FEATURE BRIEF

FireCloud Total Access, The Secure VPN Alternative

The User VPN Challenge

For decades, virtual private networks (VPNs) were the go-to solution for enabling remote user access. They created encrypted tunnels into the corporate network, giving employees a way to connect to applications and data from anywhere.

VPNs were originally designed for a different era, when applications were hosted in data centers, most employees worked on-site, and being "inside the network" meant being "trusted." Firewalls and VPNs typically have public-facing IP addresses on the Internet, allowing authorized users to navigate the web and find entry points into the network. However, these access points are also visible to everyone, including cybercriminals who will attempt to breach them. This approach of broad visibility and open trust is no longer safe. The rise of remote work, cloud applications, and hybrid IT environments has turned VPNs into both a performance bottleneck and a significant security risk.

The FireCloud Zero Trust Alternative

Zero trust turns the VPN model on its head by assuming nothing is safe, "never trust, always verify" with each session. Every user, device, and session is authenticated, authorized, and continuously inspected, no matter where the connection originates. This model ensures remote workers receive the same level of protection as on-premises users, and dramatically reduces attack surfaces available to adversaries. FireCloud Total Access delivers these zero trust principles.

> VPN Challenges & Costs

- **Flawed Implicit Trust Model**
  Once connected, users have broad access, creating lateral movement risks.
- **Cyberattack Risks**
  Visibility to IP addresses and code complexity has led to brute force and vulnerability-based attacks.
- **Operational Complexity**
  IT teams must manage VPN policies, tunnels, and firewall rules across a sprawling environment.
- **User Frustration**
  VPN latency, dropped sessions, and poor performance erode productivity and increase support costs.
- **Hidden Operational Costs**
  Maintaining tunnels, certificates, firewall rules, and client agents creates significant costs in man-hours of management.
- **Compliance Risks**
  VPNs don't provide visibility, segmentation, or identity-aware controls regulators demand leading to compliance struggles.

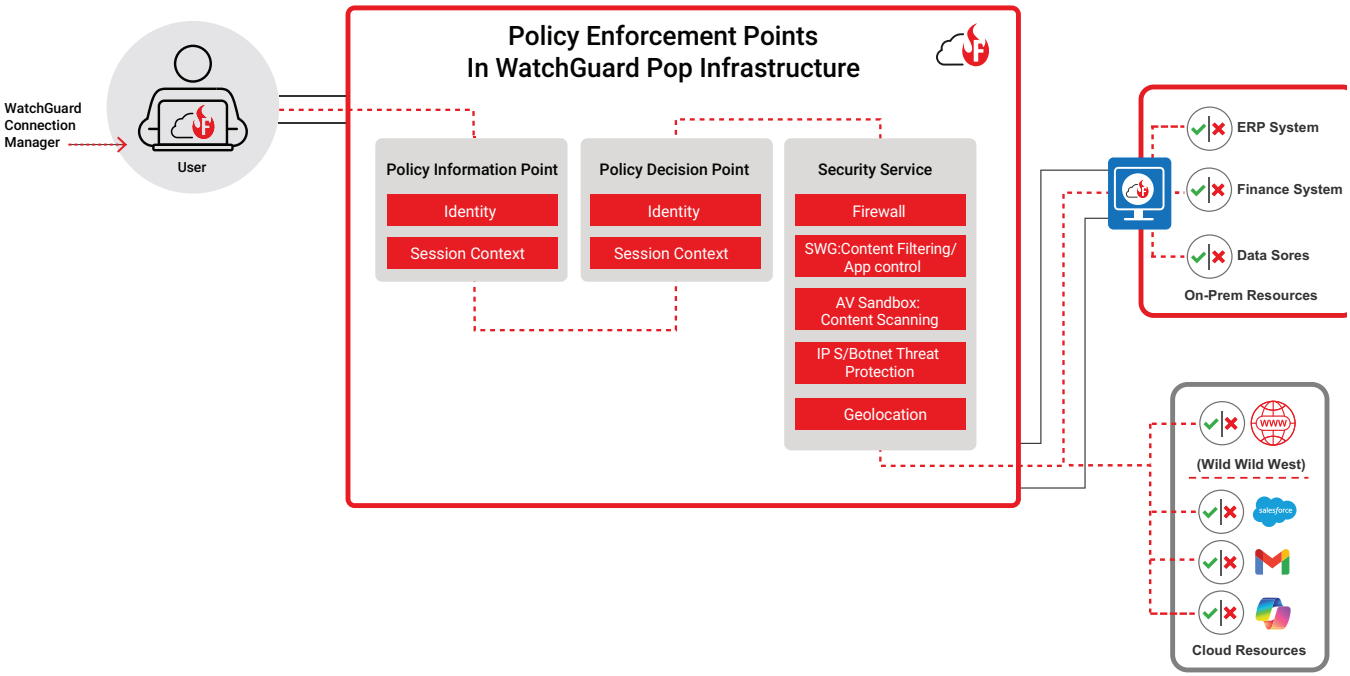
Identity-Centric Security
Access is granted based on verified identity and context, not network location.

Least-Privilege Access
Users only access the specific applications and resources they are authorized for, eliminating unnecessary exposure.

Continuous Validation
Security checks don't stop at login. Traffic is inspected in real time for threats, misconfigurations, or anomalies.

Unified Policy Control
IT teams can centrally enforce policies across all users and devices, eliminating complexity and gaps in coverage.

FEATURE BRIEF



FireCloud Total Access: Built for the Modern World

FireCloud Total Access combines Firewall as a Service (FWaaS), Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA) into a single, cloud-native platform delivering:

- **Zero trust:** every session is identity-verified, least privilege enforced
- **Centralized, cloud-native policy enforcement** across all users and devices
- **Optimized routing** with cloud points of presence for faster performance
- **Continuous inspection of traffic** for SaaS, private apps, and Internet access
- Purpose-built for **secure hybrid and remote access** in a cloud-first world

Real Talk:
A VPN isn't free.
It's a hidden cost center
and a security liability.

VPNs were built for yesterday's networks. Today's distributed, SaaS-heavy, hybrid environments demand a new approach; one that assumes nothing is trusted by default, enforces continuous verification, and delivers security at the edge. FireCloud Total Access is more than a VPN replacement. It is a zero trust-powered access platform that reduces risk, improves user experience, and creates a predictable, high-margin service opportunity.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases business scale and velocity while improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect over 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.