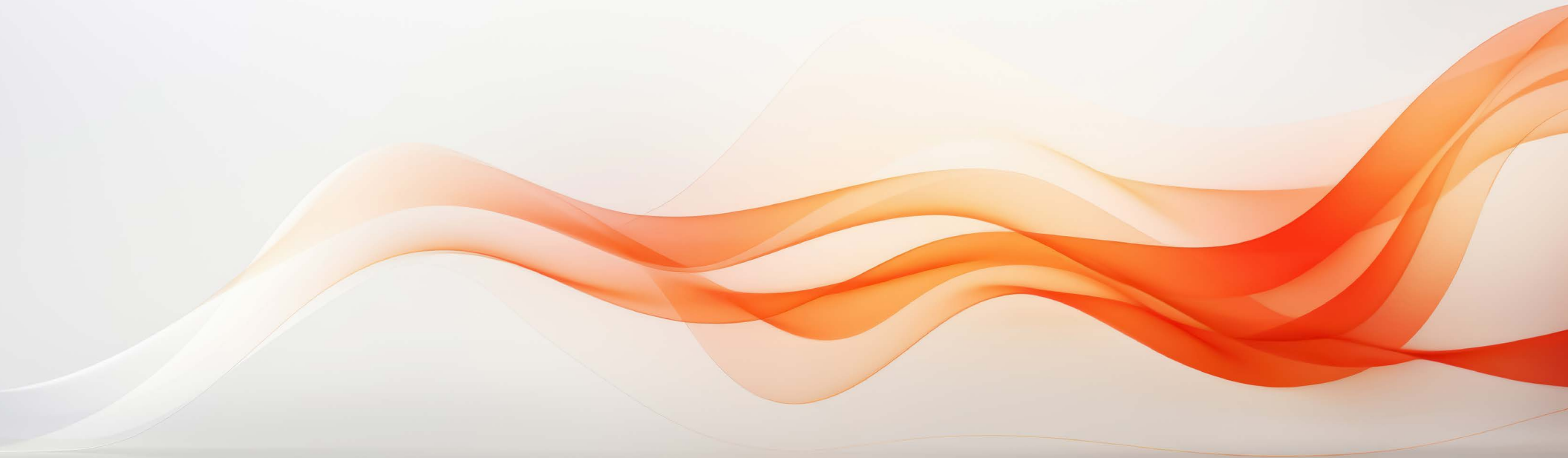
keyva

Maintaining Smooth IT Operations with an Enterprise-Scale Observability Strategy



Contents

Introduction

IT has transitioned from being a backroom adjunct to business operations to becoming a focal point for revenue and growth. While IT operations teams have historically done well in maintaining smooth operations, increasing complexity has raised the stakes. **There are now more regulations to comply with and more stringent demands for competitive system performance. Failure to keep up in either area can be costly to the business.**

Maintaining a competitive advantage through technology requires operations teams to solve problems faster than ever, continuously monitor system performance to reveal trends before they become problems, proactively improve performance for a competitive advantage, and understand how a code update will affect other processes.

In this rapidly evolving landscape, a robust observability strategy is crucial for the smooth operation and success of enterprise-scale IT environments. The complexity and diversity of modern IT systems demand a comprehensive approach to monitoring, event correlation, and data integration.

By implementing a unified observability framework, organizations can benefit from enhanced visibility into their infrastructure to streamline incident resolution processes and proactively address potential issues before they escalate.

Consolidating Disparate Observability Processes

The current approach to root cause analysis, troubleshooting, and routine performance monitoring generally involves different IT teams using different tools and processes. Each team may have its own budget and make decisions independently. They may buy different tools and use different types of scripts and programming languages.

In this environment, there is often no single tool that provides comprehensive end-to-end visibility, so operations teams don't get detailed descriptions about the relationships affecting an event. Not having this information becomes more critical for revenue-impacting outages.

Unified dashboards and aggregated views enable organizations to review their infrastructure at scale and efficiently isolate root causes of service disruptions. However, achieving single-pane-of-glass visibility can be a challenge. Since IT professionals are generally focused on running the business, they often don't have the flexibility to develop a strategy, identify data sources, and create the integrations necessary to develop a unified dashboard with data presented in a weighted manner. **While a unified dashboard can be viewed on any platform, the focus must be on refining the underlying metrics and their associated sources.**

A Framework for Unified Observability

While there is no out-of-the-box solution for unified observability, organizations can use a framework to develop a strategy.

Identify Patterns, Practices, and Protocols

Implementing unified observability starts with treating and designing it as a service that unifies patterns, practices, and protocols, which become the roadmap for implementing a full solution.

