Secure networking options.

Fixed Wireless Access

When making decisions about network access, agencies need to be aware and assess the security implications associated with network technology to help keep their digital assets protected. Cyber hygiene best practices include device security, cyber security education, and secure networking strategies.

Agencies considering adopting fixed wireless access (FWA) solutions – whether over 4G LTE or 5G networks – should understand both the security advantages of and potential pitfalls associated with the technology ahead of a deployment.

Modern security challenges

Data from the Verizon 2024 Data Breach Investigations Report (DBIR) shows that the three primary ways in which attackers access an organization are stolen credentials, phishing and exploitation of vulnerabilities. All of these attacks can occur regardless of network access type, whether it's cable, fiber, DSL or wireless.

Hackers take advantage of out-of-date systems, software, and known security issues. This shows that many modern cyber security challenges are network-agnostic, which means the most popular cyber attack methods typically don't focus on the network technology the agency uses to access the internet. However, outdated operating systems can be more vulnerable to security risks because they may lack the latest security updates and patches, serving as an entry point for hackers to infiltrate networks.

What is fixed wireless access?

Fixed wireless access is a type of 5G or 4G LTE wireless technology that enables fixed broadband access using radio frequencies instead of cables. FWA can be used to connect agencies, and organizations to the internet using radio waves to send high-speed signals that offer data transfer to and from devices. And as organizations are seeking fast speeds and quick deployment of access services to both pubic and private networks, FWA is becoming an increasingly attractive option.

Constituents in rural areas with minimal or no wired broadband options can benefit from a fixed wireless solution. The need for improved rural internet service has been recognized by both governments and businesses alike. The Infrastructure Investment and Jobs Act includes multibillion dollar investment in broadband with the aim to "deliver reliable, affordable, high-speed internet to every household." The U.S. Department of Agriculture's ReConnect Program furnishes loans and grants to provide funds for t construct, improve, or acquire the facilities and equipment needed to provide broadband service in eligible rural areas.

Compared to satellite connectivity, FWA reduces latency (it's faster and more efficient) and is less expensive. According to CTIA.org, FWA can be defined as a last-mile technology to provide internet service by using wireless links between fixed points – such as a cell tower and an antenna located at an individual location – instead of running fiber or cable lines.

FWA offers streamlined deployment, since in many cases it allows constituents to install the service themselves, rather than waiting for a technician to visit their location. In an FWA deployment, transmitters located on a cellular tower send their signal directly to a fixed location. Once a receiver accesses the wireless signal, it can then be connected to a router to provide wired or Wi-Fi access within a building, a temporary worksite, or even a food truck, depending on constituents' needs.

The benefits of FWA.

- Can provide high-speed internet to areas without existing infrastructure as FWA does not require a physical wired connection
- Reduces the need for separate wiring at all locations which provides cost-effective network architecture
- Provides an easy and fast deployment, for example, many FWA solutions are designed to be "plug and play"
- Provides flexibility in being able to move a router/receiver, such at a construction site
- Can achieve last-mile network access diversity as a strategy for agency application resilience
- Has the ability to manage and configure multiple locations nationwide over a centralized management platform

verizon

Use cases for FWA.

Forecasts show the total amount of 5G fixed wireless access connections are predicted to reach 236 million connections worldwide by 2028, highlighting the demand for connectivity.

Several use cases for fixed wireless access deployments for business include:

- Setting up branch offices in rural areas where a wired connection is not available
- Supporting internet access for remote employees working in hybrid office/home environments
- Providing connectivity after a natural disaster
- Installing temporary internet access for an event or interim location
- Providing additional capacity at large events to support increased crowds
- Providing secure internet access to agencies that set up pop-up locations
- Providing backup or failover options for companies that want to have extra protection, such as preventing "backhoe" incidents that can often disrupt a wired connection within an urban area

Wireless networking is secure networking

Point-to-point (P2P), or device-to-device, is a private transmission, meaning the voice, data, video being sent is not traveling over public internet lines. Additionally, 4G LTE and 5G NR (new radio) technologies encrypt data and signaling to help prevent it from being heard or accessed on the radio access interface. Verizon's fixed wireless access allows users to enjoy speeds comparable to a wired broadband connection while our 4G LTE or 5G Ultra Wide Band networks.

5G FWA and security

5G networks can provide secure networking because it has additional attributes such as separation of keys, backward and forward security for keys at handovers, idle mode mobility and secure algorithm negotiation. 5G also includes secure identity management, enhanced authentication and a core network architecture that can support network slicing, continuous secure connectivity for mobile devices and lower latency.

Agencies considering fixed wireless access secure networking options would benefit by working with a reputable provider that offers a robust suite of cybersecurity solutions to help identify and manage potential security issues. The Verizon Threat Research Advisory Center provides monthly webinars packed with insightful analysis to help unmask threat actors' evolving tactics, techniques and procedures (TTPs), and provides other insights to help you stay informed.

Security vulnerabilities

Did you know devices that connect to your agency's internet can put your entire agency at risk? Users on your network accessing business tools, social media, streaming services, or files are oftentimes unaware of the potential dangers of navigating to a malicious website or the consequences of clicking a seemingly innocuous link they received in an email. Constituents with questions about 5G security should discuss their security concerns with their FWA providers.

Verizon Business Internet Security Plus and Preferred are add-on solutions which can help block devices connected to your Verizon LTE or 5G business internet solution from accessing malicious sites or downloading malicious content. Every website request is checked for threats and zero-touch deployment delivers protection via the network with nothing to install. constituents can review reports on threats blocked via a special portal. And with Verizon Business Internet Security Preferred, constituents also gain the ability to manage which websites users can visit, using a customizable dashboard in the portal.

Help protect your agency by applying sensible internet security practices, such as data encryption, authentication, access control and proper employee training to avoid hacking attempts such as phishing or malware. The benefits of fixed wireless access and new 5G technologies provide agencies with more options to meet their business and security needs than traditional wired choices.

Learn more about how Verizon fixed wireless access can provide your agency with the right internet solution.

Learn more

To learn more about Verizon solutions and how it can keep your government locations connected, contact your Verizon Government Account Manager or call 1.877.920.0816

verizon