
# WiZ-Knight

## Portable Encryptor

### Cyber Resilience for Hybrid Workforce

The rise of hybrid workforce has unleashed a critical security challenge. As employees connect to untrusted Wi-Fi, organisations lose visibility and control, exposing the endpoint devices to cyber attacks, data leaks, and escalating threats across an expanded attack surface.


WiZ-Knight is a portable encryptor designed to isolate and protect endpoints while securing remote connections from cyber threats. It introduces a new category of security—hardware-enforced network isolation, providing robust barrier against attacks, ensuring zero-trust security.

SECURE
WHAT MATTERS

# Exposing the VPN Blind Spot in the Hybrid Workforce

Professionals are increasingly dependent on public networks, not only in public spaces such as cafés, hotels, and airports, but also on unsecured home Wi-Fi. As the workforce extends beyond traditional security boundaries, organisations face significantly heightened cyber risks, underscored by a 107% surge in IoT malware attacks and an average data breach cost of US$4.88 million in 2024.[1]

While software VPNs are popular, they have become major attack vectors for ransomware, phishing, and lateral movement attacks, with hackers disguising malware as VPN software. Organisations need to reassess their remote connectivity security strategies.

The lack of organisational control over these connections presents critical security risks:

**Limited security coverage:** VPNs mainly protect data-in-transit but fail to address endpoint and network edge vulnerabilities.

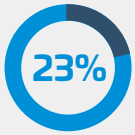
**Uncontrolled access points:** The hybrid work model allows employees to connect from anywhere, increasing cybersecurity risks particularly on laptops, prioritising productivity over security.

**Exposure to local network attacks:** Endpoints remain exposed on the public network, leaving them susceptible to malicious extraction of sensitive information and vulnerability exploitation of host devices.

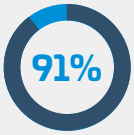
# The Hidden Vulnerabilities of Software VPNs


**DID YOU KNOW?**

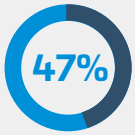
**56%**[6] of organisations experienced a VPN-related cyberattack in 2024.




of people use public Wi-Fi[2] to cut down on cellular data usage when travelling




expressed concerns about VPNs leading to a compromising breach[3]




increase in reported VPN vulnerabilities in 2023[4]


The annual average cost of cybercrime is expected to grow by 174% by 2027, compared to 2022[5]

[1] Cyber Management Alliance. (2025, January 20). Top 10 biggest cyber attacks of 2024 & 25 other attacks to know about!

[2] Forbes. (2024, October 15). The Real Risks Of Public Wi-Fi: Key Statistics And Usage Data.

[3] CIO. (2025. February 11). Why firewalls and VPNs give you a false sense of security.

[4] Top10VPN.com. (2024, January 18). VPN vulnerability report 2023.

[5] Informa TechTarget. (2025, January 10). 35 cybersecurity statistics to lose sleep over in 2025.

[6] GlobeNewswire. (2024, May 7). VPN risk report finds more than half of organizations experienced a VPN-related cyberattack in the last year.


# WiZ-Knight - Built on Zero-Trust Security

WiZ-Knight is a groundbreaking, USB-powered portable encryptor that establishes a hardware-enforced security barrier for mobile professionals. Even when using software-based VPNs, endpoints remain vulnerable to local network attacks and host compromises. WiZ-Knight overcomes this with a zero-trust approach and three-tiered defence that secures remote connectivity anywhere.

## Network Isolation

WiZ-Knight establishes a secure, invisible shield around the endpoint device. When connected to untrusted Wi-Fi, it isolates the laptop from the network, preventing hackers from detecting or interacting with it. By blocking rogue access points and network scans, WiZ-Knight delivers a robust layer of zero-trust protection, keeping device hidden and secure.

## Hardware-Enforced Security

Built on a tamper-evident, security-hardened platform, WiZ-Knight operates independently of the host system. Its dedicated firmware and secure operating environment minimise attack surfaces and offer robust resilience against cyber attacks. This hardware first approach ensures uncompromised protection at the device level.

