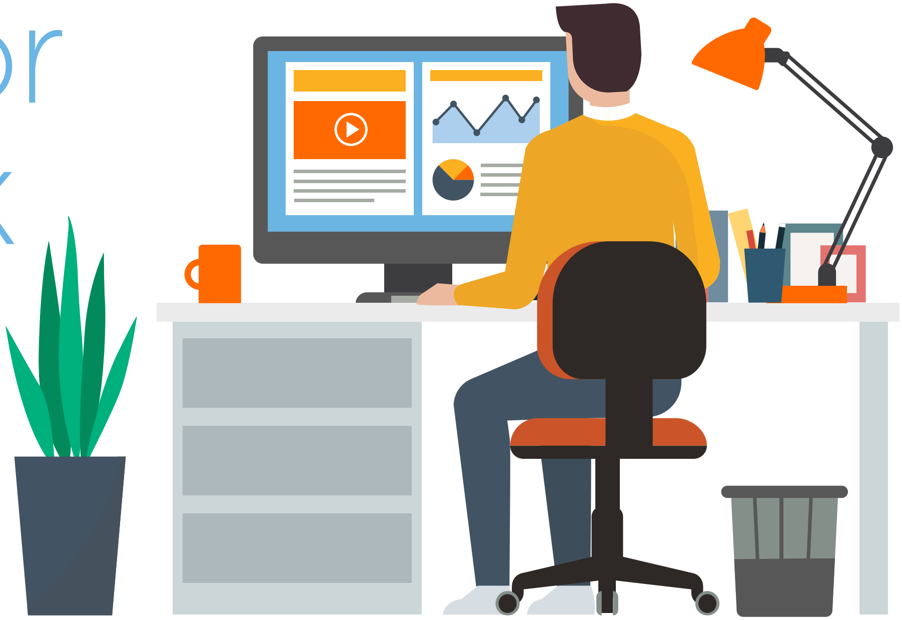
riverbed®

Buyer's Guide for Unified Network Performance Management



The New Requirements for Work-from-Anywhere

Table of Contents

3 You’re still on the hook

4 From WAN to LAN

5 What’s changed?

7 How to assess which solution works for you

8 10 questions to ask

9 Tips to improve network resiliency and security for remote workers

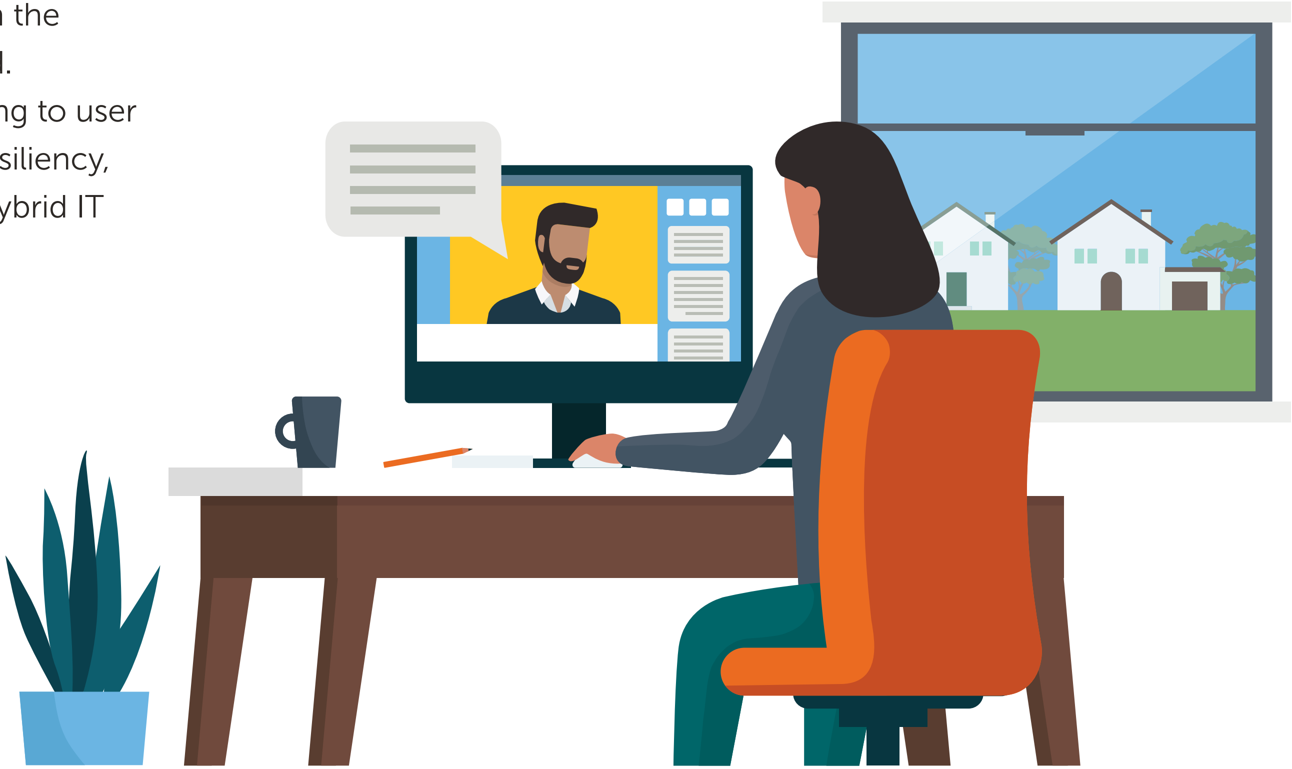
10 How to communicate the value to key stakeholders

