DATA SHEET

Remote WorkForce ZTNA

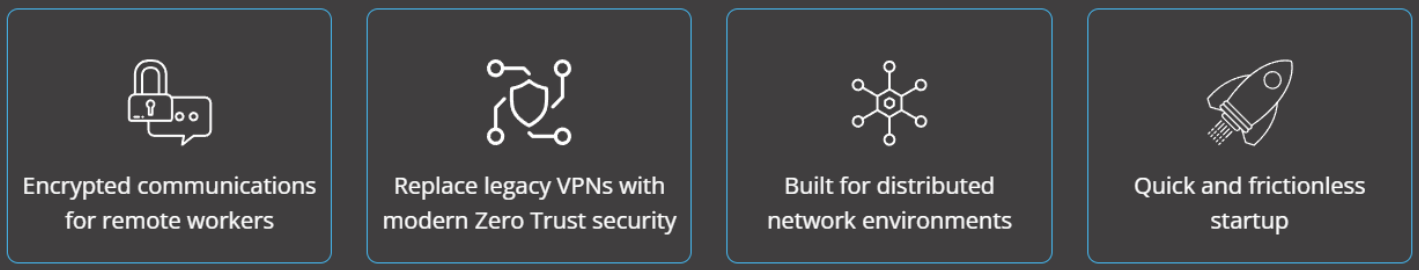
Zero Trust Security Purpose-Built for SMEs

Experience Zero Trust the Way It Should Be

Remote WorkForce ZTNA delivers enterprise-grade Zero Trust Network Access designed specifically for small and medium businesses. Get effortless deployment, fortified security, and limitless scalability without the complexity and costs of traditional enterprise solutions.

Core Value Proposition

Encrypted Communications for Hybrid Workers and Distributed Networks



Security Foundation

- Implement end-to-end encryption for all user communications
- Upgrade your cybersecurity with modern ZTNA architecture
- Employees only have access to IT resources that they are specifically authorized to use
- Enhance online protection with Multi-Factor Authentication (MFA)
- Malware blocking prevents access to known sources of viruses, phishing attacks, etc.

Common Use Cases & Benefits

Real Solutions for Real Business Challenges

Primary Use Cases

Secure Remote Work Enable employees to securely access company resources from home, coffee shops, or anywhere. Replace legacy VPNs with modern zero trust architecture that provides better security and user experience.

Third-Party Access Provide contractors, vendors, and partners secure access to specific resources without exposing your entire network. Granular permissions ensure users only access what they need.

BYOD Security Secure personal devices accessing corporate resources. Verify device health and compliance before granting access, protecting against compromised endpoints.

Cloud Migration Modernize your security architecture as you move to the cloud. Seamlessly secure access to cloud applications and hybrid environments.

Compliance Requirements Meet regulatory requirements for data protection and access control. Comprehensive logging and reporting support compliance audits.

The Challenge for SMEs

Legacy tools like VPNs and firewalls were built for centralized workplaces—but today's SMEs are decentralized, cloud-enabled, and location independent. These traditional solutions:

- Create excessive access, increasing lateral movement risk
- Fail to protect hybrid workers users and cloud-based apps
- Complicate management and reduce network speed
- Offer outdated protection against modern threats

Core Features & Capabilities

Comprehensive Security Without Complexity

Primary Features

Provides direct access to all company networks.

Including LANs, cloud-based (AWS/Azure/GCP) and SaaS

Users can easily access authorized resources.

From wherever they are (in office, at home, traveling), to wherever they are implemented (LAN, Cloud-based, SaaS)

Private Communications

End-to-end encryption for all user communications. Secure tunneling ensures data privacy and integrity.

Easy Management

Centralized cloud-based management console. Configure policies, monitor activity, and manage users from anywhere.

Multi-Factor Authentication

Enhanced protection with MFA integration. Supports various authentication methods including SMS, email, and authenticator apps.

Malware Blocking

Real-time protection against malware, phishing attacks, and known malicious sources. Keep your network clean and secure.

Real-time Monitoring

Comprehensive visibility into user activity, device status, and security events with detailed reporting and analytics.