## Independent Encryption

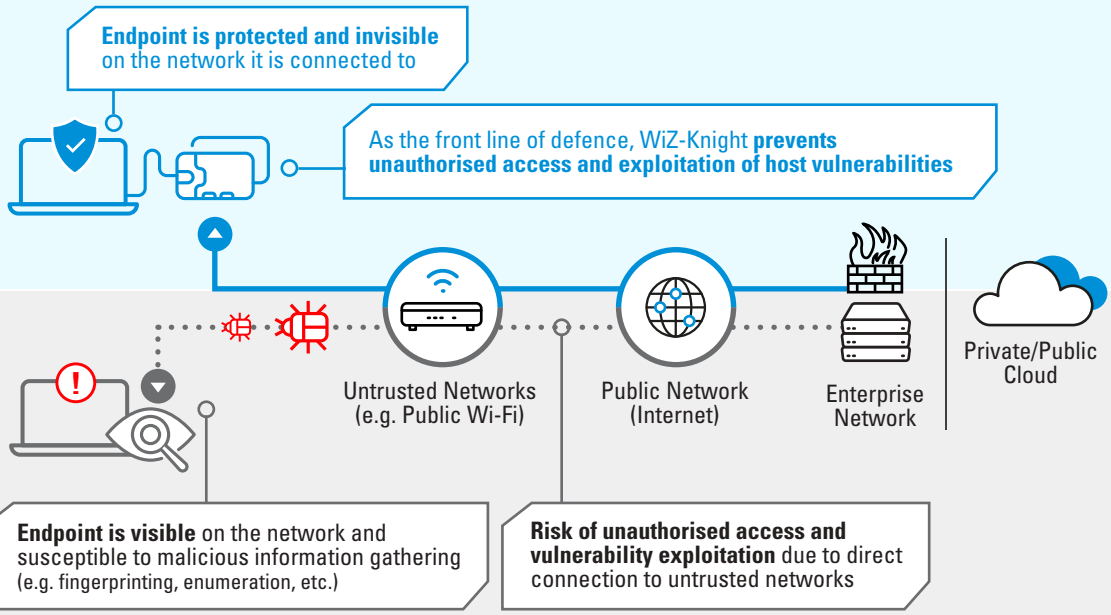
Traditionally, VPNs reliant on the host device, WiZ-Knight performs encryption independently, maintaining a secure VPN tunnel even if the host is compromised. This self-contained security layer ensures that sensitive data remains encrypted and protected, regardless of the system's integrity—upholding zero-trust principles at every stage of connection.

WiZ-Knight delivers instant, secure wireless connectivity with a simple plug-and-play design, requiring minimum installation. Ideal for rapid deployment and minimal IT support, it provides seamless protection for all mobile professional.

# Time for a More Secure Approach

WiZ-Knight delivers unbreachable 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




## Connecting with Software VPN




## Key Features

- **Security isolation** with the world's smallest portable encryptor.
- Supports up to **50 Mbps** encrypted throughput.
- **Multi-factor authentication** to strengthen access security.
- **Tamper-evident design** alerts users to unauthorised physical access attempts.
- **Centralise management** for real-time monitoring, automatic security updates, blacklisting of lost devices, and more.
- **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 through **plug-and-play functionality** and automated provisioning.
- **Quantum-ready encryption** for future-proof protection against emerging quantum computing threats.

## Ideal For

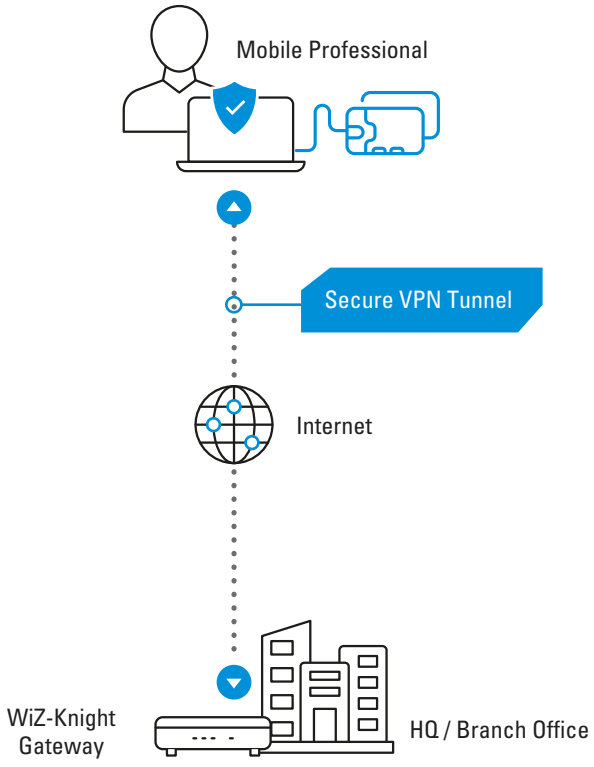
- **Hybrid workforce** professionals who frequently travel or work from home.
- **C-Suite executives** who handle highly confidential or sensitive data.

# Flexible Deployment Variants for Secure Remote Connectivity

## WiZ-Knight On-Premises

**On-premises deployment** ensures maximum security and control, using encryptor to establish a hardware-enforced VPN tunnel for secure remote access to headquarters or branch offices.

