riverbed

U.S. Public Sector

WHITE PAPER

Deliver Visibility into Network Issues with Unified Observability

For several years, whenever there were issues with a large federal agency's IT systems, users were quick to blame the network.

They didn't think much about the details, such as application error, a lag on the network caused by a new product, application update, or out-of-date network capacity planning.

Marlin McFate, CTO for the Public Sector at Riverbed, said that in the past, it might take hours, days, or even months for network managers to do a root cause analysis and identify the problem.

With Alluvio, Riverbed's Unified Observability portfolio, federal agencies can have all the network data from the cloud, network operations (NetOps), security operations (SecOps), and end user teams fed into a single console. The data can be stitched together and analytics can be run against it to identify the issue.

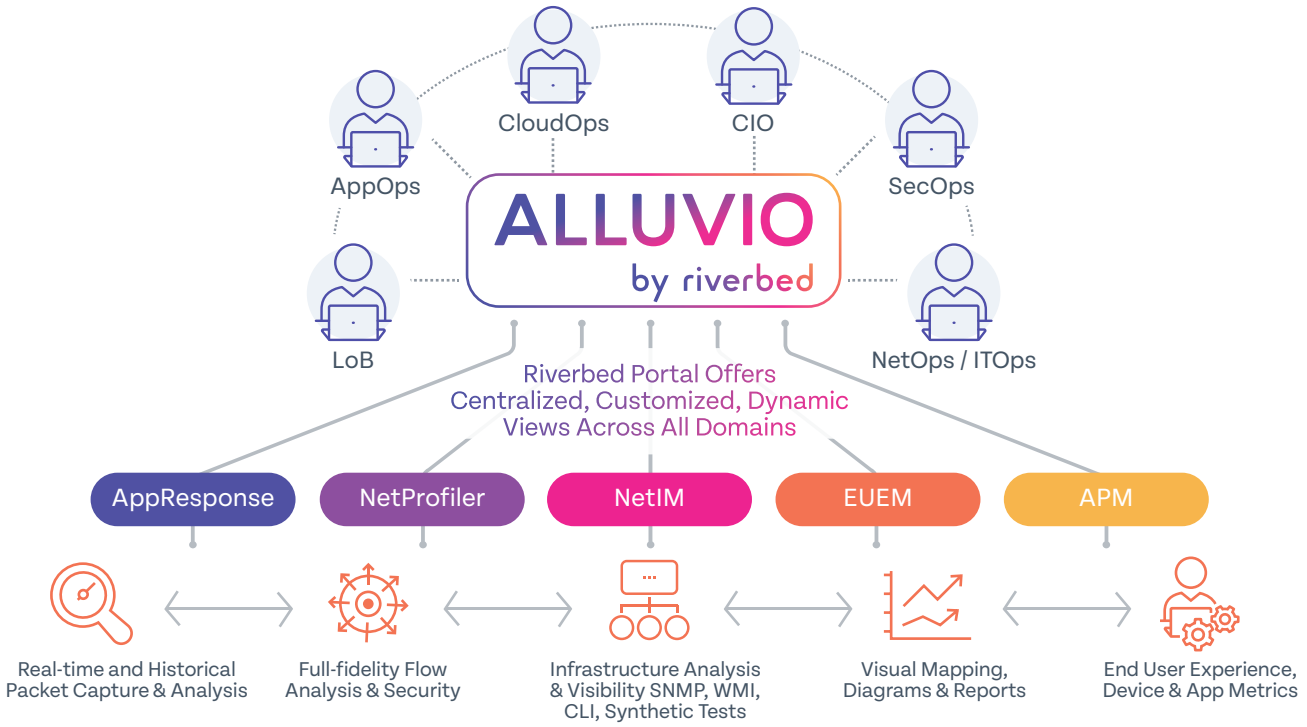
Unified Observability, said McFate, offers a way for agencies to run processes for visualizing, monitoring, troubleshooting, and reporting on the health and availability of the network, end users, and applications which all make for a better end user experience.

"Network managers can click on a console and get information on the devices, ports, where the data traveled, what happened to the databases, and what took place on the web tier," McFate said. "And this is for information across all teams and departments. When a networking person only looks at network data, they are not looking at the periphery, they don't know what's on the edge of the network, and more importantly how it effects or is contributing to the problem at hand. Riverbed's Unified Observability solutions gives them a common foundation of data."

> Getting true end-to-end visibility has always been difficult and complex. When the pandemic hit almost overnight, it became even more difficult.

Getting true end-to-end visibility within organizations has always been difficult and complex. When the pandemic hit almost overnight, it became even more difficult, including the biggest changes—how users connect and where they work. With the new demands for remote work, the cloud exploded, both on the development and infrastructure side, and with Software-as-a Service (SaaS) applications.

