Intelligent Visibility

Beyond the Silos: The Unified Infrastructure Management Fabric

An Integrated, Co-Managed Approach to Modern IT Operations

Intelligent Visibility

April 2025

Executive Summary

For many enterprise IT leaders, IT Ops is filled with static. Vital information about data centers, cloud environments, networks, and applications lives in separate consoles—DCIM, IPAM, monitoring, ITSM, automation, and vendor-specific operational tooling —creating blind spots and forcing manual correlation ('swivel chairing'). This inherent fragmentation doesn't just slow incident response; it obscures the bigger picture. Herein lies the opportunity: to cut through the noise, unify these disparate views, and gain true operational intelligence that drives reliability and proactive decision-making.

The **Unified Infrastructure Management Fabric** offers a strategic framework to overcome this fragmentation, not by replacing every tool, but by *integrating* them into a cohesive, interoperable ecosystem. This fabric centers on two pillars: a **Unified Source of Truth** (combining DCIM and IPAM for authoritative asset and network data) and comprehensive **Observability** across hybrid environments.

Around these pillars, the fabric incorporates **AI-driven Operations (AIOps)** for intelligent correlation and prediction, seamless **ITSM integration** (preserving existing workflows like ServiceNow), robust **Automation & Orchestration** for efficiency and remediation, and hooks into **Data Lakes** for long-term analytics.

Delivered as a **co-managed service**, Intelligent Visibility provides and operates the core fabric technology (Source of Truth, Observability, AIOps, Automation) while

integrating seamlessly with customer-owned systems like ITSM. This approach accelerates time-to-value, provides expert guidance, and ensures the solution aligns with business outcomes like faster incident resolution (MTTR), accurate planning, reduced manual effort, and enhanced operational resilience. This white paper details the vision, architecture, benefits, and roadmap for adopting this unified approach.

Introduction - The Modern IT Operations Challenge

Enterprise IT infrastructure has become a complex mosaic of on-premises data centers, multiple cloud platforms, intricate networks, and distributed edge locations. While this hybrid reality offers flexibility, managing it effectively presents significant challenges. Specialized teams—NetOps, SecOps, CloudOps, DevOps—often operate in distinct silos, each equipped with preferred tools for tasks like Data Center Infrastructure Management (DCIM), IP Address Management (IPAM), performance monitoring, security analysis, and service ticketing.

This specialization, while deep, leads to fragmentation. Critical data about assets, configurations, and operational state resides in isolated pockets. Engineers frequently resort to "swivel chair management," manually piecing together information from multiple consoles during troubleshooting or planning. A network issue might require correlating data from network monitors, log aggregators, the DCIM system for physical context, and the ITSM tool for related changes – a slow, error-prone process. This operational friction manifests as:

- **Delayed Incident Resolution:** Difficulty correlating events across domains leads to longer Mean Time To Resolution (MTTR).
- **Inconsistent Data & Risk:** Multiple, unsynchronized "sources of truth" increase the risk of configuration errors and security gaps.
- **Inefficient Resource Utilization:** Lack of holistic visibility hinders effective capacity planning and cost optimization.
- **Tool Sprawl & Complexity:** Maintaining numerous overlapping tools drains budgets and requires diverse skill sets. According to EMA, 25% of large enterprises use eight or more network monitoring tools alone.
- **Impeded Automation:** Automation initiatives stall without reliable, unified data to drive them.

The traditional response – attempting to find a single "do-it-all" vendor platform – often fails due to compromises in functionality and the high disruption of rip-and-replace projects. A more pragmatic and effective path forward is needed: one based on intelligent integration.

Vision - The Unified Infrastructure Management Fabric

We propose the **Unified Infrastructure Management Fabric** as an architectural framework designed to address operational fragmentation through strategic integration. This isn't about forcing a single tool, but about creating an interoperable ecosystem where your existing best-of-breed tools can work together, augmented where necessary, to provide a cohesive operational experience.

