SOLUTION BRIEF

Conquering Alert Fatigue

Transforming Managed Network Services with Predictive Intelligence and Agentic Automation

Aizen Corp

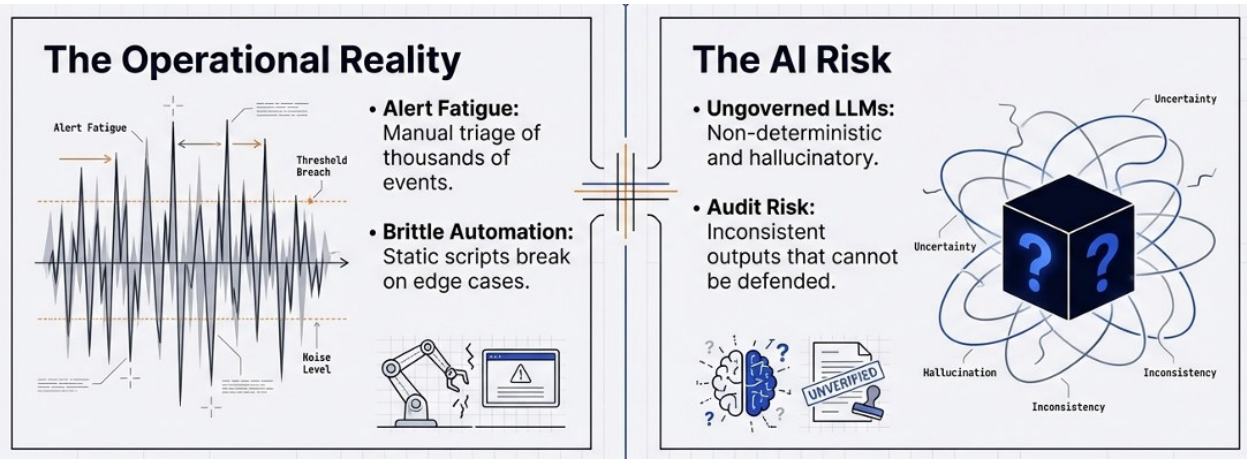
aizencorp.com

The Crisis of Noise in Managed Network Services

Managed Network Services (MNS) operations are currently pushed to a breaking point by the sheer scale of modern infrastructure. In environments where thousands of devices are monitored 24/7, traditional Network Management Systems (NMS) operate on rudimentary binary triggers: any device transition to a "down" state, regardless of context - automatically generates an incident ticket in ServiceNow.

This methodology fails to account for the deterministic vs. non-deterministic operational states of the network. Many network devices are intentionally power cycled, updated, or transitioned as part of routine daily maintenance windows. Because traditional systems cannot distinguish between these expected transitions and genuine failures, operations teams are forced to manually triage every ticket, even when no technical fault exists.

This continuous influx of non-actionable data creates a significant technical and psychological burden. The reliance on manual review for "expected" events prevents engineers from focusing on high-priority, service-impacting outages, effectively burying critical failures under a mountain of digital "noise".



The High Cost of Traditional Monitoring

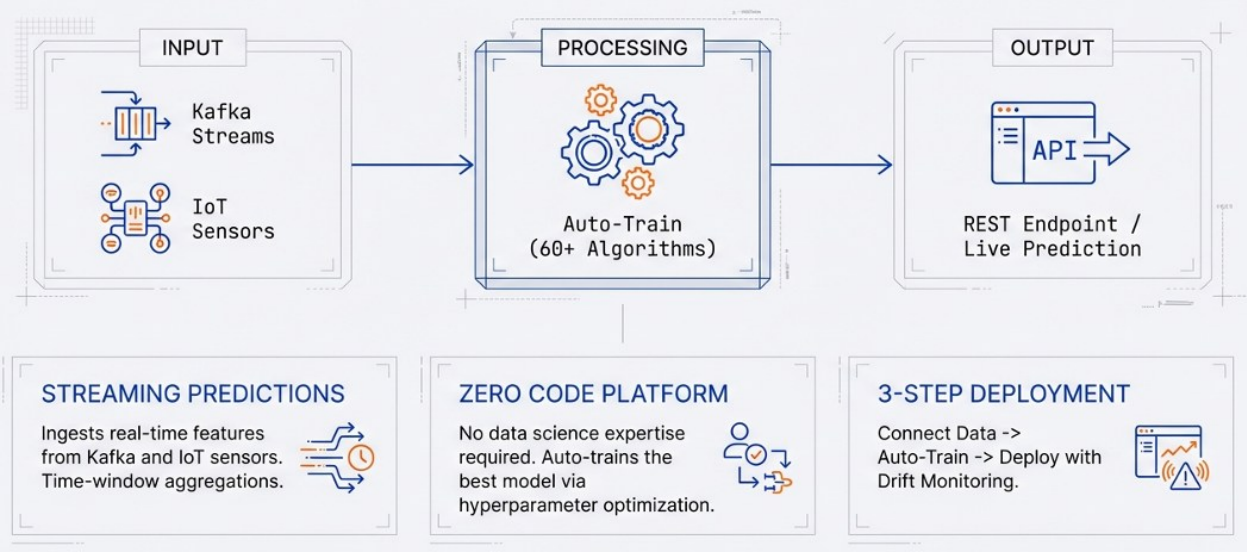
- **Alert Fatigue:** Constant exposure to false positives leads to desensitization, increasing the likelihood of missing critical "black swan" events.
- **Wasted Effort:** Significant operational capital is spent on manual closures of tickets generated by intentional power cycles and scheduled outages.
- **Delayed Response Times:** Genuine service threats remain unaddressed while L1 engineers sift through thousands of "expected" device transitions.

