Data Sovereignty with Confidential Computing and Networking

Confidential computing with post-quantum crypto networking

Designed to protect sensitive workloads and their data from external attacks.

Well-suited for shared or managed infrastructure outside the customer's direct control e.g. the public cloud, and highly sensitive applications such as AI or user data processing.

Allows the hosting service provider to process and transmit data without any visibility, granting full sovereignty and reducing liability.

Arqit NetworkSecure™ uses Intel® Trust Domain Extensions (Intel® TDX) to help increase confidentiality of both data in use and data in transit for sensitive workloads deployed across hosted environments

Highly sensitive workloads require greater security controls, particularly when running on shared or managed infrastructure. Intel TDX creates a Trust Domain (TD), designed to isolate Virtual Machines (VMs) from the underlying physical hardware, operating system, hypervisor, and other VMs. This robust security boundary increases VM security, even if attackers compromise the physical host.

However, data entering or leaving the TD may still be at risk as it passes through a network interface or system bus. Arqit's quantum-safe Symmetric Key Agreement Platform (SKA-Platform™) allows services running within a TD to create symmetric encryption keys that are considered safe, even from quantum computers. This ensures data is encrypted securely before it leaves the TD boundary. The data can be shared with other TDs running on the same or different hosts with full end-to-end encryption. Encryption keys are ephemeral and never shared outside of the TD.

How we've been able to demonstrate this

Arqit NetworkSecure is a software agent that integrates with network devices and open-source implementations of existing protocols such as IPsec. Arqit's NetworkSecure strongSwan product is used to integrate the strongSwan IPsec library and the strongSwan vici interface for external key retrieval.

NetworkSecure strongSwan supports several Linux-based operating systems (OS) with both VM and virtual network function (VNF) options. Ubuntu 24.04 LTS was chosen in this instance as it could be converted from a regular VM image to a TD image, enabling Intel TDX features. Both strongSwan and NetworkSecure were running directly inside the TD images. A TD image was deployed in two connected environments: one within an on-prem server, and one on a cloud-based host, both with Intel TDX enabled.

Once the TD image boots, NetworkSecure automatically enables symmetric keys to be generated within the TD, ensuring that only the TD itself knows the final keys. This is a split trust mechanism that ensure that no other entity, including Arqit SKA-Platform knows or can access the symmetric keys. NetworkSecure is automatically connected to strongSwan via the vici interface, enabling out-of-band symmetric key delivery into IPSec VPN tunnels created between strongSwan VPN endpoints.

The result

The result is quantum-safe IPsec tunnels between TDs, where all encryption keys are secured directly within the TDs. No third party can access the keys, including the cloud service provider (CSP) in the case of the cloud environment. Keys are rotated in line with zero downtime periodically to provide enhanced forward secrecy; the rotation frequency is customizable and can be as little as every few minutes.

Finally, with the IPsec tunnel active and running, attestation via Intel® Tiber™ Trust Authority was used to verify the integrity of the TD images. We could confirm that tokens were created by the independent attestation service, and a verification step was completed to help ensure that the machine can be trusted, including a check of the Trusted Computing Base (TCB) status.

