CYBERSECURITY

Scaling up the Nation's Armed Forces in a Zero Trust World

A how-to guide on improving the nation's cybersecurity posture by achieving complete observability.

RAVENTEK | riverbed

Improving the Nation's Cybersecurity

On May 12, 2021, the United States Presidential Administration issued Executive Order (EO) on "Improving the Nation's Cybersecurity (14028)" to bolster the United States' security poster in the digital age. To modernize federal government cybersecurity as mandated, the EO requires for all federal agencies to develop a plan to implement a zero trust architecture. Part of this fulfillment puts the onus on the National Institute of Standards and Technology (NIST) to publish new standards and guidelines to enhance software supply chain security, including defining critical software and its required security measures, criteria to evaluate software security and practices to be strictly followed by all federal agencies.

In proactive alignment and compliance with the EO, branches of the United States Department of Defense (DoD) have released plans to position itself advantageously against rapidly paced technological advances in space, cyber, information, and electronic warfare capabilities—resulting in the most expansive modernization program for the department in forty years. A modernized unified network centered around supporting Multi-Domain Operations (MDO) is a critical component for secure and global operations. The success of a modernized network plan is its foundation built on the zero trust framework.

Given it's sizable, complex, and multi-tenant organizational structure, designing for and maintaining a large-scale unified network is generally constrained for branches of the DoD. To accomplish successful modernization, the selection and use of the right data and technology allows for effective implementation of a consistent enterprise-wide unified network architecture. In a modern enterprise, uniformed top-level policies and governance on how data is securely created, transmitted and stored is the driving force behind any modernization approach. Architectures that are too restrictive decrease efficiency while architectures that are too unrestrictive introduce risk and vulnerability.

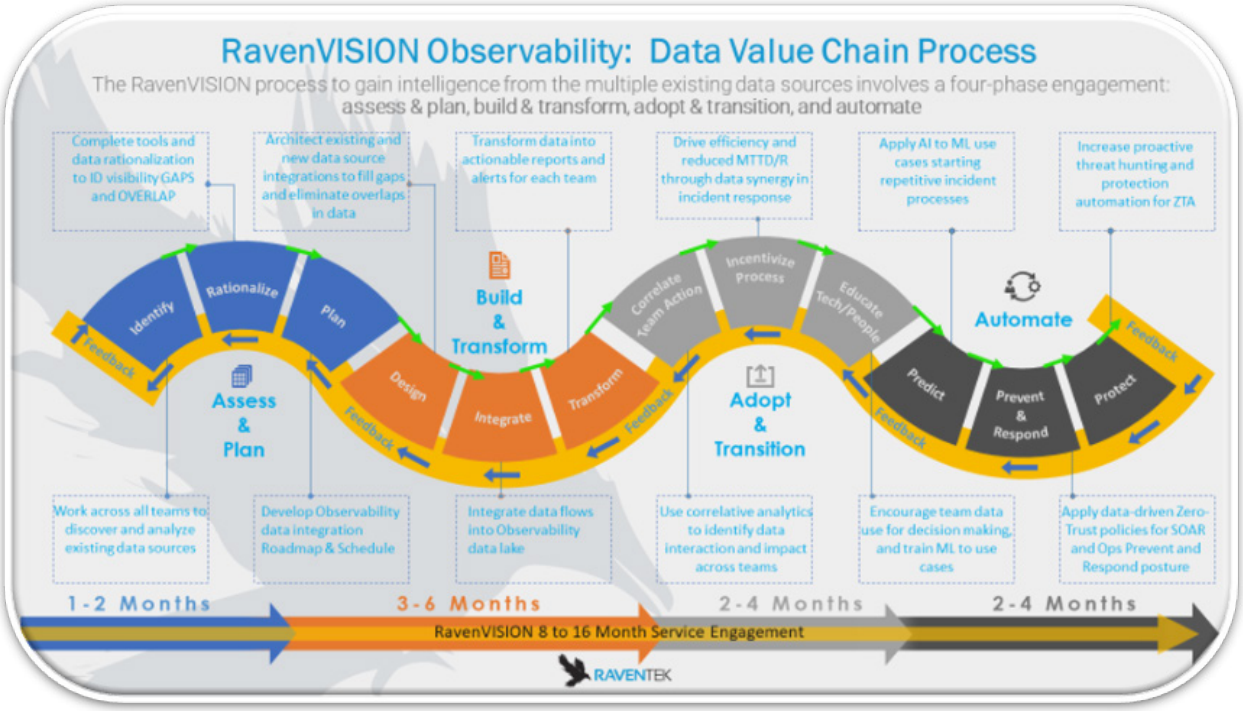
Establishing a baseline of the overall data architecture within an enterprise network, and then using that data to drive the modernized design and integration is paramount. This methodology allows for organic organizational change to ride inside the vehicle of top-level policy and governance which is driven by data centric, dynamic decisions. Enterprise agility, which allows for change to occur rapidly, is critical to the effectiveness of a new modernized organization. To achieve this, a streamlined method to evaluate and approve changes is required.

