Connected laptops

Find out why public sector organizations from police and fire departments to healthcare agencies are choosing this secure, smart choice for reliable mobile communication—and new productivity.

By Patty Roze
Vice President
Verizon Public Sector

Cyber threats are escalating and the public sector is often the target. In response, more and more public sector organizations are turning to connected laptops as a strategy to help reduce risk and streamline communication. Here's why I think connected laptops are here to stay—and why their popularity will continue to rise.

A connected laptop is exactly what it sounds like—a laptop that stays connected to the internet thanks to built-in cellular connectivity via an eSIM or physical SIM card. A wide range of public sector organizations rely on connected laptops, which deliver a winning combination of seamless connectivity, enhanced productivity and improved security while providing reliable, cost-effective mobile communication.

Who uses connected laptops? First responders, police/sheriff departments, fire departments and other public safety groups benefit from the fast, always-available connectivity of connected laptops, which keep team members in touch during critical situations when every second counts. Large state and local agencies turn to them when they need fast, reliable and secure communication for mobile or hybrid workers. With a connected laptop, behavioral health workers, child support workers and others doing outreach gain a readily available connection to their co-workers, constituents and the internet, enabling them to work productively from almost anywhere. Colleges and universities use connected laptops to protect research and proprietary data.

Public Wi-Fi convenience comes at a cost

When we talk to our customers about connected laptops, some of the first questions they ask are about Wi-Fi. "Doesn't Wi-Fi do all that? Why pay for a connected laptop when I can use my own and get Wi-Fi almost anywhere for free?" These are fair questions to ask. Yes, Wi-Fi provides wireless connectivity. And it's convenient and often complimentary. But a lot of concerns lurk behind the convenience of Wi-Fi. Wi-Fi isn't always available, particularly for people working far afield. And its bandwidth may also be limited, hindering productivity.

Most importantly, public Wi-Fi is often vulnerable to cyber attacks. In fact, in a recent survey, 40 percent of respondents reported having their information compromised while using public Wi-Fi[1] Old-fashioned phishing attacks still fool users into giving up their sign-in credentials and other information. However, the attacks are becoming more sophisticated, using AI and other technologies to create elaborate fraud scenarios that can fool even tech-savvy team members. Our 2025 Data Breach Investigations Report (DBIR) looks at the latest public sector security incidents and breach trends.

Delivering high security that can keep organizations safe

In this era of increased threats and vulnerabilities, a growing number of government agencies, organizations and educational institutions are choosing the safe harbor that connected laptops provide. They're equipping their teams with connected laptops for fast, secure connectivity and other advantages. Why? Their reasons vary, but security is at the top of the list. No public sector organization wants to deal with the hassle and expense of a breach, ransomware attack or other security issue. Their communications are often sensitive, containing strategic organizational, financial or private personal information (PPI) – making it of high value to cyber criminals. And public sector organizations need to ensure that their operations are uninterrupted to continue serving their constituents and communities.

At Verizon, we offer a secure alternative – connected laptops that eliminate the vulnerabilities of Wi-Fi connectivity. Verizon is a major security innovator, and our Verizon 4G LTE/5G cellular network is protected by extensive built-in security. We built the Verizon 5G network from the ground up for maximum security. For example, the Verizon 5G radio access network (RAN) data is fully encrypted. Public Wi-Fi can't do that.

Bringing speed and reliability to connected laptops

Connected laptops depend on secure, reliable, fast and readily available connectivity. The Verizon network combines reliable connectivity with near-ubiquitous coverage. More than 99% of the U.S. population is covered by the Verizon network, with over 280 million people are covered by Verizon's 5G Ultra Wideband network. Its fast connectivity can streamline communication and collaboration – and raise productivity – for any team. For example, the Verizon 5G network can handle even the most bandwidth-intensive use cases for connected laptops, from traditional video conferencing to AI applications that require low latency. And it's America's most reliable 5G network.[2]

Simplifying device management while lowering costs

Public sector organizations providing laptops, tablets or other centrally managed devices eliminate one of the most significant sources of security issues – use of private devices, which are often shared with others, poorly managed and vulnerable to security breaches. That said, organizations want to be able to offer appropriate device options to their people, whether they're firefighters or educators. At Verizon, we work closely with key laptop manufacturers to ensure a broad selection of the latest models, form factors and price points certified for connectivity on Verizon's network.

When deciding to adopt connected laptops, I think it's essential to look beyond the initial purchase price to consider ongoing expenditures and risk reduction. Connected laptops simplify maintenance and upgrades by public sector IT groups, which often have limited resources. They don't require additional hardware, such as Wi-Fi hotspots or third-party security software. And while the damage and disruption caused by a security breach may seem abstract, its cost is very real. The financial, operational and reputational cost of stolen data or a paralyzing malware or ransomware attack cannot be underestimated.

Who should consider connected laptops?

The considerable benefits of connected laptops make them an appropriate option for many public sector organizations. Public safety organizations are consistently among the top users of connected laptops or other devices within the public sector community, since their mission-critical work requires security, speed and always-on connectivity. Any state or local agency, large or small, with hybrid or mobile outreach workers should consider connected laptops, particularly if they're handling sensitive or restricted data (e.g., healthcare data) that shouldn't be entrusted to public Wi-Fi. Higher education institutions might consider connected laptops if they need to secure research and proprietary data of students, faculty and administrators. Since they support all of these potential users, IT groups often drive the adoption of connected laptops because they simplify operations and maintenance while reducing risk. Device refreshes or software upgrades (e.g., a major Windows upgrade) often provide a convenient juncture for IT groups to adopt connected laptops.

The future will be even more connected

When we talk with our customers, partners and industry analysts, it's clear that connected laptops represent a growing category. IDC reported that 4G/5G connected laptop shipments rose by double digits in 2024[3] – and analysts expect this upward trend to continue. Why? Because more and more public sector organizations want to empower their teams with reliable, secure connectivity that boosts productivity, encourages innovation and enables them to achieve their mission.

Here at Verizon, we'll be ready with advice, expertise and incentives to help our customers make the move to connected laptops.

Find out more about connected laptops.

[1] The Real Risks Of Public Wi-Fi" Key Statistics And Usage Data," Forbes Advisor, October 2024
[2] Based on RootMetrics® State of 5G Report, United States, 2H 2024. Experiences may vary. Not an endorsement of Verizon.
[3] Worldwide Connected Notebook Forecast, 2023-2027, IDC.

verizon