13 Improve network resiliency and security with Riverbed®

You're still on the hook

You haven't had your coffee, but your users are already complaining about the slow performance of their web apps. So slow, in fact, that some of them have written them off as unavailable. The head of Sales, working remotely from her home office, is battling to approve an order before quarter-end close but is highly frustrated by application performance or lack thereof. To make matters worse, your VP of operations, working on the go, isn't any happier.

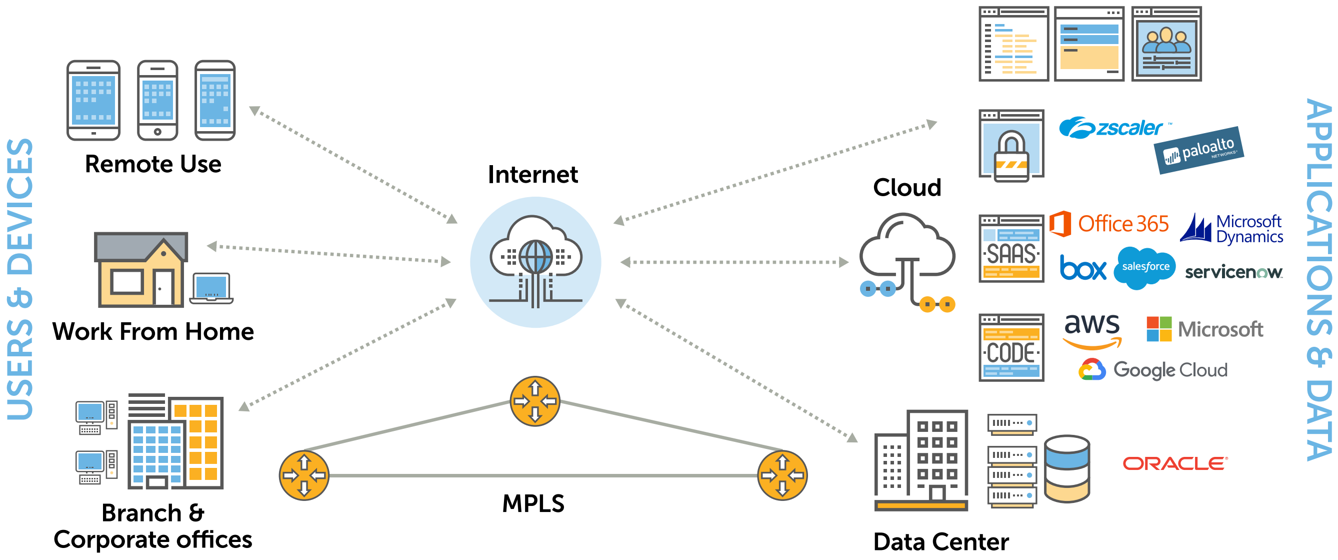
Although the application is hosted in the Cloud, some things haven't changed. You're still on the hook for responding to user complaints and ensuring network resiliency, and security across your complex, hybrid IT environment. Must be Monday...