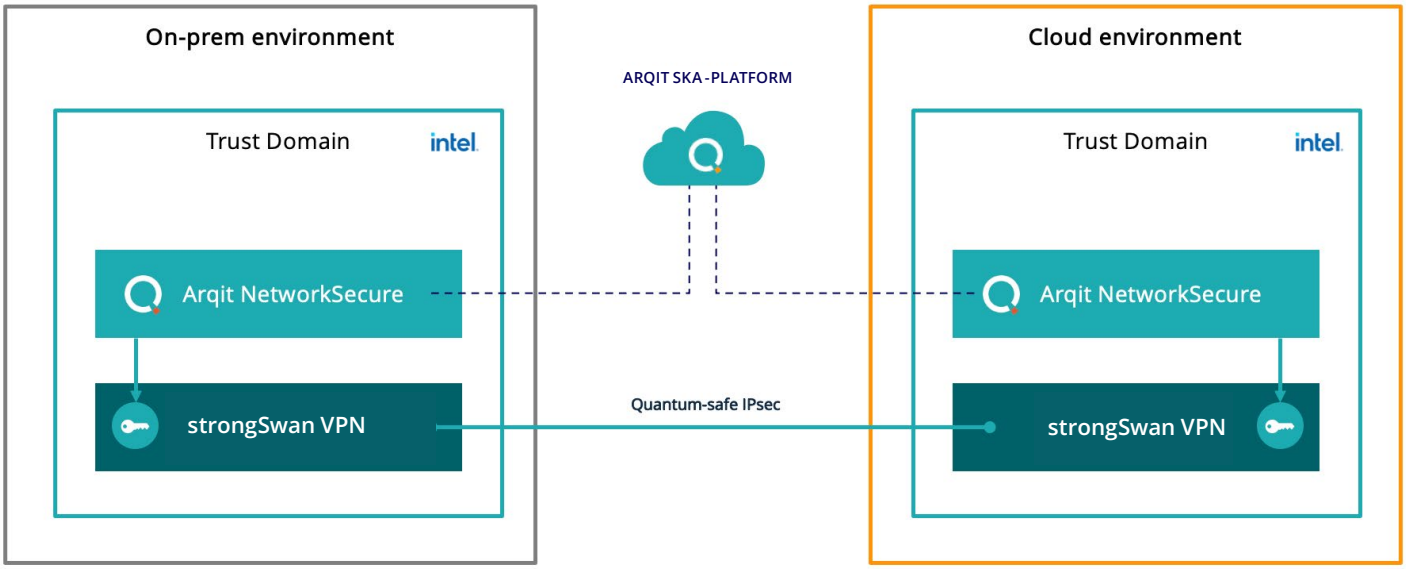

Figure 1: Arqit NetworkSecure running inside a TD provides quantum-safe symmetric keys to a strongSwan VPN client. The keys are ingested by the client and used to secure the IPsec tunnel between the clients.

Target applications: RAG AI and sensitive data workloads

Retrieval-augmented generation (RAG) is transforming how businesses leverage large language models (LLMs), offering a way to customize AI capabilities without the high costs and complexity of fine-tuning. This approach enables organizations to deploy AI-driven applications that integrate proprietary data, enhancing accuracy and contextual relevance while reducing operational burdens. Today, organizations can optimize RAG implementation into company assistants, collaborators, and co-thinkers.

However, RAG applications present serious security challenges for enterprise:

- AI models are fed with sensitive proprietary data from disparate sources which must be gathered and shared with utmost security.
- Workloads must be protected from interference to ensure model outputs are accurate and the models themselves have not been tampered with.
- Special hardware requirements often motivate deployment on shared infrastructure, e.g. public cloud, outside of the customer's control and security boundary.

Arqit and Intel's collaboration addresses these issues and more by providing robust confidentiality to both computation and network transmission, allowing customers to leverage public cloud infrastructure while maintaining the security posture of an on-prem deployment. Intel TDX helps shield sensitive AI models from interference by either the host provider or bad actors who may have compromised the host, ensuring model outputs are trustworthy and preventing model exfiltration.

Arqit's data-in-transit security, provided by quantum-safe symmetric keys, protects sensitive data even on public networks, ensuring model data cannot be interfered with or decrypted in the future.

Beyond AI, Arqit and Intel's solution can help organizations comply with local sovereignty requirements and has applications in:

Financial Services

Healthcare

Government

Future enhancements

Beyond data-in-use encryption, Intel TDX also provides remote attestation capabilities, meaning workloads can prove they are running within a TD and confirm other hosts are also using Intel TDX. This reduces the chance of man-in-the-middle attacks or data poisoning by rogue endpoints and ensures that workloads never share data with environments without Confidential Computing. To date, remote attestation has been used to verify that the VM is protected by Intel TDX, and Arqit's own symmetric-based active authentication service augments the PKC-based approach offered by attestation services, providing quantum-secure authentication in addition to data security.

As a future enhancement, attestation can be used to verify that NetworkSecure is running unmodified by a third party, and that information could be shared with other TDs through the quantum-safe data link. This removes the risk of tampering and ensures the integrity of Arqit's software running inside the TD.

