riverbed

DATA SHEET

Alluvio NetProfiler

Hybrid flow monitoring and security analysis

Business Challenge

"The network is slow." If you're like most netops managers, you probably hear this complaint too often. To really understand what's occurring on your network, you need an end-to-end view of the hybrid network into performance and security issues.

Alluvio NetProfiler

Riverbed® NetProfiler provides network flow analytics that you can use to quickly diagnose network issues and identify security threats before end users ever know there's a problem. Alluvio NetProfiler combines network flow data with packet-based flow metrics to provide proactive monitoring, analysis, and reporting. Use NetProfiler to answer questions such as how much traffic do I have, who is using it, where is it going, and how is it prioritized?

Behavioral Analytics

IT organizations need to understand how degraded performance affects network and application performance, and ultimately business performance. NetProfiler uses behavioral analytics for proactive monitoring. It baselines normal performance and alerts on changes as soon as they occur—typically before users are even aware that performance is degrading.

Dependency Mapping

NetProfiler automates the mapping of application transactions to their underlying infrastructure so that application definitions and interdependencies are accurate. This helps you create service maps that accelerate the identification of issues across complex application ecosystems, and plan for data center consolidation, cloud, disaster recovery, or virtualization initiatives.

Ubiquitous Visibility

Deploy anywhere and everywhere you need for on-premise, virtual, or cloud visibility. NetProfiler is designed to meet your hybrid and cloud needs, supporting both Azure NSG Flow Logs and AWS VPC Flow Logs.

Advanced Security Module

NetProfiler Advanced Security Module optional security analytics software. It leverages flow data to detect, investigate, and mitigate advance threats. NetProfiler Advanced Security Module is especially suited for threat hunting, incident response and network forensics.

For more information on Alluvio NetProfiler, please visit: riverbed.com/netprofiler. For Advanced Security Module, go to, riverbed.com/network-security.

Integrations

Alluvio NetProfiler integrates with several other Riverbed® NPM solutions to enrich your every day IT operations functions.

These one-click integrations include:

- **Riverbed® AppResponse and AppResponse Cloud:** network forensics and networked application analysis
- **Riverbed® NetIM:** infrastructure management with network path analysis
- **Riverbed® SteelHead™:** WAN optimization and functions as remote data source for NetProfiler
- **Riverbed® Portal:** single source of truth for network, application, infrastructure performance, and end-user experience monitoring

"Riverbed NPM has reduced the time it takes us to identify network slowdowns and application performance issues. It saves my network team a lot of time."

Operations Manager,
Small Business Consume Products Company

"The reporting capabilities of Alluvio NetProfiler are awesome. It can generate any type of report I need!"

Network Administrator,
Large Enterprise Electronics Company

Key Benefits

Improve cloud and hybrid network visibility and performance

Speed problem identification and resolution

Mitigate cyber-security risks

NetProfiler Home Screen

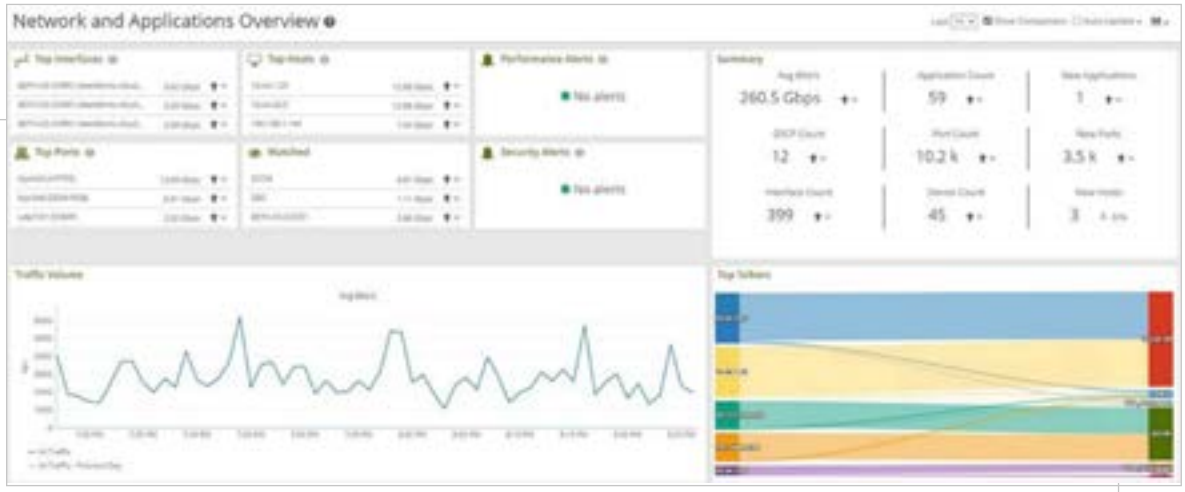

Figure 1: Personizable to each user, the NetProfiler Home Screen offers an at-a-glance summary of the network and how it's changed; recent alerts; To Talkers Sankey; overall traffic charts, and a watch list so you can see what's important to you.

