riverbed

SOLUTION BRIEF

# Alluvio IQ Automates Security Forensic Investigations

## Improves effectiveness of traditional SIEM and SOAR tools with access to full-fidelity NPM data.

Intelligent security is a persistent concern for all hybrid networks today. As organizations expand beyond the data center, so increases the threat exposure to the extended network from remote offices, campus, and cloud resources. To keep pace with pervasive threats, SecOps teams need to apply intelligent automation while having access to rich network forensics for active threat detection and threat hunting. Traditional security tools often fall short due to unreliable or sampled telemetry and the inability to automate incident response. The result is time-consuming, labor-intensive manual investigations, which are frequently less accurate. This presents significant challenges for security teams who are under constant scrutiny to reduce secure risks while maintaining reliable digital experience for employees and customers.

### Enriching traditional security tools with automated investigations

Alluvio™ IQ, Riverbed's SaaS-delivered unified observability service, drives collaboration between NetOps and SecOps teams, aiding in the investigation of pervasive threats using intelligent automation based on full-fidelity network data, including flow, packet, and infrastructure metrics. Alluvio IQ investigates threats found in traditional security tools like Security Information and Event Management (SIEM) or Security Orchestration, Automation, and Response (SOAR) and leverages powerful low-code runbooks to automate the collection of supporting forensics from across the Alluvio™ Network Performance Management (NPM) portfolio. Alluvio IQ distills the forensic data to provide actionable insights that help SecOps focus on resolving real threats, instead of manually chasing false positives. Automated security forensics provide only the most pertinent data by applying highly customizable, security-specific runbooks, giving SecOps teams the data they need to drive intelligent security investigations and mitigate cyber threats.

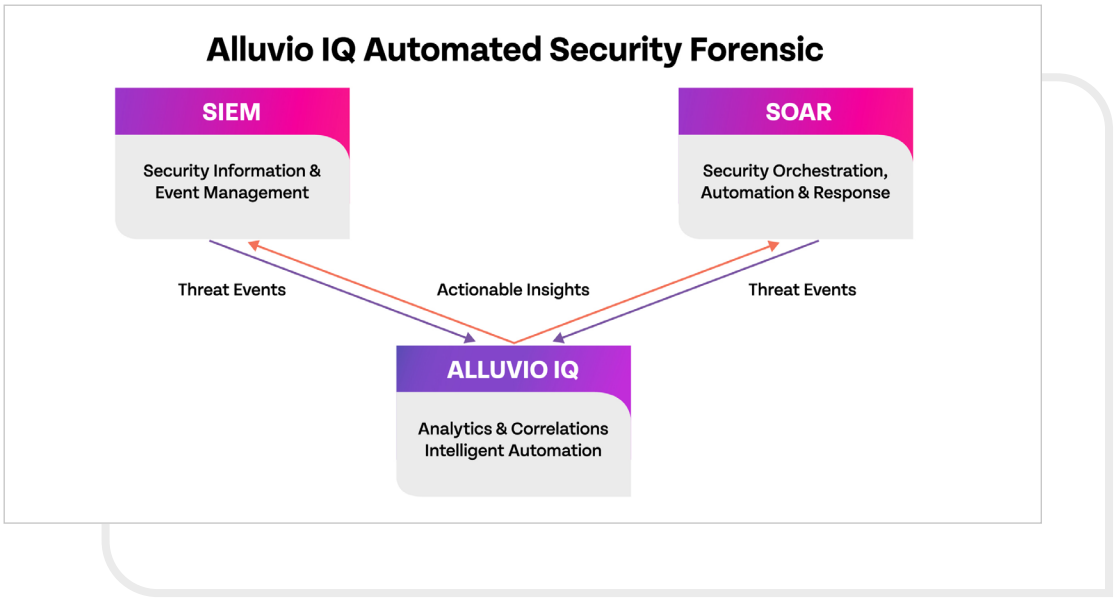



**Figure 1:** Alluvio IQ investigates threats found in traditional security tools like SIEM or SOAR and leverages powerful low-code runbooks to gather supporting forensics from across the Alluvio NPM portfolio.

## Get network intelligence and security forensics from a single vendor

Businesses often must curate several products from multiple vendors to gain end-to-end visibility across their hybrid networks. Alluvio IQ and Alluvio Network Performance Management (NPM) solutions are part of the Alluvio Unified Observability Portfolio by Riverbed, providing both full-fidelity telemetry and unified observability, making our data highly valuable to both organizations. Riverbed unifies data, insights, and actions for all IT, including NetOps and SecOps. With Alluvio IQ unified observability, IT can eliminate data silos, war rooms, and alert fatigue. IT can make more effective decisions across domains, apply expert knowledge more broadly, and continuously improve digital experience and business performance.