Data comes from in the form of: logs, netflow, transactions, packets, conversations, traps and events. From disciplines like: Security, APM, NPM, ITIM, EUE.

The key to being able to realize required changes comes from many things but ultimately technology teams need to have a system that can quickly provide analytical verification and validation of changes. In turn, this means that the IT infrastructure needs to be instrumented in a way that all nodes provide their inputs to a common data decision driven system.

RavenVISION

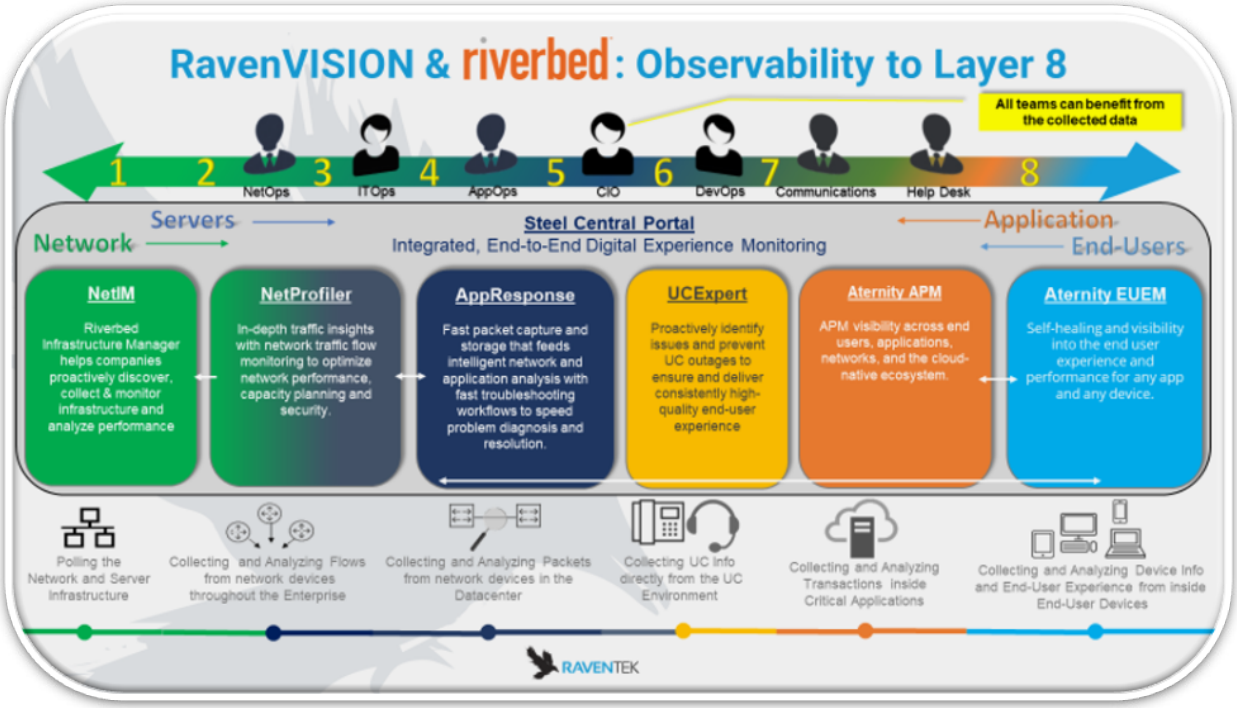
The first steps in a modernization strategy should be to analyze the organization's existing infrastructure to understand its current visibility tools across the ITN and the IEN. For this purpose, RavenTek has designed the RavenVISION framework to help identify visibility gaps as well as weed through duplicate and overlapping technologies.



