WiZ-Knight Wireless Encryptor

Securing the future of hybrid work

ST Engineering

The future of work, a hybrid of in-office and work- from-anywhere, is here to stay.

So are the cyber threats.

58% of Chief Information Security Officers (CISO) have seen **more targeted attacks** since enabling widespread remote work.

– 2021 Voice of the CISO Report

US$1m **increase in average data breach cost** whenever remote work was a casual factor.

– Cost of a Data Breach Report 2021

Asia was the **most attacked region** of 2021.

– X-Force Threat Intelligence Index 2022

Remote working increases the cyber-attack surface of businesses.

Due to poorly protected network and software systems, the hybrid workforce is exposed to an alarming array of cyber threats when working from home or in public.

Top Cyber Threats

Malware

is secretly installed on your device when you open **infected attachments** or click on **malicious links**, allowing attackers to gain access to your device and execute unauthorised actions.

Denial of Service (DOS) attacks

disrupt network services by overwhelming the target with traffic to trigger a crash, adversely affecting business functions.

Packet sniffers

are deployed to monitor and capture data packets flowing across public and corporate networks. From the captured data packets, cyber criminals can **extract passwords**, **email addresses** and other sensitive information.

Rogue WiFi

are wireless access points offered at hotels, cafes and in public areas, that have been installed with malware to gain **unauthorised access** to your device.

Is software VPN safe enough?

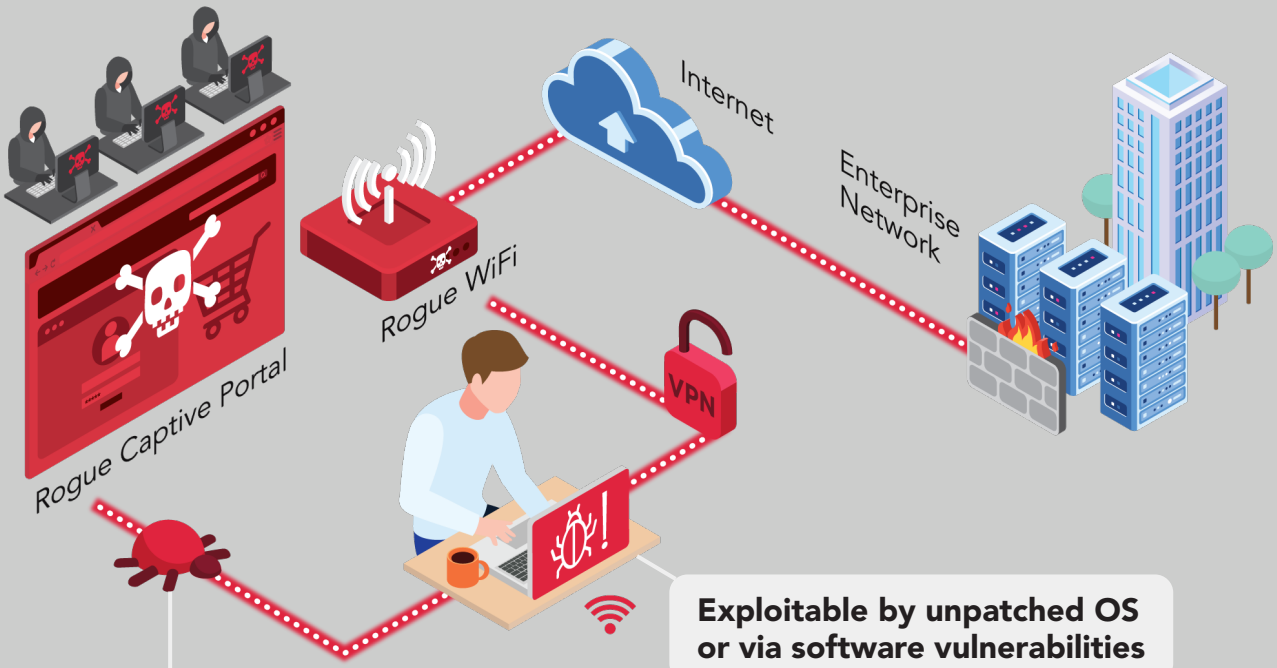
Software VPN are programmes that are easily exploitable with unpatched operating system (OS) and highly susceptible to software vulnerabilities.

