myworkdrive

2025

MyWorkDrive Buyer Brief

Secure File Access Without Migration

+1 (415) 692-1843
support@myworkdrive.com
101 Europa Dr, Suite 150
Chapel Hill, NC 27517

Why IT Teams Choose MyWorkDrive

Eliminate VPN friction in hours, not months

Stop VPN tickets, performance complaints, and security exposure for file access. Users get instant HTTPS access to existing files while data stays exactly where it is.

Keep what works, fix what doesn't

No migrations, no re-permissioning, no disruption. Your NTFS permissions, Microsoft 365 ACLs, and identity provider remain unchanged. Add modern controls like DLP and device approval without touching storage.

Right-size your Microsoft licensing

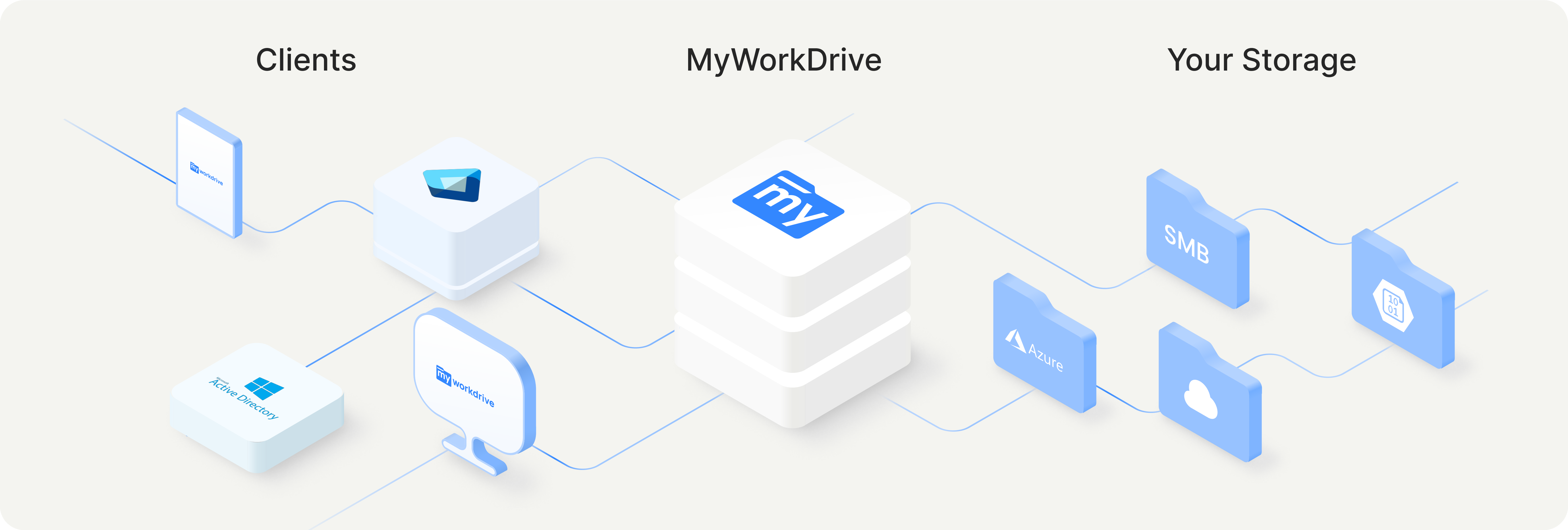
Enable browser editing for light users while files stay on SMB shares. Heavy users keep desktop Office. You control who gets what level of Microsoft 365 access.

What MyWorkDrive Does

A secure access broker for files you already have. Users connect over HTTPS from web browsers, mapped drives, or mobile apps. Your identity provider handles authentication (Active Directory with SAML SSO, or Microsoft Entra ID with native sign-in).

Files never move to MyWorkDrive servers.

For browser editing, files stage temporarily in your OneDrive or SharePoint tenant, then write back automatically.



