

WiZ-Knight

Quantum Safe Portable Encryptor



The remote work landscape is evolving. As critical communications extend beyond traditional security boundaries, exposure to untrusted networks, endpoint vulnerabilities and emerging quantum threats continues to grow. Organisations must secure remote connectivity against today's cyber threats while preparing sensitive communications for the quantum era.

WiZ-Knight is a palm sized, USB-powered portable secure connectivity solution enabling secure remote access with Zero Trust protection, seamless deployment and future ready security for mobile professionals.

Remote Connectivity Built for Quantum Resilience

Built on an independent root of trust, WiZ-Knight protects sensitive communications beyond traditional security boundaries. Its hardware enforced, quantum resilient architecture reduces exposure to today's cyber threats while strengthening long term protection for the quantum era.

Endpoint Isolation
WiZ-Knight acts as an isolator, shielding the host from untrusted networks and blocking unauthorised access. By reducing exposure to network-based threats and rendering the endpoint invisible on the networks it joins, it shrinks the attack surface before threats can reach the host.

Quantum Resilient Encryption
WiZ-Knight provides cryptographic agility through hybrid post quantum key exchange, combining AES-256, HMAC-SHA2/3, ECDH and ML-KEM-1024. This strengthens sensitive communications against current threats while preparing organisations for emerging quantum risks.

Independent Root of Trust
Built on a tamper evident, hardened platform, WiZ-Knight operates independently of the host with verified boot and runtime integrity monitoring. This independent root of trust maintains protection even if the host is compromised, reinforcing Zero Trust security at the device level.

SECURE
WHAT MATTERS



The Emerging Threats to Remote Connectivity

Remote work is extending critical communications beyond traditional security boundaries. As users connect through untrusted networks, endpoints face greater exposure to reconnaissance, interception and vulnerability exploitation. At the same time, emerging quantum computing introduces new risks to sensitive, long lived communications.

Organisations must strengthen remote connectivity against today's expanding attack surface while preparing for tomorrow's quantum threats:

Untrusted Network Exposure
Endpoints connecting through public or unsecured networks can be exposed to scanning, interception and vulnerability exploitation.

Software Dependent Protection
Software VPNs remain potential attack targets and may not fully protect endpoints from threats originating on untrusted networks.

Emerging Quantum Threats
Adversaries can capture encrypted traffic today for future decryption, putting sensitive and long lived information at risk as quantum capabilities advance.

Rise of AI Driven Threats
AI is accelerating the automation, scale and personalisation of cyber attacks, increasing exposure for remote users. As detection and response remain inherently reactive, organisations must reduce opportunities for attacks to succeed by adopting a protect first security strategy.

Time for a More Secure Approach

WiZ-Knight delivers trusted hardware-based security with endpoint protection, secure connectivity, centralised security management, and quantum ready encryption, ensuring uncompromised security for mobile professionals against malware, zero-day exploits, and sophisticated cyber threats.

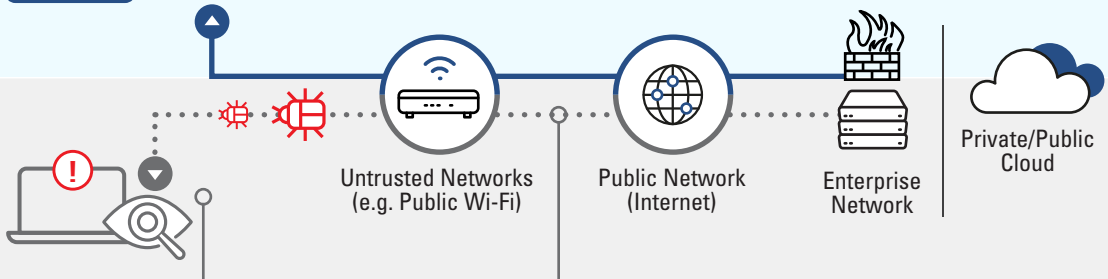
Connecting with WiZ-Knight

Endpoint is protected and invisible on the network it is connected to.

Quantum safe encryption protects remote communications against current and emerging quantum threats.

As the front line of defence, WiZ-Knight **prevents unauthorised access and exploitation of host vulnerabilities.**

Connecting with Software VPN



Endpoint is visible on the network and susceptible to malicious information gathering (e.g. fingerprinting, enumeration, etc.)

Risk of unauthorised access and vulnerability exploitation due to direct connection to untrusted networks.

Harvest Now, Decrypt Later (HNDL) puts today's encrypted data at future risk.

Key Features

The world's first secure connectivity solution with **Zero Trust** and **quantum resilient remote access.**

Supports **50 Mbps** throughput and **Over the Air (OTA) updates** for seamless security

Multi-factor authentication to strengthen access security.

Built on **Zero Trust architecture** with verified boot, continuous integrity checks and tamper evident hardware.

Centralised management enables geolocation awareness, security updates and policy control across deployed devices.

Active Directory integration with automated provisioning support scalable and streamlined deployment workflows.

Key Benefits

Secure remote connectivity that safeguards data and prevents costly breaches.

Flexible deployment variants support on-premises and cloud environments, adapting seamlessly to diverse IT needs.

