ALLUVIO™
by riverbed

Harness the Power of AIOps and IT Automation

EBOOK

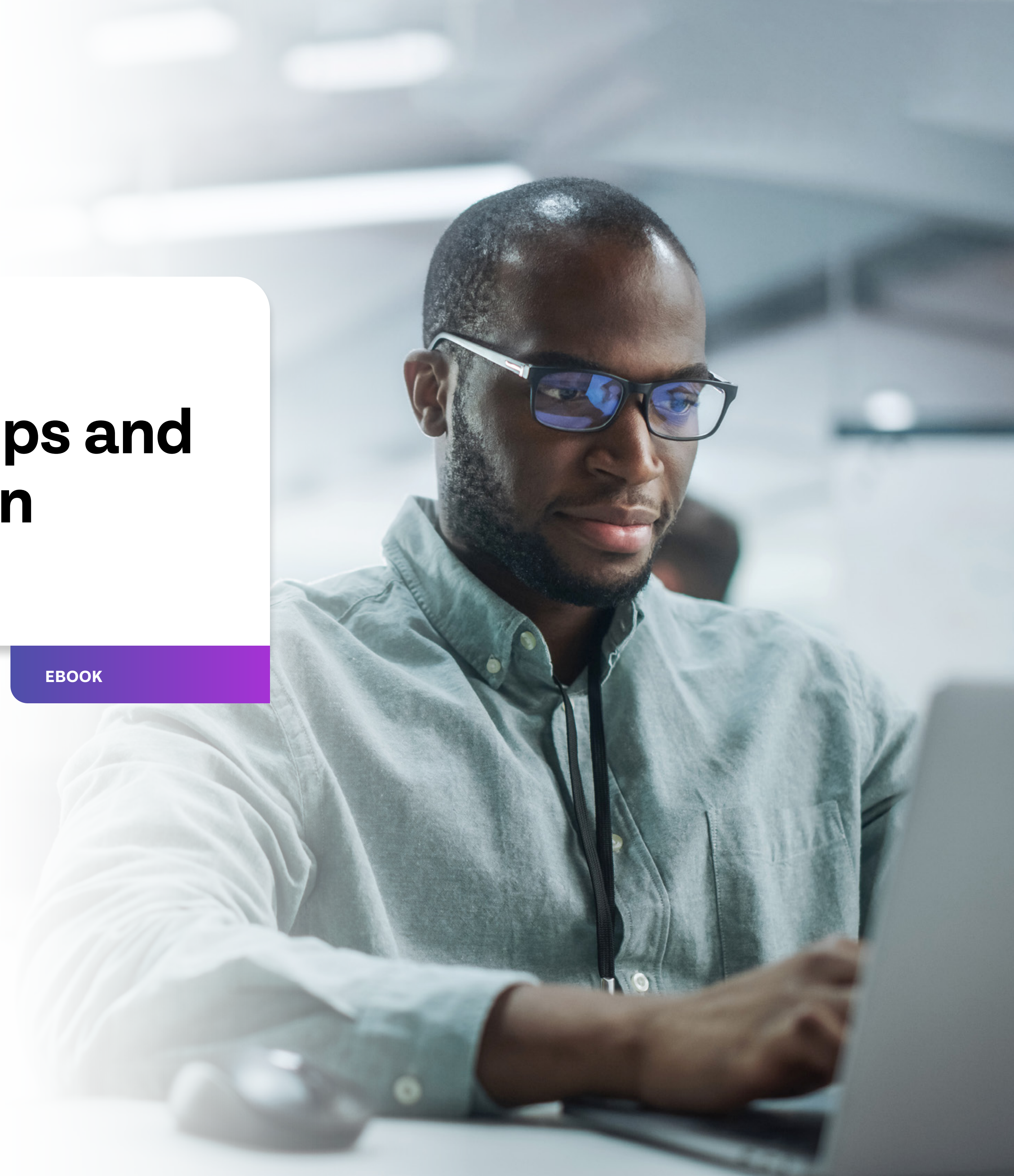


Table of Contents

Digital Business Drives Need for Change

The proliferation of new applications and services is generating an increasing volume, variety, velocity of data, leading to alert overload. It is simply no longer possible, much less practical, for IT teams to analyze and correlate this data manually and still meet operational expectations.

