ARQIT X intel ai

Enabling PQC and Data Sovereignty at the Network Edge

That's the power of Intel Inside®

June 4th

9am PST/12pm EST

Phil Burn

Director of Professional Services

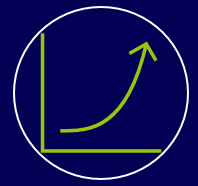
ARQIT

Mitch Koyama

Enterprise Segment Manager

INTEL

The Challenge



Expanding digital infrastructure increases cyber exposure

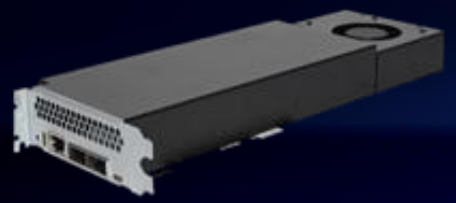
Data sovereignty and resilience requirements are becoming harder to meet

Quantum-era threats are accelerating the urgency for action

Many organisations do not know where cryptography is currently deployed

Deploy Computer Fast, Protect Workload

Intel® Netsec Accelerator Reference Design



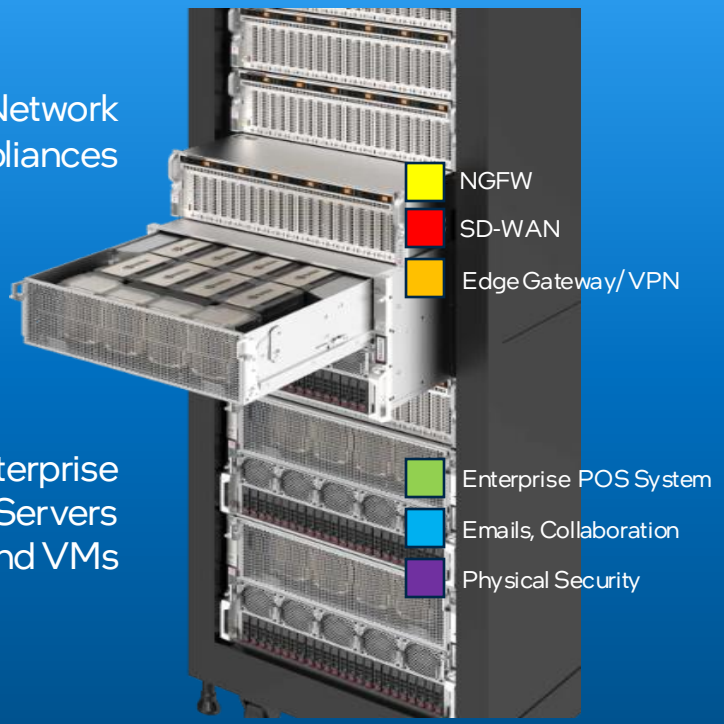
Form Factor Innovation

Confidential Computing

Sovereignty in Cloud, Edge

One Platform for Workload Consolidation

Network Appliances



Enterprise Servers and VMs

TCO Optimization
Performance Headroom
Low Latency Applications

Scale

Consolidate

Isolate

Smaller Footprint
Flexible Use Cases
Workload Protection
Enhanced Security

Intel® Netsec Accelerator Reference Design

Modular Edge Servers

Intel® Xeon® 6 processors and SoC + Intel® Ethernet

- AI Inferencing
- Data Plane and Netsec
- Crypto, PQC
- Confidential Computing

intel XEON

Intel® NetSec Accelerator Reference Design

A complete autonomous server with full Orchestration and Management on a PCIe add-in card

- Family of SoC-based Reference designs intended to offload networking and security workloads creating more server cores for real value-added applications
- Creating a higher level of security isolation and easier workload integration
- SoC value points include scalable x86 software & ecosystem, cryptography offload, and switching capabilities to drive TCO value
- Intel publishes the reference design
- ODM/OEMs deliver the cards to market