Quick and efficient setup with clientless deployment and plug and play functionality.

Quantum ready encryption for future proof protection against emerging quantum computing threats.

Ideal For

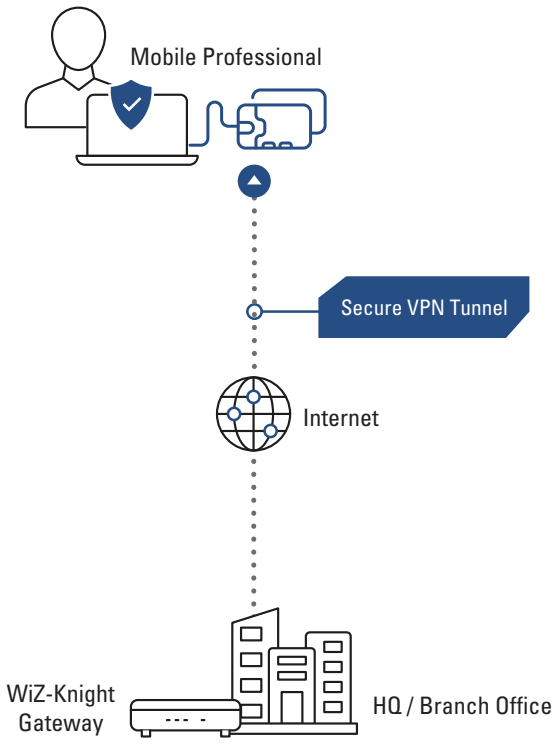
Hybrid workforce professionals who frequently travel or work from home.

C-Suite executives who handle highly confidential or sensitive data.

Flexible Deployment Variants for Secure Remote Connectivity

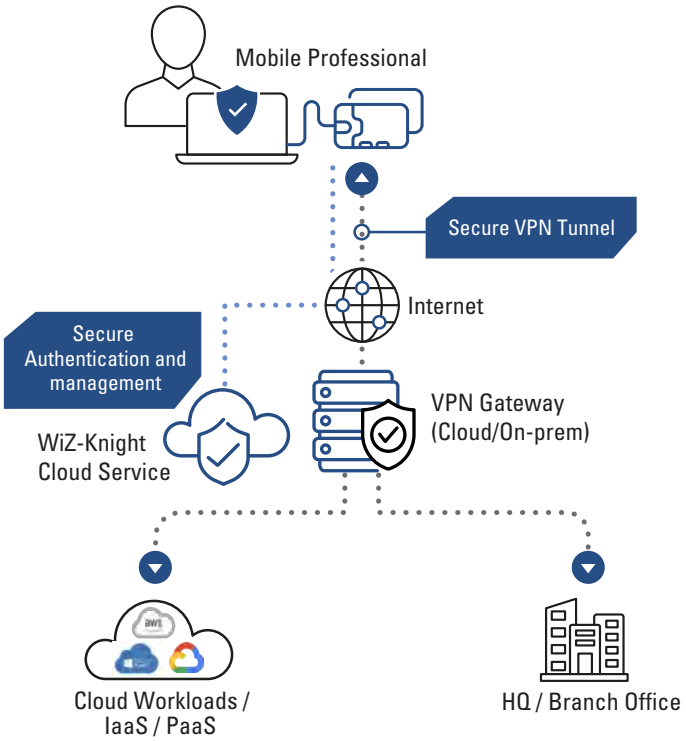
Appliance-Based VPN Concentrator

Dedicated physical appliance for secure on-premises deployment.



Virtualized VPN Server Gateway

Software-based gateway deployable on-premises or in cloud environments.



Use Cases for Wiz-Knight

Government agencies and critical industries face evolving threats. WiZ-Knight strengthens cyber resilience through Zero Trust and quantum safe protection.



Government

Secure Remote Access for Sensitive Data

Enhance the management of sensitive national security and citizen data by deploying WiZ-Knight for all travelling employees.

Benefits

- **Enhance security** by ensuring that all sensitive data transmitted over public networks are protected via strong hardware-based encryption.
- **Gain peace of mind** by securely isolating endpoints when connecting to untrusted public networks and establishing secure VPN connections back to the agency's network.
- **Fortify with enhanced defence** for higher security requirements to guard against compromised software VPN.



Financial

Secures Remote Transactions

Establish secure VPN connection for mobile professionals, essential for protecting access to banking systems, confidential client's information, and sensitive financial data.

Benefits

- **Protect business and customer sensitive data** via encryption to safeguard against unwanted interception.
- **Mitigate risks of data breaches** leading to financial losses, legal liabilities and damage to credibility.
- **Support compliance to regulatory requirements** such as GDPR (General Data Protection Regulation) and PCI DSS (Payment Card Industry Data Security Standard) via secure access control.



Healthcare

Secures Medical Records Access

Facilitate secure remote access to sensitive medical records for mobile healthcare workers during home visits, ensuring compliance with healthcare data protection regulations.

Benefits

- **Secures remote access** for mobile healthcare workers by protecting the transmission of critical data over public internet.
- **Safeguard third-party communication** with suppliers, insurers and other partners via secure authenticated communication channels.
- **Protect telemedicine consultations** by encrypting video calls and data exchanges.