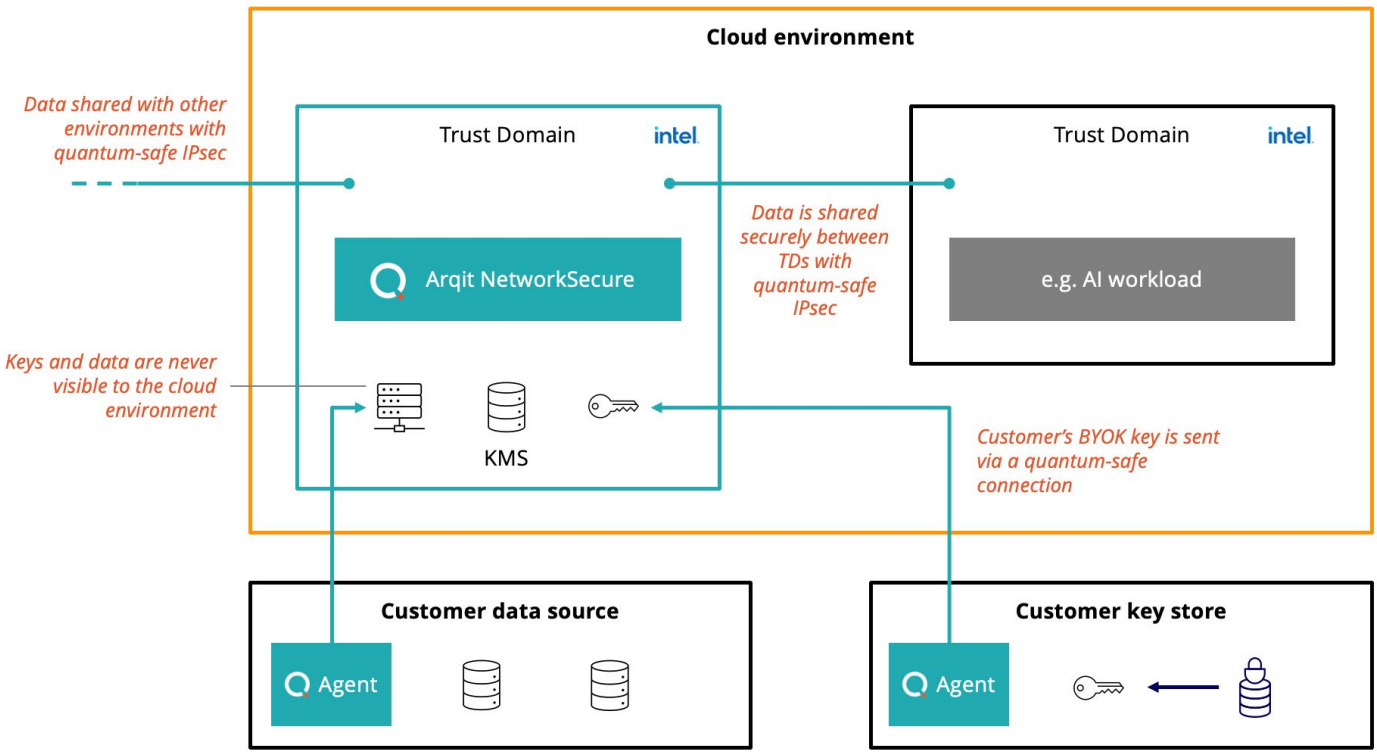

Figure 2: Hypothetical architecture showing Arqit NetworkSecure running inside a TD, designed to protect data at the TD boundary. This ensures data (including key material) is end-to-end quantum-safe protected between on-prem and cloud-hosted environments. Data can be shared between TDs or between hosts with quantum-safe IPsec encryption protected by Arqit.

Key benefits for customers and hosting service providers

Combine the powerful Confidential Computing capabilities of Intel TDX with Arqit's quantum-safe data-in-transit network security, designed to keep data and applications safe from attack even on shared infrastructure.

Encryption keys are created and stored inside an Intel TDX-protected virtual machine, never injected from outside, designed to maintain full confidentiality and data ownership.

Deploy existing workloads across multiple cloud hosts with minimal effort due to the simplicity of Intel TDX and Arqit's overlay architecture.

For hosting providers, prevent inadvertent data leaks, reduce liability, and offer your customers quantum-safe data security with minimal customer configuration.

Independent workload attestation with Intel Tiber Trust Authority.