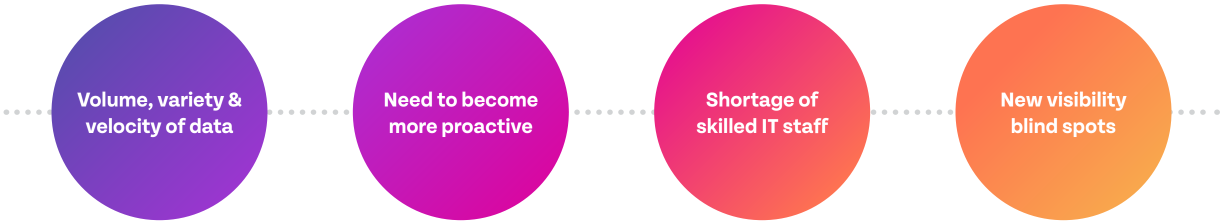
Data overload is compounded by today's scarcity of skilled IT resources. Whether due to layoffs, an inability to hire enough qualified staff, or Boomers retiring – fewer IT staff are left to do more of the work. Already short-staffed IT teams are often chasing events that don't impact digital experience. The result is longer resolution times of critical issues and higher error rates. In short, the automation gap negatively impacts user experience and business performance, plus IT productivity and efficiency.

Additionally, IT operations teams no longer have the luxury of responding to issues after they occur. Instead, they are trying to become proactive, working to address problems before users are materially impacted. At minimum, the service desk wants to be able to tell callers that they are aware of the problems and are "working on it."

Likewise, the job of becoming more proactive is complicated by the introduction of new visibility blind spots. Technology like hybrid cloud, work from anywhere, and advanced networking architectures, e.g. CASB, SASE, SD-WAN, etc., often require new approaches to monitoring that only can only be effective addressed with unified observability.

> "Staffing issues are not just about shortages and gaps – they also include a misappropriation of talent that drives up costs and job dissatisfaction."
>
> IDC

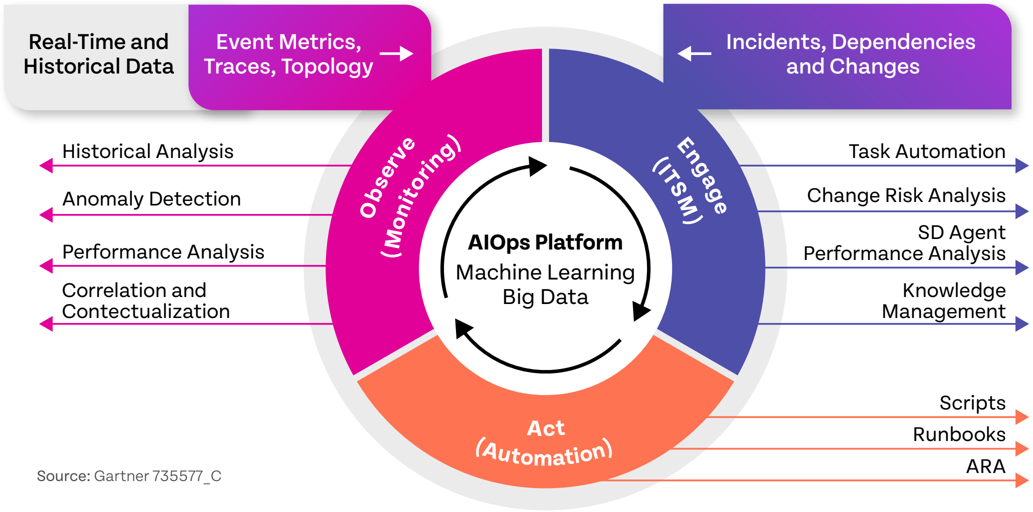
Challenges that analytics and automation address


Volume, variety & velocity of data
Need to become more proactive
Shortage of skilled IT staff
New visibility blind spots

What is AIOps?

Gartner, who originally defined AIOps (AI for IT Operations), states AIOps:

“Combines big data and machine learning functionality to support all primary IT operations functions through the scalable ingestion and analysis of the ever-increasing volume, variety and velocity of data generated by IT. The platform enables the concurrent use of multiple data sources, data collection methods, and analytical and presentation technologies.”



Source: Gartner 735577_C

AIOps platform enable continuous insights across IT Operations Management (ITOM)

AIOps Decrease Time to Detect

The digital infrastructure is only as resilient as its weakest component. The inability to manage large amounts of data is a key reason IT hasn't been able to identify and resolve incidents effectively. AIOps empowers IT to break down data silos and gain comprehensive analysis that drives actionable insights that can be used by IT staff at all skill levels.