Once malware infiltrates your computer, criminals can disable the software VPN, take control of your computer remotely and access your company network to commit data theft and cyber attacks.

How unauthorised access is possible via rogue captive portals with software VPN

In common software VPNs, remote workers are connected to public/home WiFi before a secure VPN connection is established to corporate network.

Within this short time span, hackers can inject malware into the laptop via rogue WiFi before the network connection is successfully secured.



WiZ-Knight

The world's first and smallest wireless encryptor for your hybrid workforce

The vision to **re-engineer the huge, conventional encryptor** typically deployed at the backend of the server room, into a **lightweight and portable device** for the hybrid workforce.

The synthesis of multi-disciplinary cybersecurity expertise including software/ firmware, hardware, system and testing, crypto, mechanical, and production.

The result of rigorous testing of innovative new security architecture ergonomically designed for remote workers.

WiZ-Knight

Provides a secure wireless VPN connection to corporate office

The **smallest wireless encryptor** in the world specially designed for the hybrid workforce.

Delivers the **highest network security** that cannot be disabled even in a compromised computer.

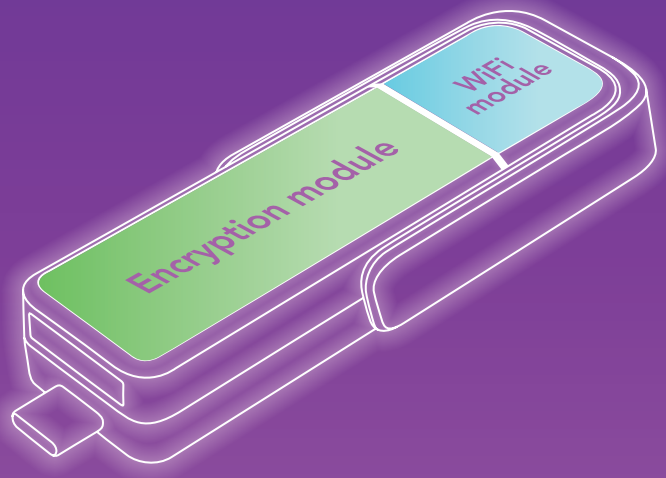
Ease of use with two simple steps to access networks securely.

Cybersecurity by Design backed by **quality assurance** to provide peace of mind for organisations.

CES INNOVATION AWARDS 2022 HONOREE

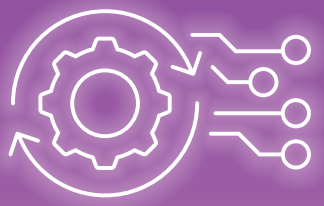
Connect to networks with confidence

Hardware-enforced encryption technology enhances protection against cyber threats in home and public networks including hotel, cafes and airport lounges.



Physical separation of encryption and WiFi modules in a 2 piece design eliminates OS vulnerabilities exploitation and blocks network access to hackers.

Cybersecurity by Design including AES-256-CBC algorithm for data confidentiality, Secure Hash Algorithm (HMAC SHA-256) for integrity protection and multi-factor authentication.