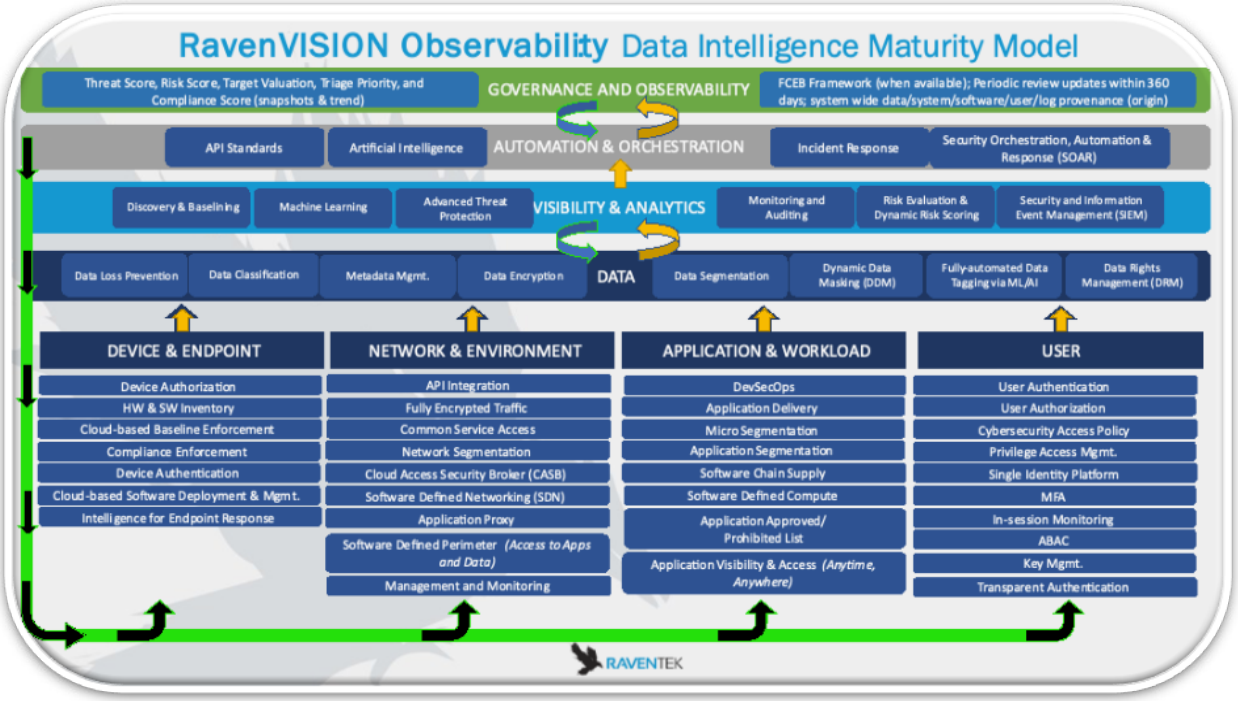
RavenVISION is an integrated service offering which encompasses the Visibility Integration of Security, Infrastructure, Operations and Network data and is designed to focus on the end-state mission objective of a single context observability command center. To accomplish this mission, RavenTek accesses the current state of the enterprise by working closely with traditionally siloed IT teams to gain a holistic view of the organization's data. RavenVISION is intended to help organizations modernization successfully and resiliently through complete observability. Modern AI/ML automation is a critical component in the RavenVISION framework which supports a zero trust architecture. Observability not only exposes where operations and processes may be vulnerable or weak, but also verifies those that are stable. Resolving visibility gaps for complete observability should be accomplished before making major modernization decisions or changes to any enterprise.

