



ESG WHITE PAPER

Riverbed Unified NPM Can Support and Improve Network Security and Operations

By Jon Oltsik, Senior Principal Analyst and Fellow, Enterprise Strategy Group

June 2021

This ESG White Paper was commissioned by Riverbed and is distributed under license from ESG.



Contents

Contents	2
Executive Summary	3
The State of Network Security.....	3
The Organizational Gap between Networking and Security	5
Network Visibility Provides a Foundation for Security Operations	6
Riverbed for Network Visibility.....	8
The Bigger Truth	9

Executive Summary

ESG research indicates that 43% of organizations use network traffic analysis (NTA) tools as a first line of defense for threat detection and response.¹ This strategy parallels the old security adage that, “the network doesn’t lie.” Cyber-attacks move laterally across networks and connect to external resources (e.g., C2 servers, malware servers, etc.) as part of attack campaigns. Identifying malicious connections or payloads in the network can accelerate threat detection and minimize dwell time.

Organizations may use NTA and network detection and response (NDR) technologies today, but ESG data indicates something is still amiss. Many firms struggle to scale, optimize, and operationalize network security as needed. Why is network security so difficult and how can organizations address this complexity? This white paper concludes:

- **Network security grows more difficult each year.** Organizations are using internal and cloud-based networks (i.e., hybrid enterprise networks) for business initiatives like digital transformation and support for work-from-anywhere teams. Clearly, networks are business-critical, making it all the more alarming that 85% of security professionals say that network security has become more difficult over the past two years because of the increasingly dangerous threat landscape, growing attack surface, and the proliferation of network security tools.² These difficulties lead to increasing cyber-risks, rendering organizations vulnerable to costly cyber-attacks.
- **Security and network operations teams don’t always play well together.** Addressing network security must be a team effort between security and network operations, but nearly half of organizations believe that these two groups don’t always work well together and struggle to overcome communications and collaboration issues.
- **Organizations can address these issues with shared data sources and end-to-end network visibility.** Networking and security teams often use different tools to monitor network behavior, leading to confusion, redundancy, and excess costs. Since both groups really look at the same data, ESG believes that organizations can benefit from implementing solutions that collect, process, and analyze network data for both security and operations use cases. Riverbed Unified NPM applies here, as the combination of NetProfiler and AppResponse provides comprehensive network visibility, full-fidelity network data, and the ability to view network behavior from many angles (e.g., internal networks, cloud-based networks, WAN, etc.). Over the past few years, Riverbed has instrumented its NPM tools for security needs and has an aggressive roadmap to accelerate security support in the future. In this way, Riverbed Unified NPM can act as a single source of truth, improving efficiency and productivity for security and network operations teams.

The State of Network Security

Network security technologies have been around since the 1980s when Digital Equipment Corporation (DEC) introduced the first commercial firewall. With over 30 years of experience, it would be safe to assume that network security is mature and well under control, but ESG data reveals that this isn’t true at all. ESG research indicates that 85% of organizations believe that network security is more difficult today than it was 2 short years ago. Why? There are several reasons, including (see Figure 1):³

- **An increase in cyber-threats.** The first six months of 2021 featured highly visible cyber-attacks like SUNBURST and those targeting specific organizations like the South Korean nuclear research agency, Carnival Cruise Lines, JBS beef plants, Colonial Pipelines, and Wegmans supermarket chain. This partial list illustrates the fact that no geography,

¹ Source: ESG Master Survey Results, [The Threat Detection and Response Landscape](#), April 2019.

² Source: ESG Research Report, [The State of Network Security: A Market Poised for Transition](#), March 2020.

³ Ibid.