AIOps is the process of identifying unusual patterns or outliers in IT operations data. It combines big data and machine learning to automate IT operations processes, including event correlation, anomaly detection, and root cause analysis. AIOps applies advanced analytics and logic-based techniques – such as machine learning (ML), statistics, and correlation – to automate and streamline operational workflows.

AIOps can be leveraged equally across technology domains — e.g., networking, server, cloud, security, and applications. It uses a combination of techniques to help automate decision-making, including:

1. Collect and aggregate large amounts of cross-domain data, including infrastructure, networks, applications, user experience and cloud data.
2. Leverage analytics techniques to identify meaningful patterns in the data.
3. Correlate the anomalous results to identify related or redundant events associated with an incident.
4. Automate the diagnosis of root cause analysis and remediation to resolve the issue with minimal human intervention.

> “40.8% rank anomaly detection as the most critical troubleshooting features.”
>
> Enterprise Strategy Group by TechTarget

Automate for Efficiency, Quality, Speed and Repeatability

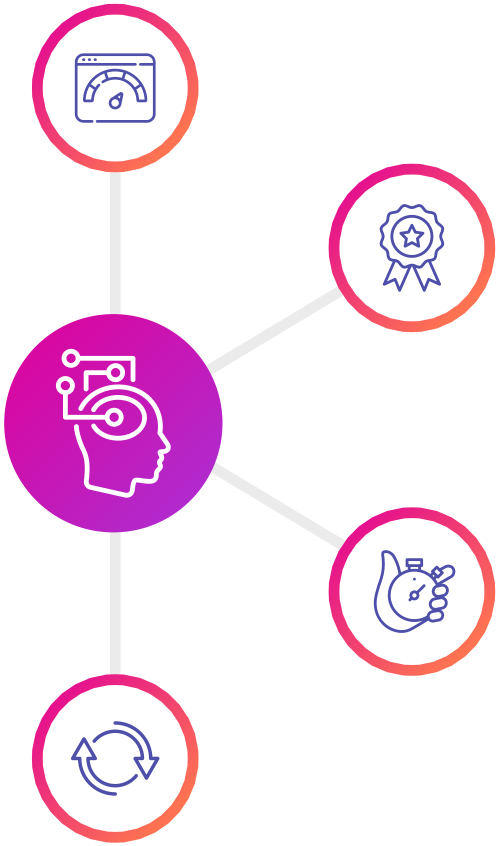
For ITOps teams, the increase in the generation and consumption of data also means there is a growing need to automate the process of gathering IT insights for faster problem identification and remediation. Organizations are struggling to reduce incident response times because of delays around manual incident analysis with cross-team collaboration challenges. Automation is not new, but it is under adopted.

IT automation is a high priority for most organizations. Forrester data shows that 92% of enterprise data and analytics decision-makers are currently using, planning to establish, or improve their use of automation technologies in the next 3 years.

Automation helps growing businesses scale IT operations. By providing detailed and actionable intelligence with speed and accuracy, automation drives faster and more accurate problem diagnosis and remediation. Automation also reduces operator drudgery by increasing the speed, quality, and repeatability of analysis.

Automation can be used in several common IT use cases, including:

- Guiding incident response with data-informed decision-making
- Auto-populating trouble tickets with supporting context, incident severity, priority, and team assignment
- Automating PC and Mac remediation processes
- Automate forensic analysis of security threats



What Sets Alluvio Apart

Alluvio by Riverbed, a Unified Observability portfolio, unifies data, insights, and actions, empowering all IT teams to deliver seamless digital experiences and end-to-end performance visibility. It leverages a combination of cross-domain data collection, AIOps, and intelligent automation to speed common and repetitive IT tasks.

Here's how Alluvio IQ helps IT teams improve results:

Breadth and depth of data

From infrastructure to network to full Digital Experience Management (DEM) with user sentiment metrics to third-party data, Alluvio provides broad and deep enterprise IT visibility. A key gap with many AIOps tools is a lack of rich data to train analytics models. With more meaningful and varied data, Alluvio IQ drives smarter machine learning models that identify meaningful, business-impacting events, while weeding out those that don't.

Diverse analytics techniques

Alluvio uses a variety of machine learning algorithms to identify events. Alluvio takes a dual approach, offering robust analytics within individual Alluvio products for domain-level monitoring and enterprise-level, cross domain analytical intelligence in Alluvio IQ, a SaaS-delivered Unified Observability service. Using techniques ranging from thresholds to dynamic baselining to variance and clustering, Alluvio identifies problems earlier.

