freshworks

WHITEPAPER

Building the intelligence-driven IT organization

From fragmented data to unified service operations

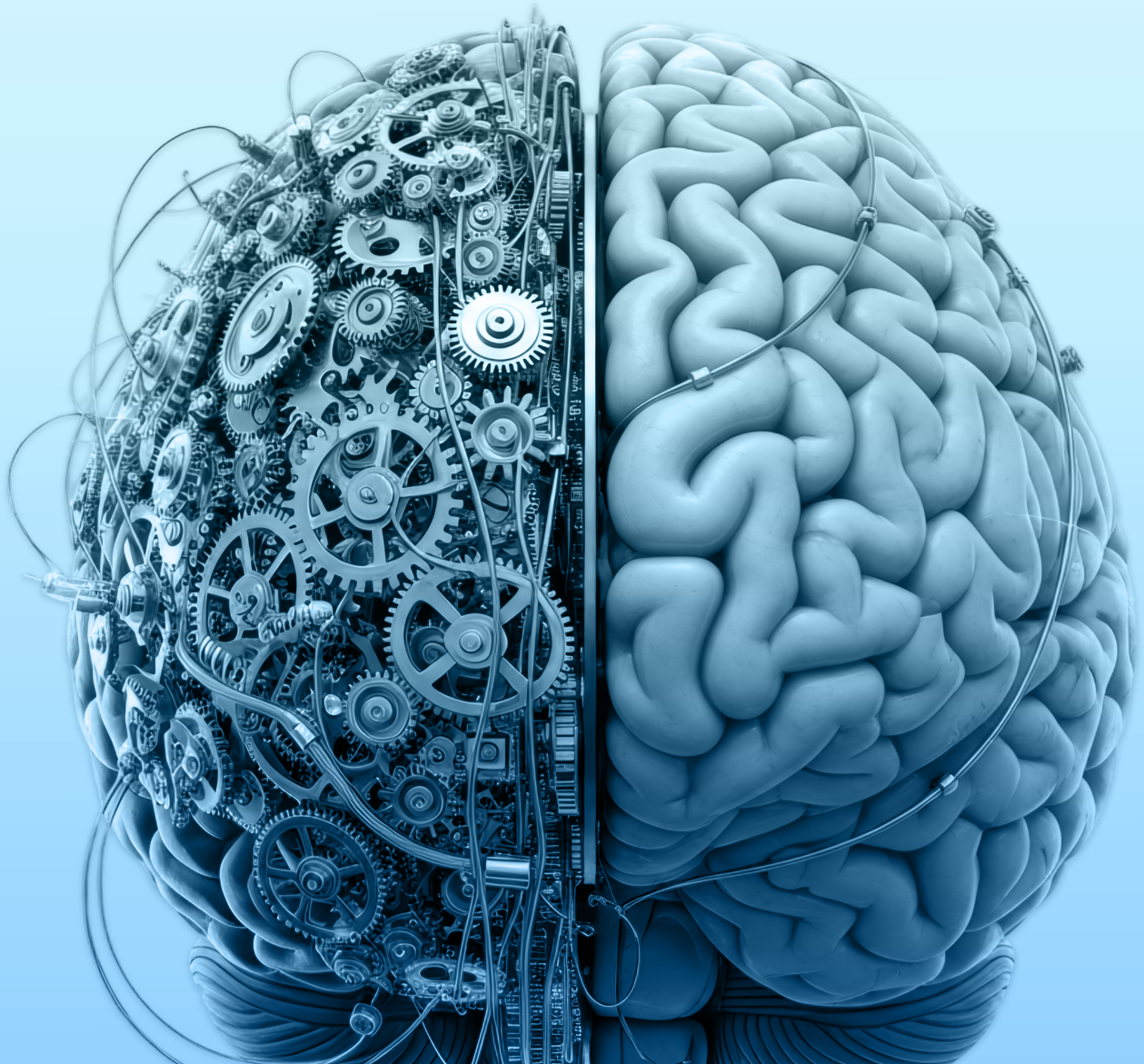


Table of contents

CHAPTER 01

How data fragmentation erodes operational integrity

Modern service operations are at a breaking point, not for a lack of tools, but for a lack of truth. While enterprises have invested heavily in high-speed automation and AI, these engines are being fueled by fragmented, stale data trapped in departmental silos.