Another key component of the RavenVISION framework is Riverbed's suite of visibility tools which provide critical data to make real-time intelligent decisions. Riverbed's solutions instrument on-prem and cloud-based environments and provides a common portal to visualize the entire enterprise. Utilizing Riverbed's suite of products as well as the open Rest API's, enterprises are able to gain observable data from layer 1 to layer 8. The RavenVISION framework relies, in part, on a modified OSI and uses layer 8 to represent the true end-user in any communication flow.

RavenVISION and Riverbed



In recognizing the need for interoperability, RavenTek finds value in Riverbed's ability to integrate with other products to provide for the unique needs of individual enterprises. The top of RavenVISION's data intelligence maturity model demonstrates how all data can be fed to inform the dynamic policy and governance that is needed in a successful and sustainable zero trust architecture for not just network but also the entire enterprise IT environment.

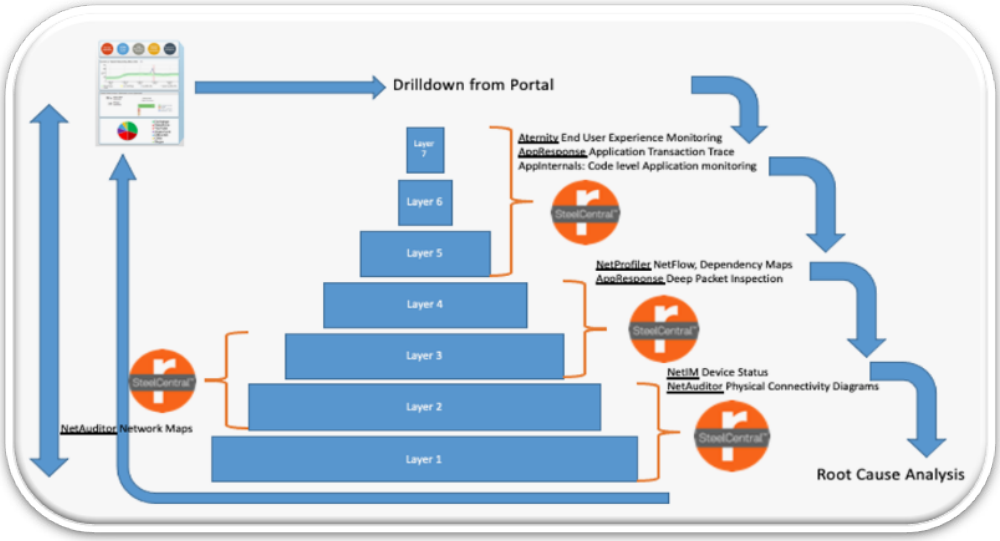


Complete Observability

Getting the big picture

One of the primary tenants of zero trust is to monitor everything - visibility is paramount in meeting this requirement. This visibility is needed throughout the lifecycle of any such undertaking. It both identifies and validates critical design decisions.

Riverbed's advanced visibility solutions provide comprehensive network intelligence from telemetry collected throughout a complex working environment. Telemetry is collected from all layers of the OSI model to provide a comprehensive unified view into how networks and applications are preforming in past, present, and future. The telemetry provides data on network performance (NPM), application performance (APM), and end user experience (EUEM). Each operator can have a unified view of the networks and applications for the missions they are responsible for supporting.



Having such a broad collection of telemetry allows RavenVISION the ability to create an accurate full fidelity model of both the physical and logical network. Traffic flow and routing are also modeled.

Simulations can be run against the model to provide break/fix analysis of any change to the network or application that is being proposed. Using the simulation environment provides for the ability to predict how the network or application will perform in the future without the cost of time and equipment to setup an expensive lab environment.

Riverbed NetProfiler provides an excellent starting point for analysis of your network. It can receive flows from your existing infrastructure or dedicated probes can be deployed. These probes are able to leverage existing packet broker networks to provide a more in-depth analysis with packet capture abilities as well. NetProfiler allows for useful visualizations of flow data to provide insight into the network's current health status.

