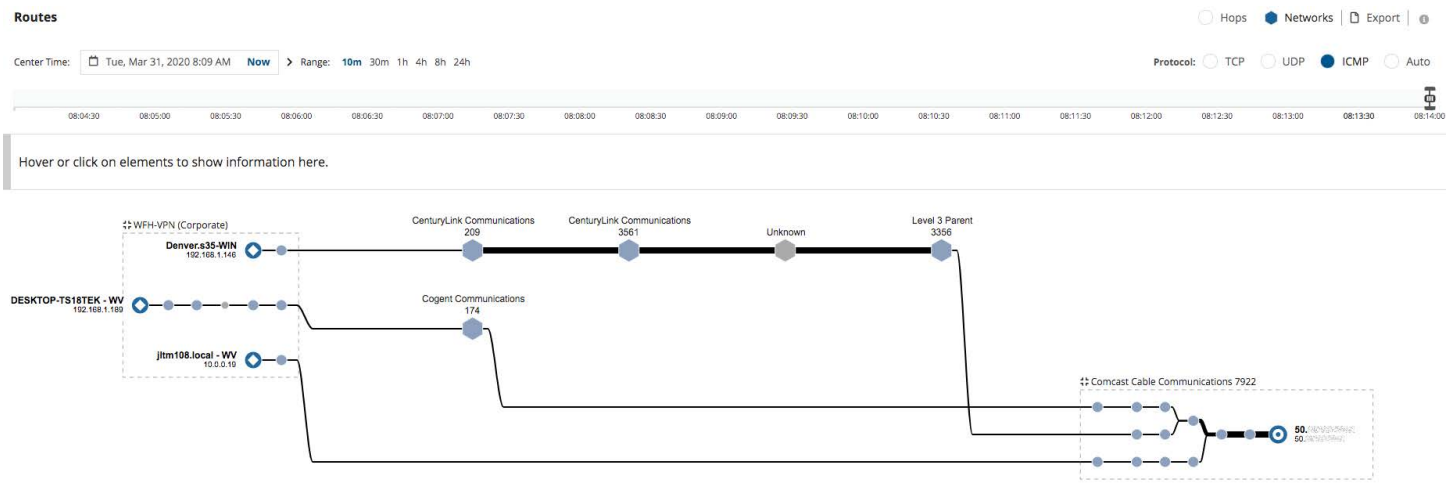
DATASHEET

# How to Monitor Work-From-Home Users and VPN Connectivity

To better serve a distributed workforce forced to adopt 'work-from-home' (WFH) as a new normal, many enterprise networks are taking on a completely new look. While some enterprises have already adapted networks to accommodate remote work, technology in place today may be limited or insufficient for the rapid increase in network complexity.

For instance, there is increased stress on technologies like VPN gateways as employees try to access core systems from home. While IT may have been prepared for some remote access to network data, the level that is common today requires a different solution.




*This visualization allows IT to understand the route and the performance per network segment. It shows underlay performance from WFH users to the Corporate VPN Gateway (50.*).*

Visibility into the service delivery chain, 3rd-party networks, and last-mile transmission is essential for IT to respond quickly to complaints from remote employees. Actionable information for the end-to-end path also helps identify when wireless and residential Internet connections are causing connectivity issues instead of widespread VPN or WAN.

## Active Monitoring for WFH Users

AppNeta Performance Manager provides the most visibility when deployed in a bi-directional setup, with an AppNeta Monitoring Point at the data center, network hub, or corporate office to use as a target, and a Software Sequencer deployed on a laptop or workstation to act as the source of monitoring. This allows AppNeta to provide performance measurement to critical systems through dual-ended monitoring and, when split tunneling is in use, 3rd-party apps hosted in the cloud via single-ended monitoring.

## See VPN Performance Metrics from the End User Perspective

AppNeta provides IT teams with the ability to actively test the user experience of remote workers. Performance can be measured through VPN tunnels and independently on the underlay to compare performance and isolate what might be causing degradation.

