



Ensuring Encrypted Data Transmission via VPN

End-to-End Encryption | Zero Trust

Why Encrypted Data Transmission Matters?

- Sensitive data is exposed during transmission



Unencrypted traffic can be **intercepted, captured, or modified.**

- Regulatory requirements demand encryption



NIS2, CRA, ISO 27001, and industry standards require encrypted communication paths.

- Internal networks are not inherently secure



Unsecured devices or malicious insiders can exploit unprotected channels.

- Encryption prevents interception & tampering



Protects against **data interception, replay attacks, and unauthorized access.**

How a VPN Ensures Encrypted Data Transmission?

Encrypted Tunnel

Creates an encrypted tunnel to prevent interception and unauthorized listening.



Secure Across Any Network

Keeps data encrypted and unreadable across untrusted networks.

Integrity & Authorized Access

Ensures data integrity and restricts access to authenticated users/devices.



VPN Risks for Enterprises

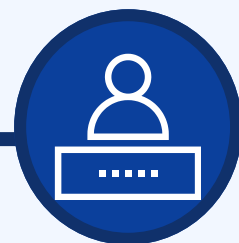
**Overly Broad
Access for
VPN Users**



**Unsecured or
Infected
Endpoints**



**Shared Accounts
and Weak Access
Control**



**Outdated or
Unpatched
VPN Gateways**



**Limited
Visibility and
Monitoring**



A dark blue rounded rectangular box with a white border, containing the text "ZTA VPN Solution" in yellow. The box is centered horizontally and partially overlaid by a decorative background of blue wavy lines.

ZTA VPN Solution

Traditional VPN v.s ZTA VPN



Traditional VPN

- Implicit trust
- Broad access
- Password-based
- High exposure



ZTA VPN

- **Never trust**
- **Least privilege**
- **Passwordless + MFA**
- **Risk-based checks**

Four Essentials of ZTA VPN Security

End-to-End Encryption

IPsec / TLS secure all data in motion.



Authentication

MFA, Passwordless, Passkey to eliminate credential theft risks.



Access Control

Least privilege, role-based access, per-session verification.



Protection

AI detects anomalies and fills gaps in traditional rules.



End-to-End Encryption



ZTA VPN > Client-to-Site **IPv4**

ZTA VPN Setup Client List Page Setting Connection Status Connection Log

Server Setting [Modify the Server Setting](#) * means that after the configuration changes, you need to redownload the certificate to apply the new settings.

Service Status	Start
Enable	<input checked="" type="checkbox"/> Note : It will take a while to activate the ZTA VPN. Please wait patiently.
Local Interface	<input type="checkbox"/> <u>Hide</u> 192.168.190.95 172.16.10.1

- **5x faster** than mainstream VPNs
- **UDP/TCP encryption** for low-latency transmission
- **ChaCha20 + Poly1305** modern cryptography with no known security flaws
- **Lightweight codebase**, smooth on any device

Multi-Factor Authentication



Administrator Account Security Setting IP Address Clear Data

Custom the Rules of Password :

Enable

The shortest length(3-64 characters)

Must Contain Uppercase Letters Lowercase Letters Numerical Digits Non-alphanumeric Letters

The password can not contain the previous password

PSWD cannot be the same as old one(s) times

Change password every day(s) (0 means no limit)

2-Step Verification Rule :

Verify every time you login

After the account verification is successful, how long does it take for the 2-step verification to be unnecessary Hour

- Requires users to verify identity with **password + second factor**



- Uses **Google/Microsoft Authenticator**

- **Protects accounts** even if passwords are compromised

- Works for **account login, web auth, and SSL VPN**

Passwordless Authentication



- **Stores private keys on user devices** to block phishing attacks
- Users complete one-time binding through the **ShareTech Authenticator** app
- Reduces management costs and enables **fast, large-scale deployment.**

Access Control

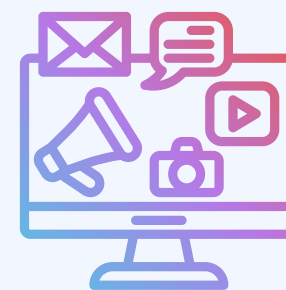


● Role-Based Access Control



Assigns access by user role and department

● Application-Level Control



Controls access by application, not just IP or port.

