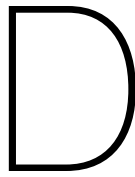


3 factors that help ensure safe, **fast, reliable** **network connectivity**





DIGITAL TRANSFORMATION efforts are causing organizations to

reevaluate connectivity. The entire user ecosystem – including employees, customers, partners, and vendors – requires strong and resilient network connections to work at the speed of business today.

What steps can IT leaders take to assure safe, fast, and reliable connectivity? That’s the question we asked the CIO Experts Network, a community of IT professionals, industry analysts, and other influencers.

Here are their insights into three factors that should be considered for network connectivity.

Improve network performance

Latency and network disruptions can cause untold user frustration and kill productivity. Yet the distributed workforce, digital transformation, and cybersecurity issues make it ever more imperative to ensure consistent, reliable network connectivity.

That’s why enterprises should act now to address performance issues, say the experts:

“Enterprises can’t expect to be running today’s businesses ‘as-is’ two to three years from now. Today leaders must consider growing supply chain risks, evolving to a hybrid future of work, leveraging AI [artificial intelligence]–driven experiences,

and testing AI/VR [virtual reality] – including digital twins and metaverse applications – as opportunities driving the second wave of digital transformation.” – Isaac Sacolick, president of StarCIO and author of Digital Trailblazer

“One way to provide the highest level of consistent network performance is to understand the workforce and customer journeys – to ‘see’ the network, which can also include human touchpoints through the eyes of the users, including their preferred devices.” – Gene De Libero, chief strategy officer, GeekHive.com

“Start with a full network and security audit. Based on the findings, the IT team should prioritize actions to remediate issues such as system

configuration and environment weaknesses, information handling processes, user practices, and gaps in security practices.” – Will Kelly, writer and analyst focused on the cloud and DevOps

Some network service providers can even provide separate direct connectivity to corporate networks for at-home and remote workers. Also, because many employees now work remotely, IT should be proactive in providing tips to help them maximize connectivity from their home office, said Peter Nichol, chief technology officer at OROCA Innovations.

Nichol explained, “First, check to ensure the modem is getting a signal. Next, validate [that] the router is receiving and broadcasting. Then, ensure the WiFi signal. Lastly, make sure friends or other access points aren’t draining bandwidth by changing the name of the home network.”

“Today leaders must consider **growing supply chain risks**, evolving to a **hybrid future of work**, ... **driving the second wave of digital transformation.**”

Provide safer connectivity

The cyberthreat landscape has become nightmarish. The sophistication of attackers makes it imperative to use robust cybersecurity measures. Yet these tactics shouldn’t degrade the user experience or network performance, said the experts:

“Internet-based attacks run on internet traffic. They take up bandwidth while jeopardizing the safety and security of data, apps, and users. You want to maximize cybersecurity while adding as little additional overhead as possible.”
– David Greer, thought leader and cybersecurity expert

“Make user security protocols simpler without reducing safety. Finding dual authentication platforms that reduce the frustration of checking basic business data is both a security and worker satisfaction issue.” – Frank Cutitta, CEO and founder, HealthTech Decisions Lab

“Consider a multilevel security model with clear business and technical checkpoints to keep pace with the increasing speed of security innovations. These checkpoints should cover UCaaS/VoIP [unified communications as a service/Voice over Internet Protocol] security, mobile app security testing, API [application programming interface] security offerings, layered managed data security services, or even locking down cloud security privileges through a next generation of privileged access management.”
– Adam Stein, principal,
APS Marketing

And don't forget to lock down public WiFi, said Jack Gold, president and principal analyst, J. Gold Associates, LLC. “The best avenue for protection is to not rely on public WiFi and instead outfit the workforce with 5G-enabled mobile devices, which are becoming affordable and hard to spoof,” he said. “As a result, 5G is more secure while also offering compelling speeds for nearly any application. If you must rely on public WiFi, at the very least equip the endpoint with a VPN [virtual private network] and strong security.”

Ensure network resilience

Another factor to consider for resilient network connectivity: a backup plan. Disruptions come in many forms: weather-related incidents, cybersecurity attacks, and routine maintenance or upgrade efforts.

To assist, wide-area network (WAN) redundancy is recommended:

“Procure a second and maybe third source of WAN connectivity for your business. Whether you roll your own SD-WAN/SASE [software-defined wide-area network/secure access service edge] using discrete CPE [customer premises equipment]-based network options or subscribe to a hosted/bundled cloud option, this is an essential business requirement for workers and clients, regardless of location. Also, architect a real-time customer data storage and disaster recovery solution. Storage virtualization, disk mirroring, and cloud-based hyperconvergence help businesses maintain up-to-date copies of data in geographically dispersed locations, not just in a single primary data center.” – Adam Stein

Ensuring safe, fast, and reliable connectivity should be an ongoing effort, said Scott Schober, president/CEO, Berkeley Varitronics Systems, Inc.

“Over the past few years, there has been a tremendous shift in wireless connectivity [in terms of] speed, throughput, latency, and lower costs,” he said. “IT leaders need to continually look at how they can improve communications and efficiencies. I think it is important for them to carefully embrace the improvements that wireless technologies continue to offer in conjunction with the internet and WANs.”

“Over the past few years, **there has been a tremendous shift in wireless connectivity [in terms of] speed, throughput, latency, and lower costs**”.

Learn how to improve your [network connectivity](#) experience by partnering with Spectrum Enterprise.

SE-MS-AT005

This post is brought to you by CIO. The views and opinions expressed herein are those of the author and do not represent the views and opinions of Spectrum Enterprise.