Intel® NetSec Accelerator Reference Design Evolution

Intel Atom® P5700

Silicom
P425G2SNx
IAONIC SmartNIC

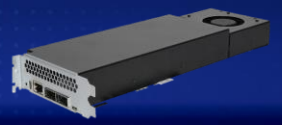
Version 1.0
(Intel Atom®: 8C, 16C)

Intel ® Xeon® D

Senao Networks
SX904 SmartNIC

Version 2.0
(Intel® Xeon® D: 4C, 8C, 10C
w/ Intel® Ethernet E810)

Intel ® Xeon® 6 SoC

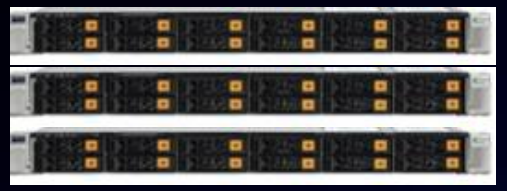


Lanner
IAC-PTL301A
Available Now

Senao
SX906
Coming in Q2'26

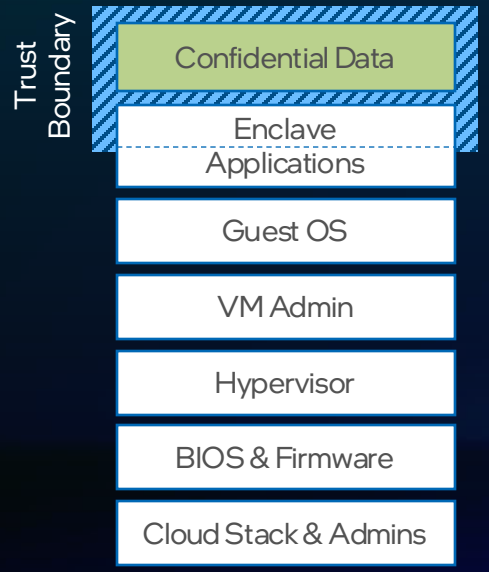
Version 3.0
(Intel® Xeon® 6 SoC w/Intel® Ethernet E810)

Cost Optimization with Modular Hardware Design

Platform	Resources	Server Platform Cost	Headroom Scalability
Supermicro SYS-322GA-NR  NetSec Accelerator  https://www.thinkmate.com/system/superserver-322ga-nr	One Server Xeon 6 (6952P) 196 Cores 9 NetSec Cards Xeon 6 SoC 36 Cores Ea. Total of 520 Core of Xeon 6 3 RU Consumed Cooling Capacity 3044W (Air) 20 QSFP ports required	Approx. $ 78,300	In-chassis
Supermicro SYS-122H-TN  https://www.thinkmate.com/system/superserver-122h-tn	Three Servers Xeon 6 (6768P) 172 Cores Ea. Total of 516 Cores of Xeon 6 3 RU Consumed Cooling Capacity 2100W (Air) 6 QSFP Ports	Approx. $ 179,400	Additional chassis
Supermicro SYS-222C-TN  https://www.thinkmate.com/system/superserver-222c-tn	Three Servers Xeon 6 (6768P) 172 Cores Ea. Total of 516 Cores of Xeon 6 6 RU Consumed Cooling Capacity 2100W (Air) 6 QSFP Ports	Approx. $ 127,800	Additional chassis

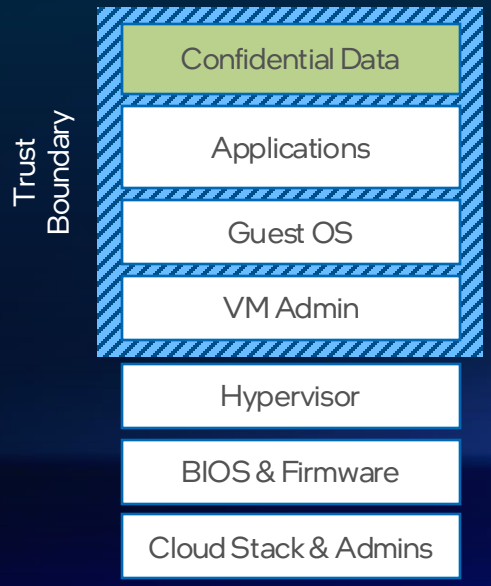
Confidential Computing – Establish Sovereignty

