WatchGuard | BRALIN technology solutions

The New Perimeter:

Remote Access, Zero Trust, and the End of VPNs



TABLE OF CONTENTS

01 Introduction

02 Trust Nothing, Verify Everything

03 The End of VPNs, Really?

04 The Problem with VPNs

05 Zero Trust Network Access: A Modern Alternative

06 APractical Path Towards ZTNA

07 Introducing FireCloud Total Access





WatchGuard

01

Introduction

In the game of chess, a single weak point can expose a player's defenses, opening up vulnerabilities in their position that were once easily defended and not a concern.

The same is also true in network security. A development, such as a new technology release, a change in operations, or a discovered exploit, can have dramatic consequences on an organization's security posture.

Today, organizations are facing that exact scenario. Remote work, SaaS adoption, and cloud migration have blurred the network perimeter. Employees, contractors, and partners are connecting from anywhere, often on unmanaged devices. Relying on legacy security models like virtual private networks (VPNs) and banking on firewalls alone is risky in this environment. A single stolen password, a misconfigured device, a firewall software vulnerability, or a phishing email can lead to a breach that can be disastrous for a company.

And as you likely know, "security through obscurity" is a thing of the past. Small and midsize enterprises (SMEs) face the same cyber threats as the largest enterprises but have fewer resources to fight back. Attackers increasingly view these organizations as easy targets, often with weaker defenses, fewer security staff, and overextended IT teams.

Managed service providers like you are at a crossroads with VPN technology, which is becoming increasingly vulnerable.

The time for zero trust has arrived.



02 Trust Nothing, Verify Everything

For years,"zero trust"was seen asan enterprise buzzword.It meant complex frameworks, endless consulting engagements, and expensive tools that SMEs could neither afford nor manage.

That's no longer the case. Today, zero trust is both achievable and urgent for SMEs.

Zero trust turns the traditional security model on its head by not assuming *any* inherent trust. Instead, every access request, whether it's for a SaaS application, a private file store, or even the open web, is verified in real time. Access is granted only if the user's identity, device security, and overall context align with established policy requirements.

In a zero trust approach, youtrust nothing and verify everything.

Zero trust is no longer a someday project. For SMEs, it's a survival strategy. Remote work is here to stay, and security needs to be just as flexible. Waiting only increases risk, while attackers look for the easiest doors to open.

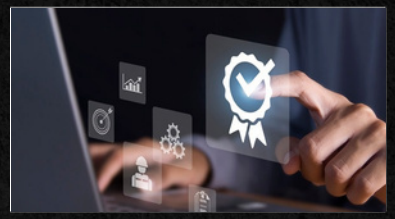
This has led to an acceleration among MSPs to shift away from VPNs, once the gold-standard of remote access security, toward Zero Trust Network Access (ZTNA) – a modern model better designed for our current threat landscape.

> Why Zero Trust?



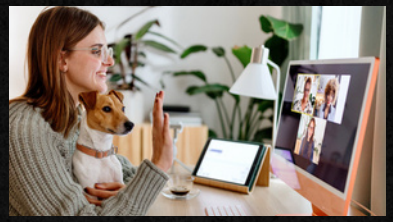
Attackers Exploit Trust

Once inside a flat network, attackers can move laterally. Zero trust limits their movement to only what's explicitly allowed in their position.



Regulatory Compliance Demands Proof

Cyber insurance demands zero trust controls. Compliance frameworks and cyber insurance policies expect organizations to enforce least-privilege and MFA.



Hybrid Work Is Permanent

Models trained in the cloud are distilled to the endpoints to decide in milliseconds, reducing latency and dependency on connectivity.



Breaches Are Business-Ending

Your customers simply don't have the cushion of billion-dollar budgets to recover. A single incident can be catastrophic.



03

The End of VPNs, Really?

> The Workplace Has Changed

- Employees access SaaS applications directly from the Internet, meaning they often work outside the corporate network perimeter.
- Teams are distributed around the world.
- Sensitive data lives across private data centers, public cloud environments, and hybrid systems.

A VPN has been the default way to connect remote employees to company resources for more than two decades. In its time, VPN was a breakthrough – creating encrypted tunnels back to the corporate network and giving road warriors a way in. There may have been a little slowdown, but it worked.

The VPN's all-or-nothing approach is no longer good enough. The gaps are ever-increasing, wearing down VPN usefulness into a niche service.

VPNs are one of the most targeted technologies in cybersecurity. Attackers exploit flaws in VPN software, steal credentials through phishing, and abuse misconfigurations to gain a foothold inside corporate networks.

