riverbed

Data Sheet

SteelCentral NetProfiler

Enterprise-wide network flow and security analytics.

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.

Riverbed SteelCentral NetProfiler

Riverbed® SteelCentral™ NetProfiler provides network flow analytics that you can use to quickly view network performance and identify security threats to troubleshoot issues before your end users ever know there's a problem. SteelCentral 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 the end user, 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.

Hybrid Visibility

In addition to monitoring your enterprise network, NetProfiler provides insight into cloud environments, such as AWS. It answers those cloud-specific questions, such as what resources are you using, who's using it, are you being efficient with your cloud resources, are you incurring unknow costs, and how can you fix problems?

Advanced Security Module

The Advanced Security Module is optional software that leverages flow data for cyber intelligence. It provides essential visibility and forensics for threat detection, investigation, and mitigation into a broad range of advanced threats. The Advanced Security Module adds threat intelligence, DDoS detection, security analytics / forensics, and threat hunting to NetProfiler.

Learn more about the Riverbed SteelCentral NetProfiler at: riverbed.com/netprofiler.

Integrations

SteelCentral NetProfiler integrates with several other SteelCentral solutions to enrich your every day IT operations functions.

These one-click integrations include:

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

"SteelCentral 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 SteelCentral NetProfiler are awesome. It can generate any type of report I need!"

Network Administrator,
Large Enterprise Electronics Company

Key Benefits

- Improve hybrid network visibility and performance
- Speed problem identification and resolution
- Mitigate cyber-security risks

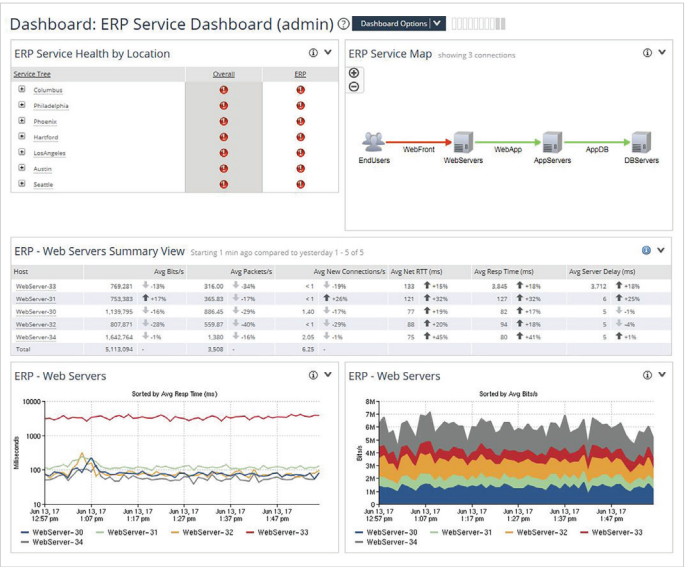

Figure 1

NetProfiler dashboards include everything you need to know from the highest level to the most granular detail with one-click drilldown for root cause and problem isolation and deep application visibility.

Key Features

Traffic Analysis

- NetProfiler captures full-resolution network data—flow records (NetFlow, sFlow, IPFIX, etc.), and performance metrics—across all internal and cloud network paths

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 SteelCentral AppResponse, SteelCentral 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
- Requires SteelCentral Insights for SteelConnect

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 WAN 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 SteelHead quality of service (QoS) site and classes
- Rich application visibility/monitoring through deep packet inspection (DPI)

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

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

NetProfiler 10.10 is IPv6 and USGv6 certified, and can support both IPv6 and IPv4 addresses simultaneously.

Server Virtualization and VMware NSX SDN

- NSX-aware IPFIX format enables SteelCentral 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

- Supports AWS
- Hybrid cloud and cloud-specific reporting
  - AWS Information
  - AWS Billable Data Transfer

Advanced Security Module

Optional software module that adds the following cyber security features:

Threat Intelligence

- Blacklists alert on known IP addresses, CIDRs, etc. that have been previously determined to be associated with malicious activity
- Threat feeds are analyst-generated information about potential threats. Threat feeds let you read more and investigate your network

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

Product Models

SteelCentral NetProfiler

Model	SCNP-042803[3,4]	SCNP-04280[5,6] Expansion	
	SCNP-04280	SCNP-04280-EX	SCNP-04280-DP
De-Duplicated Flow Capacity (Flows per Minute)[1]	100,000 to 1,500,000	100,000 to 1,500,000	N / A
Raw Flow Capacity (Flows per Minute)[2]	7.5	7.5	N / A
Raw Flow Capacity with Advanced Security Module (FPM)[2]	7.5	7.5	N / A

1. Flow capacity can be expanded up to the amount listed.
2. A flow reported by a single network interface is a raw flow. NetProfiler will de-duplicate up to 10 individual interfaces reporting the same flow into 1 de-duplicated flow.
3. SCNP-4280 and SCNP-04280-EXP equipped with RAID 10 (48 TB) and RAID10 (3.8 TB SSDs).
4. Up to 19 SCNP-4280-EXP expansion modules may be added to each SCNP-4280 system.
5. Each additional SCNP-4280-EXP adds 1.5M de-duplicated FPM.Maximum of 30M de-duplicated flows/min supported.
6. SCNP-4280-DP is required with addition of sixth SCNP-4280-EXP.

SteelCentral NetProfiler Virtual Edition Series

Models	SCNP-VE Series										
Configuration	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11
Flow Capacity	15,000	30,000	60,000	90,000	200,000	400,000	600,000	800,000	1M	2M	3M
Raw Flow Capacity	150,000	300,000	600,000	900,000	2M	4M	6M	8M	10M	20M	30M
Hypervisor	VMWare ESXi 6.0 and 6.5										

SteelCentral NetProfiler Virtual Edition runs on VMware vSphere to provide you with added deployment flexibility for virtualized data centers and software-defined networks For complete configuration details and product models, please visit riverbed.com to download the SteelCentral specification sheet.

Gartner Magic Quadrant Recognition

Riverbed is a six-time leader in the Gartner Network Performance Monitoring and Diagnostics (NPMD) magic quadrant.*

*Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

About Riverbed

Riverbed®, The Digital Performance Company™, enables organizations to maximize digital performance across every aspect of their business, allowing customers to rethink possible. At more than $1 billion in annual revenue, Riverbed's 30,000+ customers include 98% of the *Fortune* 100 and 100% of the *Forbes* Global 100. Learn more at riverbed.com.

riverbed®