Help Your Security Team Sleep at Night

Chief Information Security Officers (CSOs) and their information security teams are paid to be suspicious of everything and everyone who might—just might—pose a risk to the business. They lie awake pondering how to safeguard your company's intellectual property. Their sleeplessness is often justified. Every day there are new reports of application exploits, organized campaigns to impact network operations, and internal malicious behavior.

They frequently rely on you, the network and application performance management experts, for much needed insight into network infrastructure and application usage and to help resolve security issues as quickly as possible. The intent of this brief is to help both you and your beleaguered (and beloved) CISO speak the same language and take advantage of the Riverbed® SteelCentral™ platform's unique ability to make all the moving parts in your infrastructure visible.

Based on our experience helping customers augment and enhance their security programs, most CISOs become strong champions of the SteelCentral platform. They get excited about having actionable intelligence 24/7 to enhance your organizations' security posture and often sponsor joint initiatives. They may be eager to invest in automating routine and or expert tasks to reduce error, developing custom dashboards for forensic analysis, and integrating existing IPS/SIEM solutions with SteelCentral to ensure they have extended visibility.

Visibility Drives Security Value

SteelCentral's primary purpose is to deliver actionable intelligence that empowers teams to make effective resourcing decisions and resolve application performance problems efficiently. It accomplishes this by combining varying data types from multiple sources to provide holistic views of the application and network performance ecosystem, as shown in Figure 1.

[1] IPS—Intrusion Prevention System
SIEM - Security information and event management

© 2015 Riverbed Technology. All rights reserved

StreelCentral Platform Architecture

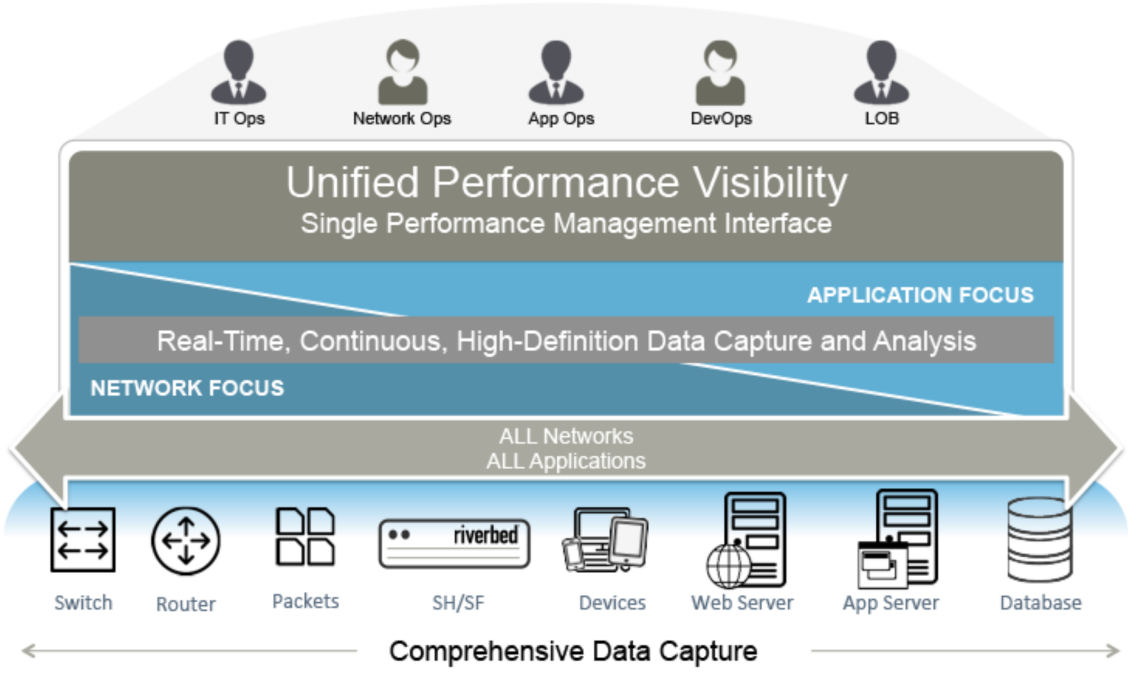

Figure 1: SteelCentral Platform Architecture

The devices and applications in the data tier (bottom third of the diagram) can vary widely based on the environment's instrumentation. Fortunately, Riverbed supports a comprehensive set of vendor and device types.

The middle tier consists of focused solutions that give you visibility into all network and application domains. Performance monitoring and analysis solutions use built-in "big data" analytics to turn high-volume packet, flow, application and transaction metrics information into actionable intelligence on a continuous basis. The SteelCentral network planning and configuration solutions integrates the physical map with application and logical network maps to give a view of changes to the infrastructure and device configurations that can be blended with network and application performance views.

The upper tier delivers the comprehensive and blended view of your infrastructure. It provides true unified visibility via customizable metrics dashboards that allows you to navigate in context between modular solution components.

