USE CASE

Enterprise Visibility
and Performance

Federal Agency Boosts Scalability with Unified Enterprise Visibility

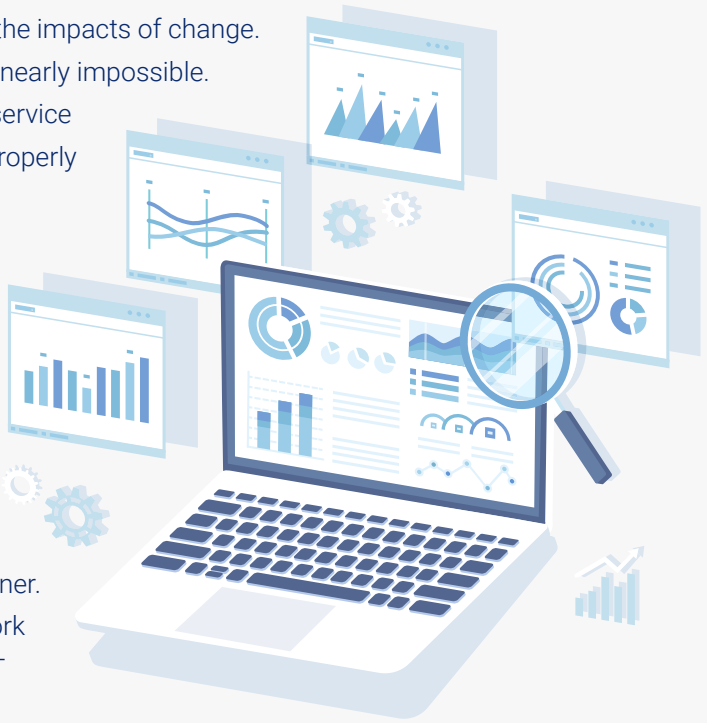
RavenTek and Riverbed Deliver Integrated Network and Performance Monitoring Solution

RAVENTEK | riverbed®

Background

An independent federal agency that works to promote fundamental research and education manages over 3500 end users. In order to successfully support internal end users and external clients with applications for grants and projects, the agency operates in a hybrid cloud environment. Over the years, the agency has continued to expand in size of its workforce and scope of its mission. As federal IT teams know, scaling IT infrastructure can be a huge challenge, be it the proliferation of new data centers, networks, servers, and applications.

To be able to successfully scale, IT teams need to understand the impacts of change. Without an end-to-end monitoring solution, this task can seem nearly impossible. To deploy new services, whether it be on premise or via cloud service providers, IT teams need visibility on the effects of change to properly scale components of their services.



Compounding the complexities of scaling its IT infrastructure out, the agency has a number of IT teams involved in maintaining its hybrid cloud environment, including the Network team, Operations, Server, Engineering, and Help/Service Desk team. Each team used several disparate toolsets that provided fragmented visibility across the enterprise, making it increasingly difficult to troubleshoot performance issues or end user complaints in a proactive manner. The agency needed a solution that could provide utmost network performance, connectivity, and visibility, while ensuring every IT team was on the same page.

By turning to RavenTek's consultative approach and engineering expertise and applying Riverbed's SteelCentral Network Performance Monitoring (NPM) solution set, the agency was able to boost scalability through integrated network and infrastructure visibility.

The Challenge

Overcoming Fragmented Visibility Into the Network and Siloed IT Products

With disparate tools to manage and limited visibility into the network, it becomes increasingly difficult for agencies to successfully scale out their IT infrastructure to meet the new demands of changing missions.

As agencies add new services or platforms, their IT teams typically acquire more new toolsets to help accommodate the shift in size and scope. This results in an ever-expanding toolbox of IT products that don't communicate with each other, making network visibility especially challenging. Not to mention the security ramifications this can have, with as many as 67% percent of IT teams admitting that network blind spots are one of the biggest challenges they face when trying to protect an organization's data.

Additionally, this leads teams to be more susceptible to the infamous "IT Blame Game" where one federal IT team gets scapegoated for end user complaints and performance issues outside their realm of control and responsibility.

Like many other agencies, this particular agency struggled with legacy network visibility systems combined with disparate point solutions that couldn't communicate with each other. With each IT team having different priorities and limited visibility of the entire IT ecosystem, pinpointing performance issues on the network became extremely difficult.

- Ever-expanding toolbox of point solutions
- Lack of correlation between IT products
- Siloed solutions that only provide limited data into one or two aspects of the network (i.e. flows, packets, or servers)
- Fragmented visibility for IT teams into network performance issues
- Multiple maintenance and support contracts

> ***"If an issue or problem is indicated in one tool, but you can't corelate that poor performance with another necessary tool, IT teams can't understand what's happening in the broader scheme of the IT ecosystem, which can make troubleshooting very difficult."***
>
> **Marlin McFate**
> Public Sector Chief Technology Officer,
> Riverbed Technology

The Approach

IT Tool Consolidation and Comprehensive Training

RavenTek's Unique Consultative Approach for Quick and Seamless Implementation

RavenTek's investments in well qualified engineering professionals and continuous training through the Riverbed Partner Training Portal make them a premier partner of Riverbed. RavenTek has extensive network architecture, virtualization, and IT support experience in executing enterprise-level IT implementations for civilian and Department of Defense (DoD) agencies.

Through a consultative approach, RavenTek ensured the agency's IT teams had extensive professional demonstrations of the Riverbed solutions that would be best suited to meeting the agency's network infrastructure and visibility needs.

