Deploying Connected Laptops for Improved Hybrid Employee Security

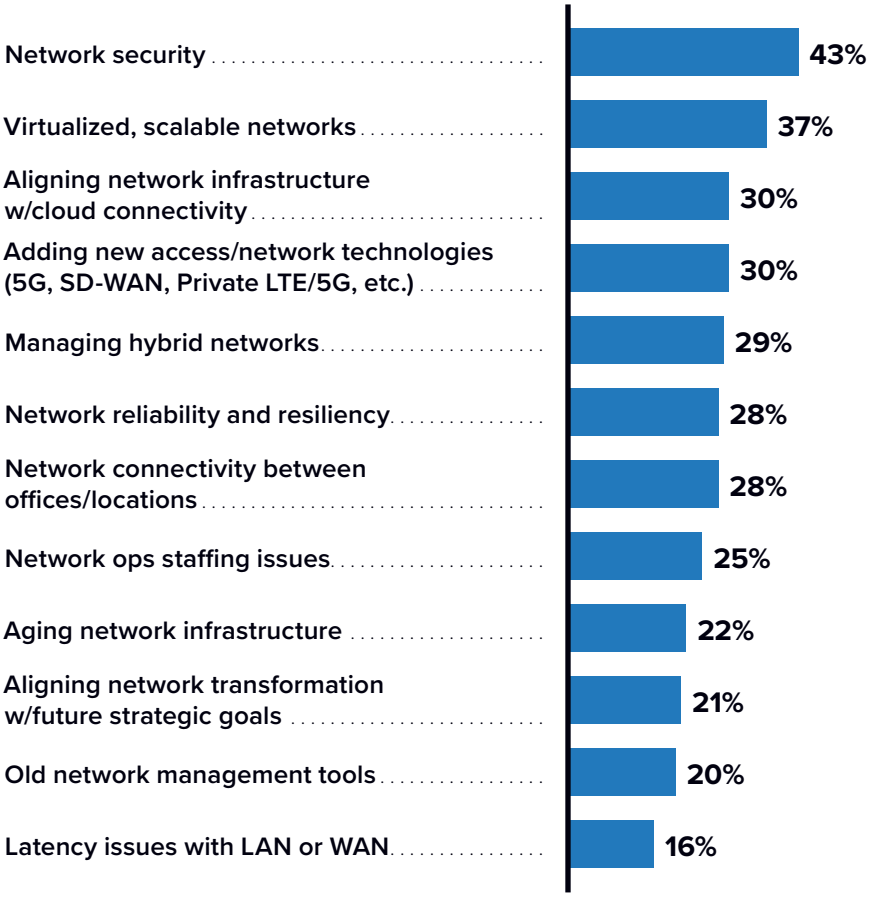
Utilizing laptops equipped with cellular connectivity can aid in protecting corporate networks and resources from external security risks

Jason Leigh
Research Manager,
Mobility, IDC

Pahul Preet Singh
Senior Research Analyst,
Mobile and IoT Communications Services, IDC

From a networking perspective, what are the top connectivity-related challenges your organization currently faces?

U.S. Companies' Top Connectivity-Related Challenges



n = 770, Base = 220 (U.S.); Source: IDC's *Worldwide Future of Connectedness Survey*, June 2023

Just over 43% of U.S. companies say that network security is the top connectivity-related challenge that their organization currently faces (*IDC Future of Connectedness Survey*, June 2023, n = 220). As a result, 68% of U.S. companies plan to increase spending on network security applications and tools over the next 12 months.

An often overlooked but nonetheless critical element of network security occurs at the connectivity layer, especially for remote, hybrid, and mobile employees. Nearly 60% of enterprises believe that mobile technology (devices, apps, and services) use by employees presents a serious risk to corporate data security, and 78% believe that the mobile operators they use provide adequately secure networks (IDC's *2023 U.S. Mobile Security Survey*, February 2023, n = 510).

Continue reading >

A key tool in helping improve network security is the connected or cellular laptop. While connectivity for employees working on the corporate campus can be reasonably controlled and secured, those employees working farther afield present a greater security risk.

The connectivity-related security risks are varied. Consider the work-from-home employee with minimal network security training who hasn't changed their Wi-Fi password in years and shares that connection with a spouse or kids, the road warrior hopping on the unsecured coffee shop Wi-Fi while en route to see a customer, or the field repair tech who cannot access maintenance manuals or process a customer payment on company point-of-sale systems due to a lack of broadband connectivity. In fact, more than 25% of enterprises report that Wi-Fi-based mobile device attacks (connecting to malicious/spoofed Wi-Fi) occur frequently or daily (IDC's *2023 U.S. Mobile Security Survey*, February 2023). Each of these connectivity scenarios presents unique challenges that can be addressed via the use of cellular laptops.

While there are some alternative solutions that also leverage cellular — mobile hotspots and smartphone-enabled hotspots — the link between those devices and the laptop could be susceptible to vulnerabilities. Ultimately, the fewer interconnects between the cellular network and the end-user device, the better from a network security perspective.

Bolstering Network Security with Connected Laptops

Given challenges that can exist in securing the connections of remote or hybrid workers, an increasing number of companies are investing in cellular laptops. Nearly 56% of U.S. companies increased spending on cellular laptops in 2022 (IDC's *Future Enterprise Resiliency & Spending Survey, Wave 9*, October 2022), with those increases seen across a myriad of industries. Some of that adoption may be driven by network security and employee productivity needs. However, for some highly regulated industries, such as healthcare and financial services, data protection requirements can lend themselves to the use of more secure connections by using cellular laptops.

Opting for a connected laptop helps ensure that employees are linked to a secure cellular network encrypted from the radio access network and through the core network, thereby helping to ensure the safety of company data. Since the connected laptops leverage the built-in security of a cellular network, companies may be able to reduce their spend on third-party security applications or software. Additionally, cellular-connected laptops can offer further cost-efficiencies by reducing the need for additional equipment for mobile employees (mobile hotspots) and eliminating the need for corporate-liable home broadband connections or reimbursements.

Produced by: IDC Custom Solutions
Info Snapshot, sponsored by Verizon
January 2024 | IDC #US51575723