Multi-dimensional correlations

By correlating the results of the AIOps analysis across multiple dimensions, including time, location, users, devices, and applications, Alluvio identifies related or redundant events associated with an incident. In contrast, most competitive solutions build models from time series only, which is less effective.

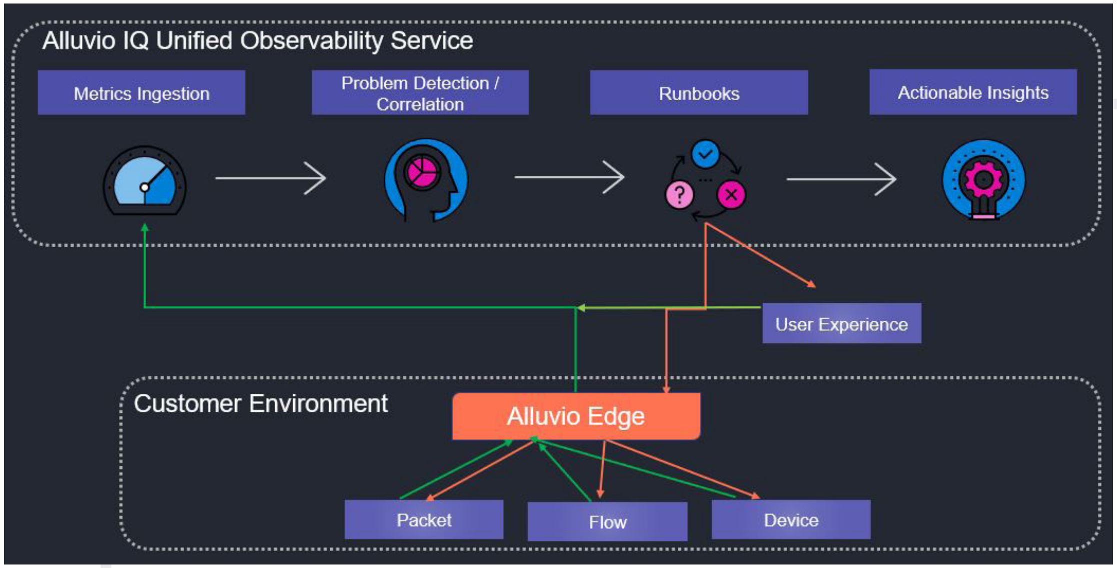
Evolving insights

Once an event is correlated, it then triggers the automation process. Out-of-the-box runbooks automate the gathering of supporting data relevant for accurate problem diagnosis, root cause analysis, and remediation. These intelligent insights drive more repeatable, accurate, and faster results, while also enabling more IT to participate in incident response, not just the IT experts.

Full-Fidelity Telemetry

The basis of any unified observability solution is broad support for different telemetry for a complete understanding of your IT environment. Preferably, this telemetry should not sample the environment, but collect high-fidelity data to ensure no events are missed.

Alluvio IQ uses both NPM and DEM data, including packet, flow, network device, application, and device-based user experience metrics. This richness of data gives IT a complete picture of what is happening and provides a strong platform from which to apply our analytic and correlation techniques.



Alluvio IQ leverage packet, flow, network device, application, and device-based user experience data from the customer environment as the basis of observability.

Alluvio Leverages AIOps to Identify Cross-domain Events

By using a variety of AIOps techniques, Alluvio by Riverbed catches incidents that might previously gone unnoticed. These techniques are used to discover and interpret meaningful patterns across data from the Alluvio full-fidelity portfolio. Identified patterns can indicate significant and complex performance issues and inform decision-making.

Among the analytics techniques Alluvio leverages include:

- **Thresholds**, simple "trip-wires" applied to metrics that quickly create an indicator when the associated threshold is violated. Thresholds are used to detect issues like device down or interface utilization above 90%. Thresholds work well in situations where there is a known range, such as with interface utilization.
- **Outlier detection** assesses performance by comparing actual measurements to a historically derived baseline. Baselining is useful for handling performance metrics that do not have a fixed range and where it is difficult to know when a performance indicator has entered a bad state. For example, organizations today use hundreds of applications, and the performance across the applications varies widely. Outlier detection continuously learns what is normal behavior for each metric and then creates events when the metric is outside the normal range.

  Thresholds can also be paired with outlier detection to handle cases where high values are normal.
- **Variance analysis** compares predicted and actual outcomes.
- **Clustering analytics** is the grouping of objects such that objects into groups that are more like each other than they are to objects in other clusters. The classification into clusters uses criteria such as smallest distances, density, or distribution of data points to group data. The main objective of cluster analysis is pattern recognition.