App Isolation
Intel® SGX



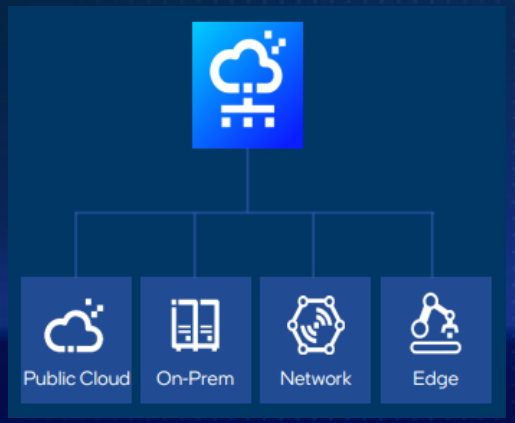
Smallest trust boundary for greatest data protection & code integrity

VM Isolation
Intel® TDX



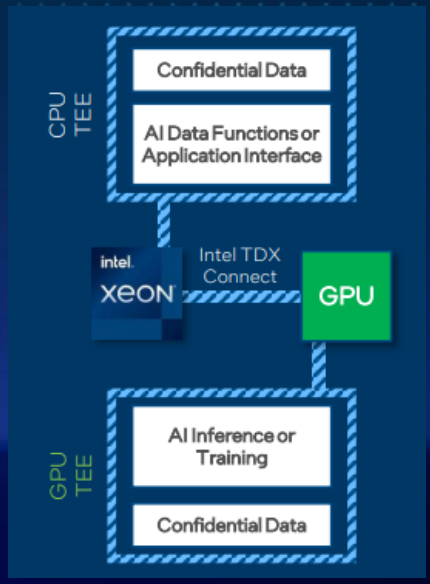
Most straightforward path to greater security for legacy apps