● Least Privilege



Users only access what they truly need

● Source & Device Control



Device- and location-based access policies

Threat Detection & Protection

VPN x Firewall x Switch Integrated Protection



01

Encrypt

VPN encrypts all traffic



02

Inspect

Firewall inspects and logs VPN traffic



03

Block

AI identifies and blocks zero-day and unknown threats in real time



04

Isolate

Automatically isolates infected devices at the switch port level



05

Prevent

Stops internal spread and data leaks

Key Benefits of ZTA VPN Security

Stronger Security Posture

Reduces risks from credential theft, lateral movement, and unknown threats.



Better Data Protection & Compliance

Protects sensitive data in transit and helps meet regulatory requirements.

Lower Operational Risk & Cost

Minimizes breach impact, simplifies access management, and reduces long-term security costs.



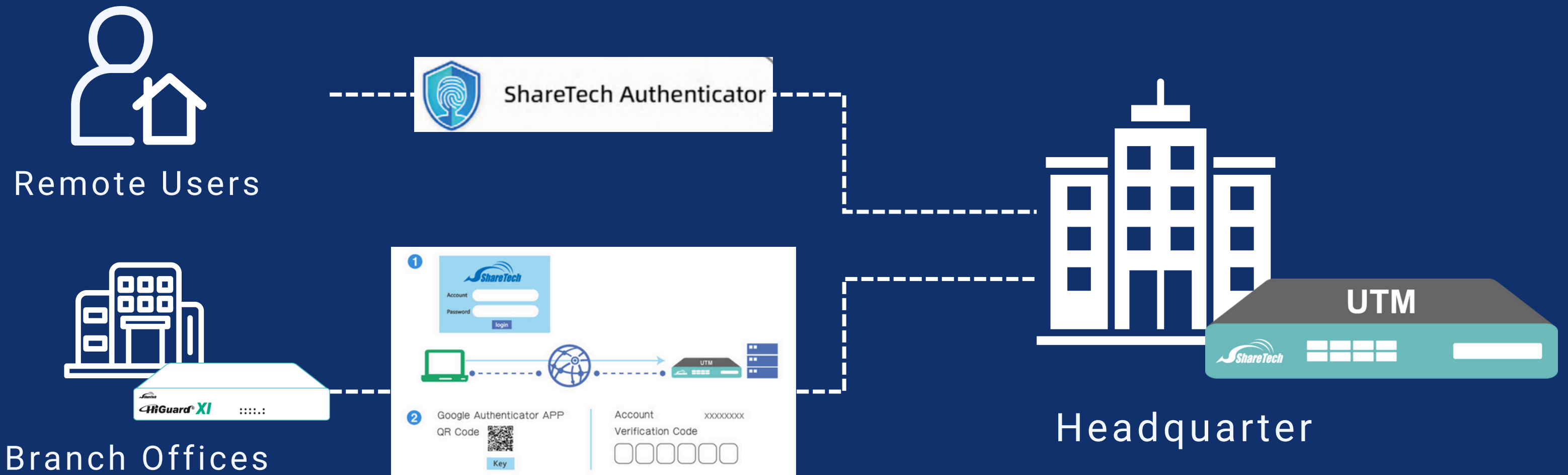
A dark blue rounded rectangular box with a white border, containing the text "Use Cases" in a bold, yellow, sans-serif font. The box is centered horizontally and is surrounded by a decorative background of light blue wavy lines that create a sense of motion and depth.