Foresight: Predictive Noise Suppression

The Aizen Foresight platform addresses the noise crisis at the source through intelligent event filtering. Built on a "Train Anywhere. Deploy Everywhere" philosophy, Foresight allows

enterprises to serve real-time predictions on streaming data without requiring extensive data science expertise.

By utilizing advanced AutoML, the platform distinguishes between normal operational signatures and true anomalies. At its core, Foresight leverages an **Enterprise Feature Store** to manage production-grade features with low-latency serving and "time-travel" capabilities for historical analysis. This allows the system to analyze historical device behavior-learning typical downtime windows, power-on sequences, and acceptable timing variations. When a device event matches these learned patterns, the system automatically suppresses the alert, ensuring only unexpected downtime generates an actionable incident.



Foresight Methodology

1. **Connect Data Sources:** Integrate historical training data and live streaming sources (Kafka, IoT sensors) with Automated Feature Engineering to prepare data for model consumption.
2. **Auto-Train Best Model:** Users specify a target variable, and Foresight automatically tests over 60 algorithms, optimizes hyperparameters, and selects the optimal model.
3. **Deploy REST Endpoints:** One-click deployment provides REST APIs for real-time predictions, supported by built-in drift monitoring and CI/CD integration.

Technical Capabilities

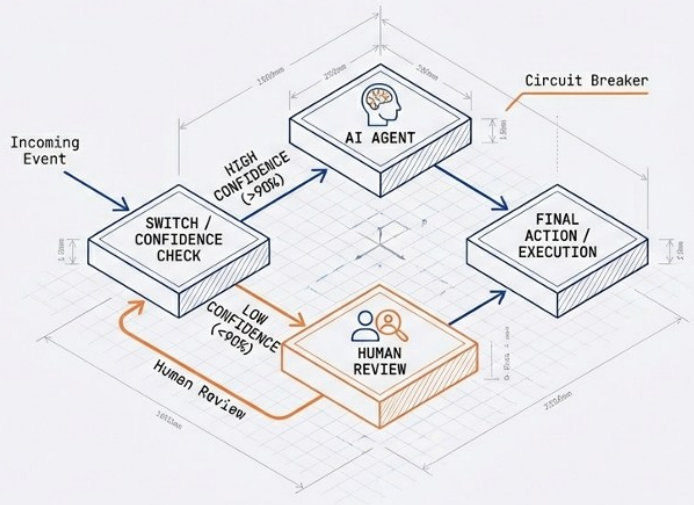
- **90% Faster Deployment:** Move from raw data to production-ready ML in a fraction of the traditional time using automated pipelines.
- **Real-Time Streaming Predictions:** Process features from Kafka streams with low-latency time-window aggregations and point-in-time joins.
- **Zero-Code Requirements:** An AutoML platform designed for accessibility, removing the need for specialized data scientists to maintain the suppression logic.

Orchestrate: Moving Beyond Suppression to Agentic FLT

When an event is not suppressed by Foresight, the system transitions to active resolution via the Orchestrate platform. Orchestrate utilizes a "Multi-Method" approach, combining LLM-based AI agents with deterministic business rules. This architecture handles complex First Level Troubleshooting (FLT) through stateful multi-step coordination and **fork-join parallelism**, allowing the system to handle non-linear network outages where multiple diagnostic paths must be explored simultaneously.

Layer	Component	Function
Interaction	LLM Agents	Intent extraction, context management, and RAG-powered policy Q&A for human-like reasoning.
Orchestration	Workflow Engine	Stateful coordination, fork-join parallelism, and the ability to pause/resume external events.
Decision	Business Rules	Deterministic eligibility checks, policy enforcement, and a full compliance audit trail.
Intelligence	ML Platform	Risk scoring, anomaly detection, predictive maintenance, and drift monitoring.
Data	Integration Platform	Connection to CRM APIs, Feature Stores, and document processing for data enrichment.

- **Core Philosophy:** Deterministic workflow + LLM decision-making.
- **Event-Driven Execution:** Pause/resume on events, no polling.
- **Circuit Breakers:** Automatic recovery from downstream failures.
- **Human-in-the-Loop (HITL):** Seamless escalation for low-confidence events.



Orchestrated Intelligence

Unlike ungoverned AI frameworks that produce non-deterministic or brittle outputs, Orchestrate is purpose-built for high-stakes, regulated environments. Decisions are explainable, actions are auditable, and every workflow is recoverable. This provides the control required for enterprise operations, ensuring that AI flexibility is always governed by deterministic guardrails.