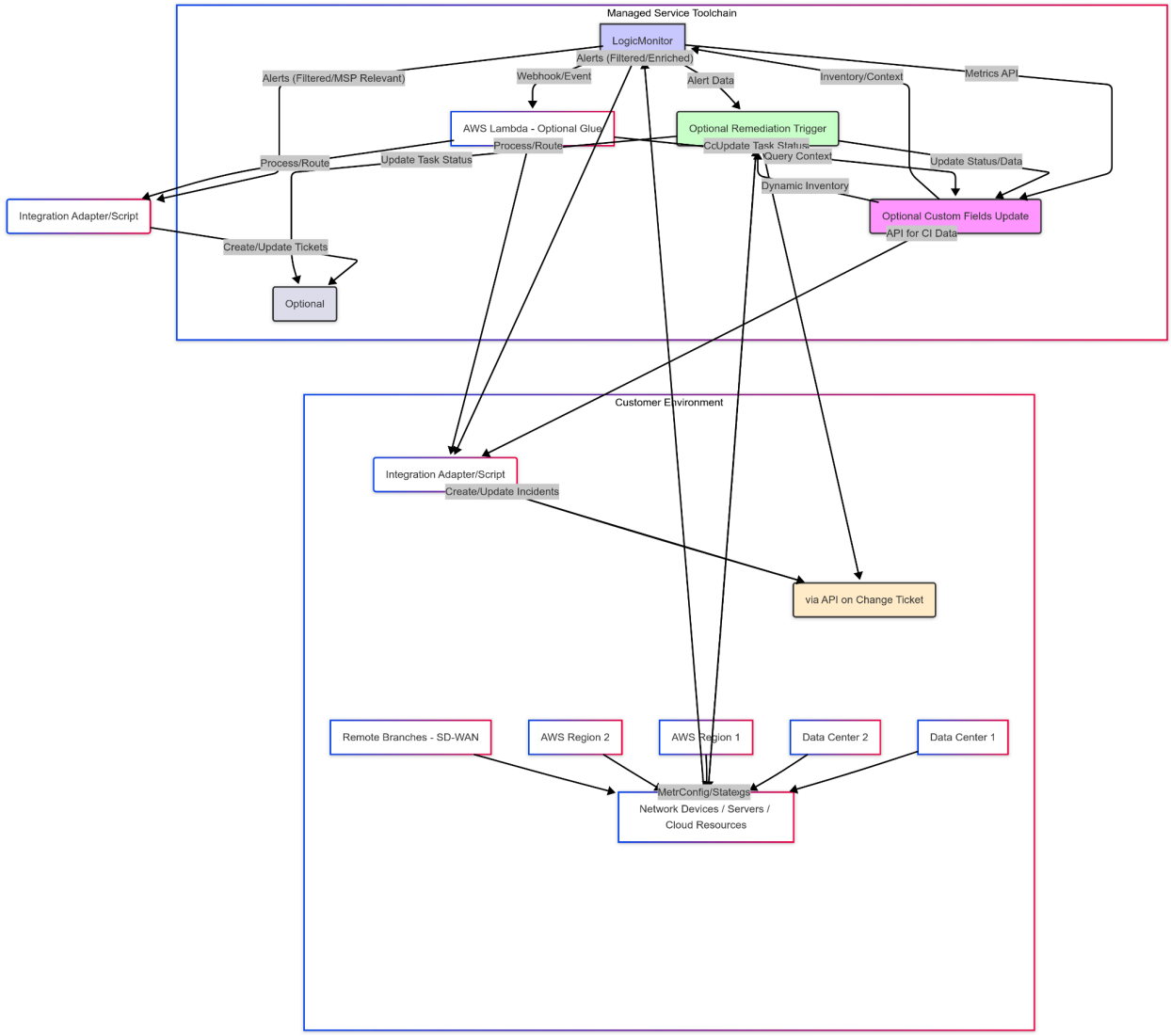


Diagram showing data sources (DCIM, IPAM, Monitoring Tools, Cloud APIs, Logs) feeding into the central "Fabric" (Unified SoT, Observability Data Store, AIOps Engine, Automation Engine). Outputs connect to ITSM, Dashboards, Data Lake, and direct remediation.)