In short, Alluvio surfaces discrete anomalies as indicators that require attention. These indicators then flow into the data analytics pipeline to the Correlation Engine to determine if there are any commonalities.

Correlation Engine

The Alluvio Correlation Engine applies a variety of algorithms to group related indicators into a single incident. It looks at all events from the previous 20-minutes to identify potentially related incidents and determines if there are any commonalities or relationships between them. Unlike other solutions, Alluvio correlates across five dimensions – time, location, application, devices, and users. This is done to reduce the number of alerts IT teams need to investigate.

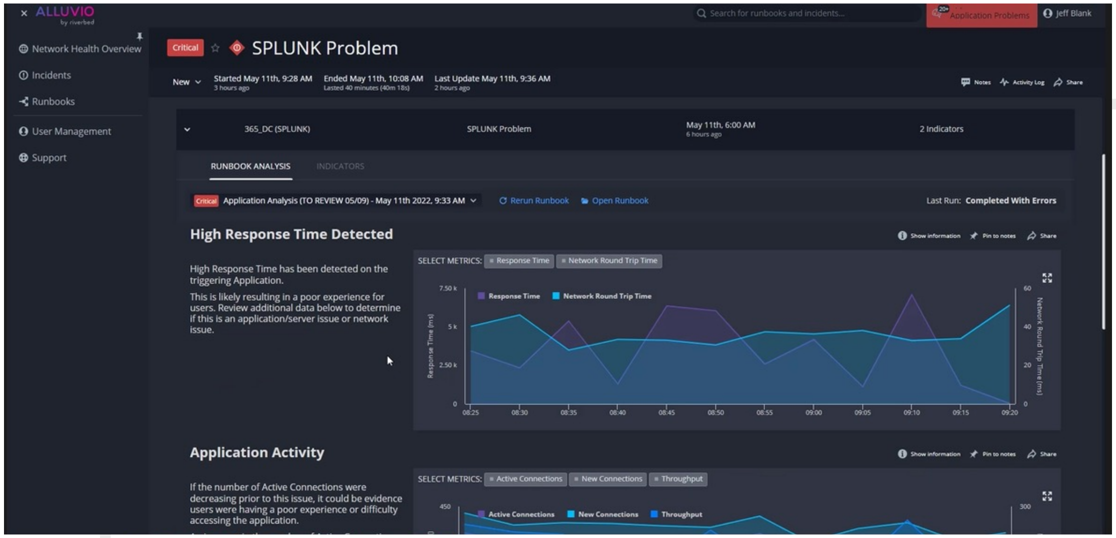
The Correlation Engine can identify one or more triggers. For example, it might create a single trigger for a well-defined indicator that is distinct or a converging set of indicators, like rolling up interface issues related to a downed device. Or it can create multiple triggers for a group of related incidents that need additional context to help better characterize.

Alluvio LogiQ Engine Automates Processes

The Alluvio LogiQ Engine automates incident response and remediation of IT problems by executing low-code runbooks in response to a correlated event. Alluvio uses automated investigative workflows to replicate the troubleshooting practices of your ITOps and Service Desk experts. These low-code runbooks gather supporting evidence, build context, and set priorities so IT teams can automate:

- Incident response and security forensics with data-informed decision-making.
- Populating trouble tickets with more actionable alerts.
- Recovery actions of common device, OS, or app issues so user experience is not impacted.

Alluvio Automation Engine links back to the originating source telemetry to assemble the supporting troubleshooting data. Data collected can include network, infrastructure, application, end user experience and sentiment.



SPLUNK Problem

Started May 11th, 9:28 AM
3 hours ago

Ended May 11th, 10:08 AM
Lasted 40 minutes (40m 18s)

Last Update May 11th, 9:36 AM
2 hours ago

365_DC (SPLUNK) | SPLUNK Problem | May 11th, 6:00 AM 6 hours ago | 2 Indicators

Application Analysis (TO REVIEW 05/09) - May 11th 2022, 9:33 AM

Last Run: **Completed With Errors**

High Response Time Detected

High Response Time has been detected on the triggering Application.

This is likely resulting in a poor experience for users. Review additional data below to determine if this is an application/server issue or network issue.