This "intelligence gap" creates a dangerous paradox: the faster an organization tries to move, the more it accelerates its risk. Without a unified, up-to-date understanding of infrastructure dependencies, automation becomes a force multiplier for errors, incident response remains trapped in a reactive "war room" cycle, and AI initiatives fail to deliver on their strategic promise.

The crisis: Modern service operations are breaking

Enterprises are investing heavily in automation and AI. Yet outages remain elusive and expensive. Change failure rates remain high. Incident response is still reactive.

The issue is not tools. It is the lack of actionable intelligence to execute playbooks with confidence. Most organizations lack trusted, continuously updated infrastructure intelligence.

What actually happens?

- Stale data renders the incident playbooks obsolete because manual updates cannot keep up with deployment velocity
- Dependencies are unclear so teams do not know what breaks when a component fails
- Tools operate in silos without shared context
- AI initiatives stall because they consume incomplete infrastructure data

Automation without intelligence does not reduce risk. It accelerates it.

> “By 2028, large enterprises that deploy AI-powered, real-time asset discovery and service dependency mapping solutions will see 30% fewer service outages, compared to those that are populating their CMDB manually.”
>
> *Source: Gartner®, Drive CMDB Transformation Through Continuous Discovery and Service Mapping, 21 February 2025*
> *GARTNER is a trademark of Gartner, Inc. and its affiliates.*

Business impact: From technical friction to strategic exposure

When infrastructure intelligence is fragmented, the business feels it.

- Incident response depends on siloed knowledge
- Change failures increase because impact is not modeled before deployment
- Automation amplifies mistakes instead of preventing them
- AI becomes unreliable because it lacks complete context

That is not the time for strategic work. It is operational drag.

The mandate for the VP of Infrastructure & Operations

For the modern VP of Infrastructure & Operations, fragmented data is no longer just a technical hurdle; it is a source of strategic exposure that turns operational velocity into operational drag.

This creates pressure to:

- Accelerate digital transformation
- Reduce risk
- Support AI adoption
- Control cost

All while managing infrastructure that changes daily.