Complete Observability

Getting the big picture

The Advanced Security Module utilizes AI/ML to provide advanced behavioral analysis of your networks' traffic to identify potential security vulnerabilities and events that could lead to breaches. It can also give detailed dependency maps that show node-by-node what is talking to what so there's no guessing when securing assets or validating the effects of a change to an environment. This is invaluable when verifying that and organization's zero trust efforts are yielding the desired results independent of the it's tools visibility.

Riverbed SteelHeads provide WAN optimization but also can enrich NetFlow that is forwarded to a NetProfiler for higher fidelity flow data then standard NetFlow.

Riverbed AppResponse (NPM/APM) provides deep packet inspection and packet capture abilities. It also can forward enriched NetFlow data to a NetProfiler as well.

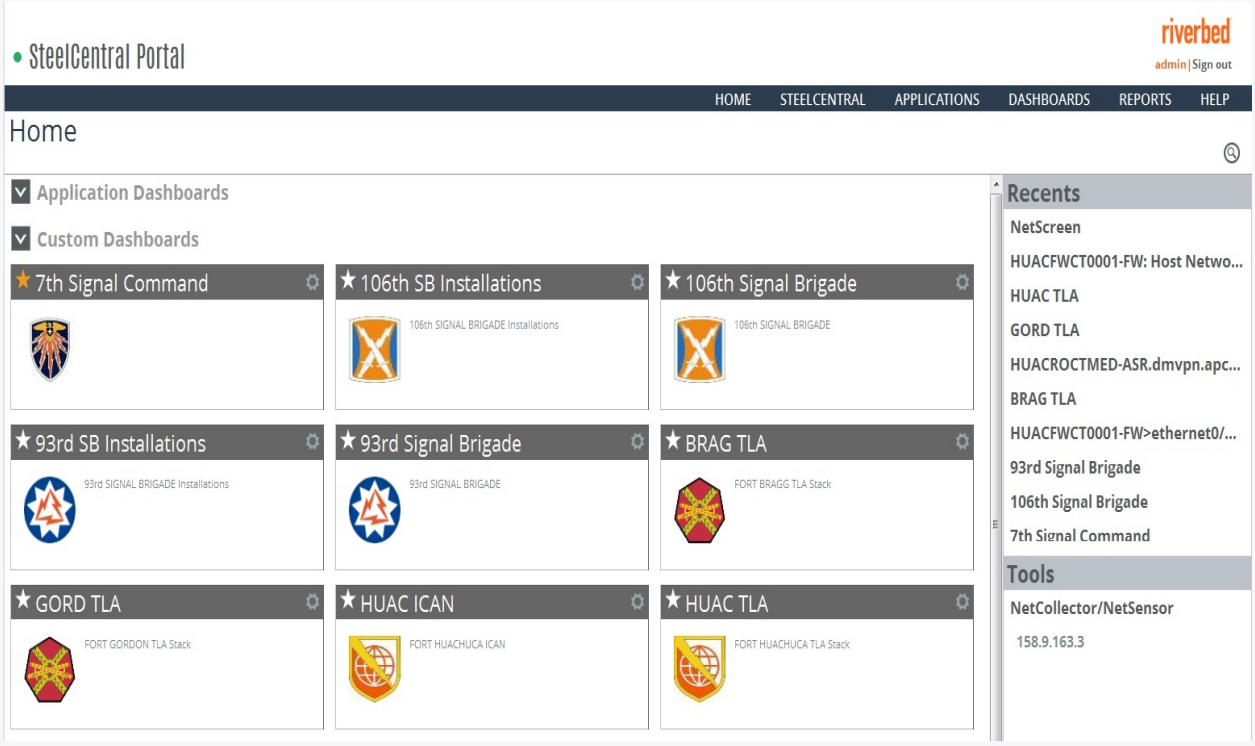
Together these products offer a rich and robust visualization of the enterprise independent of any other zero trust tools which allows for an independent way to validate changes. They provide for the necessary data to analyze an organization's current environment and plan for the next-generation infrastructure.