Trust Services
Intel® Trust Authority



Uniform, independent attestation of trustworthy environments

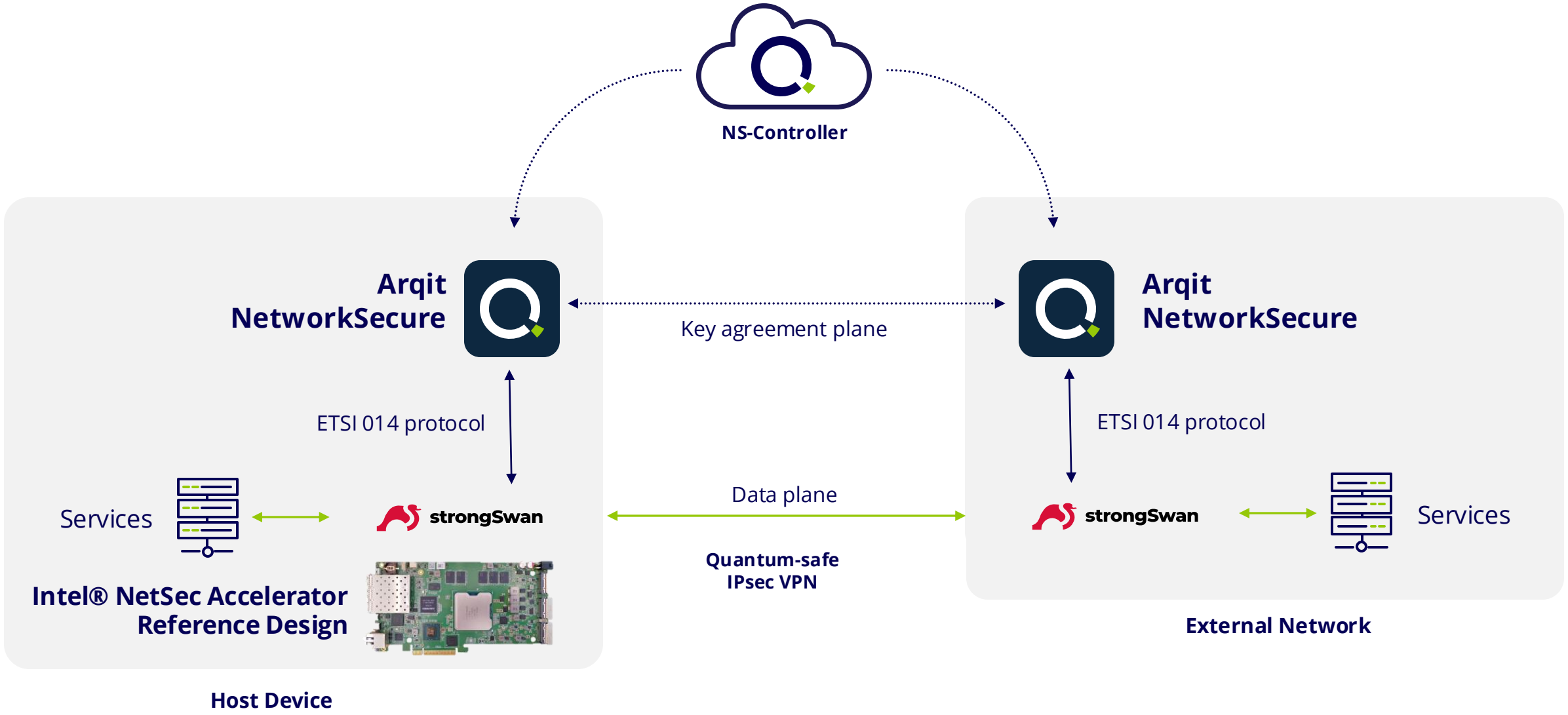
Encrypted Connection
Intel® TDX Connect



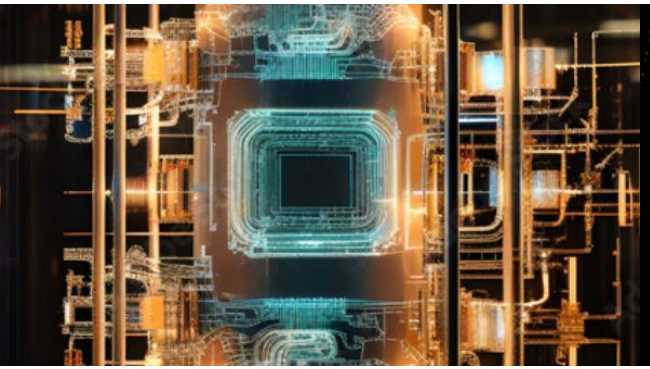
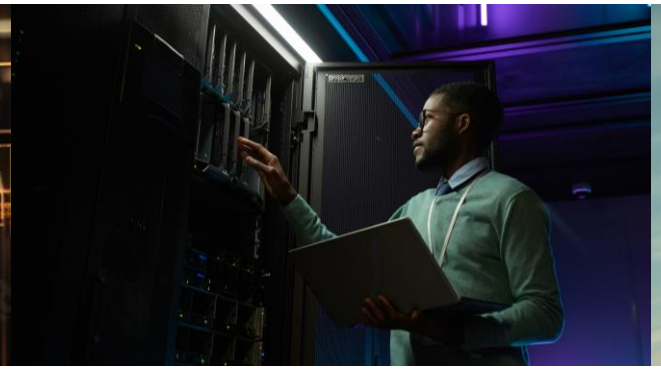
High-performance encrypted connection between CPU and PCIe devices

Alibaba Cloud · Azure · Google · VolcanoEngine ByteDance · IBM Cloud · intel XEON

NetworkSecure™ deployed on Intel-based NetSec Cards



SKA-Platform delivers a wide range of uses cases

NaaS Security

Quantum-safe network security

Telcos are migrating networks to be quantum-safe, across cloud, data centres or as part of Networks-as-a-Service (NaaS) and Private 5G infrastructure. They want more scalability and deployability than QKD, and more value and assurance than PQAs.