CHAPTER 02

The shift: unified service operations

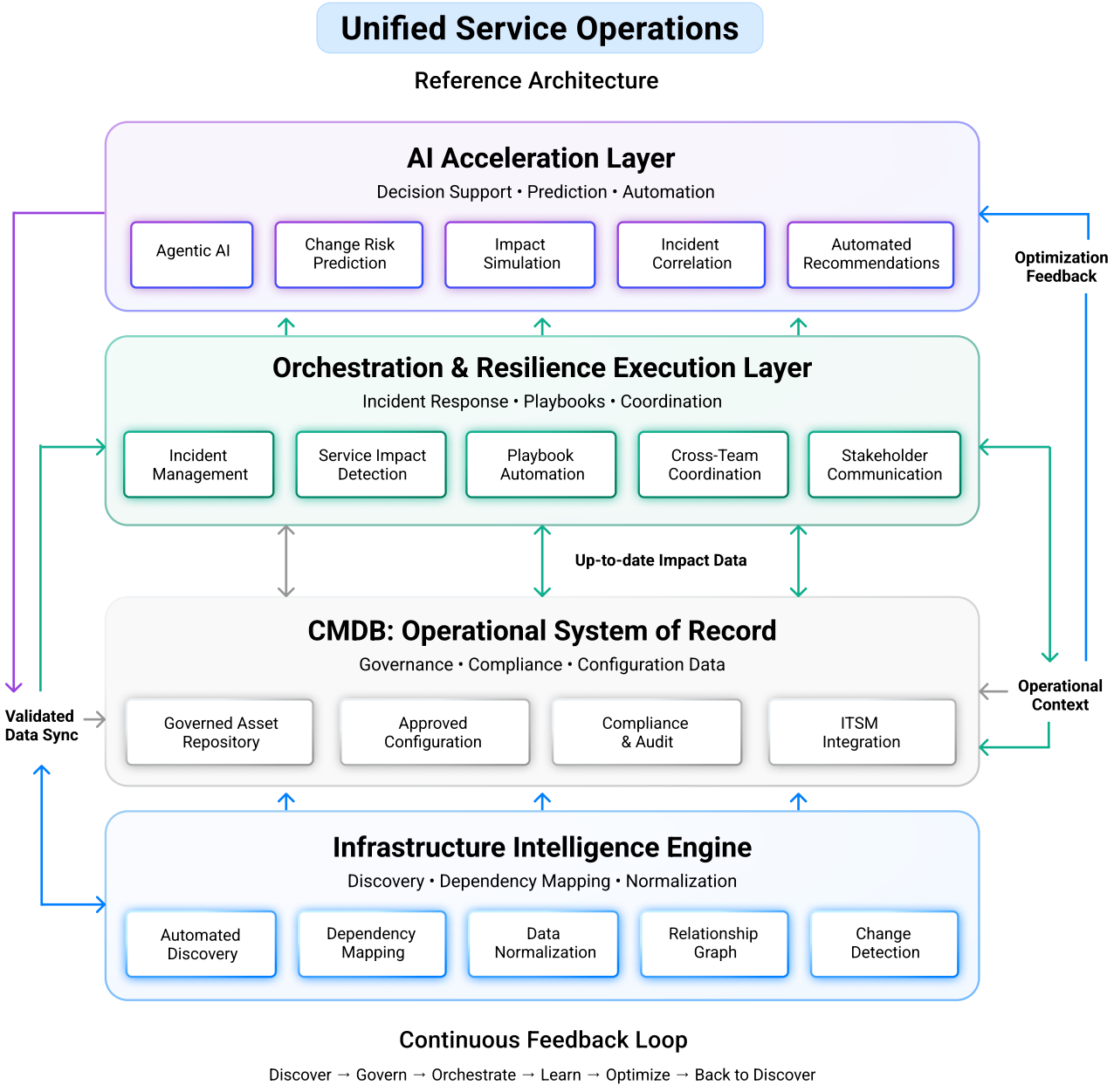
The answer is not another tool. It is a new operating model.

Unified service operations integrate infrastructure intelligence, operational execution, and AI acceleration into a closed-loop system.

Instead of siloed capabilities, it creates four connected layers:

1. Intelligence
2. Governance
3. Orchestration
4. AI acceleration

Each layer builds on the one below it.



LAYER 1 Infrastructure intelligence engine

Establishing ground truth

Everything starts here.

Before governance. Before orchestration. Before AI.

The **infrastructure intelligence engine** continuously discovers and models the current state of the environment.

It does not manage tickets. It does not enforce policy. It observes reality.

What it does

- Continuously discovers assets across hybrid infrastructure
- Maps dependencies between components and services
- Normalizes raw data into structured records
- Detects configuration and topology changes
- Generates a dynamic relationship graph

The output is a live infrastructure knowledge graph that reflects how systems connect. This becomes the operational context for every other layer. Without it, nothing above can operate with confidence.

> Infrastructure data integrity is not just an operational concern…it is a strategic lever. It reduces waste, strengthens compliance posture, enables modernization at scale, and builds the resilience required in a constantly changing environment. Without it, transformation becomes expensive and fragile.
>
> **Ido Benmoshe**, Vice President, Product Management, Freshworks

LAYER 2

CMDB as the operational system of record

Governance without bottlenecks

In this model, the Configuration Management Database (CMDB) is not the intelligence engine. It is the **governed system of record**. Instead of relying on manual updates, it receives validated data from the intelligence layer.

The separation is intentional. The Intelligence Engine observes reality. The CMDB governs approved state.

What this enables

- A governed asset repository
- Baseline configuration control
- Audit and compliance reporting
- Structured integration with service management workflows

The result is governance that remains accurate without slowing down discovery. Compliance and velocity no longer conflict.

LAYER 3 Orchestration and resilience execution

Turning intelligence into action

This is where operational maturity becomes visible. The orchestration layer consumes current infrastructure context and turns it into structured execution.