From WAN to LAN

Most of our issues for WAN monitoring of on-prem, traditional apps have largely been solved. Yet, the goal posts have moved. The surge in remote work and greater IT complexity from a mix of on-prem, cloud, and SaaS applications has shifted the focus from WAN to LAN. The last-mile represents a challenge to network teams since it relies on local ISPs and home network equipment rather than the MPLS and enterprise-grade equipment typically found in the office environment. Bandwidth contention and saturation further slow performance for at-home and remote workers.

For network teams, the new question is, how can we optimize our entire IT environment and ensure our core services and applications are performing properly for our work-from-anywhere users – wherever they work?



> "When application performance slows, it can become a blame game. The Internet service provider, credit agency, and other parties tend to assume the problem is someone else's."
>
> **Richard Hurst**
> Supervisor of Network Services
>
> **OneMain** Financial.

What’s changed?

Shift to “work-from-anywhere”
Current research indicates that companies will continue with an expanded remote work model after the concerns around COVID-19 subside. According to Gartner, 74% of companies plan to increase the number of remote workers, and nearly a quarter will move 20% of their workforce to permanent remote work.[1] This new flexibility means that IT organizations will need to ensure users are productive no matter where they are. As a result, this shift places new challenges on the network in terms of bandwidth, latency, and security.

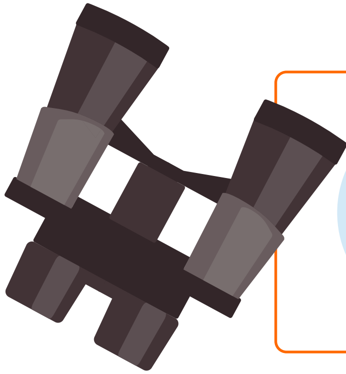
What’s changed? (continued)

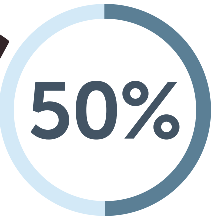
Greater IT complexity
Hybrid networks and remote work isn’t new, but 66% of IT professionals surveyed say IT is even more complex than it was just 2 years ago.[2]

The network has changed
Remote workers expect to be fully productive anytime, anywhere, but they are dependent on last mile networks that are often unpredictable and struggle with the effects of bandwidth saturation and latency.

Application hosting has changed
Applications may reside on prem, in public clouds, private clouds, or at the edge. Modern application environments can have thousands of distributed components often deployed in containers that constantly interact with each other over the network. As a result, there’s an increased burden and dependence on network health.

NetOps and SecOps collaboration
NetOps and SecOps were already collaborating to strengthen security postures and identify threats. However, this partnership has become more important in light of the increase in cyberattacks due to the pandemic and the increase in number of endpoints due to remote work.





By 2024, **50%** of network operations teams will be required to rearchitect their network monitoring stack, due to the impact of hybrid networking, which will be a significant increase from 20% in 2019.[3]

Gartner

How to assess which solution works for you

The right Network Performance Monitoring (NPM) solution can ensure network resiliency and security for your work-from-anywhere users whether they are in the office, on-the-go, or at home. It provides the insights you need to run your business with role-based views to drive both IT and business insights. There are four core requirements to consider:

Comprehensive visibility: Some solutions sample limited data, pulling metrics or data at low frequencies, or from just a subset of locations. They simply cannot scale and are not architected to collect all the data which is critical for developing the complete picture. For comprehensive visibility, NPM solutions must also collect flow, packet, and device data across on-prem, cloud, multi-cloud, and edge environments, as well as across physical and virtual environments. This combination of complete and rich data provides network teams with the ability to proactively identify and resolve complex, cross-domain issues.