Consequently, SteelCentral can supply status information and alerting to the information security team very easily.

Leveraging Built-in Security Workflows

CISOs frequently use standards-based frameworks to develop gap assessment and implementation plans. These frameworks establish guidelines that help organizations

- Understand their current-state security stance and priorities (weakness, gaps, areas requiring quick fixes, etc.)
- Define the end-state security stance needed for the business (defensible network designs, application usage policies, user privileges, etc.)
- Track network and application security posture over time (i.e., is the current operational status more secure or less secure than intended?)

© 2015 Riverbed Technology. All rights reserved

The SteelCentral security workflows in Table 1 address various security framework guidelines with little or no extra cost to the business. Each security workflow listed is based on standard, built-in functionality. There are no additions, plug-ins, or changes to the products necessary to make them work in your environment.

By nature, SteelCentral security workflows and security framework guidelines are descriptive, not prescriptive. You must incorporate them into your workplace in ways that are meaningful to your business.

For example, a very basic requirement is to audit network devices for known configuration vulnerabilities and take remediation. Your process for doing this would incorporate the network discovery, auditing, policy validation, and change configuration workflows.

Similarly, many frameworks expect you to automate the monitoring of critical application or device status. SteelCentral dashboards like the one in Figure 2 can be customized to display the metrics critical your stakeholders and used as the basis for discussing risk and setting priorities for action when problems occur.

Table1: SteelCentral Security Workflows

Security Workflow	Description
Network Device Discovery	Scans and finds all network devices (firewalls, routers and switches) within a specified IP Address range and maintains an inventory of network device configuration.
Network Mapping	Automatically build detailed network maps using network device information gathered during discovery workflow. Device compliance and error status is integrated into the maps (e.g. out of compliance devices are highlighted in red on the diagrams).
Audit Network Device Configuration.	Evaluate network device security compliance using either pre-built or custom rules and policy templates during each device discovery cycle. For example, create a rule to test for approved SNMP read/write credentials.
Network Device Reporting	Choose from a number of built-in reports or specify custom reports for auditing and status updates for example, generate a list of the ports in use across secure zones.
Proactive Policy and Change Validation	Creates a simulation network model, based on the network device configuration information, to validate network changes before implementation. For example, flow analysis is used to determine if routing behaves as expected after the proposed network change is implemented.
Configuration change Implementation	Uses automation to push configuration changes to network devices to reduce operator error. Stores snapshots of configuration before and after changes are deployed (what was changed, who implemented, etc.).
Identify Use of Insecure Protocols	Identify insecure protocols used to administrate key servers and verify communications are sourced from known IP ranges (or specific segments). Examples of insecure protocols: Telnet, FTP, or any unencrypted communications.
Behavior Based Anomaly Detection	Enable anomaly detection heuristics based on Riverbed best practices. (Optional: Send alerts sent to third party SIEM when triggered.) Example best practices: - Focus heuristics on anomalous traffic initiated by monitored servers - Raise alerts for scans and suspicious connection settings - New Server Port - Port scan - Host scan - Worm (merged host scans) - Suspicious connection (rare connection between host)s
Network Segmentation Reporting	Provide reporting to support proper network segmentation, incorporating trust zones and application tiers. Configure report templates to validate rules derived from the Client Network Security Classification Standards.
Log Connectivity	Monitor traffic from Untrusted to Semi-trusted sources. Example usage: Start with summary report showing all DMZ servers seeing traffic, then drill down to report on flow (i.e. connection) details.
Map Applications	Provide application dependency maps for all key tier 1 applications. Determine the valid (legitimate) application connections and server/client entities.
Packet Capture and Analysis	Store and capture packet information for long-term forensic analysis.
Define Critical Application and Transaction Dashboards	Create dashboards indicating real-time performance and usage patterns. Use pre-defined widgets populated with data from a wide variety of metrics and alerts.

