

## Security Solutions

### Protecting Your Digital Assets with End-to-End Cybersecurity

Cyber threats have become one of the most critical operational risks for modern organizations. **Teknoser** delivers comprehensive cybersecurity solutions that protect your information assets, IT infrastructure, and digital processes. Our mission is not only to secure your systems but also to ensure business continuity, protect corporate reputation, and maintain operational resilience.

From network security to endpoint protection, email security to data loss prevention, we offer a wide range of integrated cybersecurity services. By embedding access control and monitoring systems into your existing environment, we build a multi-layered defense architecture tailored to your organization's risk profile, industry, and scale.

## IT Security Solutions

### A Comprehensive Approach to Safeguarding the Digital Enterprise

Cyber threats are more advanced, automated, and dangerous than ever. Traditional security measures alone are no longer sufficient. **Teknoser** delivers an end-to-end IT security architecture that ensures your digital assets remain visible, controlled, and always protected.

## Network Security

Modern network security goes far beyond traditional firewalls. **Teknoser** secures your entire network infrastructure with Zero Trust principles.

### Our Network Security Capabilities:

-  Next-Generation Firewalls (NGFW)
-  SASE / SSE architectures
-  IPS / IDS systems
-  Application awareness
-  URL filtering
-  SSL inspection
-  Data Loss Prevention (DLP)
-  Micro-segmentation

## **Endpoint Security (EDR / XDR)**

Endpoints are the most targeted surface in cyberattacks. **Teknoser** provides advanced threat detection, malware analysis, and complete visibility.

### **Key Features:**

-  EDR / XDR platform integration
-  Behavioral analysis & threat detection
-  Ransomware protection
-  Full endpoint visibility
-  Automated response actions
-  Identity-based protection

## **Identity & Access Management (IAM)**

Ensuring the right user accesses the right resource at the right time is fundamental in cybersecurity.

### **Teknoser IAM Services:**

-  MFA, SSO & Zero Trust access
-  Privileged Access Management (PAM)
-  User lifecycle management
-  Identity-driven security controls

## **Email & Application Security**

Email remains the most common entry point for cyberattacks.

### **Our Solutions:**

-  Anti-phishing
-  Sandbox analysis
-  Email Gateway security

-  O365 & Google Workspace protection
-  Content filtering
-  Domain protection (DMARC / DKIM / SPF)

## **Cloud Security**

As organizations move toward hybrid and multi-cloud environments, securing workloads becomes increasingly complex.

### **Expertise Areas:**

-  CSPM / CWPP
-  Cloud firewalls
-  Zero Trust cloud access
-  API security
-  Workload protection
-  Container & Kubernetes security

## **Vulnerability Management & Penetration Testing**

Visibility is the foundation of proactive cybersecurity.

### **Our Scope:**

-  Continuous vulnerability scanning
-  Penetration testing
-  Red Team assessments
-  OT vulnerability analysis
-  Risk scoring & reporting

## **Teknoser IT Security Value Proposition**

-  Vendor-agnostic solutions
-  Large cybersecurity expert team

-  SOC integration
-  Nationwide support
-  End-to-end architectural design
-  Continuous monitoring, reporting & improvement



## OT Security Solutions (Industrial Cybersecurity)

### Security in Industrial Environments Is No Longer Optional — It Is Essential

OT systems are critical for energy, manufacturing, transportation, and other industrial sectors. Attacks on these environments can cause production loss, downtime, or even physical damage.

As one of Turkey's leading OT security integrators, Teknoser helps industrial operations become observable, isolated, secure, and resilient.

### OT Asset Discovery & Passive Monitoring

The biggest challenge in OT environments is lack of visibility.

#### Teknoser Provides:

-  Passive OT asset discovery
-  Detailed inventory (interface, firmware, protocol, vendor)
-  Industrial protocol analysis (Modbus, DNP3, S7, IEC104, etc.)
-  Unknown device & risk detection

### OT IDS / Anomaly Detection

Signature-based tools are not enough—behavior-based detection is essential.

#### Our Capabilities:

-  Network behavior profiling
-  Fake command detection
-  Unexpected traffic alerts
-  Process change detection
-  ICS/SCADA-focused threat detection

## OT Segmentation & Secure Architecture Design

Teknoser designs ICS networks aligned with ISA/IEC 62443.

### Our Scope:

-  Zone & Conduit architecture
-  OT DMZ design
-  Jump Server architecture
-  Firewall / NGFW integration
-  OT-IT separation
-  Lateral movement prevention

## Secure Remote Access (SRA)

Remote maintenance access carries significant risk.

### Our Solutions:

-  Secure Remote Access (SRA)
-  Enforced MFA
-  Fully recorded & encrypted sessions
-  Authorized maintenance workflows
-  Vendor access management

## OT Vulnerability & Risk Management

Many OT devices cannot be patched and require specialized handling.

### Recommendations:

-  OT-specific vulnerability scanning
-  Device-based risk scoring
-  Firmware, protocol & behavior analysis
-  Reporting & remediation roadmaps

## 🛡️ OT Firewall, Deception & Network Access Control

Advanced protection for critical industrial environments.

### Key Solutions:

- 🔥 OT Firewalls & ICS IPS
- 🔒 OT NAC solutions
- 🛡️ OT Deception (honeypots / decoys)
- 📡 ICS protocol validation
- ✋ Lateral movement prevention

## ⭐ Teknoser OT Security Value Proposition

- 🎓 OT/ICS-certified engineering team
- 🛡️ Experience across energy, manufacturing, public sector, transportation & telecom
- 🏭 One of Turkey's most comprehensive OT security portfolios
- 🛡️ Vendor-agnostic architecture
- 🕒 7/24 operational support
- 🌐 IT-OT integration consultancy
- 📈 IEC 62443-compliant architecture design