Security forensics: As discussed previously, network and security teams collaboration is critical to preventing security breaches. By collecting, storing, and analyzing full fidelity packet and flow data to detect security threats, NPM solutions can decrease the time from breach to detection. Common areas of focus include threats caused by data exfiltration, password brute force attempts, blacklisted sites, malware, and DDoS attacks.

Artificial intelligence (AI): By using machine learning and AI, network teams can quickly surface patterns and anomalous behaviors across domains. For accurate IT and business insights, unified NPM solutions can analyze rich datasets including user and device data, application log data, observability data, topology maps, infrastructure metrics, and network packet and flow data. For example, AI can help detect trends before their impact is felt, reduce noise due to false alarms, and capture multi-variate anomalies that could never be detected by a human.

Deep integration: In a highly complex, distributed environment, modern solutions need to have tight integration within their product portfolios or families. They must also connect just as effectively with multiple cloud services, third-party software via open APIs, and existing tools (e.g., application performance management, logging, and workflow).

Standalone vs Best of Breed? Integrated platforms are more effective at performance monitoring than standalone, best-of-breed tools.[4]

EMA

10 questions to ask

1. Does your solution provide comprehensive visibility across on-prem, cloud, hybrid, and multi-cloud environments?

2. Can it capture all packets, flows, and infrastructure metrics, all the time, so full-fidelity data is available when needed?

3. Are you able to quantify the web user experience by using network data to measure performance and availability without an agent?

4. Can you integrate end-user experience, application, network, and infrastructure performance into a single dashboard?

5. Does your solution provide role-based views for executive, business, and domain-specific use cases across all your domains?

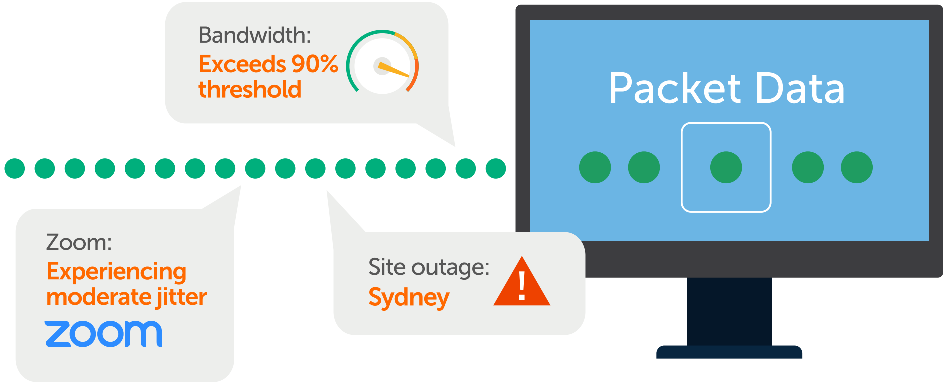
6. Does it provide insights into device and interface health, configuration monitoring, and path analysis?

7. Are you able to map network dependencies to automatically map applications to their underlying infrastructure?

8. Can you use AI and machine learning to detect patterns and anomalies that indicate poor performance or security risk?

9. Can you use network insights to identify threats caused by data exfiltration, password brute force attempts, blacklisted sites, and DDoS attacks?

10. Do you have the flexibility to deploy where you want: on prem, private cloud, and/or in the public cloud?



Tips to improve network resiliency & security for remote workers

1. **Tackle remote access and VPN issues:**
With so many employees working remotely, there is much higher traffic and workload on the VPN, and it's challenging to assure a positive experience and anticipate issues. By bringing together flow, packet, and device data, you can better understand the performance of your VPN in real time and ensure that VPN concentrators can keep up with the throughput.

