The fastest way to **connect**, **protect** and **control** OT networks and critical infrastructure.

Security Overview

WE'RE SECURE BY DESIGN

What makes Tosi so secure

1 Secure by design, secure by default
All inbound ports are closed, making your infrastructure invisible to attackers.

2 Physical matching
Tosi Key physically matched with a Tosi Node.

3 Two-factor authentication
2FA means that there are two different things required for the user to authenticate and get access.
1. **Something that the user has:** Tosi Key
2. **Something that the user knows:** Password

4 End-to-end encryption
The VPN connection is established directly between the Tosi Key and Tosi Node / Tosi Hub and the data can be decrypted only at the connection end points. Nobody - not even Tosi - can decrypt the data in between.

5 Simplicity
Simplicity is good also for security. In addition to making our products secure, we have put a lot of effort on making them easy to use. With fewer things for users to remember and worry about, Tosi products are practically impossible to misconfigure.

6 No backdoors
Tosi does NOT retain any private keys or passwords for the products. Our technical support can access the Tosi Node and Tosi Hub only after the user has explicitly turned on the remote support feature.

7 Industry standard and proven technologies
Such as the RSA crypto system, AES encryption, Diffie–Hellman key exchange and TLS, are used in our products.

8 Your data is yours
- No lockup to a specific cloud provider.
- No data stored in Tosi infrastructure.

US HQ
1212 Corporate Drive
Suite 170
Irving, Texas 75038

GLOBAL HQ
Elektroniikkatie 2a
7th floor
90590 Oulu, Finland

CONTACT US