The Fabric is built upon two foundational pillars:

1. **A Unified Source of Truth (SoT):** Consolidating authoritative data about *what* exists in your environment (physical, virtual, cloud assets, network topology, IP space).
2. **Unified Observability:** Aggregating and correlating real-time telemetry (metrics, events, logs, traces) to understand *how* the environment is performing.

These pillars feed higher-level functions integrated within the fabric:

- **AIOps:** Applying machine learning for intelligent analysis, anomaly detection, and root cause identification.
- **Automation & Orchestration:** Enabling consistent, automated actions for provisioning, configuration, and remediation.

Crucially, the Fabric is designed for **interoperability**, particularly with your existing **ITSM platform** (like ServiceNow), ensuring seamless workflow integration. It can also feed curated data into **enterprise data lakes** for long-term analytics.

Intelligent Visibility's Approach: Co-Managed Integration

We deliver the Unified Infrastructure Management Fabric primarily as a co-managed service. We provide and operate the core enabling technologies for the SoT, Observability, AIOps, and Automation while expertly integrating them with your essential existing systems (especially ITSM). This accelerates deployment, provides specialized expertise, and ensures the focus remains on achieving desired business outcomes, not just managing tools.

Once the Fabric is live our team continues to support the environment, maintaining the software that makes up the underlying toolchain, adpapting APIs to changes in dependencies, and working with your team to fine tune behavior, reporting, dashboards, etc.

Pillar 1 - The Unified Source of Truth (SoT): Knowing Your Environment

Effective IT management begins with knowing precisely what constitutes your infrastructure. The foundation of the Unified Fabric is an authoritative **Source of Truth (SoT)** that provides a reliable, consistent inventory of all physical, virtual, and cloud assets, along with their network context. This goes beyond traditional Configuration Management Databases (CMDBs), which often struggle with accuracy and completeness for network and physical details.

Converging DCIM and IPAM:

Historically, Data Center Infrastructure Management (DCIM) tracked physical hardware (racks, servers, ports, power, cabling) while IP Address Management (IPAM) handled logical network assignments (IP addresses, subnets, VLANs, DNS). In modern hybrid environments, this separation is artificial and counterproductive. A virtual machine needs an IP address; that VM runs on a physical host in a specific rack connected via specific ports. A unified SoT bridges this gap by integrating DCIM and IPAM data into a single repository. Open-source tools like NetBox, or commercial platforms like Device42, exemplify this approach, modeling both the physical and logical network realms together.

Benefits of a Unified SoT:

- **Accurate, Comprehensive Inventory:** A single place to find details on servers, network gear, VMs, cloud instances, IP subnets, VLAN assignments, rack layouts, and physical connections.
- **Eliminates Data Conflicts:** Prevents inconsistencies arising from maintaining separate spreadsheets, IPAM databases, and potentially incomplete CMDBs. Reduces error-prone manual data entry.
- **Rich Dependency Mapping:** Understand relationships critical for impact analysis. If a switch fails, the SoT can identify connected servers, affected VLANs, and dependent services. If an IP range needs reclaiming, it knows which devices are using it.
- **Foundation for Automation:** Provides reliable, API-accessible data for automation tools. Scripts can query the SoT for available IPs, rack space, or configuration parameters, ensuring consistency and preventing conflicts during provisioning or changes. EMA research confirms a SoT is essential for successful network automation.

- **Improved Monitoring Context:** Monitoring tools can pull asset details (location, owner, model) from the SoT to enrich alerts, making them more informative.

Integration with ITSM/CMDB:

The Fabric's SoT doesn't necessarily replace an enterprise CMDB within an ITSM like ServiceNow. Instead, it integrates. Depending on organizational needs, the Fabric's DCIM/IPAM can serve as the authoritative source feeding the CMDB, or it can bi-directionally sync, ensuring consistency. For example, network-specific details maintained in NetBox can automatically populate relevant CI records in ServiceNow. This ensures incident tickets or change requests in ITSM always reference accurate, up-to-date infrastructure data.

Managed Service Delivery:

As part of the Unified Fabric service, Intelligent Visibility typically provides and manages a robust DCIM/IPAM platform (like NetBox or equivalent) as the foundational SoT. We handle deployment, data migration/discovery assistance, and ongoing maintenance. If a customer has a mature, reliable IPAM (e.g., InfoBlox) they wish to keep, we integrate it seamlessly. This foundational data accuracy underpins all other Fabric capabilities.