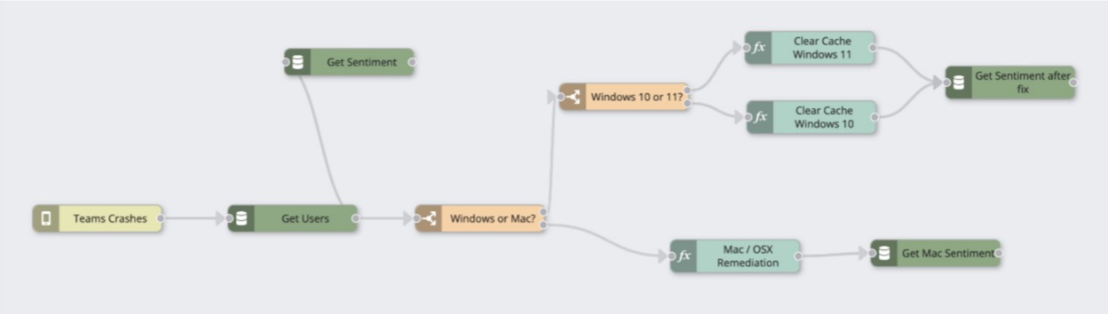
Application Activity

If the number of Active Connections were decreasing prior to this issue, it could be evidence users were having a poor experience or difficulty accessing the application.

Alluvio IQ captures data that supports faster problem diagnosis and root cause analysis.

Related to troubleshooting, Alluvio creates smart ServiceNow tickets with the proper severity assignment and designates it to the right team. It also provides supporting incident context to speed response, cutting the noise caused by traditional event-based ticketing. If the threshold criteria isn't exceeded, the behavior is treated as benign and ticket severity is marked as low priority.

Alluvio also automates common, but frequently time-consuming device remediation processes. The Service Desk can save time and fix more issues earlier in the process, reducing the number of trouble tickets that need to be expedited to the experts. Plus, the auto-remediations avoid the need to involve the user in the repair process.



Alluvio automates common device remediation processes. It identifies severity based on user sentiment, then determines which type(s) of devices are impacted and how to fix them. User sentiment is checked again after the fix is implemented to determine if the remediation was successful.

By capturing expert troubleshooting knowledge in Alluvio's reusable workflows, your incident response and remediations become more consistent, repeatable, faster, and more efficient. Since Alluvio automation workflows are easily customizable, you can quickly tweak them to your organization's exact requirements.

Supporting New Uses Cases with AI and Automation

By integrating AIOps, correlation, and automation capabilities with enterprise-wide, cross-domain data, the Alluvio Unified Observability platform enables IT operations teams to respond more quickly and proactively to slowdowns and outages anywhere across the enterprise, whether on-prem, cloud, or remote. It bridges the gap between an increasingly dynamic and difficult-to-monitor IT ecosystem, while ensuring user expectations for uninterrupted application performance are met.

IT is charged with providing fast, predictable, and secure access to all IT environments. Alluvio Unified Observability enables resolution of problems in new, difficult-to-monitor environments, like remote and SASE.

Remote work

In work-from anywhere situations, traffic typically bypasses data center monitoring, going straight to the cloud or SaaS applications. By collecting metrics from user devices, Alluvio provides in-dept visibility into where the problem resides: user experience, device, application, or network.

Secure Access Security Edge (SASE)

In Zero Trust environments, it's common to have three or more different traffic routing options: direct to internet, VPN, and Cloud Access Security Broker (CASB). CASBs tunnel traffic to improve security; however, tunneling largely obscures monitoring details from traditional performance management solutions. Alluvio leverages endpoint data to identify network, application, and end user device issues in both remote work and SASE ecosystems.

For More Information

To learn how Riverbed Alluvio can help your IT operations team:

- Reduce incident noise by creating fewer, more meaningful alerts
- Diagnose and resolve incidents faster and more proactively
- Create more actionable trouble tickets with the context needed to resolve them quickly
- Improve SLAs and user experience by reducing recovery time objectives (RTOs)
- Improve IT reliability, repeatability and efficiency by automating processes
- Enable L1/L2 engineers to resolve more first-level events without having to escalate to senior staff

VISIT RIVERBED FOR ADDITIONAL DETAILS >

About Riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user, that illuminates and then accelerates every interaction, so organizations can deliver a seamless digital experience and drive enterprise performance. Riverbed offers two industry-leading portfolios: Alluvio by Riverbed, a differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless, secure digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of partners, and market-leading customers globally – including 95% of the FORTUNE 100 –, we empower every click, every digital experience. Riverbed. Empower the Experience. Learn more at riverbed.com.