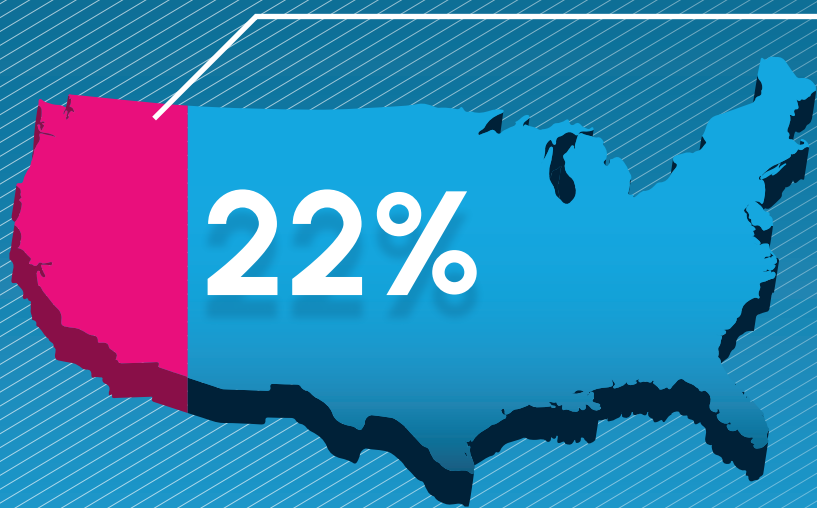


5G Connected Devices:

Superior Security for the Dispersed Workforce



22%



of US workforce is expected to work remotely by 2025



Working outside of traditional office settings has become the norm, increasing the risk of security breaches due to dependence on unsafe public Wi-Fi networks



5G connected laptop technology can help organizations connect securely from anywhere

In partnership with T-Mobile, The Futurum Group conducted the 5G Connected Laptop Survey to quantify the risks and uncover the scale of the opportunity with connected laptops.

In the office

Executives worry about the impact of remote work environments to their organizations, and many are concerned over their company's ability to withstand a cyberattack.

73%

of executives perceive remote workers as a greater security risk



On the road

Public Wi-Fi networks are unpredictable and may be unsecured

39%

of respondents confirmed that Wi-Fi attacks are their foremost security threat



In the field

The market for 5G cellular-enabled laptops is expected to grow from 1M in 2022 to nearly 10M in 2025, per Statista, driven by the need to connect work-from-anywhere business models.



Remote work environment

Connected laptops have a built-in cellular modem or wireless card that allows users to access the internet without using a Wi-Fi network, safeguarding against Wi-Fi based security threats.



Conclusion:

T-Mobile's nationwide 5G SA network, anti-tracking and spoofing features, and robust security portfolio provides a more secure connected experience. To learn more, access the report: **5G Connected Devices: Superior Security for the Globally Dispersed Workforce**,

[DOWNLOAD REPORT](#)