DATASHEET

# FireCloud Internet Access

## Enterprise-Grade Protection, Anywhere

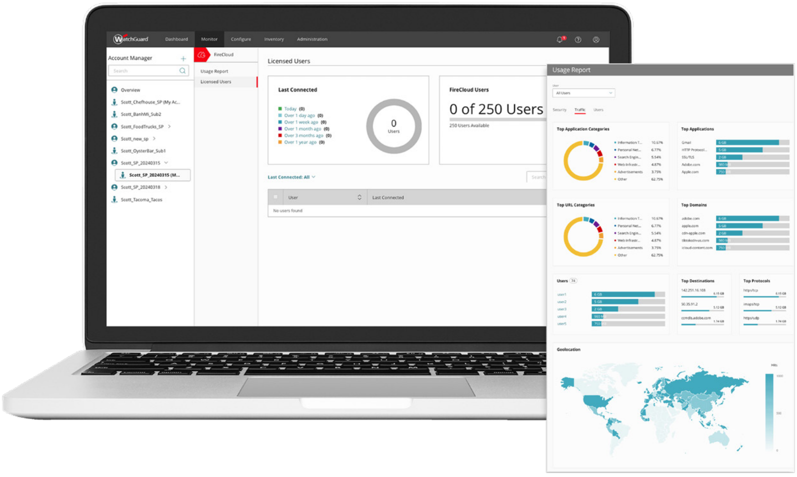
The modern workplace has evolved past the traditional office setup, with employees now working effectively from remote locations and their homes. This increased flexibility empowers businesses, but it has also blurred the boundaries of traditional networks, leading to significant security challenges. FireCloud Internet Access is a Cloud-based security solution designed to tackle these security issues while maintaining user productivity. A crucial component of a SASE (secure access service edge) solution, FireCloud Internet Access addresses the significant challenge of managing and securing remote user access to the Internet and  Cloud applications for users anywhere in the world.

## Powerful Security Beyond the Network Perimeter

While traditional perimeter security solutions are vital for safeguarding any organization, the rise in remote workers and the shortcomings of existing tools in tackling the complex threat landscape necessitate a solution that strengthens security for remote users. This new approach should provide the same level of protection that users working on-site at the organization receive.

FireCloud Internet Access is a Cloud-based security solution that extends on-premises security services to remote workers anywhere around the globe. It delivers a robust set of security and management features that include the protections enjoyed by on-premises workers, including URL filtering, intrusion prevention systems (IPS), and DNS security, to ensure safe and secure web and Cloud app access.

Use FireCloud Internet Access to protect your business from malware, phishing attempts, and other online threats, all with the flexibility needed to deploy and scale your security.



## Key Benefits of FireCloud Internet Access:

- **Enhanced Security Performance:** Extend firewall security policies and protections to remote workers with lightning-fast protection and a seamless user experience.
- **Streamlined Management & Efficiency:** Enforce consistent security policies across the organization to simplify implementation, strengthen environments, enhance efficiency, and reduce attack risks.
- **Comprehensive Threat Protection:** Defend against emerging threats with intrusion prevention systems and malware detection.
- **Secure Internet Access:** Control remote employee Internet access to enhance compliance and protect against web-based attacks.
- **Centralized Administration:** Cloud-based management reduces administrative burdens, automates updates and maintenance, and streamlines security event reporting.

## Seamless Global Security For Your Workforce

Empower remote workers and safeguard Cloud-hosted applications with FireCloud Internet Access. Seamlessly managed through WatchGuard Cloud, it integrates firewall-as-a-service (FWaaS) and secure web gateway (SWG) capabilities, delivering robust enterprise-grade security features. With WatchGuard Cloud, administrators can effortlessly configure global security services and policies, instantly propagated to our worldwide points of presence (PoPs). Users enjoy frictionless access by simply entering their credentials into the FireCloud client on any device, ensuring steadfast security coverage from wherever they connect.

### Stateful Firewall

Inspects network traffic, blocks malicious activity, protects sensitive data, and offers advanced features like intrusion prevention, malware detection, and URL filtering to defend against a wide range of threats.

### Intrusion Prevention Service (IPS)

Provides real-time protection against network attacks like spyware, SQL injections, and cross-site scripting by identifying and blocking malicious traffic to safeguard your network from potential breaches.

### Application Control

Enhances network security by preventing unauthorized software execution and potential breaches through granular control over which applications can run on devices.

### WebBlocker

Safeguards your network by blocking malicious websites and inappropriate content, empowering organizations to maintain a secure and productive online environment.

### Gateway AntiVirus

Scans incoming and outgoing traffic for viruses, malware, and other threats, providing comprehensive protection against cyberattacks to safeguard sensitive data and ensure business continuity.

### APT Blocker

Leverages AI and machine learning to identify and block sophisticated cyber threats, such as advanced persistent threats (APTs), zero-day exploits, and ransomware.

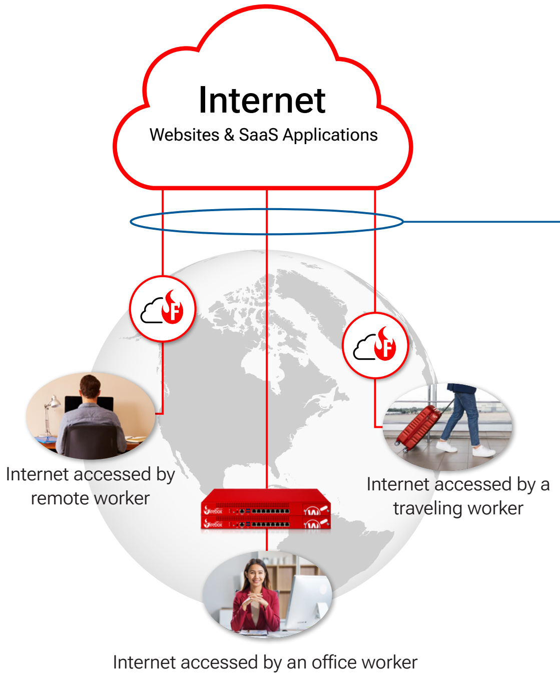
### DNSWatch

Offers advanced threat intelligence, real-time blocking, and DNS filtering to safeguard networks and users through a Cloud-based DNS security service.

### WatchGuard Cloud

Delivers streamlined visibility, control, real-time threat monitoring, and log and report data retention from a single interface, simplifying network security management, saving time, and empowering informed decision-making via a centralized management platform.

## Expand Firebox Security to Remote Workers


Internet
Websites & SaaS Applications
Internet accessed by remote worker
Internet accessed by a traveling worker
Internet accessed by an office worker

### Firewall as a Service (FWaaS)

- DNS Filtering
- Botnet Detection
- Intrusion Prevention (IPS)
- APT Blocker Cloud Sandboxing
- TLS Inspection
- Geolocations Blocking
- Gateway AnitVirus (GAV)

### Secure Web Gateway (SWG)

- WebBlocker URL Filtering
- Application Control

### User Authentication

- Connection Manager
- Identity Provider (IdP)

### Management Services

- Common policies and configuration
- Easy setup wizard
- SAML integration for IdP or set local accounts
- One platform: NetSec, Identity, and Endpoint

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. Part No. WGCE67802_013125