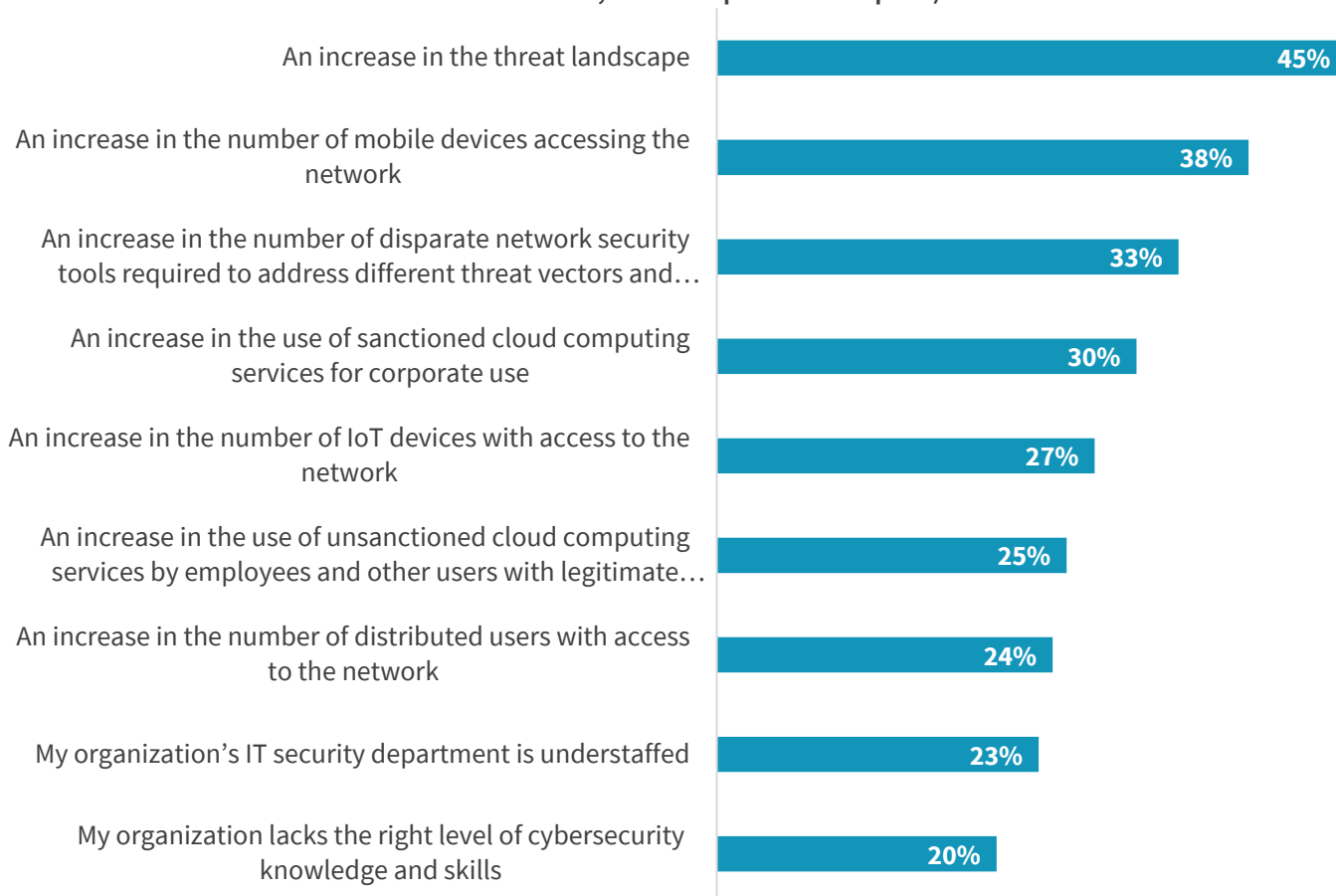
industry, or organization is immune from attack. To address this pattern, network security specialists need comprehensive visibility across networks, accurate detection rules, and deep forensic data for timely and precise investigations.