Use Cases

Remote Workforce Secure Access

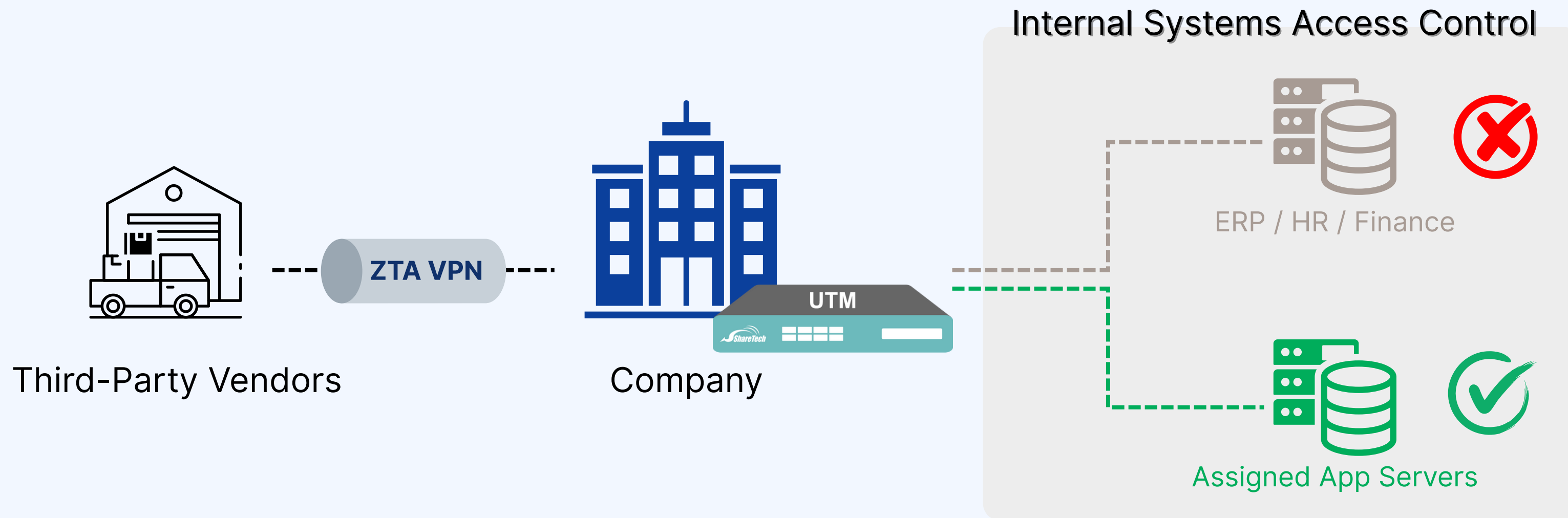
01

- Encrypted access for remote users and branch offices via **ZTA VPN**
- **MFA** enforced to prevent credential abuse
- **Least-privilege** access to internal systems only



Applicable Scenarios:

Enterprise HQ & Branches | Hybrid Workforce | Cross-Border Teams | Mobile Staff



Third-Party & Vendor Access Control

- **Time-limited, role-based** access for external vendors
- **Application-level access** instead of full network reach
- All activities inspected and **logged** by firewall

02

Applicable Scenarios:

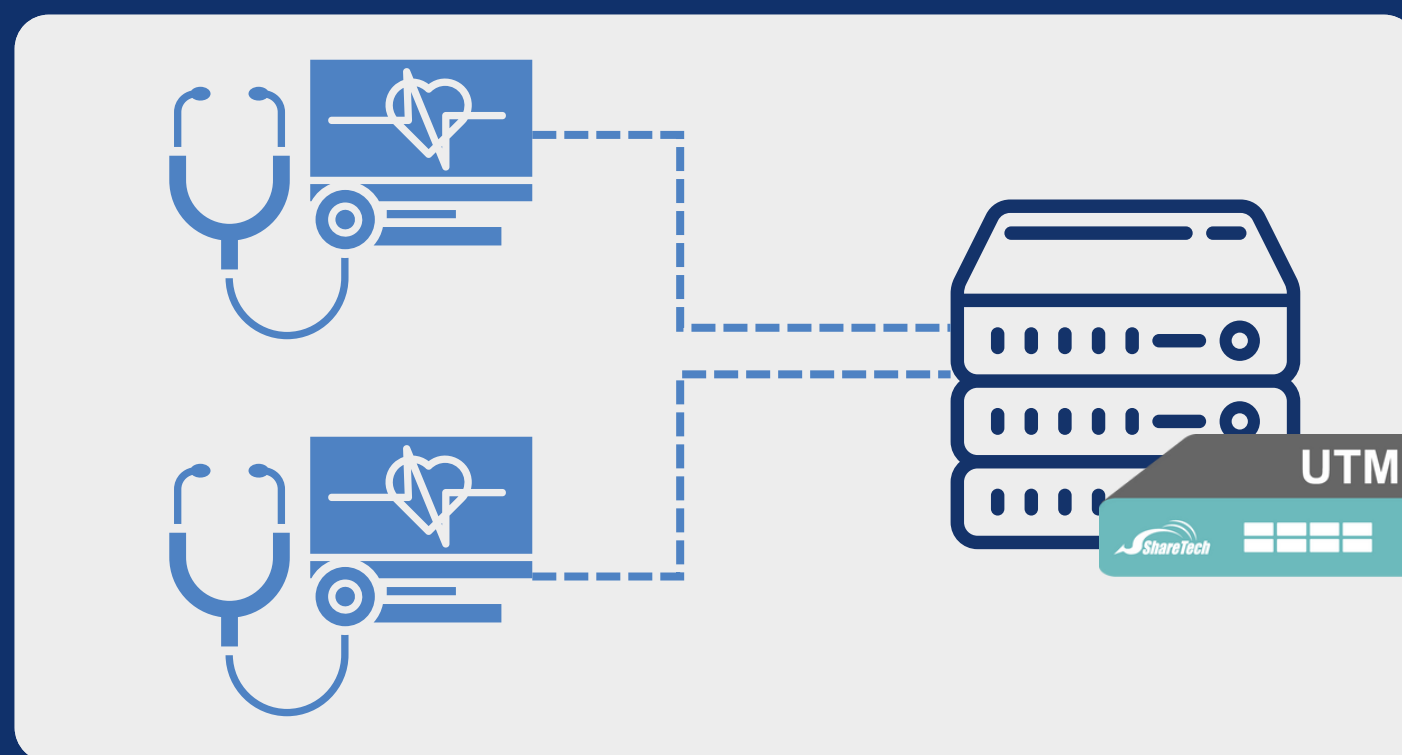
Manufacturing | System Integrators | Healthcare IT | Critical Infrastructure | Enterprise IT Outsourcing