Patterns outline the standardized behaviors and properties (guardrails) that workloads can inherently assume when consuming the observability service and apply to all platform components. Practices define the ecosystem and processes for creating and consuming observability functionality, covering the entire lifecycle of components from inception to retirement. Protocols specify the formats and functions of platform components, ensuring interoperability and a common communication model across disparate technical specifications.

Log Aggregation for Efficient Diagnosis

Effective log aggregation is a cornerstone of a comprehensive monitoring and observability strategy. By determining and monitoring critical metrics through customized dashboards, organizations can streamline the process of identifying root causes of failures. Log aggregation aids in correlating security events with specific user actions to detect suspicious activity, linking user activity with application performance or access issues, and associating IT incidents with underlying infrastructure or application problems. This holistic approach enhances the ability to diagnose and resolve issues efficiently.

CMDB to Capture Relationships

A configuration management database (CMDB) is a critical element in achieving a single pane of glass visibility. Understanding how one asset or configuration item (CI) impacts another depends on the relationships captured within the CMDB, either through a discovery process or using data pump technologies. Processes must be established to capture new CIs or update existing ones, with assigned weights reflecting the criticality and trustworthiness of the information from respective sources.

While CMDB is intended to be the single source of truth for all organizational assets, there are challenges in keeping the CMDB current and accurate. Inaccurate data can hinder intelligent decision making based on the relationships between CIs.

Event Correlation to Accelerate Problem Solving

IT operations teams are measured by their ability to reduce the meantime to resolution (MTTR) for critical issues. The ability to correlate multiple events to a single root cause according to ITIL standards, is essential for achieving quick resolutions.

Many enterprise monitoring and application performance management tools are the basis for correlating events that impact a particular service. Since a service may consist of multiple infrastructure and application CIs, understanding how each CI relates to and affects the overall service helps establish a baseline for user impact.

However, because event correlation tools don't natively integrate with the CMDB, organizations need to ensure this is set up. Data pump technology can solve for this. For example, the Keyva Seamless Data Pump and Event Integration solution enables organizations to view interdependencies among service components that extend beyond the scope of standard monitoring tools.

Data and Process Integrations

To achieve a unified view of an environment where data is collected from multiple sources, several points of process and data integration are necessary. The goal is to deduplicate, sanitize, and transform observability data using traditional extract, transform, and load (ETL) technologies to aggregate and consolidate this data from disparate sources.

Process integration facilitates the automated transfer of control between teams or tools. Best practices recommend setting up generic API endpoints at a service level. This abstraction layer removes underlying API-specific dependencies, making it easier to remain tools agnostic and reduce existing technical debt.

Infrastructure Monitoring

An organization may use multiple infrastructure monitoring tools for different use cases. For instance, the network team might use one tool to monitor network components while the server or platforms team uses another tool for storage and compute components. The cloud team may use yet another tool to monitor cloud resources, including custom dashboards specific to cloud components.

By consolidating these tools into a single dashboard, organizations can save money and IT professionals can focus on developing a common set of skills around the consolidated dashboard rather than relying on localized expertise and knowledge limited to team-specific tools.

Application Monitoring

Application performance management (APM) tools typically trace transactions within an application to provide details about the relationships among components of the application stack and the time metrics for processing requests within individual components.

Several open-source and enterprise APM tools offer some intelligence for correlating data in the event of multiple alerts related to a single cause. However, this correlation is often limited to the scope of what the APM tool manages.

By integrating APM with a CMDB or a data analytics platform like Elastic Stack to centralize data for analysis, IT teams can significantly enhance their ability to determine relationships and proactively monitor trends that may impact application performance or user experience.

IT/AI Ops to Identify and Analyze Patterns

By integrating tools and features such as IT Service Management, CMDB, APM, infrastructure monitoring, and logging, and by pushing data from these tools into a data warehouse or data lake, organizations can perform intelligent queries and identify patterns. This approach is typically used to analyze trends, user preferences, transaction times, and to determine proactive actions that could help prevent issues before they become critical.

In addition, machine learning models that draw from dashboards with relevant metrics can be used to uncover patterns in systems and processes that degrade overall performance. This is crucial for reducing MTTR for teams with burdensome compliance requirements or strict service-level agreements.

Automated Remediation using CLIP

Automating operations center tasks, often involving repetitive and error-prone actions, can save organizations significant time, effort, and money. For example, organizations can create a self-healing framework that automates responses to alerts and events with appropriate remediation actions using a closed-loop incident process (CLIP).