- **A growing attack surface.** ESG research shows increases in the number of mobile devices, unsanctioned applications, IoT devices, and unsanctioned cloud services. Taken together, these trends equate to a growing attack surface. From a network security perspective, SOC teams must have detailed visibility into applications, devices, connections, and protocols at scale. Since many organizations don't have this level of visibility, SOC teams are forced to make educated guesses based on limited visibility and available historical data—typically, a compromise at best.
- **The proliferation of network security tools.** With the combination of sophisticated threats and a growing attack surface, many organizations have deployed new types of sensors and detection tools. Unfortunately, this has led to a spike in the number of security alerts. Somehow, SOC analysts are expected to triage, investigate, and prioritize this growing security alert volume, an impossible task for many organizations.

It is also noteworthy that 23% of respondents say that their IT security department is understaffed, while 20% claim their organization lacks the right level of cybersecurity knowledge and skills. Given the global cybersecurity skills shortage, these trends will likely continue.

Figure 1. Reasons Why Network Security Has Become More Difficult

You indicated that network security has become more difficult over the last two years. In your opinion, which of the following factors have been most responsible for making network security management and operations more difficult? (Percent of respondents, N=226, three responses accepted)

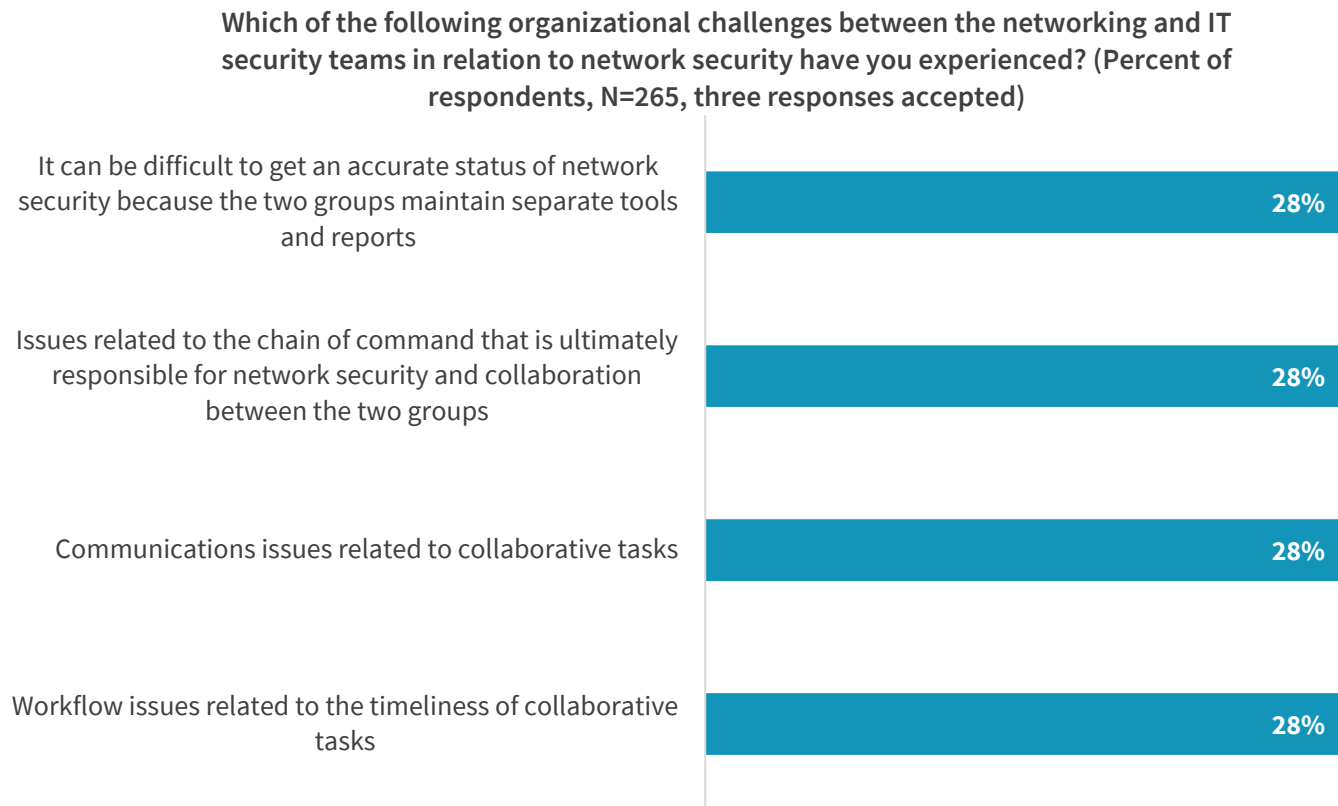


Source: Enterprise Strategy Group

The Organizational Gap between Networking and Security

Threat prevention, detection, and response is a collective effort between security and networking teams, but unfortunately, these two departments don't always work together in harmony. In fact, 44% of organizations say that this relationship does not work well all the time because the groups maintain separate data/tools, report to independent chains of command, don't communicate well on collaborative tasks, and suffer from workflow issues related to process timeliness (see Figure 2):⁴

⁴ Source: ESG Master Survey Results, [Network Security Trends](#), March 2020.

Figure 2. Top Four Organizational Challenges Between Networking and IT Security Teams

Source: Enterprise Strategy Group

The ESG data paints a disturbing picture where network security is becoming more difficult, and the two main groups tasked with managing network security don't always play nicely together. If this situation continues, cyber-risks will skyrocket as networking and security teams struggle to scale day-to-day operations, threat detection processes, and incident response. To counteract these alarming prospects, CISOs must work with their IT and networking counterparts to address these challenges as soon as possible.