Key Features

Application Recognition and Monitoring

NetProfiler offers three ways to create a custom application definition. You can map:

- Hosts, host groups, protocols, ports to an application name
- Auto-recognized applications to an application name
- URLs to an application name

Deep packet inspection of application traffic from Riverbed® AppResponse, Riverbed® NetShark and SteelHead for easy viewing and analysis in the NetProfiler dashboard to help you quickly and accurately distinguish business-critical from recreational applications that are running across your network including the optimized WAN.

Anomaly Detection

Uses baseline statistics and proactive monitoring to trigger an alert once a deviation is detected, without prior knowledge of specific applications, path dependencies, and number of users.

SD-WAN Visibility

Ensure the success of your SteelConnect SD-WAN environment by validating policies are working as expected, troubleshooting problems quickly, and enabling better planning.

Discovery and Dependency Mapping

- Includes a discovery wizard that creates application dashboards to automate the process of mapping transactions to their underlying infrastructure so that application definitions and interdependencies are accurate– including discovering through F5, Riverbed® SteelApp™ Traffic Manager and other application delivery controllers (ADCs).
- Creates service maps for accelerating troubleshooting across complex application ecosystems, and planning for data center consolidation or cloud, disaster recovery, and virtualization initiatives.

WAN Optimization Analysis

- Robust analysis of optimized Riverbed SteelHead and Interceptor environments enable you to easily plan your optimization deployments, assess the impact, and quantify benefits.
- Cost-effective troubleshooting of branch issues using a single product for visibility, control and optimization.
- Centralized reporting and monitoring of inbound and outbound quality of service (QoS) site and classes.
- Rich application monitoring of 2000+ default applications and custom-defined apps.

Streamlined Workflows

One-click dashboard creation creates NetOps-centric, application-specific, SteelHead WAN optimization-specific, and VoIP-related dashboards that quickly surface relevant data and streamline troubleshooting workflows.

Home Screen

Offers at-a-glance summary of key network and application KPIs and how they've changed; recent performance and security alert lists; Top Talkers sankey diagram; overall traffic, cloud performance; and watch list so you can monitor what's important to you.

Service Monitoring

- Monitor all network and infrastructure components involved in delivering an application service such as users, Web servers, load balancers, application servers, authentication and DNS servers, databases, and the links between them.
- Advanced analytics changes in performance, providing proactive notification of brewing issues.
- Service dashboards provide a quick view into the end-to-end health of a business service that is visually shown by red-yellow-green health status indicators.
- Guided drill down reveals details of the most critical applications and essential data for fast troubleshooting.

Server Virtualization and VMware NSX SDN

NSX-aware IPFIX format enables Riverbed NPM products to provide detailed information about what NSX virtual overlay networks are running on the physical network, what applications are involved, and which hosts and virtual tunnel endpoints are generating the traffic.

Cloud Visibility

NetProfiler is deployable in:

- AWS
- AWS GovCloud West
- Azure
- Azure Government (non-DoD, no Iowa)

Cloud Flow Telemetry

The following flow telementry can generate and send flow for the cloud to NetProfiler in the cloud or on-prem:

- AppResponse Cloud
- AWS VPC Flow Logs
- Azure NSG Flow Logs
- Azure Government (non-DoD, no Iowa)

Advanced Security Module

Optional software module that adds the following cyber security features:

Distributed Denial of Service (DDoS) Detection

- Accurately detect volumetric, protocol and application-type DDoS attacks as soon as 10 seconds
- Act immediately to surgically redirect traffic to A10 TPS mitigation or Verisign CloudSign cloud scrubbing centers

Security Analytics

Understand changing patterns of behavior in your network that indicate security threats:

- **Suspicious connection:** when two hosts that do not normally communicate start talking
- **Worm:** a pattern of scanning among hosts, where systems previously scanned suddenly become scanners themselves. Identification of patient zero, infected hosts, and means of propagation are reported
- **New host:** a host that has not been previously identified has sent enough traffic to be regarded as having joined the network
- **New service:** a host or an automatic host group is providing or using a service over a new port
- **Host scan:** a series of hosts is being interrogated on the same port
- **Port scan:** a host or series of hosts is being interrogated across a range of ports
- **Bandwidth surge:** a significant increase in traffic that conforms to the characteristics of a DoS or DDoS attack

Cyber Threat Hunting

NetProfiler captures and stores all flow, so you have full-fidelity forensic analysis for threat hunting. Pivot and drill down to follow any lead and the data will always be there.

Incident Response/Forensics

Have the data necessary to recover from a cyber incident with speed and precision to minimize business interruption.

Learn More

For more information about Alluvio NetProfiler specifications, please visit riverbed.com/NPM.

riverbed

About Riverbed

Riverbed is the only company with the collective richness of telemetry from network to app to end user, that illuminates and then accelerates every interaction, so organizations can deliver a seamless digital experience and drive enterprise performance. Riverbed offers two industry-leading portfolios: Alluvio by Riverbed, a differentiated Unified Observability portfolio that unifies data, insights, and actions across IT, so customers can deliver seamless, secure digital experiences; and Riverbed Acceleration, providing fast, agile, secure acceleration of any app, over any network, to users anywhere. Together with our thousands of partners, and market-leading customers globally – including 95% of the FORTUNE 100 –, we empower every click, every digital experience. Riverbed. Empower the Experience. Learn more at riverbed.com.