Pillar 2 - Unified Observability & Performance: Seeing Your Environment in Real-Time

With an accurate map provided by the Source of Truth, the next essential pillar is **Unified Observability** – the ability to see how your infrastructure and applications are behaving in real-time across all environments. Traditional monitoring often focuses on siloed component health (Is the server up? Is CPU high?). Observability aims deeper: understanding the *internal state* and *why* things are happening by collecting and correlating diverse telemetry data.

Beyond Monitoring: The MELT Framework:

Observability typically relies on four key data types (often abbreviated MELT):

- **Metrics:** Time-series numerical data measuring performance and resource utilization (CPU, memory, bandwidth, latency, error rates).
- **Events:** Discrete occurrences indicating state changes or significant happenings (system startup, configuration change, deployment success/failure, security alerts).
- **Logs:** Timestamped text records generated by applications and systems, providing detailed context for events and errors.
- **Traces:** Data tracking the path of a request as it travels through various services in a distributed system, crucial for diagnosing microservice issues.

Achieving a Unified View:

The Unified Fabric aggregates these telemetry streams from across your hybrid environment – on-premises servers, network devices, cloud platforms (AWS CloudWatch, Azure Monitor), containers, and applications – into a single, correlated view. Platforms like LogicMonitor (LM Envision), Datadog, or Splunk Observability Cloud offer broad monitoring capabilities and integrations. They provide:

- **Cross-Domain Correlation:** Linking infrastructure metrics (e.g., network latency spike) with application behavior (e.g., slow transaction traces) and relevant logs or events.
- **Contextualization via SoT:** Integrating with the Source of Truth enriches telemetry data. An alert isn't just "High CPU on host XYZ," but "High CPU on host XYZ (Production Web Server, Rack 10, supporting App ABC)," immediately providing vital context.

- **"Single Pane of Glass" Dashboards:** Consolidated views tailored to different roles (NOC operators, SREs, managers) showing relevant KPIs and health statuses across the stack, reducing the need to switch between multiple monitoring tools.
- **Focus on User Experience:** Incorporating end-user monitoring (synthetics, RUM) helps correlate infrastructure performance with actual user satisfaction and business impact.

The Role of Observability Pipelines:

To manage the massive volume and variety of telemetry data efficiently and avoid vendor lock-in, the Fabric often incorporates an Observability Pipeline (using tools like Cribl or open-source alternatives like Fluentd). This pipeline acts as a smart router: it ingests raw data, normalizes formats, enriches it with context (e.g., adding tags from the SoT), filters out noise, and routes data to the appropriate destinations – critical alerts to the real-time monitoring platform, full logs to a cost-effective data lake for long-term storage, specific metrics to a security analytics tool, etc. This provides flexibility and cost control over observability data.

Managed Service Delivery:

Intelligent Visibility provides a comprehensive, unified observability platform as part of the Fabric service. We deploy collectors, configure monitoring for your specific environment (leveraging SoT data for auto-discovery), set up correlation rules, build initial dashboards, and manage the underlying platform. We work with you to integrate existing monitoring feeds where appropriate and establish data pipelines for optimal data routing and retention, ensuring you have complete visibility without being overwhelmed.

Pillar 3 - Intelligence via AIOps: Understanding Your Environment

Collecting vast amounts of observability data across a unified platform is necessary but not sufficient. The sheer volume and complexity can overwhelm human operators. This is where **Artificial Intelligence for IT Operations (AIOps)** becomes indispensable. AIOps applies machine learning (ML) and other AI techniques to the integrated data streams (telemetry from Observability + context from the SoT) to automatically detect patterns, pinpoint root causes, and predict potential issues.

Why AIOps is Essential:

- **Data Overload:** Modern systems generate millions of metrics and log lines. AIOps algorithms can process this volume at machine speed, identifying subtle signals humans would miss.
- **Complexity:** Interdependencies in hybrid environments make manual root cause analysis difficult. AIOps excels at finding correlations across disparate systems (network, server, application, cloud).
- **Speed:** Detecting anomalies or correlating events automatically dramatically reduces the time needed to identify and diagnose problems (Mean Time To Identify - MTTI).