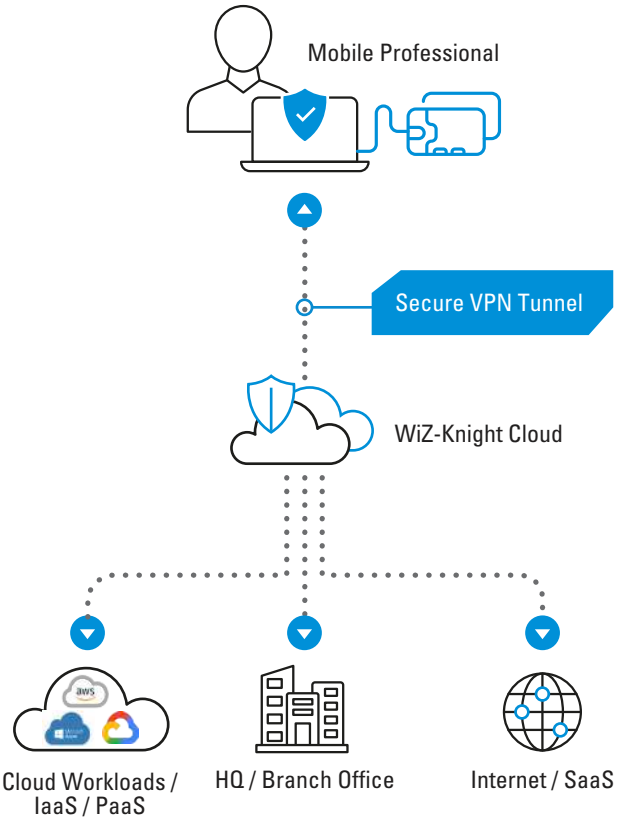
- **Dedicated High-Performance Gateway**
  A 10 Gbps aggregated throughput appliance designed for secure connectivity and managing up to 10,000 concurrent users.
- **Zero-Trust Architecture with Dual Authentication**
  Enforces certificate-based digital signature (RSA/ECDSA) and device posture validation, ensuring no entity is trusted by default.
- **Hybrid Quantum-Resilient Encryption**
  AES-256 plus ML-KEM-1024 for future-proof security against quantum computing threats.
- **Full Integration with Enterprise Networks**
  Seamless integration with Active Directory, robust key management, and granular policy controls tailored to the IT environments.
- **On-Premises Control & Data Sovereignty**
  Keeps data and VPN management within own infrastructure, ideal for classified or highly regulated environments.




## WiZ-Knight Cloud

**Cloud deployment** provides secure, scalable remote access to corporate networks without the need for additional on-premises infrastructure, enabling faster rollouts and greater agility for modern businesses.

- **Portable, Plug-and-Play Form Factor**
  Palm-sized, USB-powered dongle with dual-band Wi-Fi support (2.4GHz/5GHz) for mobile professionals.
- **Cloud-Hosted Dedicated VPN Servers**
  Each client receives a dedicated VPN server hosted on leading cloud service providers with OpenVPN protocol, ensuring scalable, isolated connectivity.
- **Multi-Factor Authentication with Mobile Token**
  Uses mobile-based digital tokens for seamless user authentication.
- **Tamper-Evident Enclosure & OTA Updates**
  Ensures device integrity with over-the-air (OTA) patching.
- **Built for Hybrid & Remote Workforces**
  Empowers professionals with secure remote access over untrusted Wi-Fi networks, ideal for flexible, modern business models.



# Use Cases for Wiz Knight

Government agencies and critical industries face rising cyber threats exploiting VPN vulnerabilities. WiZ-Knight secures remote access with encrypted data transmission, preventing unauthorised access. It protects sensitive communications, financial data, and critical infrastructure, strengthening cyber defences against ransomware, breaches, and nation-state attacks.

**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.

SECURE WHAT MATTERS

## ST Engineering Cybersecurity

With over two decades of cybersecurity expertise, ST Engineering's Cyber business has evolved from a focus on cryptography to leading in end-to-end cybersecurity solutions. We protect government entities, critical infrastructure, and enterprises against evolving threats. Our capabilities include operating over 20 global Cybersecurity Operation Centres (SOCs), training 2,500 professionals, and driving innovation through R&D. Leveraging deep engineering expertise, we integrate advanced cybersecurity into communications and industrial systems, empowering organisations to achieve cyber resilience through a comprehensive approach encompassing people, processes, and technology. We secure what matters.

www.stengg.com/en/cybersecurity  sg.linkedin.com/showcase/st-engineering-cybersecurity/

ST Engineering