Once inside, a compromised VPN connection can provide broad, flat access, making lateral movement simple. For customers relying on VPNs to secure hybrid and remote workforces, the risks are mounting, and the consequences of compromise can be devastating.

VPNs simply connect too much, too broadly, and too often at the expense of security and user experience. They are now as much or more a liability as they are a security solution. Organizations that continue to rely on VPNs are left managing complexity while attackers search for (and easily find) gaps and weaknesses.

Organizations that act now will protect their people, safeguard their data, and empower a productive and resilient workforce. Start with a practical, right-sized solution to protect your people, data, and reputation, without adding complexity.

The time for zero trust is now, and the shift from VPN to ZTNA is urgent.

WatchGuard

04 The Problem with VPNs

1 **Flat Network Access**
Once a VPN isconnected, users often have broad visibility into the network, creating unnecessary exposure.

2 **User Frustration**
VPNs are notorious for slow speeds, dropped sessions, and clunky login processes that frustrate employees, ensuring that they are seldom used given the choice.

3 **Operational Overhead**
ITteamsmust maintain concentrators, patch appliances, and constantly monitor capacity.

4 **Security Gaps**
VPNswere notdesigned for a SaaS-first world. They are inherently insecure, providing access but lacking inline protection against phishing, malware, or web-based threats. Attackers constantly exploit VPNs as a common entry point, regularly targeted by ransomware groups.



> 48% of organizations have experienced a VPN-related cyberattack, with 30% suffering multiple incidents.*

* https://www.cybersecurity-insiders.com/vpn-exposure-report-2025-why-organizations-are-adopting-a-modern-secure-access-strategy/

WatchGuard

05

Zero Trust Network Access: A Modern Alternative

VPNs werebuilt for a differentera. Today,ZeroTrust NetworkAccess (ZTNA)is the future of remote access – reducing risk, simplifying management, and improving the user experience.

ZTNA flips the VPN model on its head. Instead of granting network-wide access, it connects users only to the specific applications and resources they are authorized to use.

ZTNA aligns with the way modern businesses operate – distributed, cloud-first, and highly mobile.

Identity-Driven

Access decisions are based on user identity, device posture, and contextual signals – not simply a network connection.

ContinuousVerification

Trust is never assumed. Each session is evaluated, and policies are enforced in real time.

Per-App Access

Users are granted access to a single application, not the entire network, reducing lateral movement risk.

Inline Protection

By integrating with security services, ZTNA ensures that malware, phishing, and other threats are blocked before reaching users or apps.





06 A Practical Path Towards ZTNA

You might be thinking, “Isn’t SASE and ZTNA difficult to implement? Won’t I have to rebuild my entire security architecture and apply individual policies on a case-by-case basis for every customer? Do I even have the staff and the right skills to get this done?”

The good news – replacing VPNs doesn’t mean ripping out everything overnight.

What used to seem unattainable for customers is now accessible. Cloud-based services have made it much easier for MSPs to adopt zero trust by unifying critical features and visibility into a single platform, eliminating hardware requirements and centralizing policy enforcement.

These modern solutions are easy to use to use and designed to be multi-tenant to deliver zero trust protection to multiple customers simultaneously.

Modern ZTNA solutions give organizations a practical path to zero trust, starting with securing remote users against Internet-based attacks, then layering in identity-based access to private and SaaS applications.

> The Good News – Replacing VPNs Doesn’t Mean Ripping Out Everything Overnight.

WatchGuard

07 Introducing FireCloud Total Access

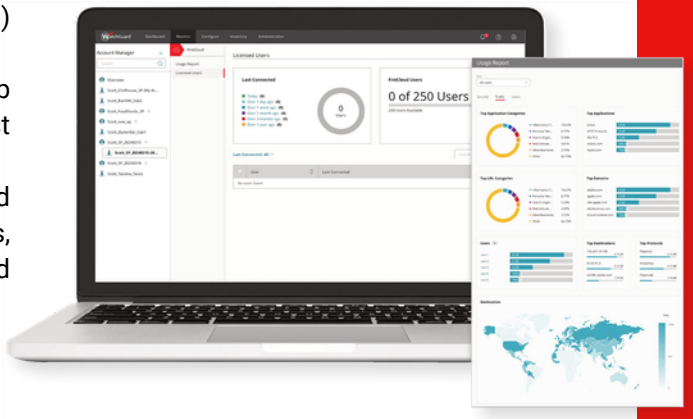
Securing a distributed workforce isn't about bolting on one more tool; it's about creating a unified, cloud-delivered approach that protects users wherever they work.

