U.S. Public Sector

riverbed | Aternity

IMPROVING RESILIENCY AND SECURITY FOR AGENCY REENTRY PLANS AND THE HYBRID FUTURE

Accelerating Network Performance and the Digital Experience

The Hybrid Future - 2022 & Beyond

"We're going to go into more of a hybrid model, a true hybrid model. It's going to be interesting because now we have to learn to operate in a few modes all at the same time."

— Steven Hernandez, Chief Information Security Officer, Department of Education[6]

One of the unintended benefits of the pandemic is that public sector organizations underwent years' worth of digital transformation in mere months as IT teams were forced to rearchitect and transform their network environments and digital services in real time to support Max Telework policies and remote workforce needs.

For many organizations, those changes were designed as short-term solutions to survive, but as the pandemic continued, government employees not only survived teleworking, but thrived. The ability for users to work anywhere and access their networks, apps, and tools needed to drive missions forward resulted in employees taking on additional work and expanding their mission scope, while experiencing unprecedented increases in engagement and productivity.

These advancements didn't go unnoticed - the Office of Personnel Management's return-to-work guidance reflects this new reality by instructing federal agencies to take advantage of these advancements and consider maximum telework flexibility.

As organizations execute reentry plans, it's clear that there is no returning to a pre-pandemic model. Many organizations are managing large-scale hybrid environments. To make this new reality possible, IT teams must ensure the peak performance and productivity of networks, apps, and users, while simultaneously identifying and mitigating security threats before attacks happen.

Having end-to-end visibility across distributed environments and networks, is the only way to ensure mission success in a hybrid public sector.

96%
U.S. TREASURY EMPLOYEES SAVED TIME AND MONEY NOT COMMUTING[3]

86%
FEDERAL IT LEADERS WANT TO TELEWORK PART TIME AFTER THE PANDEMIC[7]

50%
OCCUPANCY LIMITS PLACED ON U.S. NAVAL SHORE FACILITIES INDEFINITELY[2]

88%
DOD EMPLOYEES REPORTED BEING AS OR MORE PRODUCTIVE TELEWORKING[4]

riverbed | Aternity

Mission-Ready Digital Environments

As government organizations worldwide plan for reentry efforts and beyond, building on the digital transformations that took place during 2020 and 2021 will be critical to both the short-term success of the hybrid work environment and the long-term resiliency of the public sector.

The goal? The secure, efficient, and high performance of every user, device, application, and network, on an ongoing basis - true mission resiliency.

For organizations to successfully drive this hybrid future forward they must continue to take advantage of the modernization, collaboration and engagement enabled by cloud infrastructure, SaaS, and other software-defined tools.

However, to ensure seamless user experiences onsite, offsite and on-the-move, end-to-end visibility across the entire network, application, and user environments is crucial. This allows IT teams to proactively identify issues, model and map performance needs, and reduce network complexity while ensuring smooth, secure operations through every phase of reentry.

End-to-end visibility ensures that public sector organizations have insights into whether actions and approaches deliver both the intended return on investment and the expected operational outcome, while offering the flexibility to make adjustments in real time to drive missions forward.

72% FEDERAL EMPLOYEES GAINED ACCESS TO EXPANDED COLLABORATION TOOLS[7]

90% FEDERAL IT LEADERS[1] VIEW THEIR NETWORK ENVIRONMENT AS COMPLEX

82% FEDERAL EMPLOYEES COLLABORATED WITH COLLEAGUES[7] REMOTELY TO COMPLETE THEIR MISSIONS DURING THE PANDEMIC

riverbed | Aternity

Full-Fidelity Visibility to Secure Hybrid Environments

"It's not the fact that we can't connect the dots... We can't see all of the dots."

— General Paul Nakasone, Director, National Security Agency & US Cyber Command[8]

Christopher Cleary, the Navy's principal cyber advisor, describes true resilience as "survivability, or your ability to fight through the problems."[6] Survivability – that's the rub for every IT team, whether at large agencies that house millions of citizen records or on the front lines of a remote military post. What's more, as organizations roll out upgrades to improve agility, flexibility, speed and scalability, small flaws or missteps can undermine their initiatives or create new and sometimes unobserved attack vectors.

The SUNBURST attack demonstrated the crippling potential of unseen vulnerabilities and silent actors on government networks. "The real mindset we need to adopt is this idea that security is a horizon that we are always going to chase and that we are never going to reach," said Cleary. For the federal government, this mindset is evolving to zero trust architectures and an assumption that attackers are already inside the network environment.

