

Secure Remote User

In the age of digital transformation, cloud migration and remote work, employees need to access enterprise information from all of their devices, anywhere, anytime. This brings an increased risk of data breach, making it critical to extend security beyond the traditional perimeter and safeguard the enterprise's data.

Our Secure Remote User solution delivers a reliable and seamless experience thanks to its secure access edge (SASE) architecture and zero-trust access (ZTNA) principle. Regardless of where employees are working, they'll be connected to the application they need in a secure, compliant way.

We'll work closely with you to deliver high-performance, secure connections that have been built on a solid foundation of clear, defined access control policies. Based on SASE's ZTNA principle, no one, anywhere, can access anything, unless they're explicitly allowed. Our Secure Remote User solution facilitates secure access to applications and devices, wherever they are, from any device and location of the enterprise.

Key Benefits

Enhanced network security

Each user and device is evaluated and authenticated before they're granted access to specific applications, removing the risk of data breach. Workload and device are isolated, limiting the potential impact of a breach and lowering the risk of data loss or malware propagation.

Increased flexibility

Add or remove access policies and user authorization based on immediate business needs and adjust quickly to changing access requirements regardless of a user's location.

Key Features

This solution follows ZTNA principles with the following features:

- > Application segmentation of enterprise access
- > Strong multi-factor authentication (MFA)
- > Granular application and device-based application control
- > Application and network visibility
- > Policy-based, encrypted connections to the network

Simplified network management

Decrease IT administration burden by reducing the number of complex provisioning and provisioning policies for each location and endpoint.

Optimized performance and reliability

Proactive elimination of unnecessary hops through application segmentation, multi-factor authentication, device-based access control, encrypted connections and more.



Why Crown Castle?

Our unique, nationwide portfolio

We have approximately 90,000 square miles of fiber, towers and open access one of the largest

Our solutions

We have the network, the equipment and the expertise to meet your needs. Visit our [infrastructure solutions](#) page to learn more about our fiber, towers and open access solutions and how we can help you overcome your challenges.