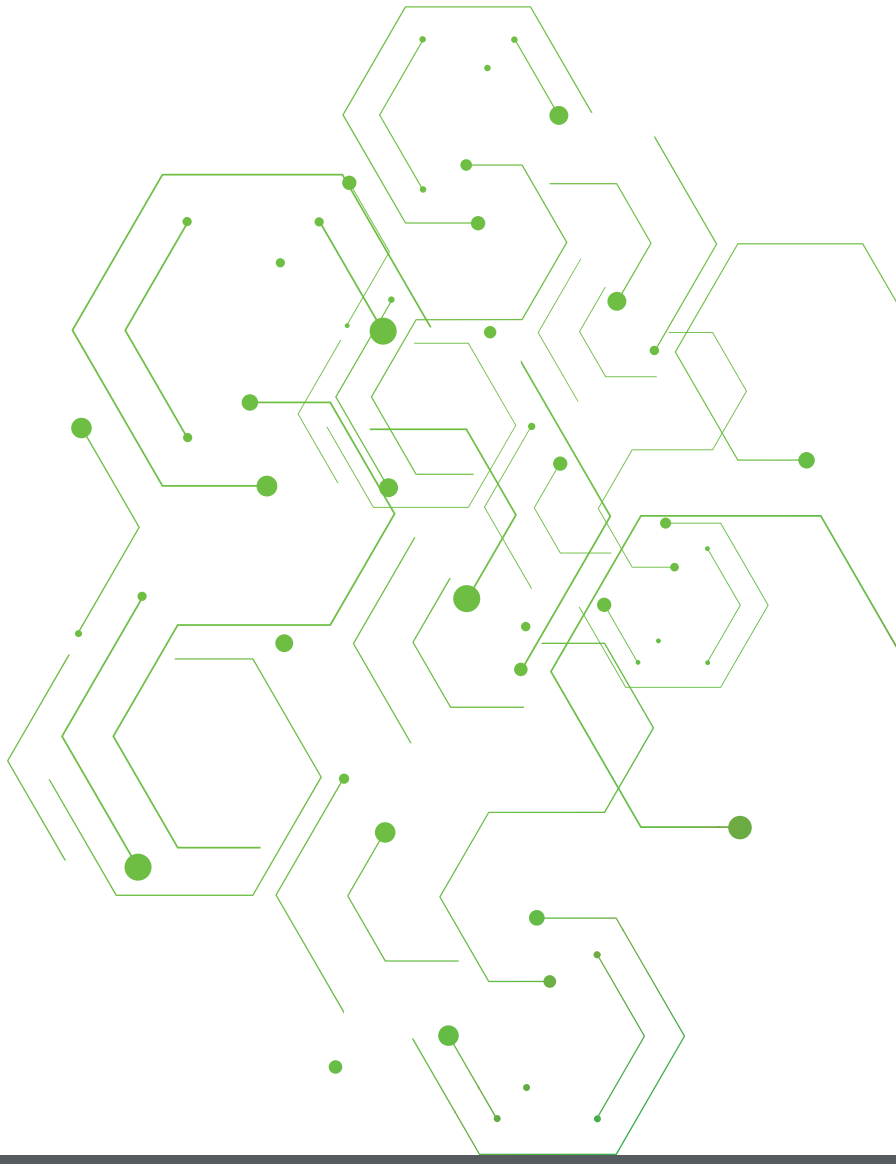
When deciding what to measure and how, it's important to think of a few key strategies and metrics for reporting on your internal customers.

Factors include geography, job function and business unit (which in turn are indicators for what applications are critical to understand), and dependency on various major and minor ISPs which your users depend on.

As an example, for customer service personnel interacting with external customers, it may be critical to understand performance at the per-agent level because customer satisfaction is so intrinsically tied to this experience. This will also help identify what apps are critical -- is the VPN critical for this role? Or, is there more dependency on cloud-based services used for unified communications and customer management?

In other cases, you may want to have at least regional geographic representation of performance to VPN gateways and concentrators, as well as a reasonable sample of the major ISPs which your end users are depending on as part of this application path.

A key strategy here is no different than what you would expect in SD-WAN methods of understanding overlay vs underlay: Measuring inside the tunnel is an indicator of VPN performance, while measuring outside the tunnel is an indicator of the critical delivery path and providers used to connect your users to the infrastructure.