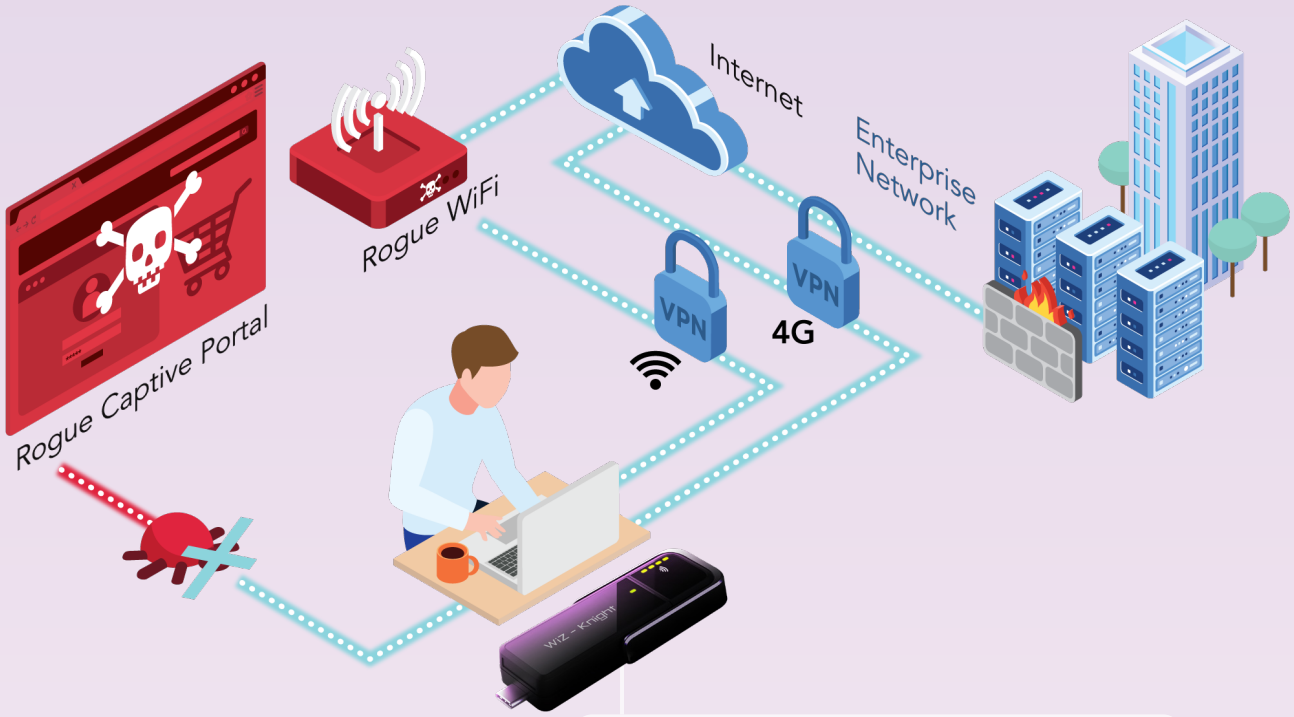
Advanced encryption allows organisations to implement their **unique customised coding**, on top of the encryption that is proven to be computationally secure with no known backdoors and used by various governments to encrypt sensitive data.

Eliminate the vulnerabilities of software VPN

As a standalone device fully equipped to run a VPN connection, WiZ-Knight's secure connection cannot be disabled, bypassed or diverted even when your computer is compromised.

How WiZ-Knight provides a secure wireless connection and prevents malicious entry into protected networks

Hardware VPNs such as WiZ-Knight minimise cybersecurity risk by reducing the entry points for cybercriminals.

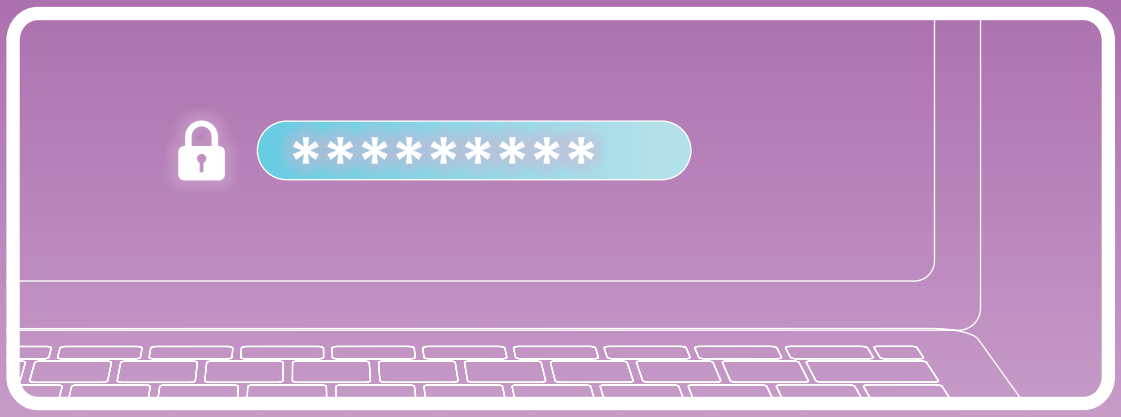


Malicious activities into protected network are blocked by the physical separation of WiZ-Knight encryption and WiFi modules

Simple and secure for the remote workforce

Small as a thumb drive and **powered by USB**, you can take this lightweight encryptor anywhere.

Designed to be easy to use, you simply **plug in WiZ-Knight** and **key in the user login** to access networks securely.



ST Engineering Info-Security Pte. Ltd.
cybersecurity@stengg.com

www.stengg.com/cybersecurity