MANAGED SOLUTIONS
Fact Sheet

CROWN CASTLE

Secure Remote User Public Access

Today's cyber threat landscape is relentless, and malware infections remain one of the most common—and damaging—risks organizations face. While essential for everyday business operations, the internet is also a vast attack surface. A single visit to a compromised site can expose a device, and by extension, your entire network. As attacks grow in scale and sophistication, protecting users wherever they connect is more critical than ever.

The most common security solution for combating internet-borne malware is a secure web gateway (SWG). Traditionally offered as on-prem appliances, SWGs have been migrating to the cloud, as they offer scalable, centralized protection. Choosing the right SWG ensures your users stay secure—whether they're in the office, at home or on the move.

The challenge

Cloud-based SWGs offer convenience—centralized visibility, automatic updates and no on-premises deployments to manage. But routing all traffic through the cloud can strain performance, especially when combined with remote access solutions like zero trust network access (ZTNA) and VPN. This often leads to split tunneling, where web traffic bypasses the secure tunnel and goes directly to the internet, leaving you unprotected and vulnerable to attacks.

Another concern is SSL decryption. Cloud-based SWGs typically perform this in an uncontrolled environment, which can raise privacy and compliance concerns. Decryption may occur in unknown geographic locations or potentially insecure datacenters, creating potential blind spots in your security posture.

On-prem SWG solutions avoid these risks by scanning traffic locally, regardless of destination. They do, however, come with their own challenges, including complex and costly deployments, ongoing maintenance and the need to backhaul remote user traffic through a centralized, on-prem location. This creates what's known as the "trombone effect," increasing latency and compromising user experience and productivity.

The solution

Secure Remote User Public Access is a hybrid SWG that eliminates the major drawbacks that traditional SWGs face. It enables a higher level of security, improved compliance, better performance and simplified operations—and won't make you compromise on security and performance. It's simple to deploy and easy to manage. And, you have the ability to embed this in our converged network security platform, which includes additional features like ZTNA and firewall as a service (FWaaS).

Key components

Direct cloud access

No matter where your employees connect from—the office, home or anywhere in between—they're always protected. With Secure Remote User Public Access, there's no need to backhaul traffic through an on-prem location. And since our solution can be in two places at once, your employees are protected even when they are not connected to the corporate network. IT managers can rest assured that corporate devices are being defended whether connecting to your company network, or not.

Bypassed traffic protection

Web bypass rules, known as split tunneling, can reduce latency and increase application performance, but can also leave your employees unprotected and vulnerable to attacks. Secure Remote User Public Access protects your users even when performance supersedes security requirements.

Malware protection

Secure Remote User Public Access ensures that legitimate web traffic isn't carrying illegitimate software. Whether an attack comes from third-party ads, trojans or zero-day exploits, the malware protection capability has you covered. This includes:

- **Comprehensive protection** that delivers on-device network protection, web filtering, threat protection and more.
- **High-speed browsing** with on-device inspection, allowing users to avoid routing traffic through the cloud for security, as well as the associated latency, complexity and privacy concerns. The result is a better browsing experience with increased speed, privacy and compliance.

Key capabilities

- User traffic protection, even when not connected to the corporate network
- Single pane of glass management from device and cloud SWG instances
- TLS inspection is performed locally on the device with no decryption of traffic outside the user's endpoint
- Secure and fast direct-to-internet connectivity
- Bypassed traffic protection (split tunneling)
- Flexible policy settings
- Flexible deployment models, (device and/or cloud-side)
- Ability to enable multiple network deployments with network-specific SWG policies
- No on-prem deployment, management or maintenance
- Public Wi-Fi connection security
- Visibility into users' web activity by filtering events
- Category-based blocking (gambling, malicious sites, etc.) for both device- and cloud-based modes
- Multi-network deployments, each with unique security policies

VALUE-ADDED FEATURES

Browser Security

Your company runs on browsers, and with web-based attacks on the rise, traditional security solutions can't keep pace, especially with remote work and BYOD policies. Our Browser Security is an add-on feature that shields against zero-day phishing, malware, credential theft and data leakage—even through GenAI apps. Deployed as an extension across all major browsers, it delivers the protection your organization needs without compromising speed or privacy.

Browser Security offers an additional security layer to your Secure Remote User Public Access, enforcing your corporate internet access policies across managed devices. Every file downloaded through a browser is sent to the sandbox and inspected for malware. From there, our proactive Content Disarm and Reconstruction (CDR) technology will produce a sanitized version of the file in milliseconds.

