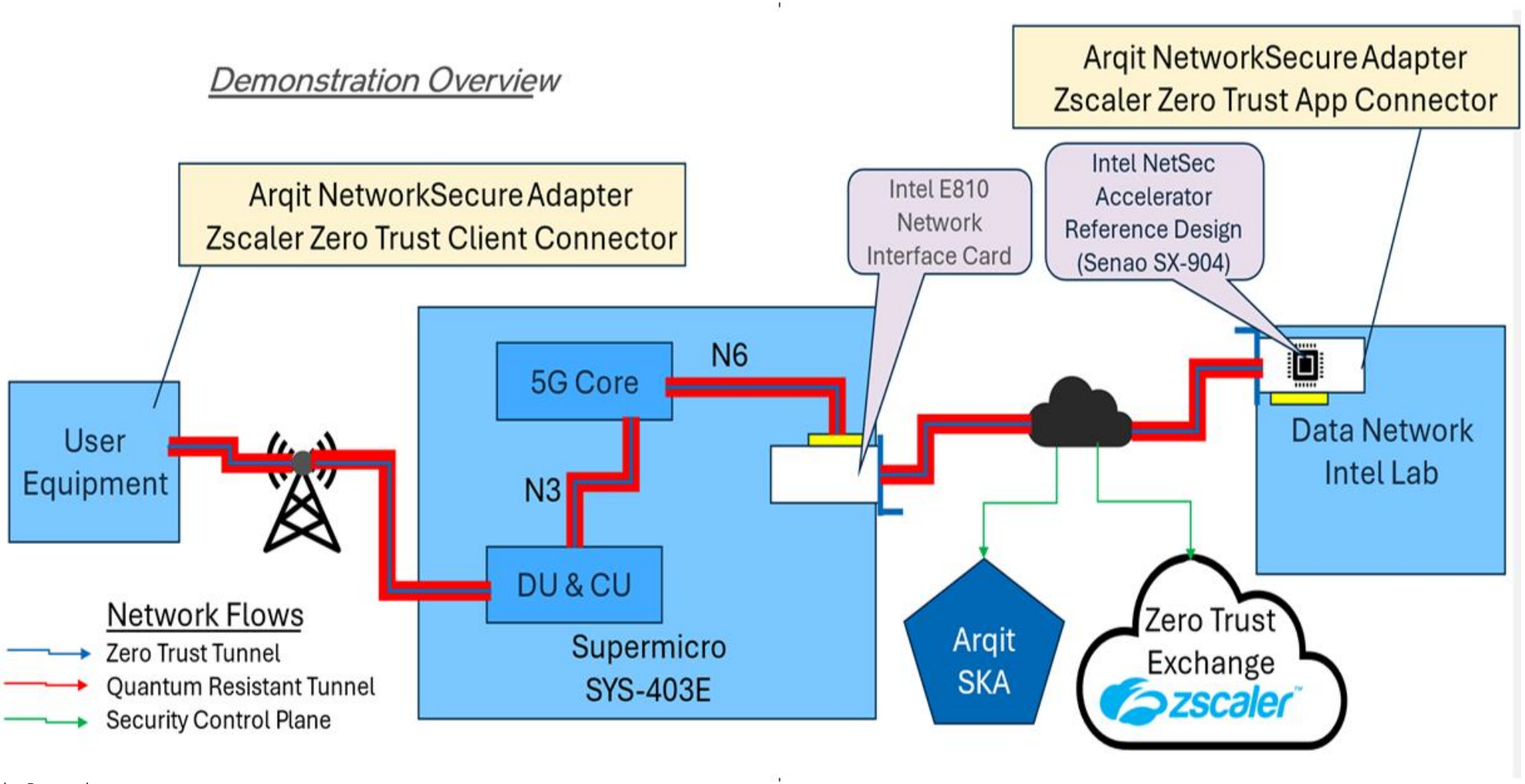
Extend security to the edge device, providing flexibility while reducing the threat surface



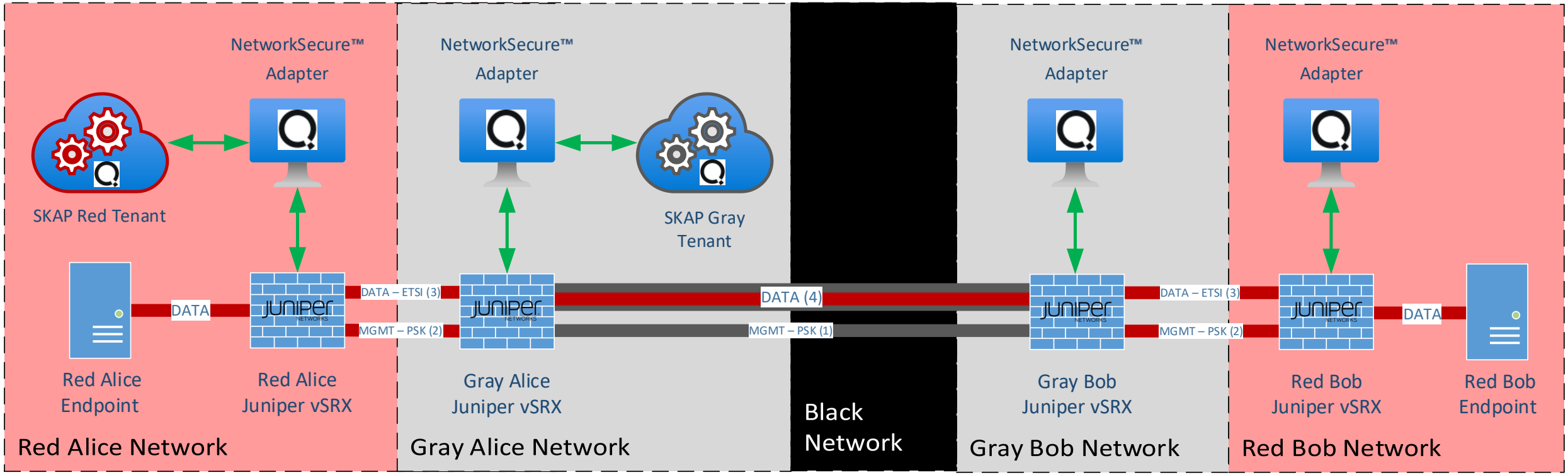
Implementation model supporting split trust / zero trust SbD architectures

Multi-nodal approach to enable dispersed and distributed operations in line with current and future deployment models

Private Tactical 5G



NSA CSfC Enterprise Gray




ARQIT
Thank you