End-to-end visibility offers organizations full-fidelity visibility by capturing all flow, packets, logs, device and end-user data, all the time. Applying analytics to this data can provide holistic and actionable insights to understand how applications are performing, where and how they are going awry and let you identify the data at risk. Without such visibility, an organization is running blind.

How can IT and security teams achieve end-to-end visibility?
Read on for further tactics and tips.

93%
FEDERAL IT LEADERS
AGREE THAT
GREATER VISIBILITY
IMPROVES
NETWORK SECURITY[1]

96%
FEDERAL IT LEADERS
VIEW NETWORK
VISIBILITY
AS VALUABLE
IN ASSURING
SECURE
INFRASTRUCTURE[1]

Did you know there's a parallel between zero trust network security and the Roman Empire?
Find out what it is in this blog post by Riverbed|Aternity CTO and Chief Security Architect Vincent Berk

riverbed | Aternity

End-to-End Visibility in Practice

U.S Armed Forces Network Integration Center

Bridging networks, applications, and cloud for the next generation of warfighters

Department of Defense agencies and the Uniformed Service Branches are expanding their networks to support a hybrid workforce, cloud transformation and a growing number of applications — creating more points of access, and more points of risk. Without end-to-end visibility into all network, application and device activity, IT teams can't detect and remediate performance and security issues effectively.

Challenge

A DoD customer that provides Network Integration Services through centralized and disperse locations wanted to improve the network management of critical IT infrastructure and alleviate bottlenecks, latency and poor end-user experiences being caused with larger number of employees teleworking due to the pandemic. The goal was to monitor and manage the network nodes, networks, connected devices, and application traffic to deliver visibility to command, mitigate any issues, and implement any network changes to support global mission-critical users.

Solution

Using Riverbed|Aternity end-to-end visibility solutions, the customer was able to deliver flow and packet analysis, including a centralized dashboard that offered complete visibility into the customer's network, application, and end-user environments.

Benefits

This end-to-end visibility enabled the tracking of infrastructure and application performance characteristics, allowing the agency to understand how the network was performing and make adjustments accordingly. By using analytics of the application traffic and coexistent behavior with the supporting cloud and networks, the agency was able to dramatically improve the end-user experiences.

More Points Of Access = More Points Of Risk.

Using Riverbed|Aternity end-to-end visibility solutions enabled this DoD customer to see across their network and proactively mitigate performance issues.

riverbed | Aternity

4 Pillars of a End-to-End Visibility Solution

The right visibility tool can help ensure network resiliency and security, while optimizing the digital experience, whether users are in the office, at home or on-the-go. When evaluating visibility solutions, look for these four core feature sets:

1

Actionable Insights

IT and security teams are constantly flooded with data from disparate systems; but data alone does not help make mission-critical decisions. The ideal visibility solution must provide full transparency for all packet, flow and device metrics for on-premises, cloud, multi-cloud and tactical edge environments. It should have the capability to leverage data feeds from existing disparate tools and deliver actionable insights to help teams prioritize action, while still providing the ability to recognize and understand application paths and dependencies.

2

End-to-End Attack Continuum Response

Organizations need visibility solutions that will analyze packet and flow data to detect security threats, including malware, blacklisted sites and distributed denial-of-service (DDoS) attacks. This becomes more critical in hybrid environments as the number of endpoints increases to support telework.

3

Artificial Intelligence (AI) and Machine Learning

Modern solutions must use AI and machine learning to become smarter about the network and user environment, and leverage analytics across domains to detect anomalies and patterns that indicate performance issues and security threats. These capabilities are critical to reduce the time to diagnose and resolve problems, while decreasing false alarms and downstream network events.

4

Deep Integration

In highly complex, distributed environments, modern visibility solutions should have tight integration within their product portfolios or families. They should also connect effectively with multiple cloud services, third-party software via open APIs and any existing tools—such as application performance management, logging and workflow products.

Learn how Riverbed|Aternity's end-to-end visibility solutions incorporates these core elements critical to tackling performance and security demands in today's hybrid environments.

riverbed | Aternity

Questions to Consider when Comparing End-to-End Visibility Solutions

What is required to achieve end-to-end visibility across distributed and dynamic network environments?