## Improve the effectiveness of security tools

Traditional security tools like SIEMs and SOARs are only as good as the intelligence they ingest. Often the network data used by these tools is sampled or difficult for SecOps to access. Choosing a data source that provides full-fidelity network telemetry by capturing every packet, flow, and device metric, coupled with actionable insights from intelligent, automated runbooks increases the effectiveness of security investigations.

## Reduce manual investigation of false positives with intelligent automation

Alluvio IQ can ingest data from Alluvio telemetry as well as third-party solutions and apply customizable automation scripts to identify high-impact security incidents. The resulting highly refined actionable insights isolate only the most pertinent incidents, while eliminating false positives. By focusing on real threats, SecOps teams can identify and remediate security threats across the modern hybrid network.

## Improve collaboration between NetOps and SecOps

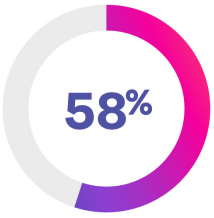
Often these two organizations are at odds over competing operational priorities that ultimately impact both network performance and security. Both teams require network data to effectively do their jobs. In the case of NetOps teams, they are concerned with keeping the network and applications traversing it performant, while security teams need network data to eliminate risks to the network and infrastructure.

With Alluvio IQ's automated investigations, collaboration occurs as there is clear delineation over ownership. NetOps owns the network telemetry while SecOps owns the traditional security tools that ingest Alluvio's full-fidelity network performance data to protect the enterprise from cyber threats.

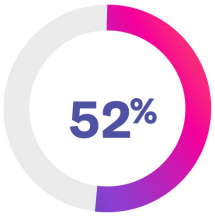
## Benefits of Alluvio's security forensics automation

In addition to improving collaboration between NetOps and SecOps teams, security forensics automation can provide the following benefits to SecOps teams:

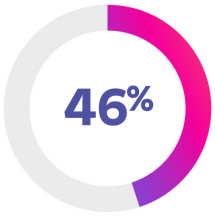
**The top 3 benefits of successful NetSecOps partnerships:**




Faster resolution of security issues




Reduced security risk




Operational efficiency

Enterprise Management Associates

- **Speed and Efficiency:** Automation can quickly process large volumes of data, identify patterns, and gather full-fidelity diagnostic data to significantly reduce the time required to identify, analyze, and mitigate security incidents.
- **Accuracy:** Automated tools are less prone to human error and can analyze more data in a more consistent and reliable manner. This significantly reduces the risk of missing critical indicators of a security breach or falsely flagging non-security-related events.
- **Consistency:** By using a combination of AI, correlation, and automation, Alluvio IQ consistently analyzes and prioritizes security incidents while also gathering supporting and related diagnostic data to ensure all related threats are identified appropriately.
- **Scalability:** Automated security forensics can easily scale to analyze large volumes of data across multiple systems and devices. This makes it possible to identify and respond to security incidents in a timely and efficient manner.
- **Cost-effective:** Automated tools can reduce the workload of security analysts, allowing them to focus on more complex security issues. This can help to reduce the overall cost of managing security incidents.

Overall, automating security forensics helps SecOps teams identify and respond to security incidents more quickly and effectively, while also reducing the workload and costs associated with manual methods.

## About Alluvio IQ

Alluvio IQ, Riverbed's cloud-native, SaaS-delivered, open, and programmable solution for Unified Observability, empowers all IT and security staff to identify and fix problems fast. It applies machine learning (ML) techniques to full-fidelity end user experience and network performance data across every transaction to identify anomalous events. It then contextually correlates the data streams to identify the most business-impacting ones. This intelligence informs the automated, investigative runbooks that replicate the troubleshooting workflows of IT and security experts to gather supporting context, filter out noise, and set priorities — reducing the volume of alerts to the most business impacting.

Alluvio IQ drives collaboration between NetOps and SecOps teams, aiding in the active search of pervasive threats across the network with automated security investigations. Automated security forensics identify the most pertinent events, applying highly customizable, security-specific runbooks to events identified in SIEM or SOAR solutions. SecOps teams get the network data they need to support intelligent security investigations.

For more information on Alluvio IQ automated security forensics, click here.

riverbed

### Riverbed — Empower the Experience

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 that users get the flawless digital experience they expect across the entire digital ecosystem. Riverbed offers two industry-leading solution areas – Alluvio by Riverbed, an innovative and differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app over any network to users, whether mobile, remote, or on-prem. Together with our thousands of partners, and market-leading customers across the world, we empower every click, every digital experience. Learn more at riverbed.com.