Key AIOps Capabilities within the Fabric:

- **Anomaly Detection:** ML models learn the normal baseline behavior of metrics and logs, flagging statistically significant deviations even before traditional thresholds are breached. This enables early warning of potential problems like resource leaks or unusual traffic patterns.
- **Event Correlation & Noise Reduction:** AIOps algorithms automatically group related alerts from different sources into a single actionable incident. By understanding topology (from the SoT) and historical patterns, it can identify the likely root cause event and suppress downstream symptom alerts, drastically reducing alert fatigue for operators. Platforms like BigPanda or Moogsoft specialize in this correlation.
- **Root Cause Analysis (RCA):** By correlating alerts, logs, configuration changes (from ITSM/SoT), and performance metrics, AIOps platforms can suggest the probable root cause of an incident, significantly speeding up diagnosis.
- **Predictive Insights:** Analyzing historical data and trends allows AIOps models to forecast potential issues, such as predicting impending capacity exhaustion or identifying components with a high probability of failure based on past behavior.

- **Intelligent Automation Triggers:** Insights from AIOps can directly inform the Automation layer. Identified anomalies or correlated incidents can trigger predefined remediation runbooks (discussed next).

AIOps as Augmentation, Not Replacement:

It's crucial to view AIOps as augmenting, not replacing, skilled IT professionals. It handles the heavy lifting of data analysis, surfaces critical insights, and reduces noise, allowing humans to focus their expertise on complex problem-solving, strategic planning, and validating AI recommendations. Successful AIOps adoption often follows a maturity path – starting with noise reduction and correlation, then moving to anomaly detection, and gradually trusting predictions and automated responses.

Managed Service Delivery:

Intelligent Visibility includes AIOps capabilities natively within the Unified Fabric service. We manage the data ingestion, model training (using your environment's data), tuning algorithms to minimize false positives, and integrating AIOps insights directly into dashboards and ITSM incident workflows. Our expertise ensures you benefit from AIOps without needing dedicated data scientists solely for IT operations.

Pillar 4 - Automation & Orchestration: Acting on Insights

Visibility and intelligence are powerful, but their ultimate value lies in enabling faster, more consistent *action*. The **Automation and Orchestration** layer of the Unified Fabric translates insights from Observability and AIOps, combined with intent defined in the Source of Truth, into automated tasks – from routine provisioning to incident remediation.

Key Tools and Concepts:

- **Infrastructure as Code (IaC):** Using tools like Terraform or AWS CloudFormation to define infrastructure configuration in code, enabling automated, repeatable provisioning and management of servers, cloud resources, and even network components.
- **Configuration Management:** Employing tools like Ansible to automate the configuration, patching, and application deployment across servers and network devices, ensuring consistency and compliance.
- **Runbook Automation:** Scripting common operational procedures (runbooks) for tasks like restarting services, collecting diagnostic data, failing over systems, or scaling resources. Platforms like Ansible Automation Platform (AWX/Tower) or specialized runbook tools can execute these scripts on demand or triggered by events.
- **Orchestration:** Coordinating complex workflows that span multiple tools and domains. For example, provisioning a new application might involve orchestrating calls to IaC tools, configuration management tools, IPAM (via SoT API), and updating the ITSM CMDB.

How Automation Integrates within the Fabric:

- **Driven by SoT:** Automation workflows query the Unified Source of Truth (DCIM/IPAM) for reliable data – available IPs, device locations, intended configurations – ensuring actions are based on accurate information.
- **Triggered by Observability/AIOps:** Events, alerts, or AIOps insights trigger specific automation runbooks. For instance:
    - An alert for "disk space critical" triggers an Ansible playbook to clear temporary files.
    - An AIOps prediction of resource exhaustion triggers Terraform to scale up a cloud service.