Arqit SKA: software-based method of symmetric key exchange for quantum-safe encryption at Layer 1 (OTNsec) , 2 (MACsec) and 3 (IPsec). Compatible with Android, Linux and Windows for mobile devices, phones, laptops etc.

NaaS Immunity

Identity management for automated networks

Network automation is accelerating. Networks are becoming more cloud-based and disaggregated, with increasing numbers of devices. Innovative approaches are needed for network orchestration and protection to build network immunity e.g. better identity management for short term virtualised and containerised environments.

Arqit SKA: API-enabled, integrates with orchestration tools to support on-demand NaaS; embraces ZTNA principles by using symmetric keys to authenticate devices.

Edge Security

Crypto agility for Defence and Government

Military and Government use physical delivery of keys and store in crypto hardware. This is inflexible and slow. Innovative approaches are needed for secure key exchange between increasing numbers of remote connected endpoints e.g. for remote workers, dispersed battlefield headquarters, and UxV operations.

Arqit SKA: A cheaper, faster, lighter, more scalable method of symmetric key exchange. Deployable as a Central Controller or smaller form factor Edge Controller. Compatible with Android, Linux and Windows for mobile devices, phones, laptops etc.

Cloud Security

Protecting sensitive AI workloads in the cloud

Compliance, lack of trust in cloud operators, or concerns about legal access requests by foreign governments mean increasing demand for *Confidential Computing* services for security and sovereignty of data-in-use e.g. during AI processing between on-prem, hybrid and multi-cloud. Cloud providers must never be able to access encryption keys.

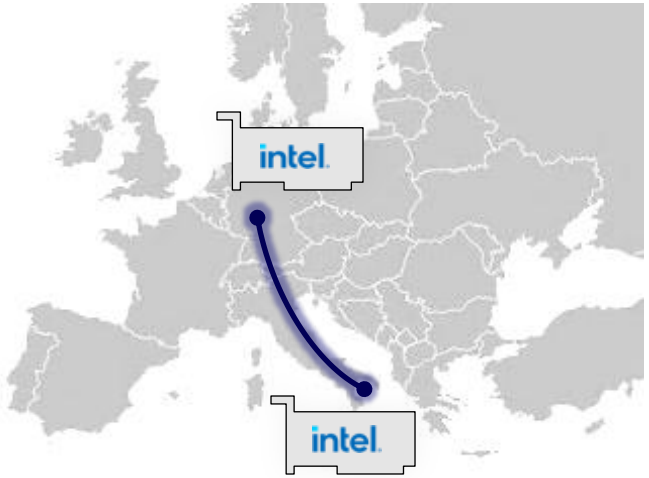
Arqit SKA: key creation in trusted domains; delivers quantum-safety for data-in-use and data-in-transit.