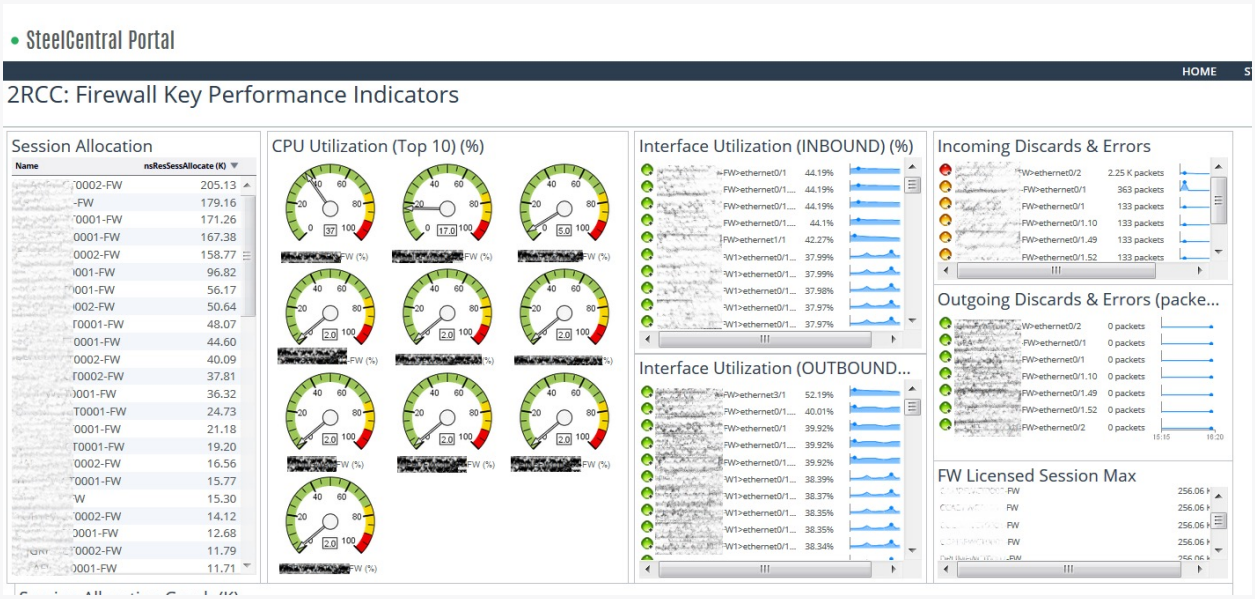
Types of telemetry collected:

- Flow data from every network device capable of exporting xFlow
- Enhanced flow data from Riverbed packet capture and WAN optimization devices (includes performance data)
- Packet data including deep packet inspection to identify applications
- SNMP data from any device capable of being polled
- WMI data from Windows devices
- Configuration files
- CLI data (ie. Show commands from routers and switches)
- Synthetic transaction data
- Syslog data
- Generic data exported from devices that are incapable of being polled by traditional means
- Application transaction data from application and database servers
- Java and .NET application code performance
- EUEM data from the actual device accessing the application
- End user device information (including hardware data and installed software)