Network Visibility Provides a Foundation for Security Operations

To address network security difficulties, sagacious CISOs know they must monitor all traffic at key points on the network (i.e., ingress/egress points, data centers, within public clouds, etc.). According to ESG research, this is already happening—87% of organizations use NTA tools for threat detection and response today, and 43% say that NTA is a “first line of defense” for detecting and responding to anomalous/suspicious/malicious network activities like lateral movement, network enumeration, C2 traffic, and data exfiltration.⁵ Many firms also rely on network visibility for:

- **Network posture and anomaly detection.** To quote marketing guru Peter Drucker, “You can't manage what you can't measure,” and this statement certainly pertains to network security. Comprehensive network visibility can identify rogue devices on the network, monitor traffic patterns, and pinpoint anomalous traffic. This applies to all traffic—north/south and east/west—and also extends to traffic within public cloud infrastructure. To detect complex multi-staged attacks, CISOs should strive to have visibility into all traffic.

⁵ Source: ESG Master Survey Results, [The Threat Detection and Response Landscape](#), April 2019.

- **Deep forensic details.** Leading network visibility tools can capture connections history detailing which assets were communicating, when this communication happened, and what the communication entailed (i.e., ports, protocols, payloads, etc.) This level of detail is critical for threat detection, investigation prioritization, and the investigations themselves. When security analysts receive an alert from some detection technology (IDS/IPS, EDR, SIEM, etc.), they generally pivot to network visibility tools, digging into NetFlow/ipfix and packet capture (PCAP) tools for a perspective of what happened, when it happened, and which network nodes were involved. From there, threat hunters can use flow and packet data for full-fidelity recall of historical events. To ensure this deep forensic data exists when needed, organizations need to maintain always-on, full-fidelity monitoring and capture. The urge to simply “sample” data (for speed or shaving expense) is real, but it leaves significant gaps in the history that can be insurmountable and far more costly when complete forensic analysis is at a premium.
- **Security strategy.** Since network visibility provides a window into network communications patterns, security engineers can use this data as a guide for ongoing projects in areas like micro-segmentation and zero trust. This can help reduce the attack surface for risk mitigation.

