Secure Cloud Connectivity Proposal

UnityIS® Cloud ↔ On-Prem ELK Intrusion Panels

Using UnityIS® Secure Gateway (Linux-Based Appliance)

Executive Summary

This document outlines IMRON's proposed method for securely enabling **UnityIS® Cloud** to communicate with on-premises **ELK intrusion panels** without exposing the customer's network or devices to the internet.

The proposed solution uses **UnityIS® Secure Gateway**, a hardened, Linux-based, appliance-style gateway deployed on customer premises. The gateway establishes an **encrypted, outbound-initiated secure connection** between UnityIS Cloud and the customer environment, eliminating the need for inbound firewall rules or port forwarding and significantly reducing attack surface compared to traditional remote access methods.

The customer's IT team retains full administrative control over the on-prem gateway, including operating system hardening, patching, endpoint protection, firewall rules, and monitoring.

Problem Statement

ELK intrusion panels reside on the customer's internal network and run proprietary operating systems that cannot support modern security agents or outbound cloud connectivity.

Traditional approaches (e.g., port forwarding or public IP exposure) introduce unacceptable security risks by:

- Exposing OT devices directly to the internet
- Increasing attack surface
- Violating common enterprise and OT security policies

A secure alternative is required that:

- Does not expose ELK panels to the internet

- Does not require changes to ELK firmware or OS
- Preserves UnityIS' existing IP- and port-based communication model
- Aligns with enterprise and zero-trust security best practices

---

Proposed Architecture Overview

High-Level Design

- **UnityIS® Cloud** runs centrally in IMRON's cloud environment
- A **UnityIS® Secure Gateway** appliance is deployed on-premises
- Both systems join a **private, encrypted overlay network**
- ELK panels remain unchanged on the local LAN
- All communication is **outbound-initiated, encrypted, and explicitly authorized**

Key Principle

Only UnityIS Cloud and the UnityIS Secure Gateway participate in the secure overlay network.
ELK panels do not run any agent and are never internet-reachable.

Component Responsibilities

UnityIS® Cloud

- Runs all UnityIS application logic and ELK driver functionality
- Communicates using existing ELK IP addresses and TCP ports
- Has no direct visibility into the customer LAN without gateway mediation

UnityIS® Secure Gateway (On-Prem Appliance)

- Linux-based, single-purpose appliance (no user activity)
- Deployed on **Protectli fanless hardware** with Intel networking
- Runs only:
    - Secure overlay networking software
    - Minimal Linux networking services (routing / forwarding)

- Forwards traffic between UnityIS Cloud and ELK panels
- Fully administered, hardened, and monitored by customer IT

ELK Intrusion Panels

- Remain on the internal LAN
- Require no software, firmware, or configuration changes
- Communicate exactly as they do today using IP and TCP

Why This Approach Is Secure

1. No Inbound Network Exposure

- No port forwarding
- No public IPs
- No inbound firewall exceptions

All connectivity is outbound-initiated, aligning with zero-trust and modern firewall models.

---

2. End-to-End Encryption

- All traffic between UnityIS Cloud and the Secure Gateway is encrypted end-to-end
- Encryption is identity-based and device-specific
- Traffic cannot be intercepted or decrypted in transit

---

3. Explicit Authorization & Access Control

- Gateway devices must be explicitly approved to join the secure network
- Unauthorized systems cannot connect
- Access can be revoked instantly by removing authorization

---

4. Minimal Attack Surface

- Only one on-prem system participates in the secure connection

- ELK panels remain isolated and non-internet-reachable
- Gateway access can be restricted to:
    - Specific ELK IP addresses
    - Specific TCP ports

---

5. Customer-Controlled Security

The customer's IT team may:

- Own root / administrative access to the gateway
- Apply Linux OS hardening standards
- Install endpoint protection or monitoring agents
- Manage firewall and routing policies
- Control patching cadence and maintenance windows
- Forward logs to SIEM or monitoring platforms

IMRON does **not** require administrative control over the gateway.

UnityIS® Secure Gateway Clarification

The term **UnityIS® Secure Gateway** refers to:

- A hardened, appliance-style Linux system
- Fanless, solid-state Protectli hardware
- No user browsing, email, or productivity software
- No application or business logic running on-prem

This design:

- Limits lateral movement risk
- Reduces blast radius
- Simplifies auditing and incident response

Comparison to Port Forwarding

Port Forwarding	UnityIS® Secure Gateway
Public exposure of ELK ports	No public exposure
OT devices reachable from internet	OT devices remain private
Static firewall holes	Outbound-only encrypted connectivity
High scanning and attack risk	Explicitly authorized access
Difficult to revoke	Instant revocation

Risk Assessment & Mitigations

Potential Risk: Gateway Compromise

Mitigations

- Dedicated, single-purpose appliance
- Customer-managed Linux hardening
- Endpoint protection and monitoring
- Least-privilege routing and firewall rules
- Immediate access revocation

Potential Risk: Over-Permissive Access

Mitigations

- Subnet and port-level restrictions
- Default-deny firewall posture
- Optional policy-based traffic controls

Summary

This solution:

- Eliminates inbound network exposure

- Preserves existing ELK communication methods
- Protects OT devices from internet access
- Centralizes application logic in UnityIS Cloud
- Aligns with zero-trust and least-privilege principles
- Allows full customer IT ownership of on-prem security

Net Result:
This approach materially reduces security risk compared to traditional port forwarding while enabling secure, auditable cloud integration.

Closing Statement

IMRON is committed to working collaboratively with customer IT and security teams to ensure this deployment meets internal security standards, audit requirements, and operational expectations.

We welcome IT ownership of the UnityIS® Secure Gateway and will support configuration, validation, and documentation as needed.