Core capabilities

- Context-aware incident management
- Service impact detection
- Automated playbook execution
- Policy governance and guardrails
- Cross-team coordination
- Automated stakeholder communication

Because this layer understands the service topology, it becomes service-aware. That means:

- Mean time to repair (MTTR) declines because impact is immediately understood
- Playbooks execute against actual dependencies
- Policy governance ensures automation scales safely without creating configuration drift or security exposures.
- Escalations are precise instead of broad
- Execution becomes consistent and repeatable.

> A fire department can't protect a city without precise location data and early warning signals. IT Operations is no different. Connected data makes ITOM predictive, helping teams anticipate risk and prevent change failures. With trusted data, IT Operations moves from reactive firefighting to proactive resilience.
>
> **Robert Ross**, Product Management, FireHydrant, A Freshworks Company

LAYER 4 AI acceleration and agentic operations

From reactive to predictive

AI only performs as well as the data it consumes.

This layer draws on:

- Infrastructure dependency mapping
- Approved configuration data
- Historical incident outcomes
- Change history

With this foundation, AI moves beyond alert reduction.

What it enables

- Change risk scoring before deployment
- Intelligent alert correlation
- Automated remediation recommendations
- Guardrails for autonomous operations

Because AI operates on validated infrastructure intelligence, its recommendations are trustworthy. Confidence increases. Automation becomes safer. Operations shift from reactive troubleshooting to predictive resilience.

> AI will increasingly act on behalf of operators, not just assist them. That shift only works when AI operates on a living model of infrastructure and service relationships. Organizations that treat infrastructure intelligence as a strategic asset will be the ones that effectively unlock autonomous operations.
>
> **Jason Aloia**, Vice President, Product Management, Freshworks

CHAPTER 03

The continuous feedback loop

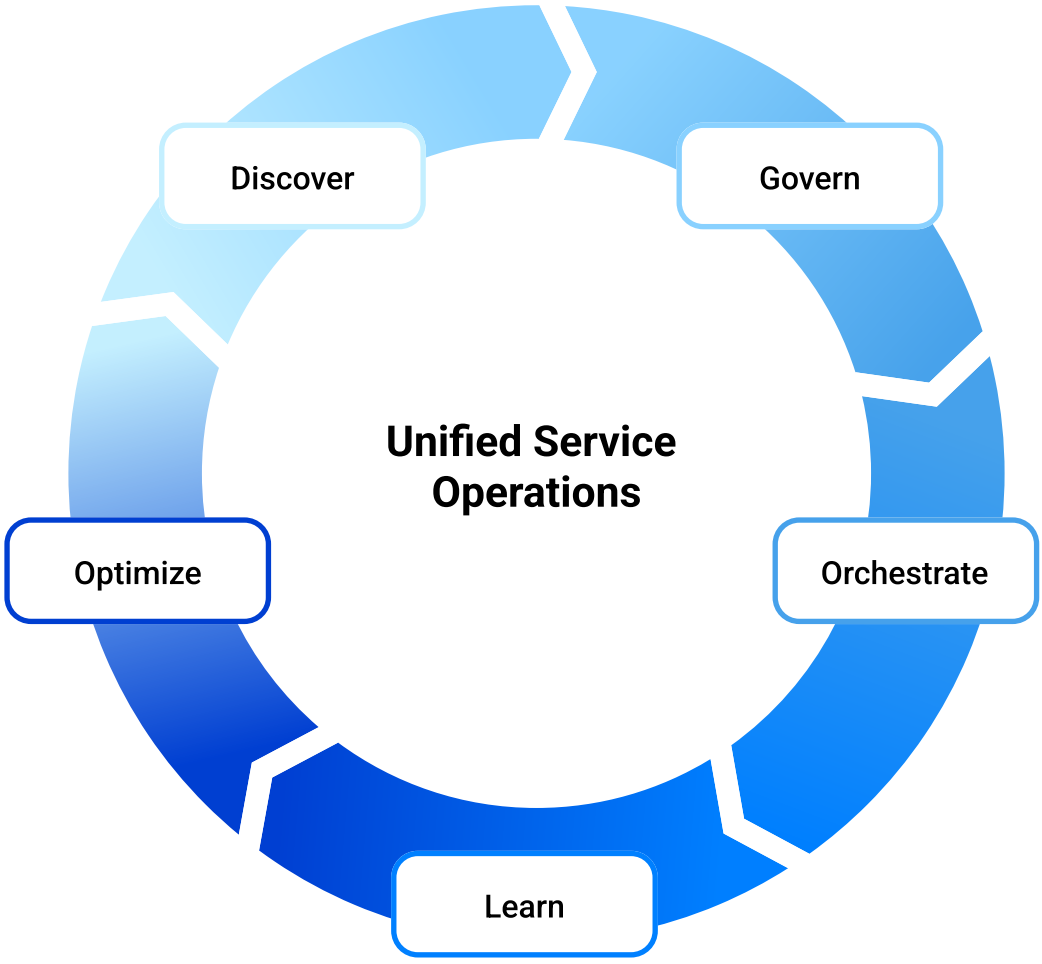
Why this architecture improves over time