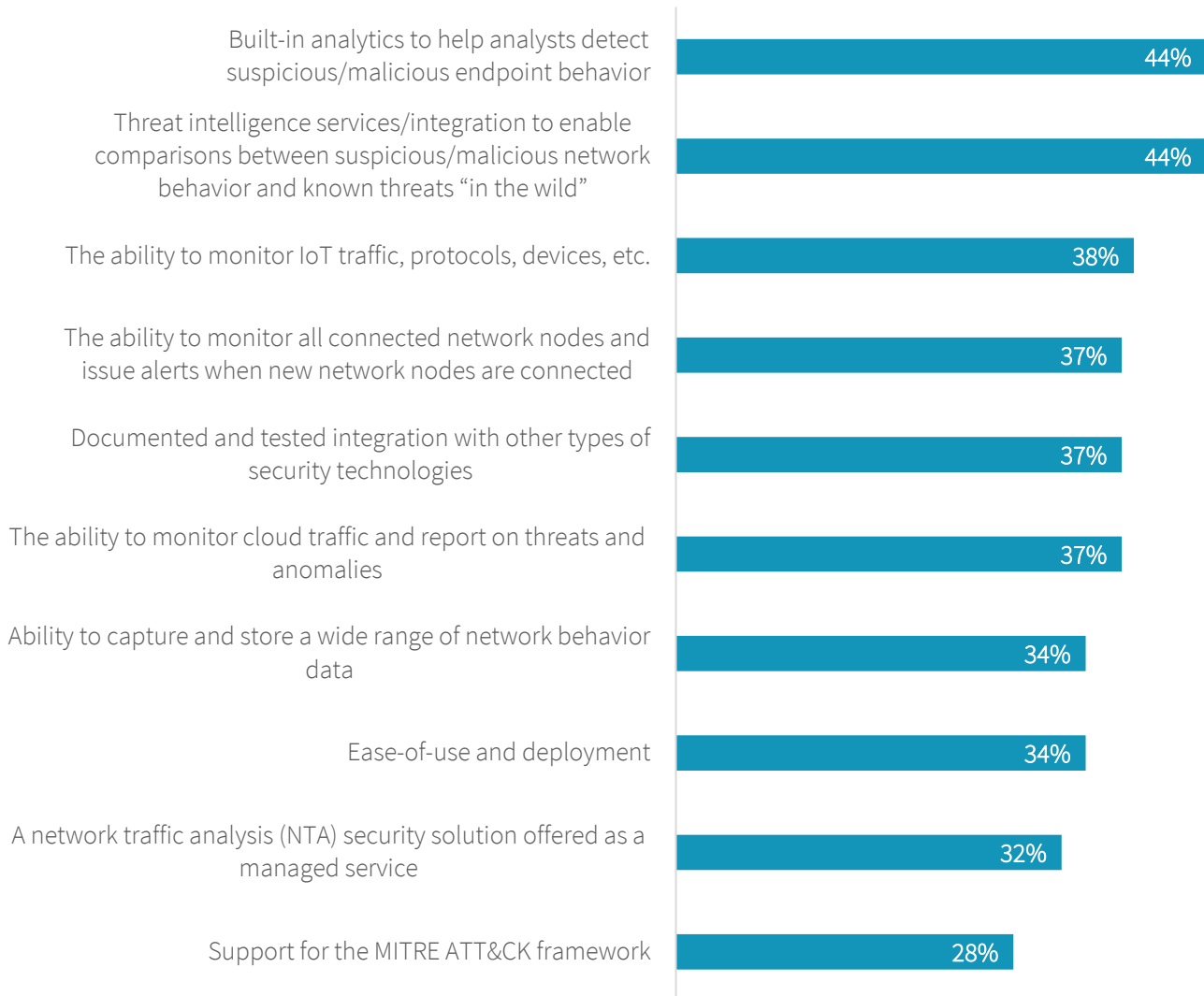
As previously stated, network visibility is often supported by network traffic analysis (NTA) tools. According to ESG research, networking and security professionals have a laundry list of requirements for this type of technology. The most important attributes of NTA tools include built-in analytics for threat detection, threat intelligence for network data enrichment, the ability to monitor IoT devices/traffic, and the ability to monitor network nodes to maintain secure network hygiene (see Figure 3).⁶

Leading network visibility tools should also help bridge the gap between security and networking teams by providing a common network data repository supporting networking use cases like application/network performance management and security use cases like threat detection, incident response and forensic investigations, and threat hunting. The best solutions will collect, process, and analyze 100% of the data at strategic points in the enterprise and cloud network, provide visibility and analytics from multiple network vantage points, and offer full-fidelity network data.

