Checklist: Network Monitoring for Remote Workforce Productivity

As organizations shift to more remote work, IT teams are challenged to find new ways to ensure remote workforce productivity. Network monitoring is a critical tool to help keep employees happy, productive, and secure.

Start with this short list to evaluate how the right solution can ensure network resiliency and security whether your users are in the office or at home.

Did you know the right network monitoring and analytics solution could allow your team to...

- ☐ **Prioritize business-critical and collaborative applications and deprioritize others?**
  Prioritize application traffic to ensure must-haves for remote work such as Microsoft 365, Salesforce, or other critical traffic have the bandwidth they require for fast, reliable, and consistent performance.
- ☐ **Resolve remote access and VPN issues?**
  The surge in remote work places greater demands on your VPN infrastructure. Ensure your VPN setup has sufficient capacity and can hold up under the additional load by monitoring VPN performance and quickly identifying any issues.
- ☐ **Gain insight into the user experience?**
  Ensure workforces remain productive whether remote or in the office. Measure the real user experience of web applications to troubleshoot performance problems and deploy synthetic testing to proactively monitor applications and infrastructure that they rely on.
- ☐ **Make capacity plans based on new usage patterns?**
  Re-plan for capacity changes based on changes in usage patterns as more employees working remotely. Optimize bandwidth usage for these new traffic flows to ensure network performance.
- ☐ **Troubleshoot poor VoIP performance?**
  Your users depend on reliable and always-available communications to work collaboratively. Monitor voice streams in real-time and detect quality problems by isolating the root cause of poor-quality flow for VoIP, Teams, Zoom, and others. Reduce telecom operating costs while delivering the high call quality that users expect.
- ☐ **Automatically identify network security threats?**
  The surge in work-from-home and remote work increases the risk of a security breach. Mitigate risk by identifying threats caused by data exfiltration, password brute force attempts, and blacklisted sites. Detect new services, hosts, and connections that can represent security threats.
- ☐ **Detect Distributed Denial of Service (DDoS) attacks?**
  Cybercriminals are taking advantage of the current situation to increase pressure with new DDoS attacks. Quickly detect DDoS so that you can make informed mitigation decisions and recover sooner. Use comprehensive network monitoring and analytics to limit the business impact.
- ☐ **Identify shadow IT usage?**
  Shadow IT projects can increase your attack surface. Deter cyberattacks by identifying and alerting your IT team when unauthorized applications are accessed.

In short, the right solution enables greater network performance and forensic insights to ensure availability and reduce risk whether your workers are remote or in the office. Riverbed's unified network performance monitoring platform provides a clear and comprehensive view of network and application performance across on-premises, hybrid and multi-cloud environments to help IT stay in full control and ensure availability and security–regardless of where and when employees choose to work. Learn more.