© 2015 Riverbed Technology. All rights reserved

StreelCentral Portal Application Security Monitoring Example

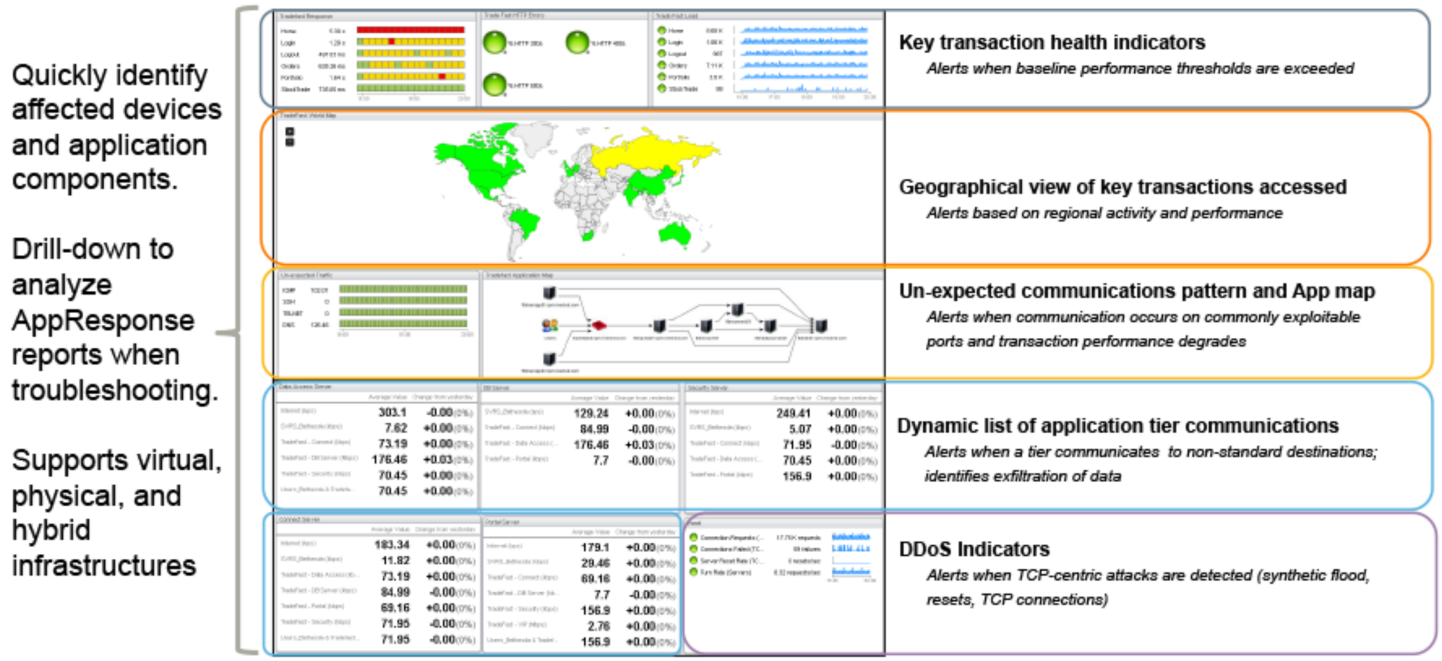

Figure 2: StreelCentral Portal Application Security Monitoring Example

Summary

The built-in reporting and monitoring workflows within the SteelCentral Platform can be directly leveraged to enhance your business' security strategy without the need to have yet another set of security-specific processes overlaying the work you do.

Everyone benefits from increased visibility. Business stakeholders benefit by focusing on views containing the metrics they need to monitor. Technical stakeholders benefit during troubleshooting due to context-sensitive navigation and powerful built-in data analytics. CISOs and information security professionals benefit from the continuous monitoring of network and application infrastructure, the ability to create reliable status reports based on truly authoritative data sources, and the wealth of historical data available for forensic analysis when needed.

No other solution today can match SteelCentral's ability to combine packet, flow, application, infrastructure, and transaction data in such meaningful ways. Visibility helps you rapidly troubleshoot and assign ownership to teams that can effect change, allows for easy customization of reports to suit your business requirements, and, ultimately, give your CISO the insight required to understand past security events and make the right choices to strengthen and monitor cyber defenses.

© 2015 Riverbed Technology. All rights reserved

Call to Action

This technical brief has given you a glimpse into what CISOs are accountable for. Use what you've learned to explore and discuss the ideas presented with your CISO and information security team. Together, you'll gain a better understanding of the broader information security domain and your CISO will learn to appreciate the wise investment your SteelCentral solution really is.

When the time is right to embed SteelCentral solutions into your company's cyber security strategy, we strongly encourage you to consult with your local Riverbed Professional Services Organization. Find out how they've helped other companies through this journey and the benefits that have been realized—everything from improved application performance, cost savings, and better sleep for the CISO.

Additional Information

Visit the following link to find out more about SteelCentral products and solutions available to address your network and performance monitoring and analysis needs

http://www.riverbed.com/products/steelcentral/index.html

To keep up to date with useful information on security and other topics, be sure to bookmark

http://www.riverbednews.com

Speaking of security topics, here are a few recent newsletter articles we hope you find interesting.

Peace Through Performance: How Riverbed Can Enhance IT's Security Posture

Better Visibility Enables Better Security with SteelCentral NetProfiler

SANS Critical Security Controls: SteelCentral Has You Covered

---

About Riverbed

Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid enterprise to ensure applications perform as expected, data is always available when needed, and performance issues can be proactively detected and resolved before impacting business performance. Riverbed enables hybrid enterprises to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed's 26,000+ customers include 97% of the *Fortune* 100 and 98% of the *Forbes* Global 100. Learn more at riverbed.com.

©2015 Riverbed Technology. All rights reserved. Riverbed and any Riverbed product or service name or logo used here are trademarks of Riverbed Technology. All other trademarks used herein belong to their respective owners. The trademarks and logos displayed herein may not be used without the prior written consent of Riverbed Technology or their respective owners.