⁶ Source: ESG Brief, [Key Attributes of a Network Traffic Analysis Solution](#), September 2019.

Figure 3. Most Important Attributes of NTA Solutions

Which of the following are the most important attributes of a network traffic analysis solution (used for threat detection/response) for your organization? (Percent of respondents, N=347, multiple responses accepted)



Source: Enterprise Strategy Group

Riverbed for Network Visibility

CISOs can choose from an abundance of tools for network visibility, but yet another security tool won’t help to bridge the gap between security and networking teams. As an alternative, organizations may benefit from network visibility tools that can support the needs and use cases of both networking and security teams.

Industry veteran Riverbed offers a hybrid solution that may satisfy the common needs of security and networking teams. A Riverbed solution can be built on top of its network performance monitoring (NPM) products: NetProfiler for flow records and AppResponse for full packet capture. Using this combination, organizations can collect data across the network to gain full visibility of all network activity. This also gives them the ability to monitor the network from multiple angles—at the

network perimeter, within cloud and corporate data centers, inside east/west traffic on internal networks, at remote offices connected to the WAN, etc. Beyond visibility alone, Riverbed provides specific functionality for network security for:

- **Active threat detection.** To improve threat prevention and detection, Riverbed security solutions support IoC blacklisting, consume threat feeds for enrichment and contextualization, and capture networking baselining for anomaly detection.
- **Forensic investigations.** When security analysts suspect they are under cyber-attack, they need the ability to look at detailed, real-time and historical network activity. Riverbed Unified NPM is designed for this job, offering full-fidelity flow and packet data for use cases like security investigations and threat hunting. Riverbed has even created an API, enabling SOC teams to perform packet capture based on specific triggers, like connections to rogue IP addresses or Internet domains.
- **DDoS detection and mitigation.** Riverbed goes beyond many other NTA tools with DDoS detection and mitigation. By consolidating this functionality into its Unified NPM solution, Riverbed can help further bridge the organizational gap between security and network operations teams.

With full-fidelity visibility, Riverbed Unified NPM can also help organizations stitch together network communications indicating “low and slow” cyber-attacks like advanced persistent threats (APTs). These campaigns use various tactics, techniques, and procedures (TTPs) following a kill chain to compromise systems, move laterally across networks, harvest credentials, and eventually exfiltrate valuable data. By providing end-to-end visibility, Riverbed can also aid organizations’ efforts to operationalize the MITRE ATT&CK framework for typical MITRE ATT&CK use cases like incident detection, security assessment and engineering, cyber-threat intelligence analysis, and adversary emulation. Finally, Riverbed Unified NPM networking and security functionality can help organizations as they plan, test, and implement architectural solutions for zero trust.

The Bigger Truth

Cybersecurity teams must support business and IT initiatives while protecting digital assets from cyber-attack. While this is a clear mission, it is getting more difficult by the day. The SOC team simply can’t keep up with the scale and complexity of its role under the weight of nebulous security alerts and patchwork network visibility. Rather, security staff must be synchronized with network operations with clear and comprehensive visibility to everything happening on the network.

While not generally thought of as a security vendor, a growing number of Riverbed’s customers use its Unified NPM solutions for security today as the combination of NetProfiler and AppResponse help organizations gain comprehensive, full-fidelity visibility of NetFlow/ipfix and packet (PCAP) across the network. Armed with these tools, Riverbed customers can identify suspicious behavior, enrich network data with cyber-threat intelligence, block malicious IoCs, and mitigate DDoS attacks while supporting network performance management requirements. This combination could be a valuable addition to security and network operations teams for improving cybersecurity efficacy, streamlining operations, and bolstering collaboration. In addition, this same data proves invaluable for deep-dive forensics to uncover root cause, entry points, and timelines of cyber-attacks, which is critical once an attack has been identified.


All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.



Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188