Unified service operations are not linear.They are cyclical.

Discover → Govern → Orchestrate → Learn → Optimize

Every incident improves intelligence. Every change refines the model. Every AI insight enhances discovery and orchestration.

Instead of degrading over time, the system strengthens. That is what enables sustainable, intelligence-driven resilience.



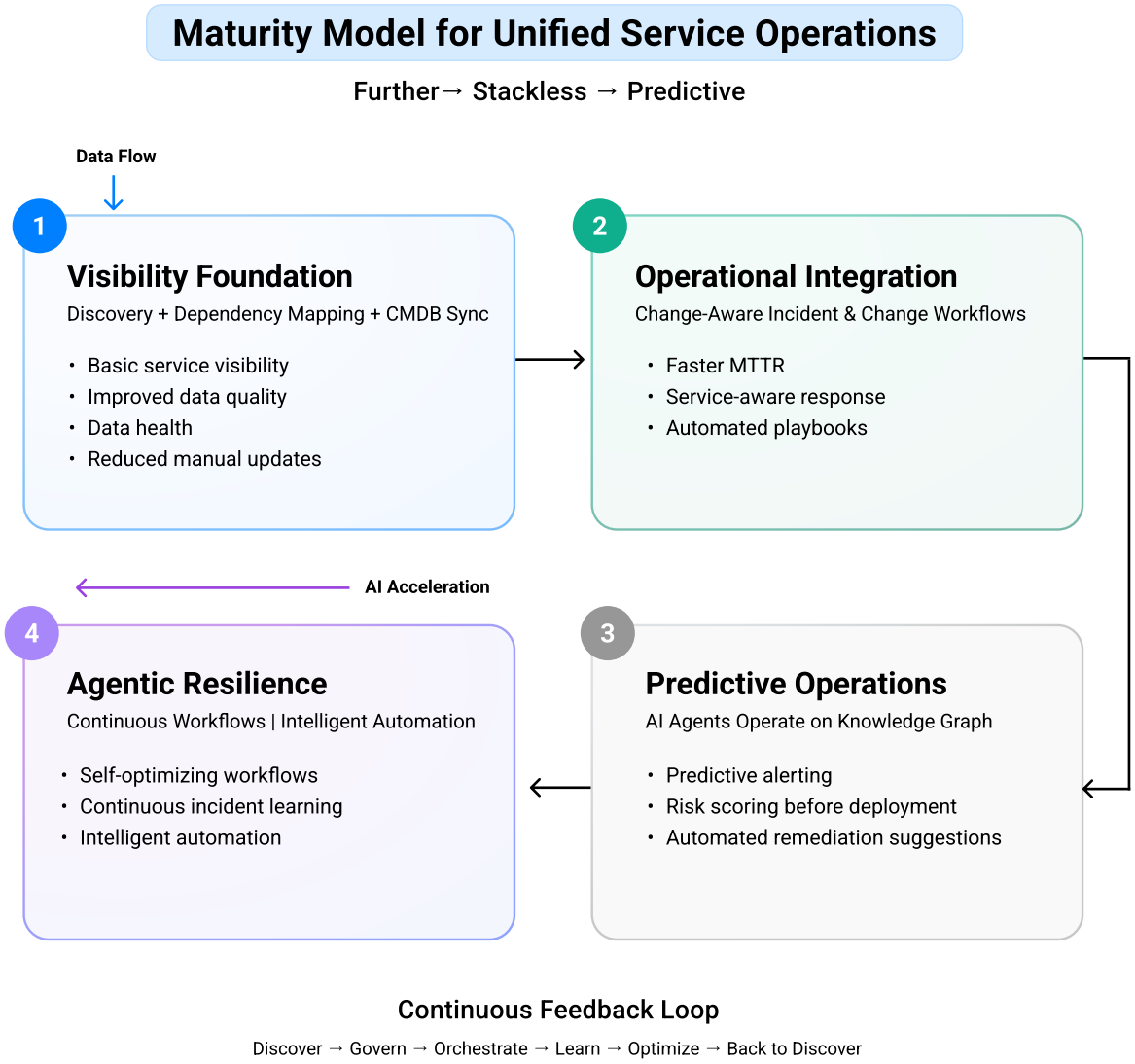
CHAPTER 04

The maturity roadmap

Transitioning to unified service operations

Unified service operations is not a technology deployment. It is an operating model shift. The journey moves from fragmented visibility and manual coordination to a self-optimizing, intelligence-driven environment.

For the VP of infrastructure and operations, this roadmap is a strategic path to eliminate unmanaged gaps, reduce operational volatility, and build a foundation for AI-driven resilience. Each stage builds on the one before it.



STAGE 1

Visibility foundation

Establishing ground truth

Modernization fails when organizations do not fully understand what they own, resulting in unmanaged assets, inconsistent naming, and unknown dependencies.

These gaps create blind spots that undermine every downstream process. Stage 1 replaces ambiguity with continuous infrastructure intelligence.

What changes

Manual updates give way to automated discovery.
Spreadsheets are replaced by structured relationship mapping.
Infrastructure is modeled as a connected system rather than isolated components.

Core activities

- Deploy automated discovery across hybrid infrastructure
- Map dependencies between applications, services, and infrastructure
- Establish validated synchronization between discovered data and the governed system of record

Business value

- Reduction in unmanaged or shadow infrastructure
- Significant decrease in manual data maintenance
- A trusted visibility baseline is required for automation, governance, and AI

This stage answers a simple but critical question: **What actually exists, and how does it connect?**

Without this clarity, nothing else scales.

STAGE 2 Operational integration

Context-aware resilience

Visibility alone does not prevent outages. It must be embedded into execution.

