

Field-Ready Packet Visibility for Federal Red Teams

Portable packet capture and full-fidelity visibility for secure, disconnected environments

Overview

Federal Red Teams perform penetration testing, adversarial simulations, insider threat scenarios, segmentation validation and physical access assessments in facilities that restrict or prohibit connection to centralized security tools. These activities require packet level evidence to validate exploitation paths, understand communication behaviors, and document findings with precision. Traditional observability platforms depend on remote infrastructure and cloud-connected workflows that cannot operate in SCIFs, diplomatic facilities or disconnected enclaves. Riverbed provides field-ready packet visibility that runs entirely within the secure boundary, enabling Red Teams to leverage full fidelity traffic to deliver defensible, evidence-based assessment results without reliance on external connectivity.

Purpose Built for Red Team Operations

Red, Blue and Purple Teams rely on detailed packet visibility to confirm exploitation attempts, assess lateral movement potential, validate segmentation controls and produce accurate findings for follow up action. Riverbed delivers this visibility directly at the point of assessment, enabling teams to reconstruct activity with precision and correlate packets and flows for clearer interpretation of results. By operating fully inside secure or disconnected environments, the solution supports consistent, evidence-based reporting without dependence on centralized tools.

Portable, Hardware-Agnostic and Easy to Deploy

Riverbed's packet visibility capability is designed for field assessments in restricted federal environments. Teams can deploy the solution in minutes once the portable system is configured, running on hardware of their choosing or as a compact physical or virtual node that can move between facilities. This flexibility ensures consistent visibility across SCIFs, diplomatic facilities, temporary testing areas, and fully disconnected sites. All packet data remains local to the facility, supporting controlled access and strict evidence handling requirements.

Comprehensive Packet Capture for Precise Validation

Basic packet capture tools often struggle with sustained data rates, diverse communication patterns, and the volume of traffic present during complex assessments. Riverbed eliminates these limitations. With NPM+, AppResponse and NetProfiler, teams can capture full fidelity packets at performance levels beyond what laptop-based tools typically support. Packet and flow correlation enable detailed reconstruction of exploitation paths, communication mapping, timing analysis, and Zero Trust segmentation validation. This gives Red Teams the depth of detail needed to substantiate assessment findings with confidence.

Supports Civilian Federal Assessment Environments

Riverbed aligns directly with the assessment requirements of Department of Justice and Department of State Diplomatic Security environments. Activities in these settings often occur inside secure rooms, restricted enclaves or controlled diplomatic facilities where external connectivity is limited or not permitted. Riverbed supports Red Team assessments including insider threat simulation, controlled exploitation, segmentation testing, physical access evaluation, security posture evaluation and traffic validation while ensuring all packet evidence remains within the approved boundary.

Why Riverbed for Red Team Assessments

Riverbed delivers the packet level visibility federal Red Teams need to perform accurate, repeatable assessments in secure or disconnected environments. The combination of portable deployment, hardware flexibility and comprehensive packet capture ensures teams can validate exploitation paths, confirm segmentation behavior and document findings with clarity. All packet evidence remains contained within the facility, supporting controlled access and strict investigative requirements.

Equip Your Red Team with Full Packet Visibility

Give Red Teams the ability to capture and analyze complete packet evidence wherever assessments take place. Riverbed provides the depth, consistency and local control required for high quality adversarial testing in civilian federal environments, ensuring teams can produce reliable results even when centralized tools are unavailable.



About Riverbed

Riverbed, the leader in AIOps for observability, helps organizations optimize their user's experiences by leveraging AI automation for the prevention, identification, and resolution of IT issues. With over 20 years of experience in data collection and AI and machine learning, Riverbed's open and AI-powered observability platform and solutions optimize digital experiences and greatly improves IT efficiency. Riverbed also offers industry-leading Acceleration solutions that provide fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of market-leading customers globally – including 95% of the FORTUNE 100 – we are empowering next-generation digital experiences. Learn more at riverbed.com.