After an extensive review process with RavenTek, the agency was able to determine the best use of Riverbed's SteelCentral suite, particularly focusing on the deployment of NetIM, NetAuditor, NetProfiler and Riverbed's Portal dashboard as a single pane of glass to tie these tools together. RavenTek then provided a Proof of Concept that included the installation of the products, which took no more than 3 months.

First, the agency implemented NetIM for device list management, data collection, grouping, link inference, and data storage. This would help the agency's IT teams troubleshoot and correct missing devices, missing data, missing links, and incorrect grouping.

Next, RavenTek worked with the agency to install and configure Riverbed's NetAuditor. This required implementing a model to import a network audit report generation through the following seven-step process:

1. Import the requisite models form NetIM
2. Configure NetAuditor, Trending, Network Difference, Inventory, and OS Compliance reports
3. Produce the network audit reports for the identified devices; then demonstrate how to resolve errors with coverage and content (e.g. false positives and false negatives)
4. Implement model import and network diagram production
5. Import the requisite models form NetIM
6. Produce the diagrams for the identified layouts; resolve errors with device content and layouts
7. Lastly, the team worked to implement Network Diagrams to ensure the solution would produce the expected diagrams according to the configured automation schedule

The Solution

Network Monitoring from a Single Pane of Glass

Riverbed's SteelCentral Suite Provides All the Data Necessary for Enterprise Network Visibility in Hybrid Environments

Unlike traditional NPM solutions, Riverbed provides a wider scope of products with end-to-end network visibility, more granularity in the data, and seamless integration of network visibility products into one platform. Riverbed's SteelCentral solution is a unified performance management suite of tools that provide broad visibility and analytics across all networks and applications.

Riverbed's SteelCentral Suite Empowers All IT Teams

As a holistic approach to complex, distributed environments, SteelCentral consists of end-user experience monitoring, application performance monitoring, cloud performance monitoring, network infrastructure monitoring, network performance monitoring, as well as professional services.

Specifically, the agency successfully leveraged the following from the SteelCentral suite:

Network Performance Monitoring

NPM Dashboard Portal

- Used at the Executive level and Engineering teams
- Combines various data into a centralized, easy-to-use dashboard so different IT and operations teams get a complete picture of the network, reducing time wasted on the IT blame game.

NetProfiler

- Used by Network, Operations and Help/Service Desk teams
- Enables teams to understand what's actually happening on the network and easily answer bandwidth analysis questions like, "How much traffic is being consumed?" "Who is using it?" Where is it going? and "How is traffic being prioritized?"

IT Infrastructure Monitoring

NetIM

- Used by Server and Network teams
- Enables IT to proactively manage and monitor IT infrastructure to detect performance issues, map application network paths, diagram the network, and troubleshoot infrastructure problems.

Application Performance Monitoring

AppResponse

- Used by Network and Help/Service Desk teams
- Delivers full stack network and application analysis to help capture, store, and analyze all application

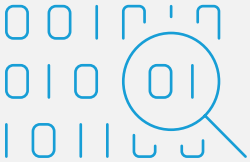
The Results

Using A "Triple Threat" Solution for Network Visibility and IT Scalability

Now the agency can confidently take on horizontal IT infrastructure scaling while maintaining end-to-end visibility.

Riverbed's SteelCentral NPM solution provides three essential components (a triple threat) to enable IT infrastructure scalability and enterprise network visibility for the agency.

Integration is essential to the success of IT infrastructure scaling. As emphasized earlier, many agencies add IT tools and products that cannot communicate with each other to accommodate an infrastructure expansion. The problem is if an end user has an issue on one specific app, the IT team can't necessarily correlate it with other apps that may be encountering the same issue, making it more difficult to troubleshoot. That's why any NPM tool must be able to integrate across all IT products in the ecosystem.



Granular data for federal IT professionals is needed to be able to capture exactly what's happening on the network including insights into data flows, packets, and servers. While many NPM solutions can capture one or two of these features at once, it's important to be able to monitor all of these data points simultaneously.

A single pane of glass helps IT teams as well as department leaders access that sole source of truth in one place without the additional hassle of manual correlation. Even as the agency adds a colocation, the IT teams can maintain visibility into those networks and ascertain how app performance will be affected before, during, and after IT infrastructure scaling.

These three essentials for scalability will enhance NPM and make it easier for the agency's IT teams to monitor, troubleshoot, and analyze what's happening across hybrid network environments. With integrated network and infrastructure visibility, the agency can successfully scale up AND scale out their IT infrastructure while having full visibility into their networks and apps whether on-premises, virtual, and/or cloud across all domains–far and near.

Summary

Integrated Network and Infrastructure Visibility is Key

As its mission continues to evolve in size and scope, the agency can better accommodate the horizontal scaling of its IT infrastructure by empowering its IT teams with end-to-end visibility. Whether it's access to reporting on the executive level or operating on the engineering or service desk teams, the agency can now confidently obtain granular data on its dispersed assets through a unified single pane of glass.

About Riverbed

Riverbed understands that every agency is on a digital journey and that every journey is unique. With a proud heritage of technology leadership and proven expertise maximizing performance and visibility for the world's largest organizations, we can help agencies reach the full potential of their network and application investments today and in the future. Learn more at www.riverbed.com.

About RavenTek

RavenTek recognizes that in today's challenging fiscal environment, federal agencies need the right partner who can help them advance mission goals through efficient and innovative IT, engineering, administrative, and program management solutions.

Learn more at **www.raventek.com**.

RAVENTEK