2. **Gain deep insight into remote user experience:**
With remote work, there is an increased load on business-critical web apps which can make it difficult to meet service level targets. By monitoring all the incoming requests that make up a page and then measuring the corresponding response times from the server, you can monitor the user experience for your business transactions and identify bottlenecks, even for SSL traffic.

3. **Optimize bandwidth and QoS for new usage patterns:**
By monitoring network usage trends and patterns, you can re-plan for capacity changes as more employees work remotely. Make sure to optimize bandwidth usage for these new traffic flows and also QoS tags for your top apps to ensure workforce productivity.

4. **Remove security blindspots:**
Cybercriminals are taking advantage of the current situation to step up their attacks. To fight back, leverage your network telemetry to strengthen your security posture. By applying security analytics with full-fidelity flow and packet capture, you can detect threats, perform forensic investigation, and mitigate breaches. Leverage your network data to better identify and respond to threats caused by worms, password brute force attempts, malware sites, and DDoS attacks.

5. **Prioritize business-critical and collaborative applications:**
Prioritize application traffic to ensure that must-haves for remote work such as Office 365, Salesforce, Zoom, or other critical traffic have the bandwidth they require for fast, reliable, and consistent performance. Set policies that account for business criticality to ensure that workforce productivity and user satisfaction don't suffer.

6. **Troubleshoot poor VoIP performance:**
Your users depend on reliable and always-available communications to work effectively whether they are in the office or remote. Monitor voice streams in real-time and detect quality problems by isolating the root cause of poor-quality flow and quickly remediate.

7. **Automatically identify shadow apps usage:**
Shadow apps, such as Box and Dropbox, can store valuable, proprietary data outside of your visibility and control. Use network data to monitor and detect usage by workers and mitigate your security risk.

How to communicate the value to key stakeholders

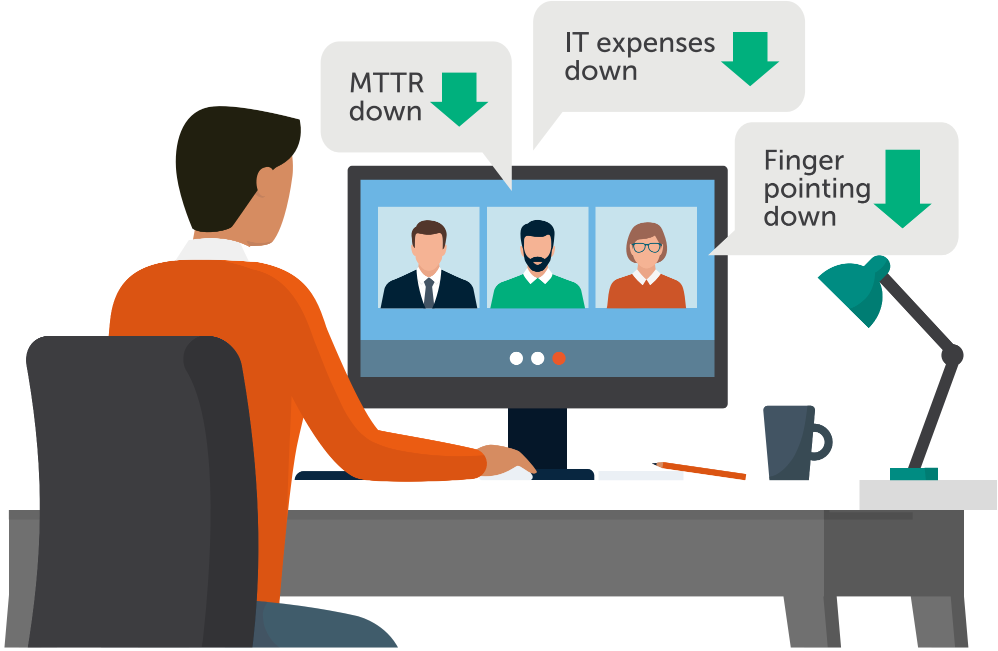
Business stakeholders and IT executives are typically looking for value across three vectors: operational efficiencies, workforce productivity, and risk mitigation.