Drilling Down

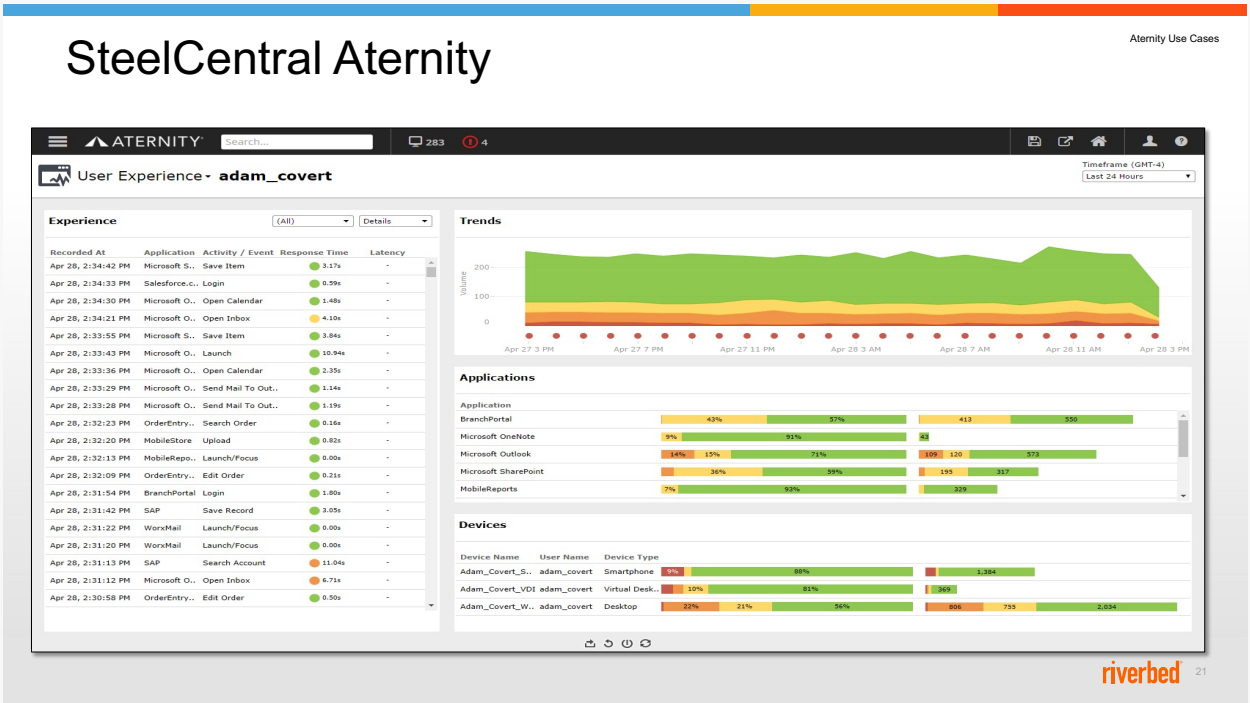
The Riverbed Aternity (EUE) solution provides deep details on an organization's end-user systems. It is extremely useful for identifying performance issues that may be the results of changes made during a zero trust lockdown of end systems. It has the ability to compare before and after views for visualizing the positive or negative effects of changes.