03

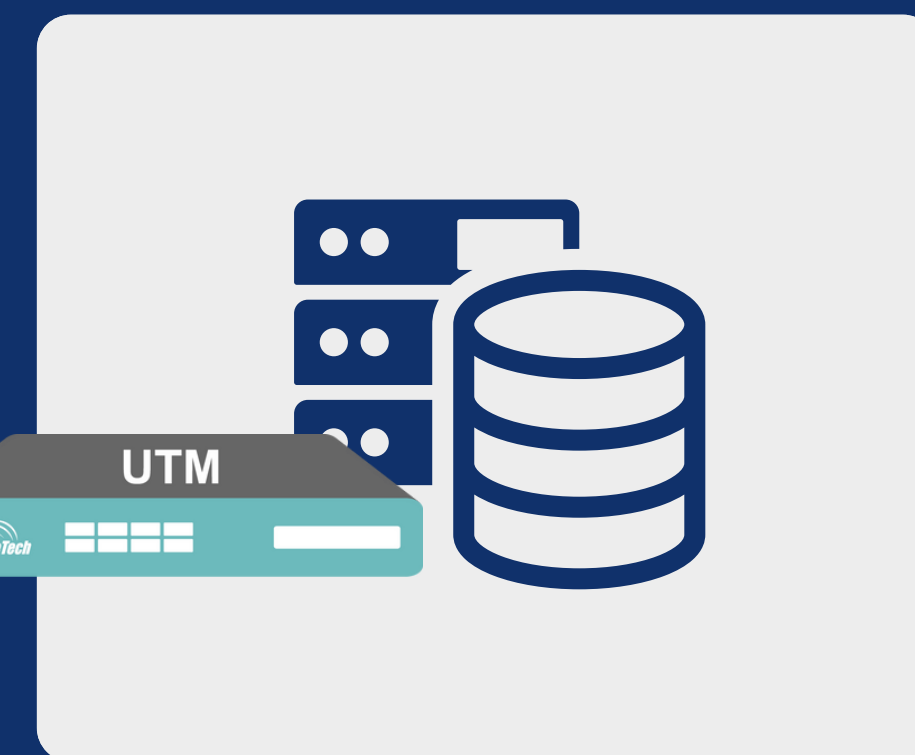
Internal Data Transmission

- **Encrypted VPN tunnels** secure data exchange between internal systems
- **Protects sensitive data** from sniffing and man-in-the-middle attacks
- Ensures secure communication across **departments, sites, and network zones**

Internal Source Systems



Central Data Center



Applicable Scenarios:
Healthcare | Financial Services | Smart Factory | Government & Critical Infrastructure



**Encrypt everything.
Verify everyone.
Trust no one by default.**

A dark blue horizontal bar containing four elements from left to right: a circular icon with four white symbols (a speech bubble, a hand holding a key, an envelope, and a hand pointing), a QR code labeled "Website", a QR code labeled "LinkedIn", and a QR code labeled "Youtube".