Use cases and customers

TELECOMMUNICATIONS

Low-touch deployment of high throughput VPNs

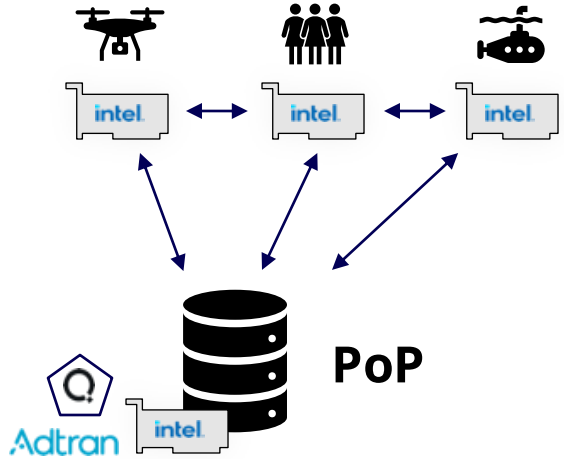
- Maximum performance using strongSwan and VPP for IPsec offload
- OEM vendors such as Fortinet, Juniper and Cisco provide out-the-box alternatives
- Low/zero-touch deployment of networks
- Extend to ZTNA/SASE networks
- Instant security of full suite of VNFs/CNFs



GOVERNMENT AND DEFENSE

Classified workloads in dynamic edge environments in theatre

- Compliance with latest requirements, e.g. NSM-10
- Highly dynamic and scalable
- Strong authentication with endpoint management