Anatomy of an Automated Workflow: The RF Link Down Case Study

The practical application of agentic automation is best demonstrated through the RF Link Down Troubleshooting SOP (v5). This workflow manages the end-to-end resolution of a link failure by interacting with various actors and diagnostic tools.

The MAIN_FLOW Summary

4. **Initialize:** The system triggers the workflow upon receipt of a non-suppressed alert.
5. **Read Auto Telco Agent Results:** The system ingests data from the primary diagnostic input source to begin technical assessment.
6. **Evaluate PE-CE Connectivity:** Automated check of the connection between the Provider Edge and Customer Edge.
7. **Check AP Reachability:** Verification of Access Point (AP) visibility within the network topology.
8. **Validate AP Health:** Deep-dive diagnostic into the operational status and health metrics of the AP.
9. **Check SU Reachability:** Assessment of the Subscriber Unit (SU) to determine if the failure is localized to the client's endpoint.
10. **Re-check SU After FLT:** A secondary validation step following any automated or customer-assisted remediation.
11. **Send Summary Communications:** Internal logging and context sharing across the management platform.
12. **Update Customer:** Proactive status updates delivered via automated channels.
13. **Verify Resolution:** Final confirmation that the link is stable before closing the loop.

The Customer_FLT_WhatsApp Innovation

A key differentiator is the **Customer_FLT_WhatsApp** subprocess. A virtual agent identifies the equipment and guides the customer through physical troubleshooting:

- Router and POE (Power over Ethernet) power cycles.
- Physical cable integrity checks.
- Router power troubleshooting.

Field Dispatch and Escalation

Human expertise is treated as a premium resource. If diagnostic checks and customer-side FLT fail, the system triggers **Field_Dispatch** or **Escalation** subprocesses, ensuring engineers receive a ticket already enriched with full diagnostic context and a history of attempted remediations.

Customer Testimonial and Business Impact

Customer Testimonial

"Before Aizen, our NOC was drowning in ServiceNow tickets. Our L1 engineers were spending hours manually reviewing routine router power cycles, which left us slower to respond to real customer outages. By deploying Foresight and Orchestrate, we completely changed the paradigm. Foresight's AutoML predicted and suppressed the noise, while Orchestrate's virtual agents handled our First Level Troubleshooting-even reaching out to customers via WhatsApp to resolve RF Link issues. It reduced our MTTR and operational costs, and because of the 5-layer architecture, every single automated decision is fully auditable. We finally have intelligent operations."

- VP of Network Operations, Managed Network Services Provider

By deploying the Aizen platform, the Managed Network Services provider transformed their operations from **reactive alert fatigue** to **orchestrated intelligence**.

Leveraging **predictive noise suppression**, the platform analyzes historical device behavior and recognizes expected power-on sequences. As a result, the provider successfully suppressed **40% of ServiceNow tickets**, eliminating the need for manual review during routine transitions. For genuine, service-impacting incidents, Aizen's virtual agents automatically execute **First Level Troubleshooting (FLT) workflows**, enabling rapid and consistent incident handling.

Moving forward, it is expected that this agentic handling of FLT will automatically close an additional **25% of ServiceNow tickets**. This will significantly:

- **Reduce False-Positive Tickets:** Predictive suppression eliminates "expected" transitions from the queue.
- **Reduce L1 Workload:** Automation handles repetitive diagnostics and initial customer contact.
- **Faster Triage:** Virtual agents correlate signals across disparate monitoring systems instantly upon ticket creation.
- **Improve Mean Time to Resolution (MTTR):** Issues are often resolved via automated customer interaction before a human engineer would have even opened the ticket.
- **Lower Operational Costs:** Significant reduction in unnecessary field dispatches through rigorous remote validation.

Throughout the entire process, every automated workflow and decision remains **fully explainable and auditable**, ensuring operational transparency and governance.

Implementation Readiness and Enterprise Security

The transition from static SOP documentation to production-ready automated workflows follows a structured, six-step lifecycle designed for enterprise-grade reliability.

Workflow Creation Lifecycle

14. **Import:** Upload existing SOP documentation, APIs, and manifests.
15. **Extract:** Auto-classify the process across the five architectural layers.
16. **Review:** Human-in-the-loop validation of the extracted logic and decision points.
17. **Test:** Validate against mock infrastructure with full execution traces.
18. **Deploy:** Package and register the workflow for production use.
19. **Monitor:** Maintain five-layer observability for performance and model drift.

Trust & Reliability Checklist

- **99.9% Uptime SLA:** Guaranteed availability for mission-critical network operations.
- **<100ms Agent Coordination:** Low-latency performance ensures real-time responses for streaming data.

Conclusion: The Future of Intelligent Operations

The combination of Foresight and Orchestrate represents a fundamental shift in how Managed Network Services are delivered. While "Ungoverned AI" presents a liability through inconsistent outputs and brittle workflows, Aizen provides **Orchestrated Intelligence**-a system where AI reasoning is balanced by deterministic control, full auditability, and circuit-breaker protection.

By providing the only AutoML and orchestration platform that delivers real-time results on streaming data without requiring extensive data science expertise, Aizen enables enterprises to eliminate alert fatigue and reclaim operational excellence.