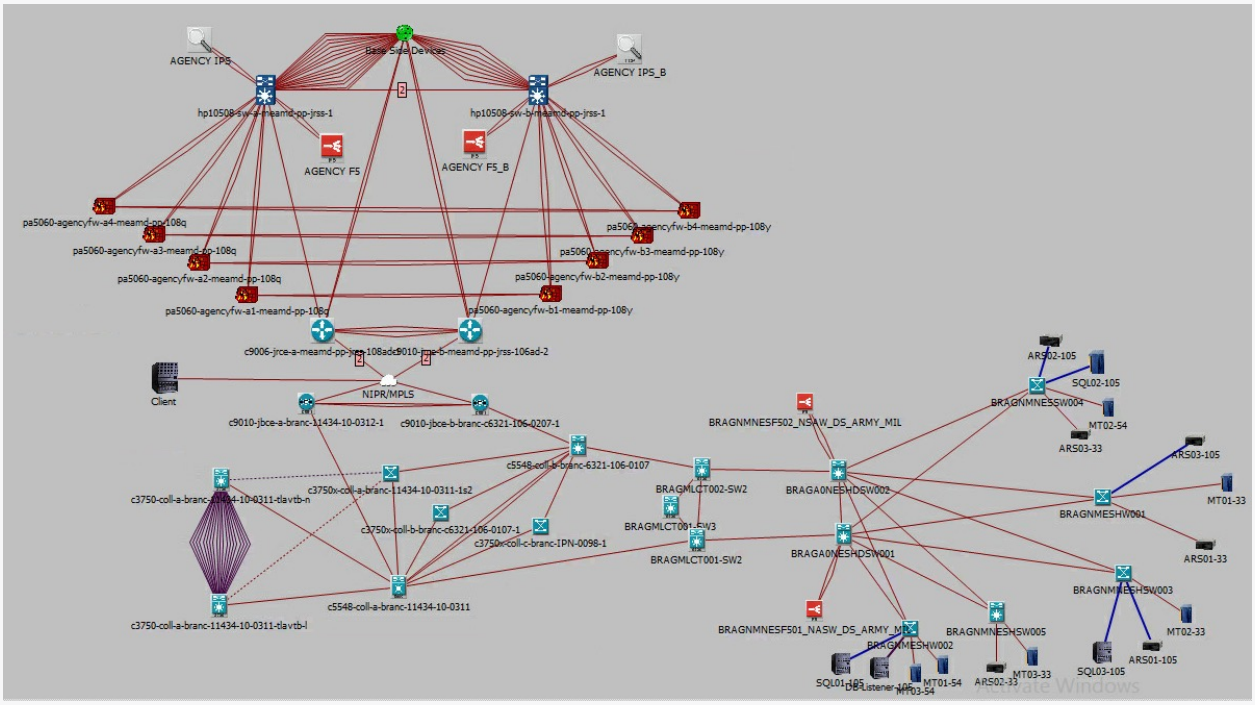
Drilling Down

Riverbed's advanced network intelligence has a proven track record of providing unified views into NPM, APM, and EUEM from the tactical edge to all levels of command and control. Dashboards can be created for each operator based on technical ability, mission, and area of responsibility, giving each operator their own unique view into the data collected. Drill down to the underlying tools collecting the data can be accomplished for more extensive troubleshooting.



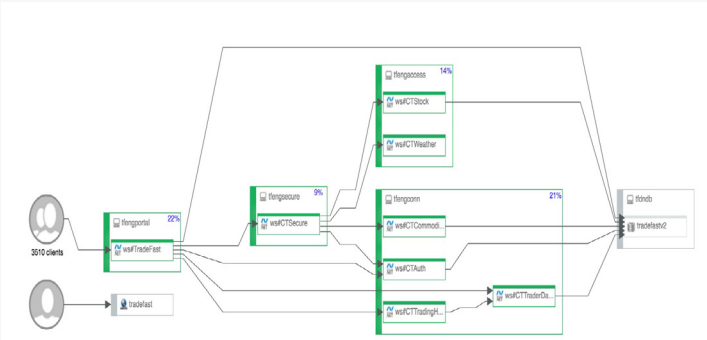
Riverbed NetIM (ITIM) provides deep details of an organization's systems via SNMP, CLI or WMI. With additional modules this platform can provide configuration management, security compliance and network modeling capabilities that are critical to verifying and maintaining a zero trust compliant enterprise.

Drilling Down



The above diagrams show the model of a network with application flows being simulated to complete a survivability analysis before an application upgrade. The top diagram includes the JRSS stack. This capability is critical before any changes or migrations are performed and assures there will be no impact once changes are implemented.

Riverbed AppInternals allows an organization to monitor their applications down to lines of code and transactions. It can show unusual behavior to help identify potential problems with applications or potential security breaches. Organizations can receive useful information to help understand application behavior when implementing a micro-segmentation solution for zero trust.



Transaction path through the classes and methods of the actual application code for Java and .NET applications.

Where To Go From Here

By utilizing RavenTek and Riverbed, branches of the DoD can access critical metrics and deep visibility into their Network Modernization project. Riverbed provides the superior tools. RavenTek provides superior integration and a framework for success through RavenVISION.

Monitoring and collecting data is just the beginning, organizations must be able to understand what it means and to be able to turn it into a resource that yields results in all theaters of operation.

The RavenVISION solution allows for the technology behind Riverbed's suite of tools as well as all other existing tools to be utilized in an integrated manner. Breaking down data silos and using data intelligence to drive decisions will allow organizations technology and teams to adapt, overcome, and modernize organically; from top down policy and governance to the bottom up data.

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