    - A detected server failure triggers an orchestration workflow for VM failover.
- **Governed by ITSM:** Automation doesn't bypass governance. Actions can be integrated with ITSM change management, requiring approval for critical changes or automatically logging executed actions against incident or change tickets for auditability.
- **Closed-Loop Operations:** The integration creates a closed loop: Monitor -> Detect (Observability) -> Analyze (AIOps) -> Act (Automation) -> Verify (Observability confirms resolution) -> Document (ITSM/SoT updated).

Use Cases:

- **Automated Provisioning:** Deploying VMs, cloud resources, network segments quickly and consistently based on templates or service catalog requests integrated with ITSM.
- **Auto-remediation:** Automatically resolving common incidents (service restarts, resource scaling, simple configuration fixes) based on predefined runbooks, significantly reducing MTTR for known issues.
- **Compliance Enforcement:** Regularly running automation scripts to check configurations against baselines defined in the SoT and automatically correct drift.
- **Scheduled Maintenance:** Automating routine tasks like patching, backups, or certificate renewals across large fleets of devices.

Managed Service Delivery:

Intelligent Visibility provides an automation framework as part of the Unified Fabric service. We manage the core automation tools (e.g., Ansible Controller, Terraform integration points) and work with you to develop and maintain a library of runbooks tailored to your environment and operational policies. We ensure automation is integrated safely with monitoring, AIOps, and your ITSM processes, helping you gradually increase automation maturity from basic tasks towards self-healing capabilities, always prioritizing stability and governance.

Integration is Key: ITSM & Data Lakes

The Unified Fabric derives much of its power from intelligent integration, particularly with core enterprise systems like IT Service Management (ITSM) platforms and potentially Data Lakes for advanced analytics.

ITSM Integration: Enhancing Existing Workflows

A fundamental principle of the Fabric is to integrate with, not replace, your established ITSM platform (e.g., ServiceNow, Jira Service Management, BMC). ITSM is often the system of record for processes and user interactions. Seamless integration ensures the Fabric enhances these workflows:

- **Incident Management:** Alerts and correlated incidents detected by the Fabric's Observability/AIOps layer automatically generate or update tickets in your ITSM. Tickets are enriched with context from the SoT (affected CIs, location) and diagnostic insights, reducing manual data entry for support teams. Resolution status can sync bi-directionally.
- **CMDB Synchronization:** The Fabric's Unified SoT (DCIM/IPAM) maintains detailed infrastructure data. This integrates with your ITSM CMDB, ensuring CI records are accurate and reflect the real state of assets and their relationships. This improves impact analysis within ITSM.
- **Change Management:** Automation workflows executed by the Fabric can be linked to ITSM change requests, ensuring changes are logged, approved according to your policies, and automatically updated upon completion. Monitoring tools can also be made aware of approved change windows to suppress related alerts.
- **Service Request Fulfillment:** Approved service requests in the ITSM catalog (e.g., "Request New VM") can trigger automated provisioning workflows within the Fabric's automation layer, streamlining service delivery.

This tight coupling ensures operational data and actions flow smoothly into established business processes, maintaining governance and leveraging existing investments in ITSM.

Data Lake Extension: Unlocking Long-Term Strategic Value

While the Fabric's core platforms focus on real-time operations and medium-term data, extending its data feeds into an Enterprise Data Lake unlocks deeper, long-term insights:

- **Cost-Effective Long-Term Retention:** Store years of normalized metrics, logs, events, and SoT snapshots affordably in scalable storage (e.g., AWS S3, Azure Data Lake Storage) for compliance, audit, and historical analysis, beyond the typical retention periods of operational tools.
- **Advanced Analytics & Business Intelligence:** Combine rich operational data with other business data (e.g., sales figures, customer support metrics) in the data lake. Analyze long-term trends, perform capacity forecasting, optimize cloud spend, correlate IT performance with business KPIs, and build custom reports for executives using BI tools (Tableau, Power BI).
- **Custom Machine Learning:** Leverage the historical dataset to train bespoke ML models for predictive maintenance, advanced security threat hunting (correlating network flows with security events over months), or highly specific performance optimization tailored to your applications.
- **Data Ownership & Flexibility:** Using open formats in a data lake ensures you retain ownership and control over your operational data, avoiding vendor lock-in for historical analysis.

