Competitive Battlecard: Remote WorkForce Enhanced VPN vs. SSL VPN

Target Audience

MSPs, and decision-makers evaluating VPN solutions for SMB remote workforce connectivity. Anyone still using the SSLVPN protocol. Sophos, Fortinet, Palo Alto, SonicWALL, etc. all have critical vulnerabilities.

Key Differentiators -- Why Remote WorkForce VPN Wins

Category	Remote WorkForce VPN (Winner)	SSL VPN (Disadvantage)
Security Architecture	**Modern cloud-based security** with real-time malware protection and automatic threat updates.	Legacy SSL VPN architecture with **known security vulnerabilities** requiring constant patching and updates.
Multi-Network Intelligence	**Intelligent routing** to multiple corporate networks (LANs, AWS, Azure, GCP) with automatic optimization and discovery.	Basic network access with **manual configuration** required for each network connection and limited multi-cloud support.
Deployment & Setup	**Cloud-based deployment in hours** with zero on-premises hardware requirements.	Requires **on-premises appliance setup**, firmware management, and days to weeks of configuration.
Total Cost of Ownership	**No hardware costs, no maintenance fees.** Simple per-user monthly pricing with no contracts or minimums.	**Expensive hardware appliances**, annual maintenance contracts, complex licensing tiers, and ongoing IT overhead.
Management Complexity	**Intuitive cloud console** designed for non-technical administrators with automated updates and zero-touch management.	Complex enterprise interfaces requiring **specialized IT expertise**, manual firmware updates, and ongoing maintenance.
Scalability	**Instant user provisioning** and automatic scaling without hardware limitations or performance bottlenecks.	**Hardware-bound limitations** requiring appliance upgrades, capacity planning, and performance monitoring for growth.

Remote WorkForce VPN

Category	Remote WorkForce VPN (Winner)	SSL VPN (Disadvantage)
Remote User Experience	**Seamless multi-device support** (up to 5 devices per user) with intelligent connection optimization and reliability.	Device limitations, **connection instability** common with SSL VPN protocols, and inconsistent performance across devices.
Monitoring & Reporting	**Built-in comprehensive reporting** including time tracking, network usage analytics, and security insights.	Limited reporting capabilities often requiring **additional management tools** and third-party integrations.
MSP Friendliness	**Native multi-tenant architecture** with simple client onboarding, centralized management, and white-label options.	**Complex partner programs** with steep learning curves, certification requirements, and limited multi-tenant capabilities.
Support Model	**Direct MSP-focused support** with quick onboarding, training included, and dedicated account management.	Support primarily through **channel partners** with enterprise-focused documentation and complex support tiers.

Sales Positioning Statements

"Close Your SSL Vulnerabilities Today"

"Traditional SSL VPN technology has well-documented security vulnerabilities that put your business at risk. Remote WorkForce VPN uses modern, secure protocols with built-in malware protection - giving you enterprise-grade security without the enterprise complexity."

"Eliminate Hardware Dependencies"

"Why maintain expensive on-premises VPN appliances and deal with capacity limitations when you can get superior functionality in the cloud? Remote WorkForce VPN eliminates hardware costs, maintenance headaches, and gives you instant scalability at a predictable monthly cost."

"Multi-Network Intelligence vs. Basic Connectivity"

"SSL VPN gives you basic network tunneling. Remote WorkForce VPN gives you intelligent routing across all your networks - on-premises LANs, AWS, Azure, Google Cloud - with automatic optimization and discovery that learns your environment without manual configuration."

"Built for Modern SMBs, Not Legacy Enterprise"

"Traditional SSL VPN solutions were designed for large enterprises and their complex requirements. Remote WorkForce VPN was built from the ground up for modern SMBs - simple pricing, easy management, cloud-native architecture, and features that actually matter to growing businesses."

Objection Handling

Common SSL VPN Objections & Responses

"We already have SSL VPN infrastructure in place"

Response: "That infrastructure is actually costing you more than you think - hardware maintenance, security patches, limited scalability, and the IT overhead to manage it all. Plus, you're missing out on modern features like intelligent multi-network routing and built-in threat protection that your remote workforce needs today."

"SSL VPN is a proven technology"

Response: "Proven, yes - but also proven vulnerable. SSL VPN has documented security issues and requires constant patching. Remote WorkForce VPN uses modern protocols that were designed with today's threat landscape in mind, not technology from 15+ years ago."

"We need on-premises control"

Response: "What you really need is reliable, secure access for your team. Cloud-based VPN actually gives you more control - instant updates, better visibility, and no single point of failure from hardware issues. Plus, you can still access all your on-premises resources."

Advantages Summary

- **No SSL vulnerabilities** - Modern protocols vs. legacy SSL VPN technology
- **Intelligent multi-network routing** vs. basic tunnel connectivity
- **Cloud-native scalability** vs. hardware-bound limitations
- **Built-in threat protection** vs. basic network tunneling
- **Comprehensive monitoring** vs. limited visibility and reporting
- **Zero maintenance overhead** vs. appliance management burden
- **Transparent pricing** vs. complex licensing and hidden costs
- **MSP-optimized** vs. enterprise-focused solutions

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

© 2025 Private Communications Corporation. All rights reserved. Remote WorkForce VPN is a trademark of Private Communications Corporation. All other trademarks are property of their respective owners.

Remote WorkForce VPN