SILVERNET® CYBERSECURITY COMPLIANCE PACK

Series 7 Industrial Ethernet Switches

Customer Edition – Version 1.0

SilverNet® – Secure. Reliable. Engineered for Performance.

SilverNet is a UK-based designer and manufacturer of professional-grade wireless and switching solutions. The **Series 7 Industrial Switch family** is engineered for mission-critical environments requiring high reliability, robust security, and long-term operational resilience.

This Cybersecurity Compliance Pack provides a clear, authoritative overview of the Series 7 security posture, aligned with industry best practice and regulatory expectations.

---

1. Introduction

The **SilverNet Series 7 Industrial Switches** are designed for secure, high-availability networking in demanding environments such as CCTV, transportation, utilities, industrial automation, and public-sector infrastructure.

This document outlines the cybersecurity controls, risk posture, and recommended deployment practices to support compliance with:

- ISO/IEC 27001:2022
- NCSC Cyber Assessment Framework (CAF)
- Cyber Essentials Plus
- NIST SP 800-82 (Industrial Control Systems)
- NIST SP 800-53
- Secure-by-Design principles

This pack is intended for procurement teams, IT security managers, auditors, and organisations requiring assurance of product security.

---

2. Product Security Overview

The Series 7 Industrial Switches incorporate multiple layers of protection to safeguard data, ensure operational integrity, and support secure deployment in critical environments.

Core Security Features

- Secure HTTPS management interface
- SSH for encrypted CLI access
- SNMPv3 with authentication and encryption
- VLAN segmentation and ACL support
- STP/RSTP protection features (BPDU Guard, Root Guard, Loop Guard)
- Port security with MAC binding
- PoE control and monitoring (PoE models)
- Hardened industrial-grade enclosure (IP-rated model-dependent)
- Wide-temperature operation for harsh environments

These features provide a strong security foundation for public-sector, industrial, and critical-infrastructure deployments.

---

3. Threat Landscape

SilverNet evaluates threats across the full lifecycle of industrial networking equipment. Relevant threat categories include:

- Interception / eavesdropping
- Man-in-the-middle (MITM) attacks
- Credential compromise
- Firmware tampering
- Denial of service (network flooding, STP manipulation)
- Physical tampering
- Misconfiguration
- Device substitution (PoE or port-based attacks)

Industrial networks are often exposed to additional risks such as untrusted field devices, remote cabinets, and limited physical security.

---

4. Cybersecurity Risk Assessment

Risk Summary

Risk Category	Likelihood	Impact	Rating
Eavesdropping	Medium	High	High
MITM Attack	Medium	High	High
Credential Compromise	Medium	High	High
Firmware Tampering	Medium	High	High
Network Flooding / DoS	Medium	Medium	Medium
Physical Tampering	Medium	Medium	Medium
Misconfiguration	High	High	High

Applying the hardening measures in Section 6 reduces these risks to acceptable levels.

---

5. Security Controls

5.1 Access Control

- Remove all default credentials
- Enforce strong, unique administrative passwords
- Implement role-based access control (RBAC) where supported
- Restrict management access to a dedicated VLAN
- Apply IP allowlisting for administrative access
- Disable remote management unless required
- Enforce session timeouts and login attempt limits

5.2 Encryption

- Enable HTTPS for all web management
- Disable HTTP
- Enable SSH (prefer key-based authentication)
- Disable Telnet
- Use SNMPv3 only (authentication + encryption)
- Encrypt configuration backups

5.3 Firmware Integrity

- Source firmware exclusively from SilverNet
- Validate checksums before installation
- Maintain a firmware version register
- Schedule quarterly firmware review
- Disable remote firmware updates unless necessary
- Document all firmware changes

5.4 Network Security

VLAN & Traffic Segmentation

- Separate management, CCTV, IoT, and untrusted devices
- Apply ACLs to restrict inter-VLAN communication
- Use dedicated VLANs for external or contractor devices

Spanning Tree Protection

- Enable BPDU Guard
- Enable Root Guard
- Enable Loop Guard
- Enable STP/RSTP where required

Traffic Protection

- Enable broadcast storm control
- Enable multicast suppression
- Enable unknown unicast filtering
- Apply QoS to prioritise critical traffic

5.5 Port Security

- Disable unused ports
- Bind ports to specific MAC addresses (where supported)
- Enable port-security violation actions (shutdown or restrict)
- Disable PoE on unused ports
- Apply PoE power limits
- Monitor PoE draw for anomalies (device substitution, tampering)

5.6 Physical Security

- Install switches in locked cabinets or enclosures

- Use tamper-proof mounting hardware
- Secure and label all cabling
- Disable physical reset button (if supported)
- Maintain asset register (serial numbers, MAC addresses, firmware versions)

5.7 Monitoring & Logging

Syslog

- Export logs to a central logging server
- Use secure transport (TLS) where supported
- Log:
  - Login attempts
  - Configuration changes
  - Port up/down events
  - STP events
  - PoE faults
  - Security violations

SNMP Monitoring

- Use SNMPv3 only
- Restrict SNMP access to monitoring servers
- Monitor:
  - CPU load
  - Memory utilisation
  - Temperature
  - Port status
  - PoE consumption
  - Error counters

Event Alerts

Enable alerts for:

- Failed login attempts
- Port security violations
- Firmware changes
- Device reboots

---

6. Secure Deployment Guidance

Pre-Deployment

- Update to latest firmware
- Remove default credentials
- Configure management VLAN
- Disable insecure protocols
- Apply ACLs and IP allowlists
- Document device identity (serial, MAC, firmware)

Installation

- Secure cabinet or enclosure
- Label and document ports
- Apply port-security policies
- Validate VLAN segmentation
- Ground and protect cabling

Post-Deployment

- Enable Syslog and SNMPv3
- Export secure configuration backup
- Review logs weekly
- Rotate credentials every 6–12 months
- Conduct annual penetration testing

---

7. Compliance Alignment

Cyber Essentials / CE+

Supports compliance with:

- Secure configuration
- Boundary firewalls
- Access control
- Patch management
- Encrypted communications

ISO/IEC 27001:2022

Relevant controls supported:

- A.5.7 Secure development
- A.8.16 Monitoring activities
- A.8.20 Network security
- A.8.24 Use of cryptography
- A.8.28 Secure coding
- A.8.29 Security testing
- A.8.31 Secure configuration

NCSC CAF

Supports:

- Managing security risk
- Protecting against cyber attack
- Detecting cyber security events
- Minimising impact of incidents

NIST SP 800-82 / 800-53

Supports:

- ICS network segmentation
- Secure remote access
- Configuration management
- Event monitoring
- Device hardening

8. Residual Risk Statement

When deployed and hardened according to this compliance pack, the Series 7 Industrial Switches demonstrate a **Low to Medium residual risk profile**, suitable for:

- Public-sector CCTV networks
- Transportation and highways infrastructure
- Utilities and industrial automation
- Local government networks
- Enterprise edge switching
- Critical-infrastructure applications (with enhanced monitoring)

Ongoing operational discipline remains essential.

---

9. Optional Appendices

Available on request:

- Secure configuration baseline
- Hardening checklist
- Risk register
- Penetration testing scope
- Supplier assurance questionnaire responses
- Customer-facing security whitepaper