Implementation Notes:

The data lake integration is often a later phase in the roadmap. The Fabric's observability pipeline can be configured to stream normalized, contextualized data to your existing enterprise data lake or one established as part of the service. Intelligent Visibility ensures data governance and security protocols are maintained during this process. This extension transforms operational data from a transient necessity into a lasting strategic asset.

The Co-Managed Service Advantage

Building and maintaining an integrated fabric requires significant expertise and effort. Intelligent Visibility delivers the Unified Infrastructure Management Fabric as a co-managed service, providing distinct advantages:

- **Faster Time-to-Value:** Leverage our pre-integrated platform and deployment expertise to see results in months, not years.
- **Reduced Operational Overhead:** We manage the core fabric tools (SoT, Observability, AIOps, Automation), freeing your team from platform maintenance.
- **Access to Specialized Expertise:** Benefit from our deep knowledge in integration, monitoring, AIOps, and automation best practices.
- **Continuous Innovation:** Gain access to new features and capabilities as we evolve the platform, keeping your operations modern.
- **Scalability & Flexibility:** Easily scale the service up or down as your environment changes.
- **Predictable Costs & Outcomes:** Transparent, often subscription-based pricing, coupled with outcome-focused SLAs (e.g., improved MTTR, reduced critical incidents).

Component/Domain	Managed Service (Native)	Optional/Provided if Needed	Customer-Owned (Integrated)
DCIM	✅ Native DCIM platform provided	–	–
IPAM	–	✅ Provided if no suitable IPAM	✅ Use customer's IPAM if sufficient
Observability & Monitoring	✅ Full-stack monitoring platform	–	–
Performance Analytics	✅ Dashboards & analytics included (with monitoring)	–	–
AI/ML & AIOps	✅ AIOps analytics engine	–	–
ITSM (Service Desk, CMDB)	–	–	✅ Integrated with customer's ITSM (e.g. ServiceNow)
Automation & Orchestration	✅ Automation platform & runbooks	–	–
Data Lake & Analytics	–	✅ Data lake if needed	✅ Customer data lake if exists

Table: Responsibilities and Tool Ownership in a Co-Managed Unified Fabric.

This partnership model allows your team to focus on strategic initiatives and business alignment while we ensure the operational engine runs smoothly and efficiently.

Phased Roadmap to Unification

Adopting the Unified Fabric is a journey best taken in phases, delivering incremental value and managing change effectively. While specific steps vary, a typical path involves:

Phase 1: Foundation & Assessment

- *Goal:* Establish baseline visibility and an accurate inventory.
- *Activities:* Assess current tools/processes, define target architecture, deploy/integrate core SoT (DCIM/IPAM), initiate basic cross-domain observability.