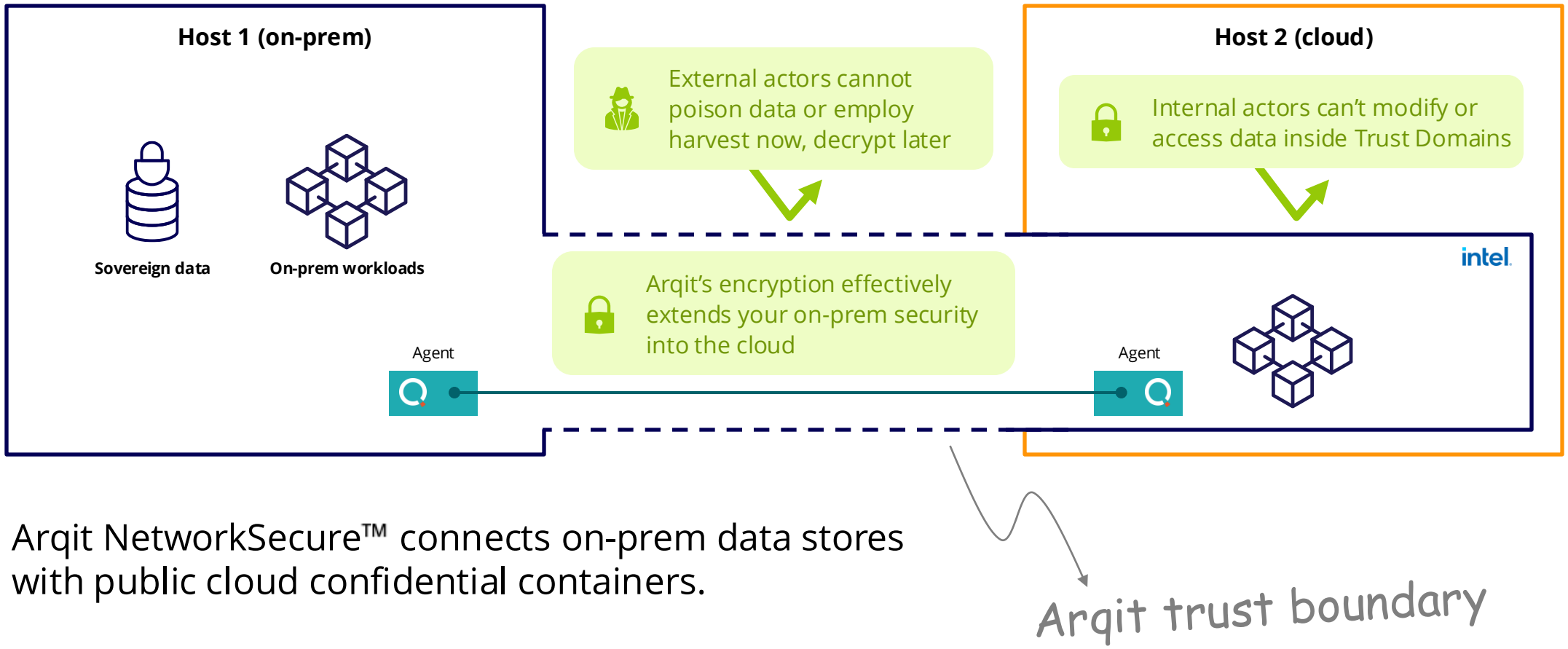


ARQIT

Distributed Confidential Computing

Extend confidential computing across multiple hosts

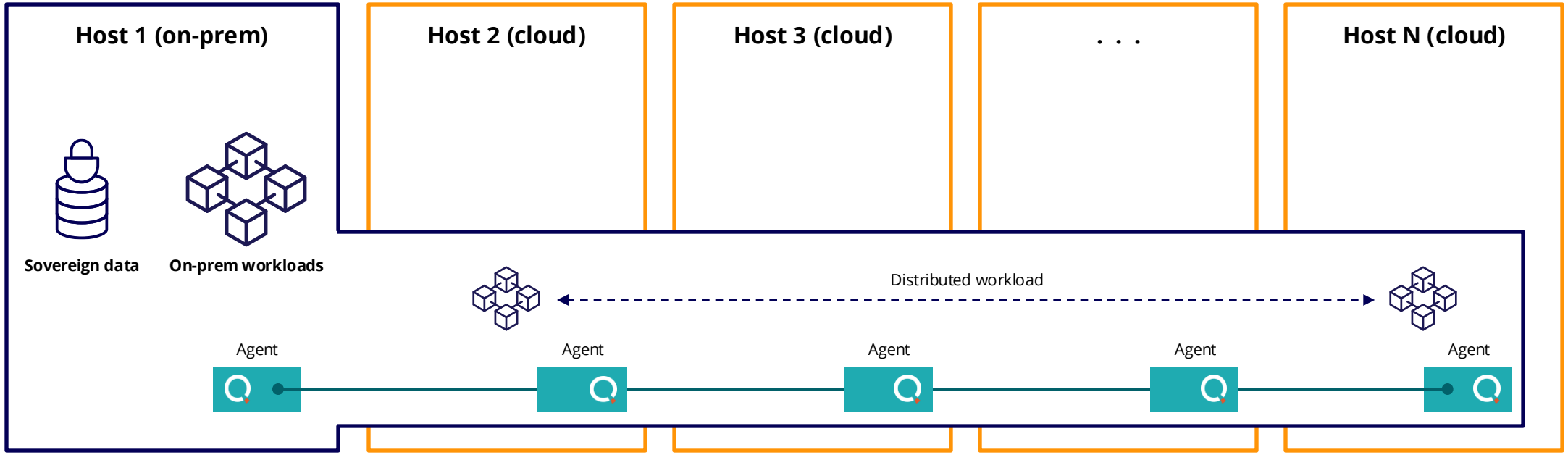
With Arqit technology, treat public cloud just like on-prem



Arqit NetworkSecure™ connects on-prem data stores with public cloud confidential containers.

This is **distributed sovereign/confidential compute**.

Extend confidential containers across hosts



Arqit NetworkSecure™ connects on-prem data stores with public cloud confidential containers.

This is **distributed confidential computing**.

Key Benefits

Cyber Resilience
Mitigates data breach, HNDL and TNFL attacks

Standards Compliance
Compliant with NIST, NSA and FIPS security standards

Operational Efficiency
Greater cost efficiency and reduced complexity

Secure Innovation
Enables secure digital transformation and AI innovation

Scalable Flexibility
Flexible, scalable licensing that grows with your business

Thank you for watching!

1. Know your risk
Audit which data needs protecting for 10+ years — it's already being harvested.

2. Start your PQC migration today
Governments mandate the switch. The clock is ticking.

3. Talk to us about a proof-of-concept
Pre-packaged on Intel hardware. Quantum-safe from the core to the edge in days, not months.

Contact us: **consult@arqit.uk**