- ☐ Does the solution provide comprehensive visibility across on-premises, cloud, hybrid and multi-cloud environments?
- ☐ Can it capture all packet, flow, infrastructure, app, device and end-user metrics - all the time - so full-fidelity telemetry data is available when needed?
- ☐ Can the IT and Security teams quantify the user experience by using network data to measure performance and availability?
- ☐ Does the solution integrate end-user experience, application, network and infrastructure performance into a single dashboard?
- ☐ Does the solution provide role-based views for executive, business, and domain-specific use across all domains?
- ☐ Does it provide insights into device and interface health, configuration monitoring and path analysis?
- ☐ Can IT and security teams map network dependencies to automatically map applications to their underlying infrastructure?
- ☐ Does the solution use AI and machine learning to detect patterns and anomalies that indicate poor performance or security risks?
- ☐ Does the solution offer network insights to identify threats such as data exfiltration, brute force password cracking, blacklisted site access and DDoS attacks?
- ☐ Can the organization deploy the product where it wants: on-premises, private cloud, or public/ hybrid cloud?

riverbed | Aternity

Tips to Improve Network Resiliency and Security for a Mission-Ready Public Sector Workforce

Leverage end-to-end visibility solutions to meet the evolving needs of the hybrid workforce while adopting to zero trust security postures

1 | Tackle remote access and VPN issues:

With so many employees teleworking since the start of the pandemic, there is higher traffic and workload on most organizations' VPNs with all users trying to access the same Trusted Internet Connection (TIC). That makes it challenging to assure a positive user experience and anticipate issues. By bringing together flow, packet and device data, IT and security teams can better understand the performance of each VPN in real time and ensure that VPN concentrators can keep pace with throughput.

2 | Gain deep insight into remote user experience:

When many employees are teleworking, there is an increased load on critical operational apps in the cloud, making it tricky to meet service level targets. By monitoring all incoming requests that make up a page and then measuring the corresponding response times from servers, the IT team can monitor the user experience for transactions and identify bottlenecks, even for encrypted SSL/TLS traffic..

3 | Optimize bandwidth and QoS for new usage patterns:

By monitoring network use trends and patterns, an organization can adapt for capacity changes as employees shift between onsite and offsite work, either temporarily or permanently. Make sure to optimize bandwidth usage for new traffic flows and QoS tags for the most frequently used apps to ensure workforce productivity

4 | Remove security blind spots:

Cybercriminals stepped up their attacks following the pandemic's onset, and they will continue to try to take advantage of the new hybrid architectures in use by public sector organizations. To fight back, agencies can leverage network telemetry to strengthen security postures. By applying security analytics with full-fidelity flow and packet capture, security teams can detect threats, perform forensic analysis, identify and respond to threats caused by worms, brute force password cracking attempts, malware, and DDoS attacks.

5 | Prioritize mission-critical and collaborative applications:

To ensure adequate bandwidth for employees working from home or other remote locations, prioritize must-have apps for telework, such as Microsoft 365, Salesforce and Zoom, to ensure fast, reliable, and consistent performance. Set policies that account for mission criticality to make sure productivity doesn't suffer.

6 | Troubleshoot poor VoIP performance:

Mission-critical teleworkers depend on reliable and always-available communications to work effectively, whether they are in the office, at home or on the go. Monitor voice streams in real-time and detect VoIP quality problems by isolating the root cause of poor-quality flow allowing for quick remediation.

7 | Automatically identify shadow apps usage:

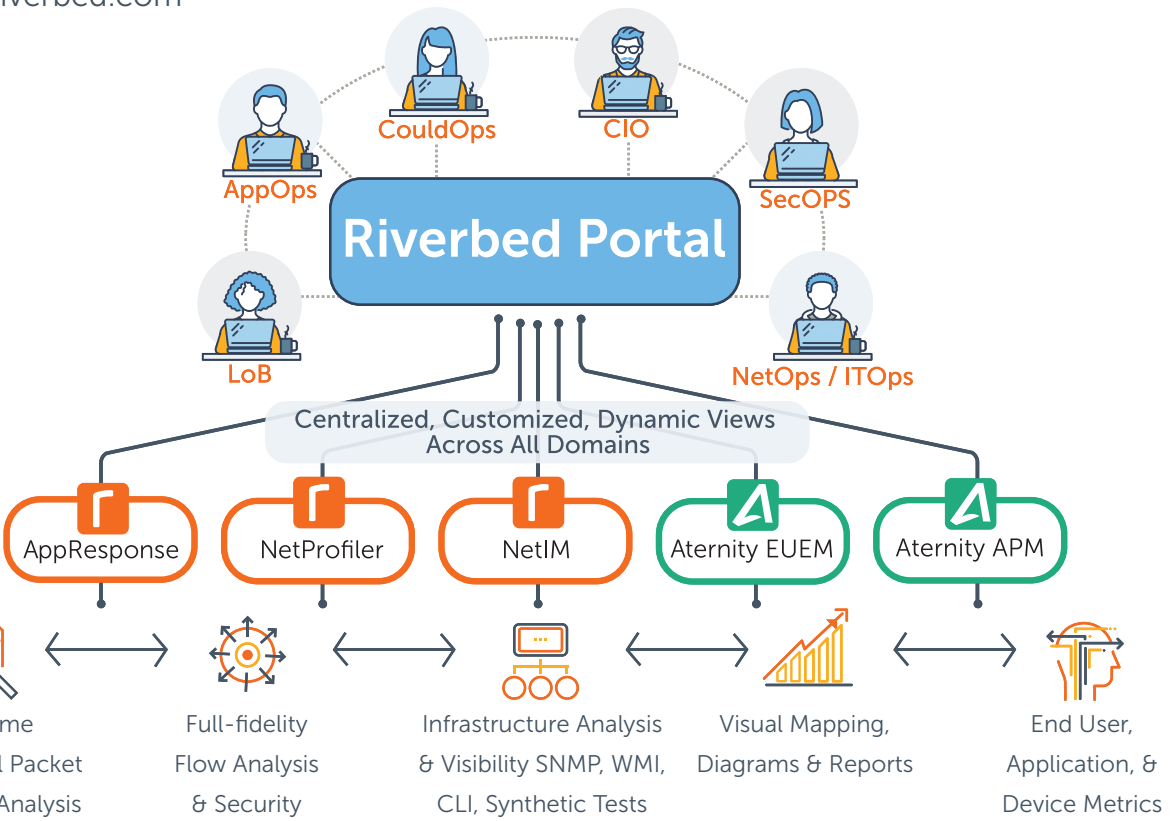
Shadow apps, such as Box and Dropbox, can store valuable, proprietary data outside of an organization's visibility and control. Use NPM data to monitor and detect use of such apps by workers to mitigate security risks.

riverbed | Aternity

End-to-End Visibility for a Mission-Ready Public Sector

Riverbed|Aternity End-to-End Visibility Solutions

End-to-end visibility solutions help organizations achieve visibility needed to improve the resiliency and security of the users, apps and networks to drive missions forward. Unlike disparate tools, Riverbed|Aternity combines cross-domain data—including all packet, flow, user and device metrics—with machine learning and advanced analytics to provide IT teams with real-time performance and security insights across any network environment. For a detailed look at Riverbed|Aternity's end-to-end visibility solutions visit www.riverbed.com



For more information on how Riverbed|Aternity maximizes visibility and performance for the networks, applications and end-users needed for mission success, please visit the Riverbed|Aternity Public Sector Solutions page.

riverbed | Aternity

SOURCES

1."The Continued Effects of COVID-19 on the Federal Contracting Industry and Your Customer" Market Connections, July 2020

2."U.S. Navy Issues Updated Guidance to Commanders On Adjusting Health Protection Conditions and Base Services During COVID-19 Pandemic" U.S. Navy, May 3, 2021

3.NTEU's Telework Survey," National Treasury Employee Union, April 2021

4.Evaluation of Access to Department of Defense Information Technology and Communications During the Coronavirus Disease-2019 Pandemic" DoD IG, April 2021

5."Building a Model Workplace with Expanded Telework and Work Flexibilities - Our First Steps" Thomas J Vilsack Memo to USDA employees, March, 2021

6.Network Transformation Summit, Riverbed Technology and FedScoop, May 2021

7.2020 Federal Viewpoint Survey," Office of Personnel Management, June 2021

8.Testimony of Gen. Paul Nakasone, Senate Armed Services Committee, March 2021

riverbed | Aternity

About Riverbed|Aternity

Riverbed|Aternity enables organizations to maximize visibility and performance across networks, applications and end-user devices, so they can fully capitalize on their cloud and digital investments. Riverbed|Aternity solutions enable organizations to visualize, optimize, remediate and accelerate the performance of any network for any application, while supporting business objectives to mitigate cyber security risk and enhance the digital experience for all end-users. The Company offers two best-in-class product lines: end-to-end visibility – including NPM, APM and EUEM – that delivers actionable insights; and network and acceleration solutions, including application acceleration (SaaS, client and cloud acceleration), WAN optimization, and enterprise-grade SD-WAN. Riverbed|Aternity's 30,000+ customers include 95% of the Fortune 100.Learn more at riverbed.com