CLIP requires clearly defined runbooks that outline automated responses based on specific conditions. The step-by-step responses are then codified within the automation tools that are integrated with ticketing systems, CMDB, logging, and other centralized services, capturing the automated actions and their results.

The Keyva Approach

While many organizations have the skills, tools, and people available to develop and implement a unified observability strategy, they would prefer to have their highly skilled personnel focused more on business outcomes rather than solving IT problems.

By outsourcing this work to a specialist with years of experience in helping diverse enterprise clients implement an observability strategy, organizations can avoid the common pitfalls and trial and error often associated with tackling something unfamiliar.

Because of our broad experience in developing and implementing unified observability strategies, Keyva can provide significant value in multiple areas.

Establishing a Center of Excellence for Observability

Keyva has helped several Fortune 100 companies define and implement organization-wide observability strategies, including collaborating with cross-functional leadership teams to establish a center of excellence for observability. The center includes employees from multiple IT teams who work together to develop a comprehensive observability strategy that meets IT operations business needs.

With guidance from Keyva, the center of excellence can work with the necessary observability components to develop a plan.

Aligning Organizational Structures

While tools and integrations are important for a unified observability strategy, the IT organization must be aligned to support it. Clearly defined team responsibilities and associated accountabilities are crucial to avoid ambiguity regarding ownership of tools or domains. Without documented ownership, issues are likely to be neglected and root cause analysis turnaround times can increase significantly.

Keyva uses the RACI model to define and map the roles and responsibilities of everyone involved across four categories:

- **Responsible:** The person who completes the task.
- **Accountable:** The person who is ultimately responsible if the task isn't completed.
- **Consulted:** The person who helps with the task in collaboration with the responsible person.
- **Informed:** The person who needs to be kept updated on the project's progress.

While functional ownership is important, it's equally essential for teams or individuals to collaborate to gather feedback before making decisions that impact the entire organization. Keyva's experience shows that RACI helps bridge common silos to foster the collaboration needed to be successful with a new observability program.

Consolidating Tools

Most organizations today have more tools than necessary, often exceeding their needs by 150%. This presents opportunities to consolidate tools based on functionality, user teams, or cost, leading to greater efficiency and cost savings. Consolidation simplifies tool maintenance and management, reduces the complexity of integrating multiple data points, and standardizes processes and technical skills to enhance operational excellence.

Support for Implementation

Keyva provides guidance for developing a unified observability strategy and assists with complex tactical implementations. Our engineering team has implemented unified observability in several large-scale environments using agile methodologies to address unknowns, uncertainties, and the need for flexibility as the project evolves.

Sprints typically last two weeks, during which DevOps or DevSecOps teams commit to specific deliverables. A scrum master conducts daily scrum meetings, where team members report on their progress, outline their plans for the day, and identify any roadblocks. These daily 15-minute touchpoints enhance communication between teams and provide architecture teams the opportunity to make mid-project adjustments to development paths or solutions.

Training and Knowledge Transfer

Every Keyva engagement includes a comprehensive training plan to ensure IT teams can continue the work after the Keyva engagement ends. Our goal is to ensure that your teams know what Keyva did, why we did it, and how we did it.

Learning paths with high-quality content help your team develop new skills and foster a culture of continuous learning that encourages ongoing skill enhancement and performance improvement. By implementing processes and tools that support code contributions, open discussions, feedback, work boards, social communication channels, and regular cadences, teams can achieve targeted collaboration and operational efficiencies with minimal effort.

Security and Governance

Keyva integrates security into all engineering activities as a fundamental quality of every IT output. Depending on the industry, we typically have a dedicated security team responsible for ensuring IT teams adhere to secure governance and practices. This team defines organization-wide security governance policies and platforms that all IT teams must follow.

Once the security framework and guidelines are established, platforms, applications, and operations teams should incorporate these frameworks into their daily activities, such as when developing infrastructure-as-code components, designing networking or compute solutions, and managing application releases.

Why Keyva

At Keyva, we are dedicated to helping our clients navigate observability complexities with tailored solutions that incorporate industry best practices and cutting-edge technologies. Our expertise spans from tool consolidation and security integration to agile practices and knowledge transfer, ensuring that our clients are well-positioned to achieve their business goals.

Whether you are looking to enhance your existing observability capabilities or embark on a new strategy, Keyva is here to support you every step of the way.

Contact us to learn more about how we can help you design, implement, and optimize your observability strategy for a future-ready enterprise.

Contact Us

info@keyvatech.com
(866) 974-5175