Drive operational efficiency gains

Gartner recommends that to increase the maturity of the digital workplace, "CIOs should develop a strategy to ensure continuity of operations, empower employees, and improve efficiency."[5] Areas of focus include streamlining incident identification and problem resolution as well as lowering expense to reinvest in value-added activities.

Riverbed's customers have:

- Reduced network and application blind spots by 53%
- Reduced mean time to repair (MTTR) by 47%
- Reduced finger-pointing by 43%
- Lowered annual IT expenses by $120,000 per 1,000 users

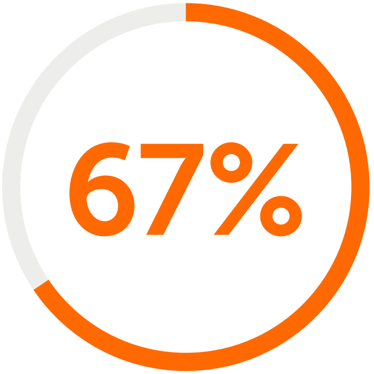


How to communicate the value to key stakeholders (continued)

Improve workforce productivity

As employees shift to remote work, IT organizations must ensure that user productivity does not suffer. By ensuring the availability and performance of all enterprise applications for on prem, work-from-home, and on-the-go, employees have improved user productivity. In addition, the Riverbed unified NPM platform uses AI to surface cross-domain insights, allowing organizations to boost productivity for IT staffs devoted to networking management.

Riverbed customers have improved user productivity by



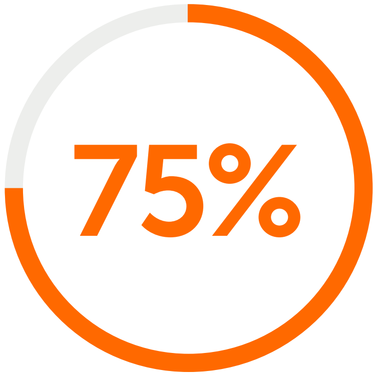
> "We've seen significant productivity improvements. We've been able to shave two minutes off the logon time for over 8,000 people. With the average number of logons a day being five, we've estimated that the productivity improvements equate to around $60,000 a day."
>
> **Dagfinn Krog,** Service Operations Manager
>
> HELSE MIDT-NORGE IT

How to communicate the value to key stakeholders (continued)

Mitigate risk and ensure business continuity

Improve speed and capability to respond to security and performance incidents using the Riverbed unified NPM platform to:

- Ensure your customer-facing web applications are performing well to protect reputation and revenues
- Know when workers communicate with blacklisted systems, such as known malware download sites or command & control sites, so you can investigate and mitigate before additional systems in the network are infected
- Baseline traffic to identify threats that generate unusual patterns, such as data exfiltration, password brute force attempts, etc.



of security experts want greater speed and capability to respond to security and performance incidents.[6]

Improve network resiliency and security with Riverbed

Riverbed's unified NPM platform helps enterprises improve network resiliency and security for your workforce whether in the office, at home, or on the go. Unlike disparate tools, Riverbed combines cross-domain data, including all packets, flows, and devices with machine learning and advanced analytics to provide you with deep visibility and insights across your hybrid environment.

To learn more about how Riverbed's unified NPM platform can provide visibility across cloud networks, infrastructure, and on prem to support your work-from-anywhere users, visit us at riverbed.com/npm.

[1] Gartner, COVID-19 Bulletin: Executive Pulse, 3 April 2020
[2] ESG, Riverbed: NPM for Modern Business, 2020
[3] Gartner, J. Chessman, Market Guide for Network Performance Monitoring and Diagnostics, 5 March 2020
[4] EMA, 2020
[5] Gartner, Coronavirus (COVID-19) Outbreak: Short- and Long-Term Actions for CIOs, Sandy Shen, Owen Chen, Arnold Gao, Lily Mok, Julian Sun, Deacon D.K. Wan, 4 March 2020
[6] Forbes INSIGHTS, 2019