SIMPLE STEPS TO IMPROVE FEDERAL CYBERSECURITY SCORES AND SECURE THE NATION'S DATA

U.S. Public Sector

riverbed®

U.S. Public Sector

Improve Federal Cybersecurity Scores with Network Visibility

The Nation's Data Remains at Risk

In August 2021, the U.S. Senate Homeland Security and Government Affairs Committee released its report “Federal Cybersecurity: America’s Data Still at Risk,” outlining significant shortcomings in federal agencies’ compliance with cybersecurity standards and regulations to protect the nation’s data from cyberattacks.

The IT security maturity of eight federal agencies was reviewed in depth, and received an overall rating of “C-“ based on the agencies displaying significant cybersecurity weaknesses and vulnerabilities

30,819 CONFIRMED FEDERAL INFORMATION SECURITY INCIDENTS IN 2020

U.S. Government Cybersecurity Report Card

USDA	**C**	HHS	**C**	NASA	**D**	SSA	**D**
DOC	**D**	GSA	**B**	NSF	**B**	DOT	**D**
ED	**D**	HUD	**C**	NRC	**B**	Treasury	**C**
DOE	**C**	DII	**C**	OPM	**D**	USAID	**B**
EPA	**C**	DOJ	**C**	SBA	**C**	VA	**D**
DHS	**B**	DOL	**C**	DOS	**D**	OVERALL	**C-**

Figure 1. Senate Homeland Security Government Affairs Committee Federal Cybersecurity Report Card

While the Senate HSGAC report found shortcomings with the agencies’ compliance efforts, two areas outlined as weaknesses can be mitigated relatively easily by leveraging Riverbed’s network visibility solutions NetIM, Aternity EUEM, and NetAuditor. With these solutions, IT teams can achieve end-to-end visibility across the entire network environment, from the infrastructure to the remote user, providing insights and actionable intelligence to eliminate vulnerabilities and strengthen network security.

Key Agency Cybersecurity Weaknesses Reported:

1. Agencies used legacy systems or applications that are no longer supported by vendors with regular security updates

2. Agencies failed to maintain accurate and comprehensive IT asset inventories

riverbed

U.S. Public Sector

Two Simple Steps to Improve Cybersecurity Postures

STEP 1:

Maintain Accurate and Complete IT Inventory

Federal agency IT infrastructure is complex, hybrid, dispersed, difficult to maintain,and susceptible to technology refresh lapses that can create vulnerabilities. It’s critical to identify and have visibility into every device on the network as well as any IT asset such as laptops, workstations, and others that can access a network.

Riverbed NetIM provides complete visibility to an organization’s underlying network infrastructure, allowing IT teams to discover, model, monitor, and troubleshoot infrastructure performance and security issues. By identifying infrastructure elements such as routers, switches and servers that are underperforming, misconfigured, or nearing the end of life, NetIM ensures that the sprawling infrastructure environment doesn’t have blind spots that can be exploited by threat actors.

STEP 2:

Identify and Remove Unsupported Systems and Apps

Federal agency networks are dynamic and can easily become unwieldy, difficult to manage, and susceptible to using systems and apps past their supported lifetime. It's critical for agencies to know what and how their network systems and apps are being used, from the infrastructure all the way to the end-user device to ensure that unpatched, out-of-date systems and apps can’t be hacked. Riverbed | Aternity EUEM offers public sector organizations the visibility they need to gain crucial insights on activities at remote user endpoints by monitoring application, device performance, and end user details. By creating baselines on how users interact with applications, networks, data, and traffic, down to the minute, unusual activities can be identified, unsupported apps and devices refreshed or removed strengthening agencies' security postures.

You Can’t Secure What You Can’t See

Having data without visibility hinders the ability to act. If organizations can’t see the infrastructure, devices, assets, and activities on their networks, and run analytics against them, they’re flying blind. To truly connect the dots and improve cybersecurity postures, agencies must be able to take action with their network data. Riverbed NetAuditor is a network configuration management solution that dynamically creates and maintains infrastructure diagrams and reports, allowing agencies to visually see what’s happening on their network. The solution discovers network elements and visually presents them in an easy-to-understand interface through a unified portal. In addition, NetAuditor ensures network integrity, security, and policy compliance by performing automated network-wide audits and alerting when out of compliance.

About Riverbed

Riverbed enables organizations to maximize performance and visibility for networks and applications, so they can overcome complexity and fully capitalize on their digital and cloud investments. The Riverbed Network and Application Performance Platform enables organizations to visualize, optimize, remediate and accelerate the performance of any network for any application, and helps to identify and mitigate cybersecurity threats. The platform addresses performance and visibility holistically with best-in-class WAN optimization, unified network performance management (NPM), application acceleration (including Microsoft 365, SaaS, client and cloud acceleration), and enterprise-grade SD-WAN. Riverbed’s 30,000+ customers include 99% of the Fortune 100. Learn more at riverbed.com.

riverbed