At this stage, infrastructure intelligence is integrated directly into incident, change, and operations workflows.

Technical data gains business context.

What changes

Incident response shifts from reactive coordination to informed execution.
Change management moves from guesswork to impact awareness.
Service relationships become visible during decision making.

Core activities

- Integrate the infrastructure knowledge graph into incident and change workflows
- Establish policy governance and guardrails to define the operational limits for automated recovery
- Enable service impact detection during component failures
- Align operational execution with service topology

Business value

- Reduced mean time to repair (MTTR)
- Faster root cause identification
- Precision communication to stakeholders based on actual impact

War rooms shrink. Escalations become targeted. Execution becomes consistent.

Operations stop reacting to symptoms and begin managing services.

STAGE 3 Predictive operations

From reactive to proactive

Once workflows are context-aware, the organization can move beyond response. This stage introduces AI-driven prediction grounded in trusted infrastructure intelligence.

AI is no longer summarizing alerts. It is modeling risk before disruption occurs.

What changes

Changes are evaluated before deployment.
Incident patterns are analyzed to anticipate future issues.
Risk is quantified instead of assumed.

Core activities

- Implement change risk scoring based on dependency relationships
- Analyze historical incident data for predictive insights

Business value

- Lower change failure rates
- Reduced production incidents
- Increased deployment velocity with controlled risk

The organization shifts from firefighting to controlled acceleration.

Innovation no longer competes with stability.

STAGE 4 Agentic resilience

The autonomous enterprise

The final stage moves from decision support to autonomous optimization. At this level, AI operates directly on validated infrastructure intelligence to maintain system health, and human intervention focuses on strategy. Routine operations become automated and adaptive.

