SILVERNET
WIRELESS-NETWORK-SOLUTIONS

SILVERNET® CYBERSECURITY COMPLIANCE PACK

PRO Range – Gen 5 Wireless Platform

Customer Edition – Version 1.0

SilverNet® – Secure. Reliable. Engineered for Performance.

SilverNet is a UK-based designer and manufacturer of professional-grade wireless networking solutions. For over a decade, our products have delivered high-performance connectivity, robust security, and long-term reliability in demanding outdoor environments.

The **SilverNet PRO Range Gen 5** represents the latest evolution of our wireless platform — engineered for enhanced throughput, improved RF resilience, and a hardened security architecture aligned with modern cybersecurity expectations.

This Cybersecurity Compliance Pack provides customers, auditors, and procurement teams with a clear, authoritative overview of the PRO Range Gen 5 security posture.

---

1. Introduction

The **SilverNet PRO Range Gen 5** is a high-capacity outdoor wireless platform designed for secure point-to-point and point-to-multipoint deployments. 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 800-30 & 800-53
- Secure-by-Design principles

This pack is intended for organisations requiring assurance of product security and alignment with recognised standards.

---

2. Product Security Overview

The PRO Range Gen 5 incorporates multiple layers of protection to safeguard data and ensure operational integrity across diverse deployment environments.

Core Security Features

- **AES-256 encrypted wireless link**
- **Secure HTTPS management interface**
- **Layer-2 bridging with VLAN segmentation**
- **Hardened operating system with reduced attack surface**
- **Directional antennas and advanced RF filtering**
- **IP67-rated enclosure for environmental resilience**
- **Configurable access control and traffic management**

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

---

3. Threat Landscape

SilverNet evaluates threats across the full lifecycle of wireless infrastructure. Relevant threat categories include:

- Interception / eavesdropping
- Man-in-the-middle (MITM) attacks
- Credential compromise
- Firmware tampering
- Denial of service (RF or network)
- Physical tampering
- Misconfiguration

Directional antennas, short-range propagation characteristics (model-dependent), and encrypted management sessions significantly reduce interception and MITM exposure.

---

4. Cybersecurity Risk Assessment

Risk Summary

Risk Category	Likelihood	Impact	Rating
Eavesdropping	Low	High	Medium
MITM Attack	Medium	High	High
Credential Compromise	Medium	High	High
Firmware Tampering	Medium	High	High
RF Interference / DoS	Medium	Medium	Medium
Physical Tampering	Medium	Medium	Medium
Misconfiguration	High	High	High

SilverNet recommends applying the hardening measures in Section 6 to reduce these risks to acceptable levels.

---

5. Security Controls

5.1 Access Control

- Strong, unique administrative passwords
- Removal of default credentials
- Management restricted to a dedicated VLAN
- IP allowlisting for administrative access
- Remote management disabled unless required

5.2 Encryption

- AES-256 over-the-air encryption
- HTTPS recommended for all management sessions
- Regular key rotation
- Insecure protocols disabled (HTTP, Telnet, SNMPv1)

5.3 Firmware Integrity

- Firmware sourced exclusively from SilverNet
- Checksum validation prior to installation
- Scheduled firmware review and updates
- Remote firmware updates disabled unless necessary

5.4 Network Security

- VLAN segmentation
- STP/RSTP guard features
- QoS to prevent link saturation
- Broadcast/multicast control

5.5 Physical Security

- Tamper-proof mounting hardware
- Secure PoE injector and cabling
- Reset button disabled where supported
- Installation at height to reduce access risk

5.6 Monitoring & Logging

- Syslog export to central logging
- Monitoring of failed login attempts
- Link-quality and RF-health monitoring
- Secure configuration backups

6. Secure Deployment Guidance

Pre-Deployment

- Update to latest firmware
- Change all default credentials
- Enable HTTPS
- Assign management VLAN
- Apply IP allowlists

Installation

- Precise antenna alignment
- Shielded, grounded cabling
- Secure mounting hardware
- Document device serial numbers and MAC addresses

Post-Deployment

- Enable centralised logging
- Maintain secure configuration backups
- Review logs regularly
- Rotate encryption keys every 6–12 months
- Annual penetration testing of the management plane

---

7. Compliance Alignment

Cyber Essentials / CE+

The PRO Range Gen 5 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 the following principles:

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

---

8. Residual Risk Statement

When deployed in accordance with this compliance pack, the PRO Range Gen 5 demonstrates a **Low to Medium residual risk profile**, suitable for:

- Enterprise networks
- Local government
- Public-sector CCTV backhaul
- Industrial and IoT environments
- Critical-infrastructure applications (with enhanced monitoring)

Ongoing operational discipline remains essential.