Completing OT Zero Trust:

A System Integrator's Guide to Zuul

How to Close the Device-Level Gap and Win More Business

Most OT security stacks are built around the right instincts — segmentation, remote access control, network monitoring — but they stop at the device boundary. The interior of every OT controller is ungoverned: configuration state, active packages, administrative credentials, and protocol interfaces are all invisible to network-level tools. As deployments adopt secure protocols like BACnet/SC, fleet-scale certificate management becomes an additional requirement — one that an on-device agent is best suited to address. **Zuul closes all of it.**

Zuul Solves the Gaps Network Tools Can't

Interior Visibility	User Management w/Break-Glass Governance	Configuration Integrity & Certificate Management
Zuul provides real-time visibility into the complete interior of every governed device — configuration state, active packages, and protocol interface status — through an OEM-signed agent operating from inside the device.	Integrates with Enterprise IdM systems (OAuth2.0, OIDC, AD/DC). Manages on devices users, and protects the built-in administrative maintenance account in real time. Zuul governs the break-glass credential at the Operations Center level — closing the most powerful ungoverned access path on any OT device.	Zuul continuously compares every device against its authoritative target state and automatically restores drift — replacing point-in-time audits with continuous enforcement across the entire fleet. This feature is also used to provide continuous certificate lifecycle management.

Certificate Management Solved	Fleet-scale certificate management continues to be a major pain point for SIs. The same capabilities required to address the three gaps above also solve it: continuous device contact, trusted interior access, and authoritative knowledge of target state are exactly what certificate lifecycle management requires. For deployments rolling out BACnet/SC and other certificate-dependent protocols, this is not a separate workstream — it is a natural capability of the same platform.

Why SIs Choose Zuul

Win More Business

- Answer device-level questions competitors can't
- Map proposals to NIST SP 800-207, SP 800-82r3, and ISA/IEC 62443
- Demonstrate continuous compliance — not point-in-time audits
- Reframe the conversation from features to Zero Trust outcomes

Deliver Faster and More Repeatably

- OEM-aware templates ship pre-configured —minimal site-specific work
- Bulk device onboarding and automated certificate provisioning
- Monitor mode de-risks commissioning before enforcement goes live
- Each deployment builds institutional knowledge for the next

Turn Security Into a Revenue Line

- Include Zuul in proposals as a billable line item
- Offer continuous monitoring and managed compliance packages
- Automated drift correction reduces post-handover support calls
- Change logging provides audit trail evidence of secure delivery

The Competitive Position

Completes the Story

Leading Zero Trust and OT security frameworks all require device-level controls. Zuul satisfies NPE credentialing, deny-by-default enforcement, configuration monitoring, privileged access governance, and certificate lifecycle management in a single platform.

Differentiates Proposals

OEM-signed agents cannot be replicated by configuring existing tools. That OEM partnership is a moat. SIs who include Zuul answer questions that network-only competitors are not equipped to address.

Delivers Cleanly

Default Deployment Models are largely pre-configured. Monitor mode supports safe commissioning. Each deployment builds SI institutional knowledge that makes the next engagement faster and lower-risk.

How Zuul Completes the Stack

Boundary security is becoming table stakes. Proposals that include Zuul answer device-level questions that network-only proposals cannot — and showing it reshapes the relationship from vendor to trusted advisor.

Zuul Agent

OEM-signed software inside every OT device

OEM-signed & device-bound — Compiled by the manufacturer — trusted OS-level access to device internals.

Continuous enforcement — Compares actual vs. target state at every check-in. Restores drift automatically per policy.

Break-glass detection — Detects and reports admin account invocation in real time, regardless of network visibility.

Outbound-only mTLS — Agent initiates all communication. ZSE never polls inbound. No impersonation attack surface.

Zuul Security Engine (ZSE)

Fleet governance platform — the OT Operations Center

Monitor & Manage modes — Monitor observes and alerts during commissioning. Manage enforces target state continuously.

Certificate authority platform — Hosts unlimited private CAs — per protocol, per building, per zone — with full lifecycle automation. Integrates with enterprise PKI. Default 47-day cert lifetimes, 7-day rotation cycles.

Three dashboards — Inventory, Onboard Security, and Network Defense — all exportable to enterprise SIEM.

Cloud or on-prem — ZSE deploys on-prem or in cloud. Optional Gatekeeper appliance preserves outbound-only architecture for cloud deployments.

Network Monitor (optional) — Hardware and software OT network monitors available as optional components. Purpose-built around the ZSE's approved communication map for high signal-to-noise OT alerts.

The Zuul SI Program

● Evaluation Software

Full-featured ZSE for pre-sales evaluation, lab testing, and demonstration. Stand up a working deployment — including governed devices — before committing to a project.

● Training & Certification

Technical training covering deployment architecture, Vendor and Deployment Models, commissioning workflows, and ongoing fleet management. Certified SIs deploy faster with fewer support calls.

● Joint Marketing Support

Co-branded collateral, campaign support, and introductions to Zuul's OEM and customer network. Zuul helps certified SIs get in front of opportunities they wouldn't reach alone.

● End-Customer Engineering Support

Direct access to Zuul engineering during pre-sales and deployment. Scope complex projects with confidence and escalate difficult technical questions directly to the platform team.

Framework Alignment

NIST SP 800-207	NIST SP 800-82r3	ISA/IEC 62443	DoD Zero Trust Strategy
Zero Trust Architecture	**OT Security Guide**	**OT/ICS Security**	**Zero Trust for Defense**
NPE credentialing, deny-by-default, workload identity	Device configuration, privileged access, OT threat models	Zone segmentation, device-level security, identity governance	Device, network & workload pillars — 45 capabilities framework

Questions That Open the Conversation

1. Do you have admin credentials that haven't been rotated since installation — and who currently holds them?
2. Can your current stack detect use of a device's built-in admin account and alert on it?
3. When were your OT devices last audited for configuration drift? Was that a point-in-time snapshot or continuous monitoring?
4. As you roll out BACnet/SC and other secure protocols, how are you managing the certificates those protocols require at scale — with automated rotation across hundreds of devices?

Ready to complete your OT Zero Trust stack? Contact Zuul · www.zuuliot.com · info@zuuliot.com

Companion document: Completing Zero Trust in OT — available at www.zuuliot.com ·