What changes

The system identifies risk, initiates remediation, and optimizes configurations within defined guardrails. Every operational event strengthens the intelligence model.

Core activities

- Deploy AI agents capable of executing predefined remediation and optimization actions
- Enforce continuous policy alignment to ensure autonomous agents never deviate from security or compliance baselines
- Establish closed-loop optimization across discovery, governance, and execution

Business value

- Reduced operational overhead
- Faster recovery without manual coordination
- Continuous system improvement without periodic replatforming

Resilience becomes embedded in the architecture, and the environment maintains itself within defined policy boundaries.

This is not automation layered on complexity. It is intelligence embedded into operations.

CHAPTER 05

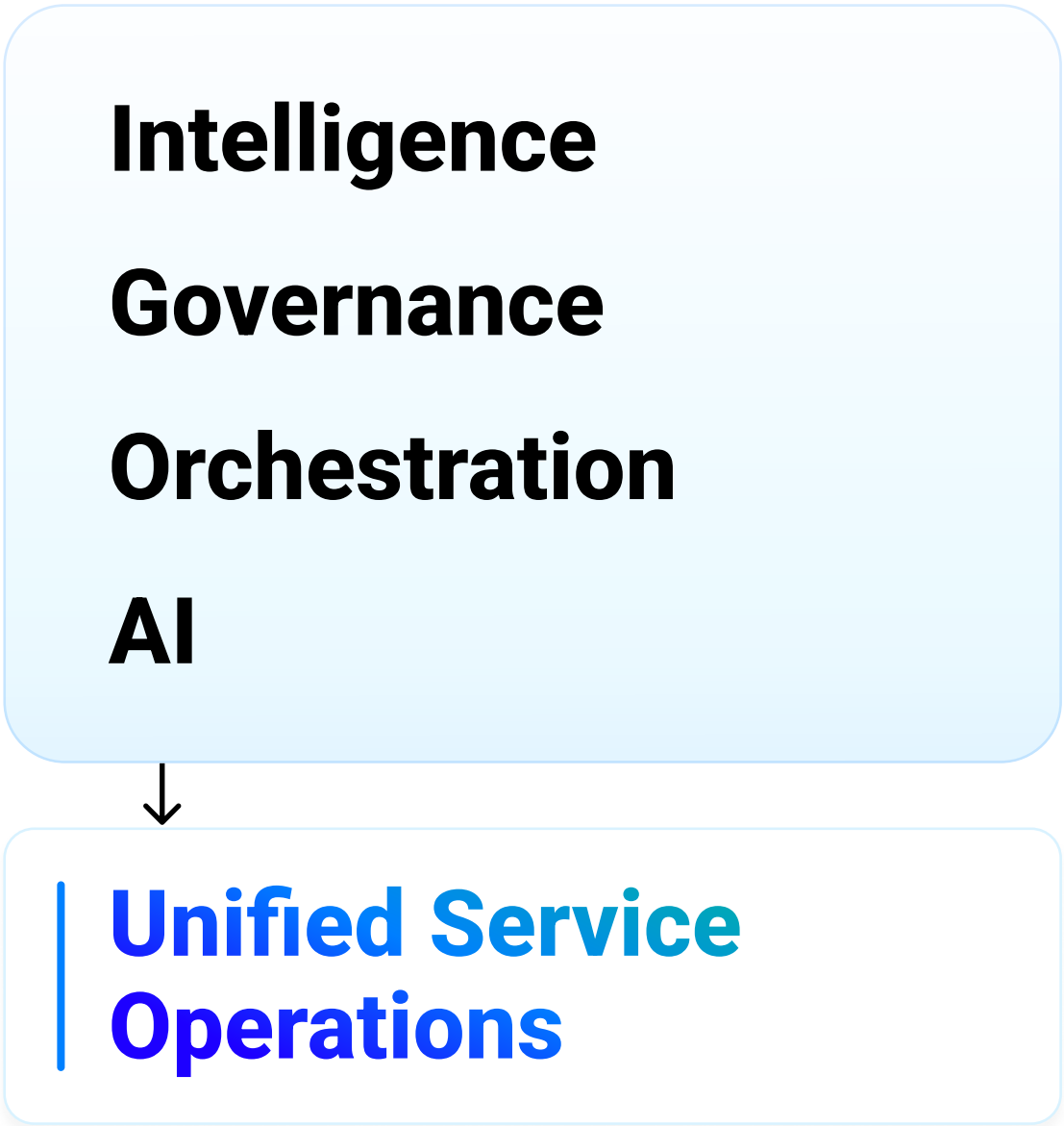
Strategic outcomes

Beyond the IT perimeter

Unified service operations do more than streamline technical workflows. They change how Infrastructure and IT operations create value for the enterprise.

When intelligence, governance, orchestration, and AI operate as a closed-loop system, resilience stops being defensive overhead. It becomes competitive leverage.

Infrastructure performance translates directly into revenue protection, faster innovation cycles, and measurable operational efficiency, with an impact that extends well beyond IT.



Outcomes for the business and the enterprise

For executive leadership, infrastructure maturity is not about servers and tickets. It is about reliability, speed, and risk control. Unified service operations convert infrastructure intelligence into business clarity.

What improves

Change decisions are informed before disruption occurs.
Incidents are resolved based on actual service impact.
Business owners gain transparency into what supports revenue-generating services.

Key outcomes

- **Reduced change failure rates**
  Every change is evaluated against a living infrastructure knowledge graph. High-risk deployments are identified before they affect production systems.
- **Faster mean time to repair (MTTR)**
  Service impact detection identifies affected business services immediately. The organization moves directly to resolution rather than losing time in manual triage.
- **Improved service visibility**
  Business leaders gain a current view of how infrastructure dependencies support specific digital services, customer experiences, and revenue streams, making infrastructure measurable in business terms.

Outcomes for IT employees and operational culture

Operational maturity is not just about technology. It is about how people work. When unmanaged gaps are removed, teams stop operating in crisis mode and start operating with control.