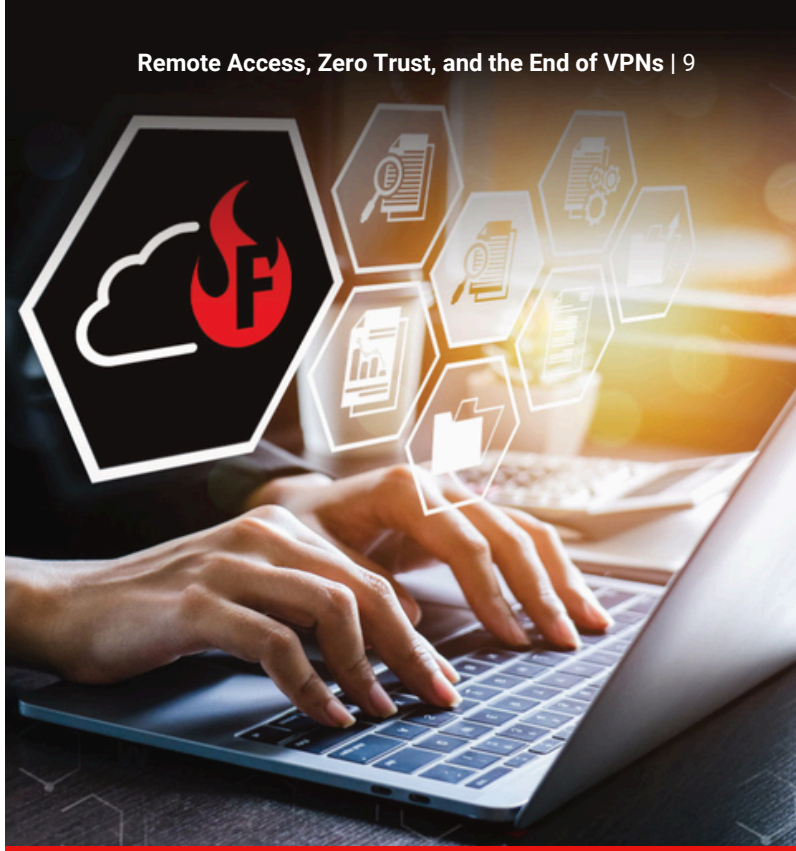
FireCloud Total Access is a cloud-native, scalable, recurring-revenue solution purpose-built for MSPs. It's ideal for protecting your customers' remote users without deploying hardware or VPNs. Managed through WatchGuard Cloud, it's easy to onboard, simple to scale, and perfect for partners looking to expand their Firebox security services to remote users without complexity.

It combines WatchGuard's unified secure access service edge (SASE) solution - including Firewall as a Service (FWaaS). Secure Web Gateway (SWG), and Zero Trust Network Access (ZTNA) - to protect remote workers and hybrid environments with seamless, always-on security and centralized management.

BecauseFireboxfeatures true multi-tenant architecture within WatchGuard Cloud, allowing you to manage dozens — or hundreds — of customer environments through a single interface. FireCloud's licensing is designed with MSPs like you in mind, enabling predictable monthly recurring revenue and simplified service packaging.

Unlike competitors that require enterprise-level overhead, FireCloud is sized and priced to help partners win in the SME and mid-market segments, while reducing operational complexity and increasing service margin.





> With one service, you can:

- Shield users from phishing, malware, and web threats.
- Enforce identity-based, per-app access to private resources.
- Manage policies and visibility from one cloud console.
- Scale easily without appliances or complex integrations.

Ready to Learn More?

Don't let sunk costs keep you tied to your VPN. Explore how FireCloud Total Access can help you retire VPN headaches and embrace a zero trust approach to secure connectivity.

Use our VPN cost calculator to see the true cost of your remote-user VPN and how FireCloud Total Access can pay for itself.

Get started now!



About WatchGuard

WatchGuard® Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers. Unlike others, WatchGuard delivers *Real Security for Real World* environments through its Unified Security Platform®, bringing networks, endpoints, and identities together with AI and zero trust advances for strong protection that scales. Trusted by more than 17,000 security resellers and managed service providers protecting over 250,000 companies, WatchGuard helps partners grow fast, eliminate operational drag, and deliver strong outcomes – without added vendors, consoles, or complexity. WatchGuard is headquartered in Seattle, Washington, with offices worldwide. Learn more at WatchGuard.com.

NORTH AMERICA SALES 1.800.734.9905 INTERNATIONAL SALES 1.206.613.0895 WEB www.watchguard.com

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. ©2025 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, Firebox, and Unified Security Platform are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67894_120925

WatchGuard