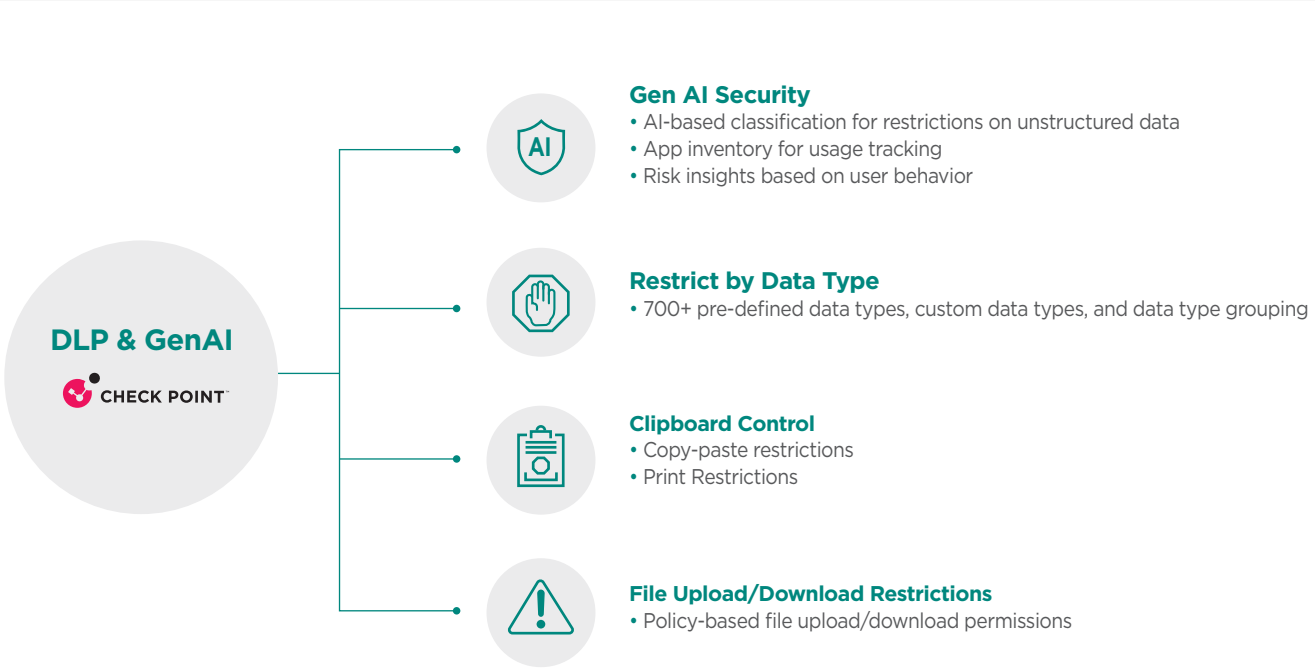
Preventing risky clicks

Website reputation intelligence and URL filtering prevent users from clicking on malicious links or accessing links that are blocked by your corporate policy, as defined by the admin in Browser Security. When a user performs a search through a search engine, the results will be marked with colored icons: green for safe, red for unsafe and orange for blocked by company policy.

Key capabilities

- Prevents users from visiting zero-day phishing sites, downloading zero-day malware, accessing non-compliant websites, re-using corporate passwords for non-business web content and more
- Provides fast web browsing, without adding latency, by eliminating the need to reroute traffic through the cloud for inspection
- Enforces corporate internet access policies across managed and unmanaged devices
- Allows single management over different platforms and browsers
- Enables simple deployment using an innovative extension directly into the browser
- Eliminates the risk from BYOD policies or third-party contractor network access
- Enforces user data privacy, keeping browsing history private to comply with data privacy regulations

Browser Security Additional Features		
Feature	**Secure Remote User Public Access**	**Browser Security add-on**
On-Device network protection	✓	
DNS filtering	✓	
URL filtering	✓	
TLS inspection	✓	
Malware protection	✓	
Single sign-on with IDP	✓	
SCIM identity synchronization	✓	
SIEM integration	✓	
Threat emulation (sandbox)	—	✓
Threat extraction (CDR)	—	✓
Zero-day phishing protection	—	✓
Data loss prevention (DLP)	—	✓
GenAI security	—	✓
Safe search	—	✓
Corporate password protection	—	✓
OCR analysis	—	✓
Microsoft Purview sensitivity labels	—	✓



