MANAGED SOLUTIONS
Product Sheet

CROWN CASTLE

Secure Remote User

In the age of digital transformation, cloud migration and remote work, employees need to access sensitive company information from all of their devices, at any location. This brings an increase in potential entry points for cyber criminals, making it critical to extend security beyond the traditional perimeter and straight to the end-users' devices.

Our Secure Remote User solution delivers a reliable and seamless experience thanks to its secure access service edge (SASE) architecture and zero trust network access (ZTNA) principles. Regardless of where your employees are working, they'll be connected to the applications they need without compromising security or user experience.

We'll work closely with you to deliver high-performance network connectivity with integrated security that's based on your unique and clearly defined access control policies. Based on SASE's ZTNA principles of "trust no one, verify everything," our Secure Remote User solution facilitates secure access to applications and resources by verifying the user, device and context of the request.

Key Benefits

Enhanced network security

Each user and device are verified and authenticated before they're granted access to specific applications, systems or other assets. Workloads and resources are isolated, limiting the potential impact of a security breach and lowering the risk of data loss or malware propagation.

Increased flexibility

Adds or removes security policies and user authorization based on immediate business needs and reduces risks by controlling access to your network regardless of a user's location.

Simplified network management

Decreases IT administrative burdens by reducing the number of troubleshooting touchpoints and synchronizing security policies for certain locations and end users.

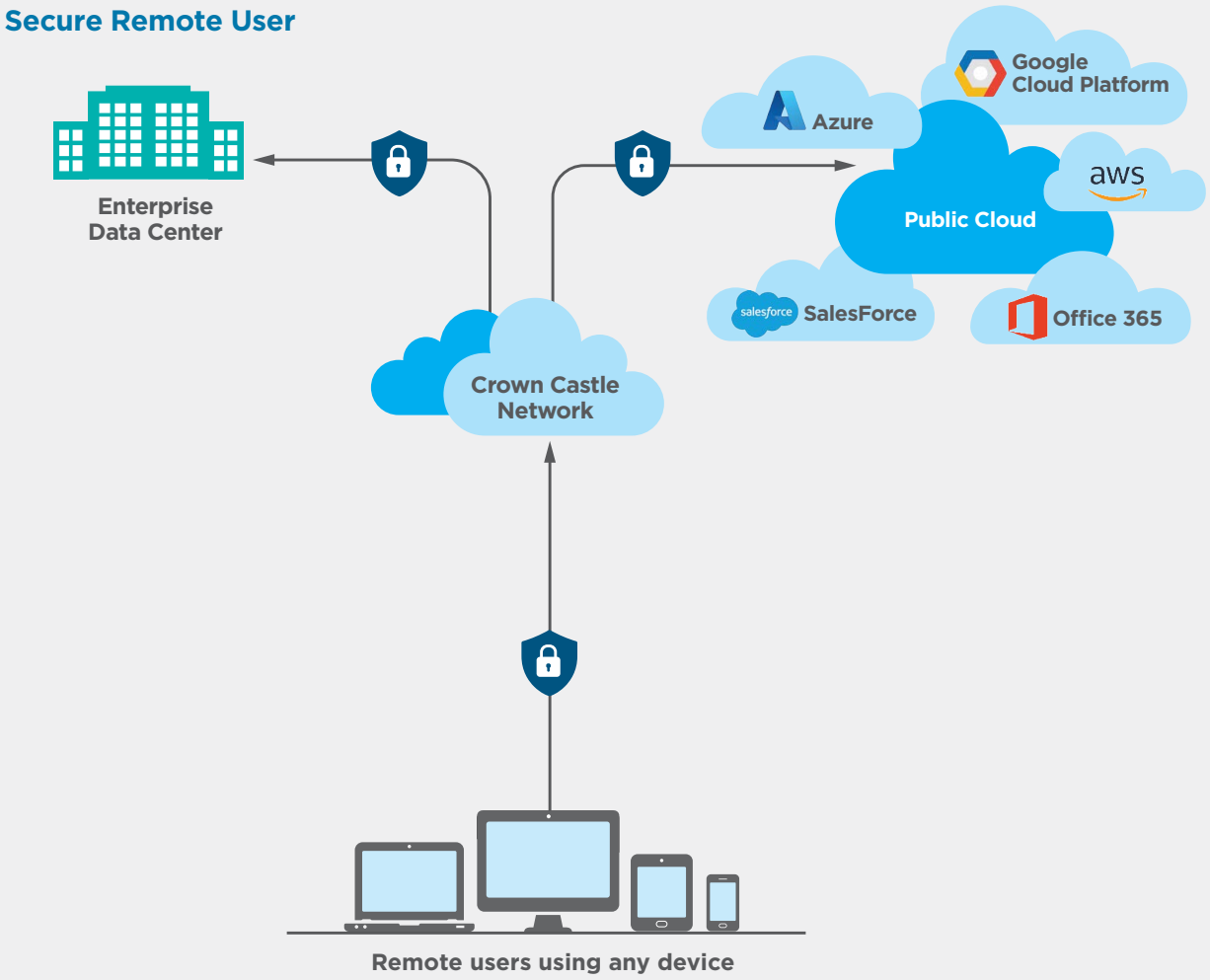
Optimized performance and reliability

Proactively eliminates security threats through application segmentation, multi-factor authentication, role-based access control, encrypted connectivity and more.

Key Features

This solution follows ZTNA principles with the following features:

- Application segmentation to restrict access
- Strong multi-factor authentication (MFA)
- Granular application and role-based application control
- Application and network visibility
- Private, encrypted connectivity to the network



Why Crown Castle?

Our unique, nationwide portfolio
With approximately 90,000 route miles of fiber, we own and operate one of the largest and densest fiber networks in the country with a presence in 23 of the top 25 US markets.

Our proven track record
In our 30 years of experience owning and operating network assets we've seen it all and we're always ready to adapt to changing network trends.

Our deep expertise
We've worked with nearly every industry so we understand your unique opportunities and challenges and can tailor solutions to meet your goals.

Our solutions
We have your networking and security needs covered. Visit our infrastructure solutions page to learn more about our suite of solutions and how they can solve your toughest challenges.

CROWN CASTLE

Crown Castle owns, operates and leases more than 40,000 cell towers and approximately 90,000 route miles of fiber supporting small cells and fiber solutions across every major US market. This nationwide portfolio of communications infrastructure connects cities and communities to essential data, technology and wireless service—bringing information, ideas and innovations to the people and businesses that need them.

For more information, please contact 1-833-635-0941 or visit **CrownCastle.com**