What changes

Manual reconciliation disappears.
War room heroics decline.
Execution becomes structured and repeatable.

Key outcomes

- **Reduced manual effort**
  Automated discovery and configuration mapping eliminate manual CMDB maintenance and spreadsheet tracking.
- **Structured orchestration**
  Teams execute defined, context-aware playbooks instead of improvising responses during incidents.
- **Shift to strategic engineering**
  Engineers spend less time searching for information and more time improving automation, resilience design, and optimization. The culture shifts from reactive firefighting to proactive engineering.

Outcomes for resilience, governance, and AI readiness

Resilience depends on alignment between operational reality and the governed state. When those diverge, risk increases.

Unified service operations permanently connect observed infrastructure conditions with approved configuration control. The result is continuous alignment.

What strengthens

Governance becomes dynamic rather than periodic.
Audit preparation becomes routine rather than disruptive.
AI initiatives operate on trusted data.

Key outcomes

- **Stronger governance control**
  Automated actions execute against approved configurations that are continuously validated against discovered infrastructure conditions.
- **Improved audit readiness**
  A centralized, governed asset repository maintains historical change visibility across hybrid infrastructure, simplifying reporting and compliance.
- **AI readiness built on trusted data**
  The infrastructure knowledge graph provides high-fidelity context for AI models, enabling reliable risk scoring, impact modeling, and autonomous decision support. AI moves from noise reduction to intelligent control.

CHAPTER 06

The unified service operations impact

When unified service operations is fully implemented:

- Infrastructure and operations shift from cost center to strategic enabler.
- Resilience becomes a system property.
- And the enterprise operates with confidence at scale.

Unified service operations are not a vision for the future.

It is a **disciplined progression**. And it begins with **trusted infrastructure intelligence**.

About Freshworks

Freshworks Inc. (NASDAQ: FRSH) provides people-first AI service software that organizations use to deliver exceptional customer and employee experiences. More than 74,000 companies, including American Express, Bridgestone, Databricks, Fila, Nucor, and Sony choose Freshworks' uncomplicated solutions to increase efficiency and loyalty. For the latest updates, visit www.freshworks.com and follow us on Facebook, LinkedIn, and X.

freshworks.com/freshservice