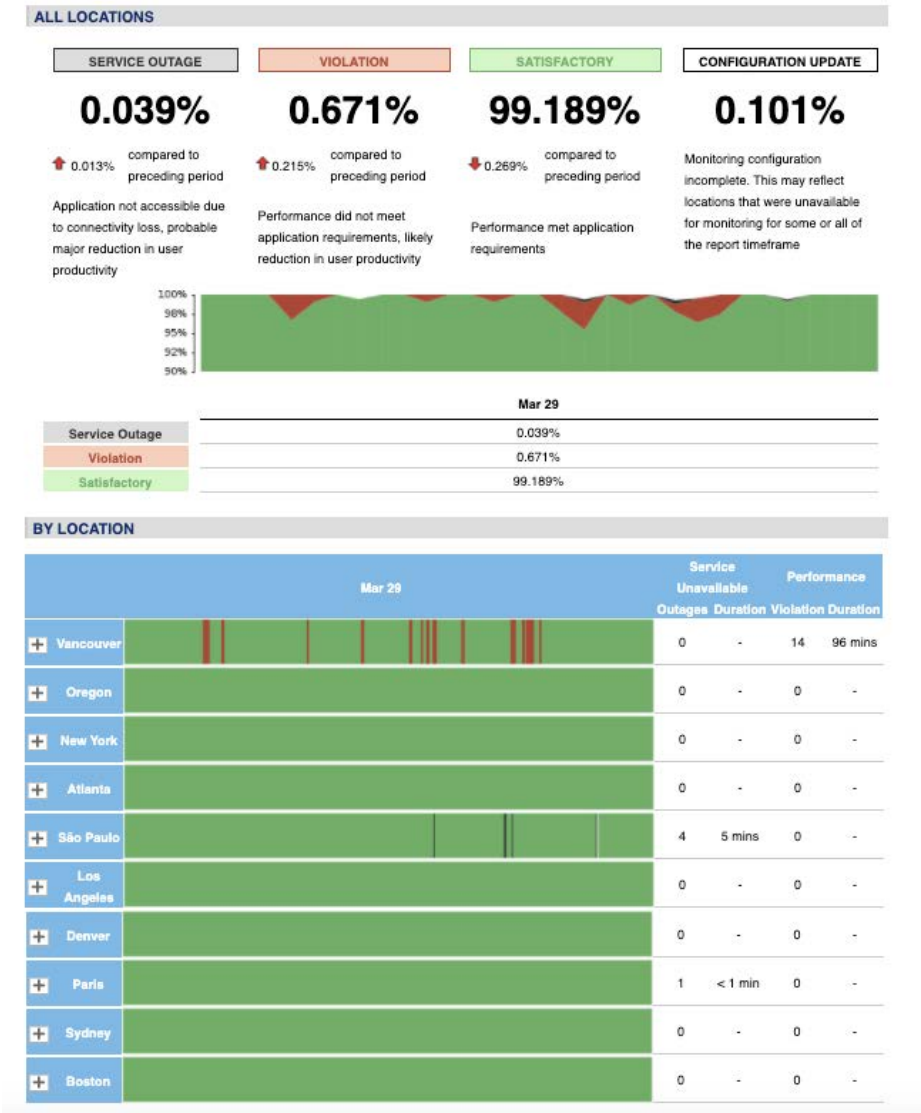


## Reporting

AppNeta provides a wide range of reporting options. Depending on who needs visibility into performance, AppNeta can provide regional roll-ups or allow IT to save specific lists to report on VPN tunnel health, gateway performance, or SaaS app performance. Reports within AppNeta can also auto-scale as more WFH endpoints are added to monitoring.

## Alerting

Leveraging a strategic set of monitoring targets and consistent alerting thresholds across the enterprise WFH environment, AppNeta will provide only the actionable alerts that are important to understand when the VPN is down or slow and impacting productivity. We understand the most important metric to be Data Loss during the Business Hours when users are active online. Alert profiles have duration to ensure that issues persist and excessive noise is not reported to IT.




## Critical Visibility from AppNeta

- Actively monitor network connections for all or critical remote users
- Measure inside and outside of VPN tunnels for service comparison
- Quickly identify if WiFi or client-side issues are the root cause of performance issues
- Understand end-to-end connections from WFH users to critical services
- Complete coverage with all major software form factors: PC, Mac, and Linux

**Request a demo today to learn more about AppNeta's 4-dimensional approach to network performance monitoring.**

### ABOUT APPNETA

AppNeta is the only network performance monitoring solution that delivers deep, actionable, end-to-end network performance data from the end-user perspective. With AppNeta's SaaS-based solution, IT and Network Ops teams at large, distributed enterprises can quickly pinpoint issues that affect network and business-critical cloud application performance, regardless of where they occur. AppNeta is trusted by some of the biggest Fortune 1000 companies, including 3 out of the 5 largest corporations in the world, as well as 4 out of the 5 largest cloud providers. For more information, visit www.appneta.com

1.800.508.5233 | SALES@APPNETA.COM | APPNETA.COM