Request for Proposal: OT Secure Remote Access Software Solution

Table of Contents

1. Introduction and Background

This Request for Proposal (RFP) seeks a comprehensive Operational Technology (OT) secure remote access software solution enabling authorized users to safely connect to and manage industrial control systems (ICS) and OT devices remotely.

Business Requirements

- Engineering remote access capabilities
- Secure system maintenance
- Emergency response support
- Security monitoring
- Plant operations oversight
- Multi-site infrastructure management

- Compliance and audit support

Target Environment Coverage

- Industrial control systems
- SCADA systems
- PLCs
- Manufacturing equipment
- Energy management systems
- Utility infrastructure
- Critical operational assets

2. Project Objectives

1. Implement secure OT remote access with robust authentication
2. Establish comprehensive security controls
3. Enable efficient remote maintenance
4. Implement continuous monitoring
5. Ensure regulatory compliance
6. Reduce operational costs
7. Support emergency access protocols

3. Scope of Work

Implementation Services

1. Software deployment
2. Security configuration
3. Infrastructure integration
4. User and role setup
5. Monitoring implementation

6. Security control integration

Required Deliverables

1. Operational remote access solution
2. Technical documentation
3. Security guides
4. Training materials
5. Support procedures
6. Incident response protocols

4. Technical Requirements

4.1 Network Mapping and Visibility

4.1.1 Discovery and Documentation

- Network Discovery
  - Automated asset discovery capabilities
  - Real-time network topology mapping
  - Device identification and classification
  - Service and application detection
  - Port and protocol identification
  - Dependency mapping
  - Network path analysis
  - Bandwidth utilization tracking
  - Performance bottleneck detection
  - Configuration verification
- Documentation Management
  - Automated network diagram generation

  - Asset inventory maintenance
  - Configuration documentation
  - Change tracking and versioning
  - Relationship documentation
  - Access path documentation
  - Security zone mapping
  - Compliance documentation
  - Risk assessment documentation
  - Recovery procedure documentation

4.1.2 Monitoring and Analysis

- Performance Monitoring
  - Real-time network monitoring
  - Traffic analysis and reporting
  - Bandwidth utilization tracking
  - Latency measurement
  - Packet loss detection
  - Quality of service monitoring
  - Application performance tracking
  - Resource utilization monitoring
  - Capacity planning tools
  - Trend analysis capabilities
- Security Analysis
  - Traffic pattern analysis
  - Anomaly detection

  - Security zone verification
  - Access control validation
  - Policy compliance checking
  - Vulnerability assessment
  - Risk scoring
  - Threat detection
  - Incident investigation support
  - Forensic analysis capabilities

4.2 Endpoint Protection and Security

4.2.1 Malware Protection

- Detection Capabilities
  - Real-time scanning mechanisms
  - File reputation analysis
  - Behavioral monitoring
  - Machine learning detection
  - Signature-based detection
  - Heuristic analysis
  - Sandboxing capabilities
  - Zero-day threat protection
  - Rootkit detection
  - Fileless malware detection
- Response Features
  - Automated threat blocking
  - Quarantine functionality

  - Malware removal tools
  - System recovery capabilities
  - Incident notification system
  - Threat intelligence integration
  - Attack chain analysis
  - Impact assessment
  - Remediation guidance
  - Prevention recommendations

4.2.2 System Security

- Access Control
  - Application control lists
  - Process privilege management
  - Memory protection
  - File system security
  - Registry protection
  - Network access control
  - Device control
  - USB security
  - Peripheral management
  - Remote access security
- System Hardening
  - Security baseline enforcement
  - Configuration management
  - Patch management

    - Service hardening
    - Port security
    - Protocol restrictions
    - Account security
    - Password policy enforcement
    - Encryption management
    - Backup protection

4.3 Core Security Infrastructure

4.3.1 Network Security

- Segmentation Implementation
    - Network zone definition
    - Traffic flow control
    - Access control lists
    - Protocol filtering
    - VLAN management
    - DMZ configuration
    - Gateway security
    - Routing security
    - NAT management
    - QoS implementation
- Security Controls
    - Intrusion detection
    - Threat prevention
    - Firewall management

- VPN infrastructure
- Encryption protocols
- Certificate management
- Key management
- Authentication systems
- Authorization controls
- Audit logging

5. Functional Requirements

5.1 Network Control and Security

Tip: Network control and security requirements focus on establishing robust segmentation and access controls to protect OT assets. Proper implementation of these controls is crucial for maintaining the security posture of industrial systems while enabling necessary remote access capabilities.

Requirement	Sub-Requirement	Y/N	Notes
Network Segmentation - Architecture Components	Network zone definition and management		
	Segmentation policy enforcement systems		
	Traffic flow control mechanisms		
	Inter-segment communication rules		
	Gateway security control implementation		
	DMZ configuration management		
	Trust boundary establishment		

To download the full version of this document,

visit https://www.rfphub.com/template/free-ot-secure-remote-access-software-template/

Download Word Docx Version