DeepShield Cloud Connector Documentation

Version 3.2.1 | Last Updated: January 11, 2024

Document Classification: CONFIDENTIAL

1. Overview and Scope

1. This Documentation ("Documentation") describes the technical and legal specifications for the DeepShield Cloud Connector(TM) ("Cloud Connector"), a proprietary software component developed by DeepShield Systems, Inc. ("DeepShield"), that enables secure cloud integration for industrial control systems (ICS) and operational technology (OT) environments.

2. The Cloud Connector forms an integral part of DeepShield's Industrial Cybersecurity Platform and is protected under U.S. Patent No. 11,234,567 and related international patents and patent applications.

2. Technical Specifications

1. Architecture

- Distributed edge-to-cloud architecture
- Containerized deployment model
- Multi-tenant isolation framework
- Encrypted data transport layer
- Real-time synchronization protocol

2. Security Features

- AES-256 encryption for data at rest
- TLS 1.3 for data in transit
- Hardware security module (HSM) integration
- Zero-trust authentication framework
- Role-based access control (RBAC)

3. Integration Capabilities

- Native support for major ICS protocols (Modbus, DNP3, OPC-UA)
- REST API endpoints for third-party integration

- Custom connector framework for legacy systems
- Bi-directional data flow management
- Automated failover mechanisms

3. Intellectual Property Rights

1. DeepShield maintains exclusive ownership of all intellectual property rights, including but not limited to:

- Source code and object code
- APIs and integration protocols
- Authentication mechanisms
- Configuration templates
- Documentation and technical materials

2. The Cloud Connector incorporates the following third-party components under license:

- OpenSSL (Apache License 2.0)
- Docker Engine (Apache License 2.0)
- Kubernetes (Apache License 2.0)
- PostgreSQL (PostgreSQL License)

4. Deployment Requirements

1. Hardware Requirements

- Minimum 8-core processor
- 32GB RAM
- 500GB SSD storage
- Redundant network interfaces
- Hardware security module compatibility

2. Software Requirements

- Linux kernel 5.10 or higher
- Docker Engine 20.10 or higher
- Kubernetes 1.24 or higher
- Python 3.9 or higher

3. Network Requirements

- Dedicated VLAN for management traffic
- Minimum 1Gbps network connectivity
- IPv6 support
- Outbound access to DeepShield cloud services
- Port requirements as specified in Appendix A

5. Compliance and Certification

1. The Cloud Connector has been certified compliant with:

- IEC 62443-4-2 Security Level 2
- NIST SP 800-82r3
- ISO/IEC 27001:2022
- DNV-GL Maritime Cybersecurity Class Notation

2. Annual security assessments are conducted by independent third-party auditors.

6. Support and Maintenance

1. DeepShield provides:

- 24/7 technical support
- Quarterly security updates
- Emergency patch management
- Configuration assistance
- Performance optimization

2. Service Level Agreement (SLA) terms:

- 99.99% availability guarantee
- 15-minute response time for critical issues
- 4-hour resolution time for severe incidents
- Monthly performance reports
- Dedicated technical account management

7. Legal Notices and Disclaimers

1. CONFIDENTIALITY NOTICE: This documentation contains confidential and proprietary information of DeepShield Systems, Inc. Any unauthorized reproduction, distribution, or disclosure is strictly prohibited.

2. WARRANTY DISCLAIMER: The Cloud Connector is provided "as is" without warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

3. LIMITATION OF LIABILITY: In no event shall DeepShield be liable for any indirect, incidental, special, exemplary, or consequential damages arising out of or in connection with the use of the Cloud Connector.

8. Document Control

Document Owner: Dr. Elena Rodriguez, Chief Security Architect

Technical Reviewer: James Morrison, VP of Engineering

Legal Reviewer: Corporate Legal Department

Document ID: DS-CC-DOC-2024-011

Classification: Confidential

Review Cycle: Annual

This document is maintained in accordance with DeepShield's Documentation Control Procedure (DCP-001-2024)