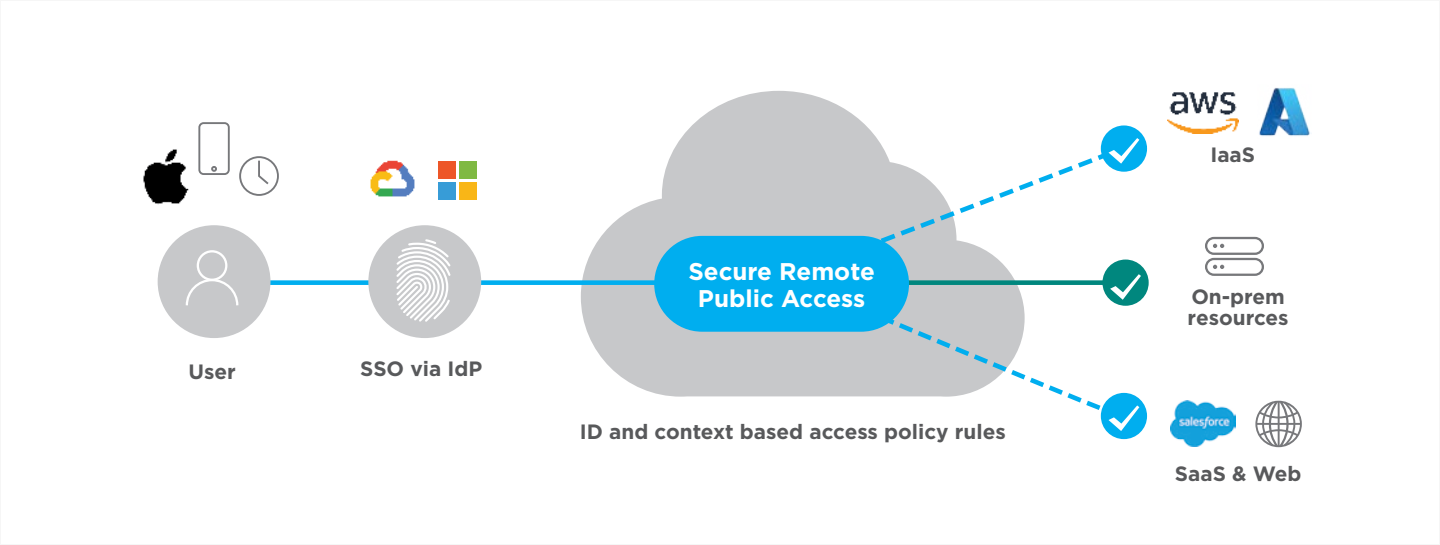
VALUE-ADDED FEATURES, CONT'D.

Private Access

Private Access is an add-on feature that helps organizations like yours manage network access for on-premises and remote employees while reducing the maintenance and scaling issues with legacy alternatives. Private Access is built on ZTNA principles, meaning each user only has access to the resources they need depending on identity and context (e.g., IP range, time of day, etc.). Private Access integrates identity provider (IdP)-based authentication, policy-based network segmentation, encrypted tunneling and real-time monitoring of device security posture and network activity—providing even more visibility and control to your IT team.

Key capabilities

- Integrates with your existing security policies across all remote users and resources for complete visibility into your network and security processes
- Reduces the attack surface by limiting access to only authenticated users and approved resources
- Monitors and maintains compliance by tracking network and application access
- Grants contractors and third parties limited access to specific apps without exposing your network
- Provides users with a streamlined, safer way to log in and authenticate
- Enforces the use of multi-factor authentication among users for extra security
- Provides your workforce with fast, reliable, high-performance connections to company resources



Policy rules

Within the platform, you can quickly segment your users into groups and create policies that define which of your connected resources (e.g., on-prem servers or apps, public cloud apps, etc.) are accessible to specific groups. Using firewall rules, your IT team can control how traffic flows within the network between objects, including users, groups, services and addresses, while device posture check denies access for endpoints that don't meet security parameters like certificates, endpoint security software, disk encryption and more.

Agentless access

Private Access also supports agentless, browser-based connections for application-specific access. Agentless access allows you to provide third-party contractors access to specific applications without exposing your entire corporate network, all while controlling and monitoring access with rules-based on identity, time, location and other relevant details.

If your employees are unable to install an agent or are using a personal device, they can easily log in to our web portal from their browser to see which corporate resources they can access.

Native remote desktop protocol (RDP) access

In some instances, a browser-based RDP application does not provide sufficient functionality, such as connecting to network printers and supporting dual monitors or a keyboard with a different language. Our native RDP capability gives your users access to zero-trust applications that run on their own client, enabling full functionality and user customization.

Dynamic user-based RDP

Hybrid workers often need to access their office desktop machines remotely, which traditionally requires setting up individual RDP applications for each user. We can help streamline this process and significantly reduce the management burden of RDP applications. Instead of managing individual applications for each user, you can set up a single application within the interface and users requiring access will automatically be validated and connected based on their unique identities.

Private backbone for fast remote access

Through our partnership with Check Point, our private backbone—with more than 70 points of presence (PoP) worldwide—offers the ability to connect your employees over a high-performance network to company resources. With support for multiple major encryption protocols, including IPSec, OpenVPN and WireGuard, you can keep connections private in the way that works best for your network infrastructure.

Private Access Additional Features			
Feature	**Private Access add-on**	**Feature**	**Private Access add-on**
Multi-platform agent	✓	Multi-factor authentication	✓
Context aware access	✓	Single sign on	✓
Agentless access to apps	Unlimited	Always-on	✓
Cloud firewall	Unlimited	User configuration profiles	Unlimited
Device posture check	Unlimited	Disable sign-out	✓
Private global network	✓	Cloud-based management platform	✓
Unlimited network tunnels	✓	Reporting and analytics	✓
Wireguard and IPsec support	✓	Log retention	60 days
Dedicated static IP	✓	SCIM identity synchronization	✓
Split tunneling	✓	API support	✓
Private DNS	✓	SIEM integration	✓
Cloud edge gateway	1 unit for every 100 users	Designated account manager	✓
Gateway bandwidth capacity	1000Mbps	Technical implementation support	✓
Local VPN access	✓	Self-service knowledge base	✓
Automatic VPN re-security	✓		

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 approximately 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 1-888-978-2982 or visit **CrownCastle.com**

CC-0825-0135