Phase 2: Integration & Intelligence

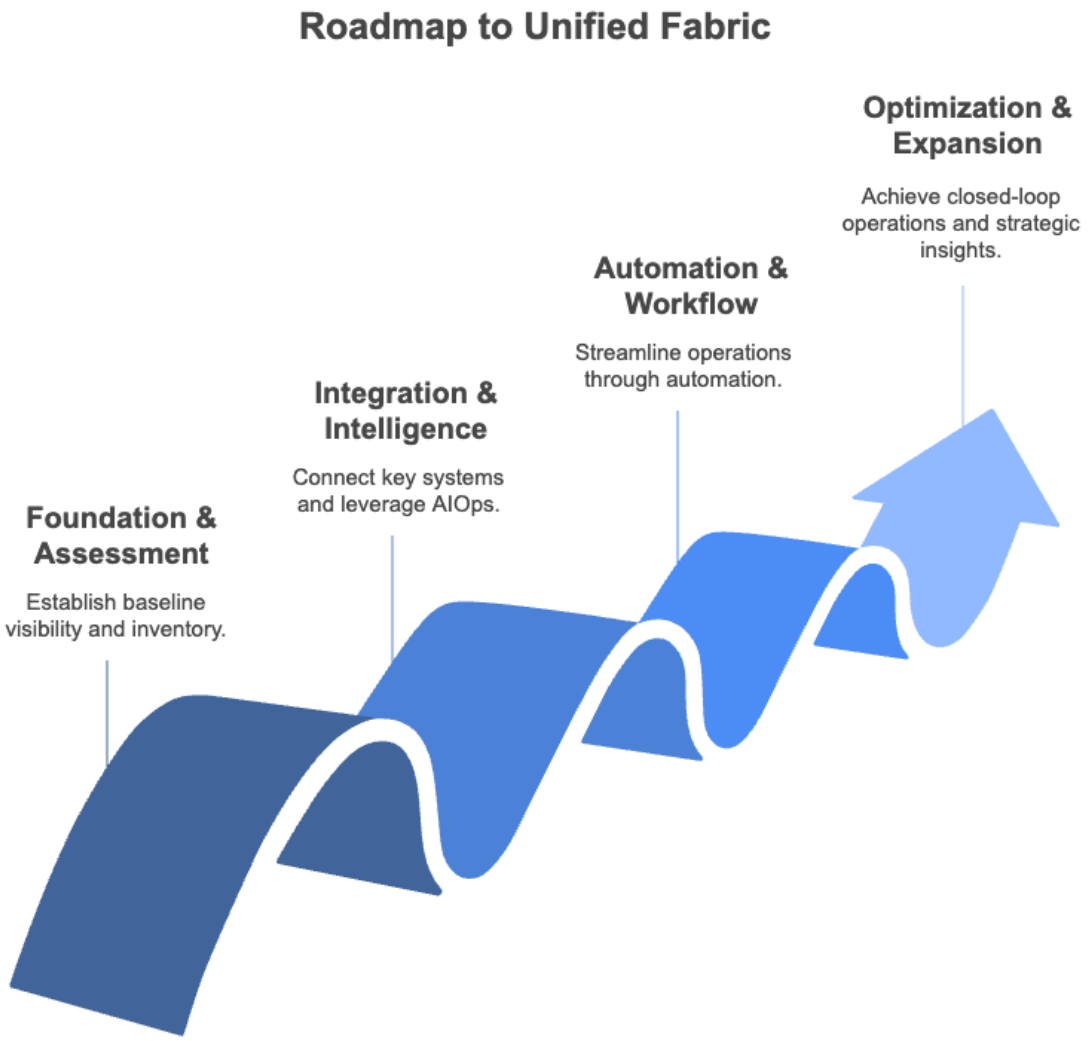
- *Goal:* Connect key systems and start leveraging AIOps.
- *Activities:* Integrate core monitoring feeds into unified observability, establish ITSM incident integration, enable initial AIOps for correlation & anomaly detection.

Phase 3: Automation & Workflow Enhancement

- *Goal:* Streamline operations through automation and deeper process integration.
- *Activities:* Implement foundational automation runbooks (e.g., diagnostics, simple remediation), integrate change management data, enhance CMDB sync.

Phase 4: Optimization & Expansion

- *Goal:* Achieve closed-loop operations and unlock strategic insights.
- *Activities:* Roll out advanced automation/auto-remediation, integrate data lake for analytics, expand fabric coverage, continuously optimize based on KPIs and feedback.



This phased approach builds confidence, demonstrates value early, and allows for adaptation based on organizational readiness and priorities.

Conclusion & Next Steps

The era of siloed IT operations is unsustainable. The Unified Infrastructure Management Fabric offers a pragmatic, powerful framework to integrate your existing tools and teams, creating a cohesive system built on authoritative data, comprehensive observability, intelligent AIOps, and streamlined automation. Delivered via a co-managed service, this approach accelerates transformation, reduces risk, and frees your team to focus on strategic value.

By embracing this integrated vision, enterprises can achieve significant improvements in operational efficiency, application reliability, security posture, and overall business agility. It's about moving from reactive firefighting to proactive, data-driven operations.

Ready to move beyond the silos?

Intelligent Visibility can help you assess your current state and chart a course toward unified infrastructure management. Contact us to explore how the Unified Infrastructure Management Fabric can transform your IT operations.

(866) 840-5456

info@intelligentvisibility.com

Intelligent Visibility

https://intelligentvisibility.com/managed-it-services/unified-infrastructure-management