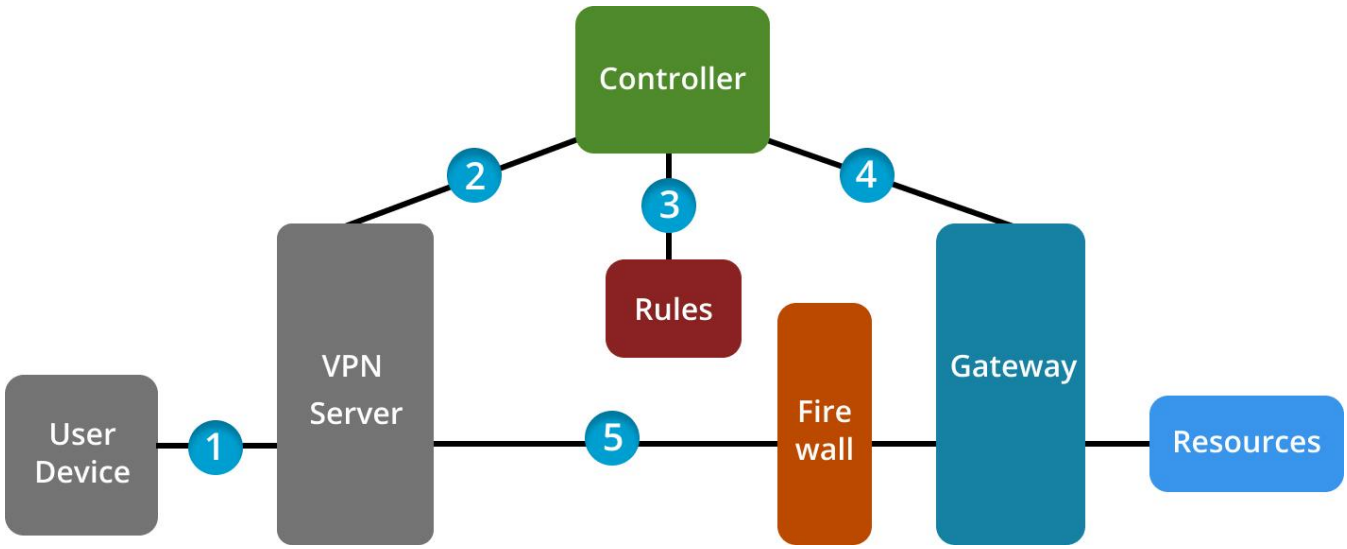
Seamless Integration

Works with existing infrastructure – networks, resources and devices.

How it Works

Zero Trust Network Access (ZTNA) operates on the fundamental principle that no user or device should be trusted by default, regardless of their location or network connection. When a user attempts to access a resource, ZTNA solutions first authenticate and authorize the user through multi-factor authentication, then establish an encrypted tunnel between the user's device and the specific application or resource they need. This connection bypasses the traditional network perimeter entirely—users never gain access to the broader network infrastructure. Instead of routing traffic through a central data center like traditional VPNs, ZTNA creates point-to-point connections using software-defined perimeters that are dynamically provisioned based on user identity, device posture, and contextual factors like location and time.

The technical architecture typically involves three core components: the ZTNA client software on user devices, a cloud-based policy engine that orchestrates access decisions, and ZTNA connectors deployed near applications and resources. When a user initiates a connection, the policy engine evaluates their identity credentials, device posture and behavioral patterns against predefined access policies before granting permission to specific applications. The connectors then establish secure, encrypted micro-tunnels using protocols like TLS or IPSec, creating isolated pathways that prevent lateral movement across the network. This approach enables granular access control down to the application level while maintaining visibility through continuous monitoring and logging of all connection attempts and data flows, allowing organizations to detect anomalies and respond to threats in real-time.



A Smarter Path: Zero Trust Network Access (ZTNA)

ZTNA is built for the modern workforce. It operates on the principle of "never trust, always verify," continuously checking identity, device posture, and user behavior.