Unified Observability Offers Complete Visibility



"There were always deficiencies, but those seemed more tolerable as long as most of the traffic flowed over a closed system," McFate said. "But all the deficiencies became much more obvious once agencies made the move to work-from-home and it became an open network."

Hackers noticed. Combine all the changes with the increased threat landscape and the reality that average users are not necessarily cyber savvy and McFate said it's become clear to federal network managers that they need the capabilities of Unified Observability to manage the new environment.

> "The idea is that network teams can be more proactive than reactive.
>
> **Marlin McFate, CTO, Public Sector, Riverbed**

"With Unified Observability, network teams now know when end users are having a problem, often before the end user knows about it so the network team can fix the issue in advance," McFate said.

The pandemic lets network teams finally see the benefits of Unified Observability.

With the increases in endpoints due to remote work and the subsequent uptick in cyber attacks because of the pandemic, network teams had to find a way to mitigate these dynamic challenges, according to McFate.

"In the past, they would lean on their IPS, IDS and firewall data and wait for alerts. Spending money on fighting zero-day attacks and threat hunting was expensive and required a lot of expertise," McFate explains. "As the sophistication of cyberattacks increased, they've recognized that they have to spend the time, money, and develop the expertise. Unified Observability always had a relationship to cybersecurity, but it's become even more relevant."

Based on research from Enterprise Strategy Group, the following are four distinct benefits that Alluvio's Unified Observability solutions offers network teams:

Less time to identify and troubleshoot issues.

Alluvio's Unified Observability solutions makes it possible for network administrators to spend less time on collecting, integrating, and correlating data. By having a unified view of the network data, IT teams can easily pinpoint the root cause and offer remedies. Time working with multiple third party tools is significantly reduced, so IT teams spend less time on collecting and integrating data manually, which results in a decreased meantime-to-resolution (MTR), freeing up the IT staff to focus more on the most critical tasks and strategic initiatives. McFate said there have been situations where the network team spent hours, if not days, working to find the root cause of an issue. With Unified Observability, organizations can dramatically cut troubleshooting time down, sometimes even fixing issues before end users experience them, cutting down on service calls and help desk tickets.

Increased visibility into the IT environment.

Riverbed Portal offers a common view of issues across the organization, from IT operations, NetOps and program management. Once they have this common view, teams can get together and more easily decide on the best course of action because they are dealing from a common set of facts. ESG's interviews also found that the increased visibility into end user consumption and traffic patterns with Riverbed DEM tools let NetOps teams do more effective capacity planning for network bandwidth. McFate said by using Riverbed's NetIM, NetProfiler and AppResponse tools, IT teams can run simulations on how any changes in capacity and traffic will affect the network. These integrated tools are especially helpful as organizations migrate applications to the cloud. The ability to have the visibility into how the network will respond helps organizations make more precise decisions on how much bandwidth to allocate and which network infrastructure to purchase.

Improved IT collaboration.

Unified Observability also applies to teams managing applications, servers, storage infrastructure, and cybersecurity. McFate said that in the past, if there was a network slowdown, end users would typically blame the network, but with the teams armed with a common set of data, they more easily agree on the root cause of the problem because they are all looking at the same data. This reduces troubleshooting time and reduces the "blame game" where one group blames another for the problem because the data is inaccurate.

Improved network security.

Security teams are also using Unified Observability to pinpoint and address various security threats, such as malware, blacklisted sites, distributed denial of service (DDoS) attacks, and advanced persistent threats. ESG notes that data collected at the application, network, and device levels can help security teams detect breaches or attacks faster. Some of the Riverbed customers ESG interviewed say how instrumental network flow data collected by the NetProfiler Advanced Security Module was in identifying security breaches. McFate adds that Unified Observability also integrates with widely used Security Information and Event Management (SIEM) products, allowing NetOps and SecOps teams to work together to drill down into packet and flow records to identity security incidents, helping shorten response and time to resolution.

Unified Observability Offers Actionable Insights

Network teams now have visibility into East-West traffic and can see all the knowns, unknowns, and drill down into why a security event is happening," said McFate. "What often happens is an adversary gains access to a system and uses it as a launch point to infiltrate other systems. Moving around laterally, attackers can avoid detection from security tools only looking at the network's perimeter. Exploiting this technique, they can operate with impunity for long periods of time. We give organizations the visibility they need so they can see into those areas." The amount of time an adversary goes undetected, can be directly connected to the damage, and cost of an incident, Unified Observability can reduce the time to detection.

McFate added that federal agencies need as much visibility as possible to correct network issues and stop breaches that can imperil mission success.

"These are often life and death situations," McFate said, adding that federal networks simply can't afford downtime when lives are at stake, whether in battle, fighting forest fires, or rescuing victims in the aftermath of a hurricane.

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.