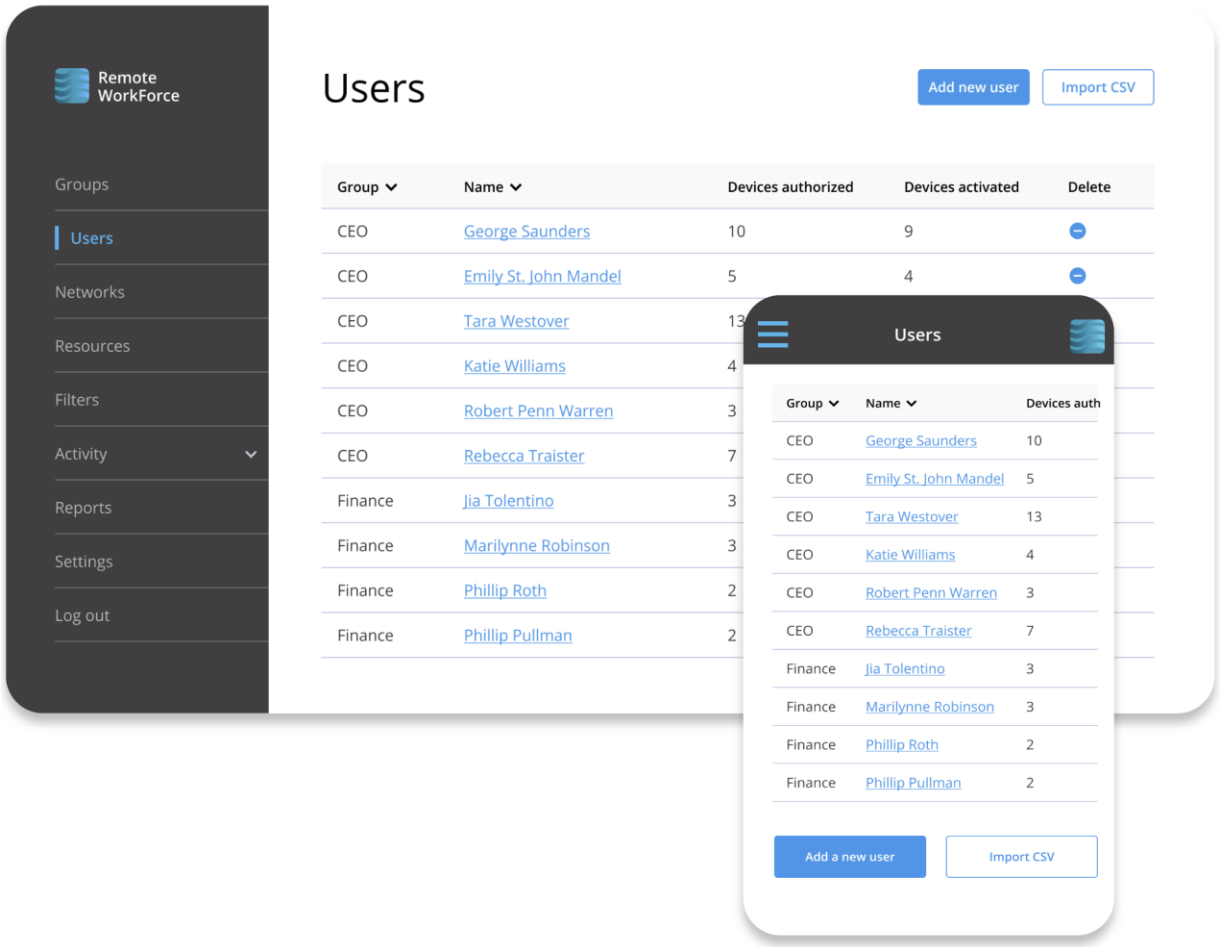
Remote WorkForce ZTNA vs Traditional VPN

Feature	Traditional VPN	Remote WorkForce ZTNA
Security Model	Perimeter-based (trust but verify)	Zero Trust (never trust, always verify)
Network Access	Full network access	Application-specific access only
Device Verification	Limited	Comprehensive
User Experience	Slow, clunky connections	Fast, seamless access
Scalability	Hardware limitations	Cloud-native, unlimited scale
Management	Complex, on-premises	Simple, cloud-based
Deployment Time	Weeks to months	Minutes to hours
Total Cost	High (hardware + maintenance)	Low (subscription-based)
Malware Protection	Not included	Built-in protection
Multi-Factor Auth	Optional add-on	Integrated

Quick and Easy Implementation Timeline

- Define companies
- Register users
- Define networks
- Install Gateway – reports access details
- Discover resources
- Apply ZTNA permissions
- Use in Discovery mode
- Switch to Operating mode and ZTNA permissions are enforced

Implementation in hours, not weeks.



Flexible Offerings

Not every SME has assets in the cloud or needs a full-on ZTNA. That's why we offer three different versions of Remote WorkForce:

Capabilities

	BASIC VPN	ENHANCED VPN	ZTNA
SECURITY			
Encrypt all Internet communications	✓	✓	✓
Direct access to corporate networks		✓	✓
Zero Trust security for corporate IT resources			✓
FILTERING			
Malware Filtering	✓	✓	✓
Customized block domains	✓	✓	✓
REPORTING			
Report time on/off network	✓	✓	✓
Detailed reports of user on-line activities		✓	✓
Specific IT resources accessed			✓

Each User can have up to 5 devices with unlimited usage. SMBs can have a 30 day trial period at no charge.

Summary

Remote WorkForce ZTNA transforms how SMEs approach cybersecurity. By replacing legacy VPNs with modern Zero Trust architecture, businesses can:

- **Enhance Security** - Comprehensive protection against modern threats
- **Improve Productivity** - Seamless access from anywhere, any device
- **Reduce Costs** - Eliminate expensive hardware and maintenance
- **Simplify Management** - Cloud-based console with automated features
- **Ensure Compliance** - Built-in reporting and audit capabilities

Contact your account executive to make Remote WorkForce ZTNA available to your clients.