Architecture & Storage Support

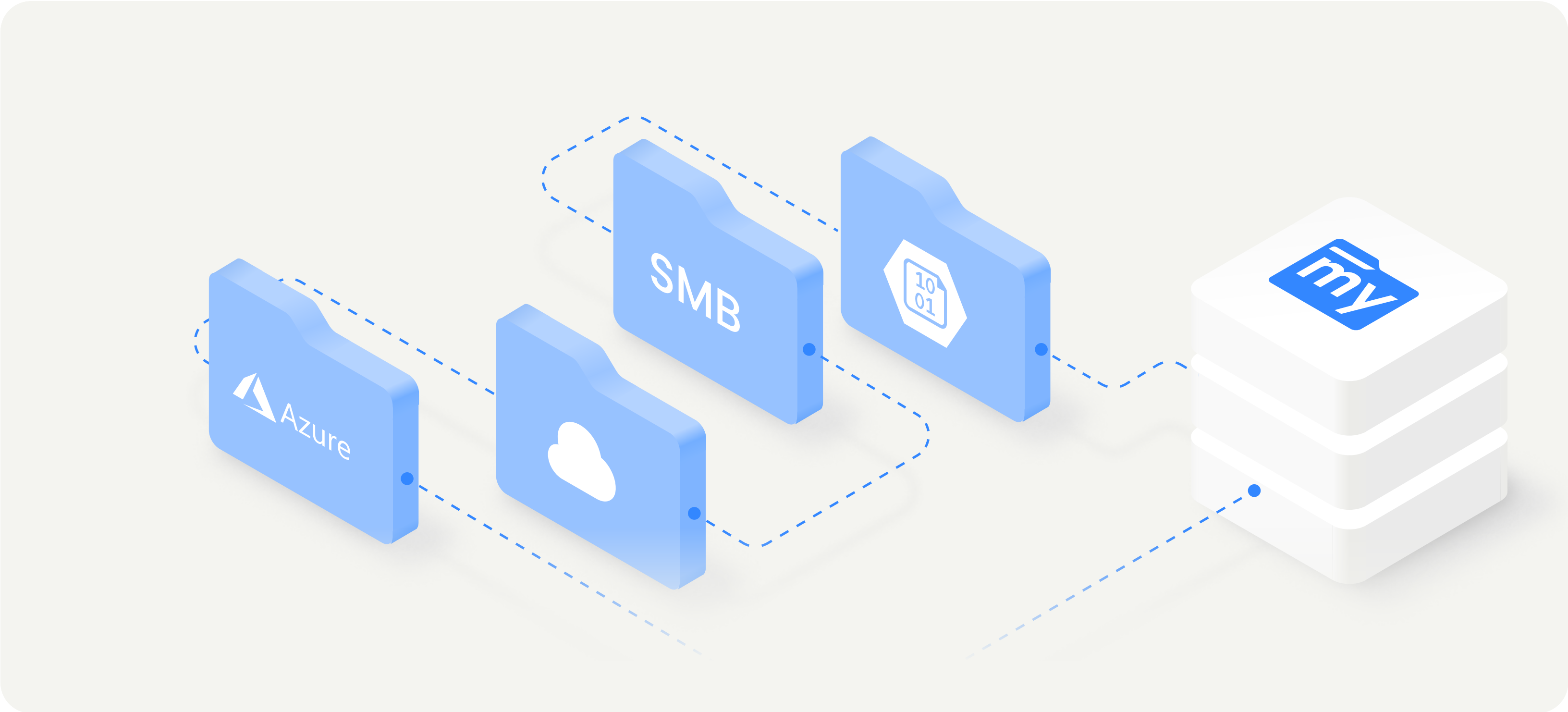
Users/Devices → Your Identity Provider → MyWorkDrive → Your Storage

Works With Your Existing Storage

- ✓ Windows SMB shares and cloud SMB (Azure NetApp Files, Amazon FSx)
- ✓ Azure Files via SMB or REST
- ✓ SharePoint and OneDrive via Microsoft Graph
- ✓ Azure Blob with Data Lake Gen2

Publishing Options

- ✓ **Direct HTTPS** - Simple deployment, requires firewall rule
- ✓ **Reverse proxy/WAF** - Behind your existing security infrastructure
- ✓ **Cloud Web Connector** - Outbound-only Cloudflare tunnel, zero inbound ports



Security That Works For IT And Auditors

Transport & Identity

- ✓ TLS 1.2+ for all connections, passwords never stored on server
- ✓ Least-privilege access honoring existing NTFS, SharePoint, and Data Lake ACLs
- ✓ Session state in memory only, short-lived and encrypted

Optional Controls (configure per-share, per-user, or per-group)

DLP 01

Block downloads, add watermarks, restrict clipboard

Device approval 02

Control which devices can map drives or use mobile apps

External sharing 03

Password-protected links with expiration

Guest access 04

Microsoft Entra B2B integration with policy inheritance

Audit & Compliance

- ✓ Complete logging with Syslog export to your SIEM
- ✓ Authentication outcomes, file actions, link creation/expiration
- ✓ HIPAA, CMMC, GDPR alignment through data sovereignty

User Experience Across All Devices

Web Client - SSO, search, familiar folder structure

Mapped Drives - Windows/Mac compatibility with legacy applications and scripts

Mobile Apps - iOS/Android viewing, editing, direct upload with policy controls

Office Editing Options

- ✓ Desktop Office via mapped drives (traditional file locking)
- ✓ Office on the Web (coauthoring with temporary Microsoft 365 staging)
- ✓ Customer-hosted editors (Office Online Server, ONLYOFFICE)

Deployment & Scale

Start simple

Single server supports 50-500 users Scale up: Clustering with load balancer for enterprise deployments (20-60,000+ users) Database required for: Multi-node clusters, Office coauthoring, public links.

Pilot Validation Checklist

- ✓ Test actual workflows, not just file copies
- ✓ Include largest files and worst network locations
- ✓ Validate Office save operations during peak hours
- ✓ Verify SIEM integration and mobile device access

What Changes (And What Doesn't)

CHANGES	STAYS THE SAME
Users get HTTPS access without VPNs	All permissions and storage locations
Optional DLP and device controls	Your identity provider and policies
Browser editing uses temporary Microsoft 365 staging	File ownership and folder structure
Comprehensive audit logging	Existing backup and disaster recovery

Bottom line

Users get modern access, IT gets modern controls, files stay exactly where they are.

Ready To See It Work?

01

Technical demo

using your actual shares and edge cases

02

Security review

with architecture diagrams and pen-test reports

03

1-day pilot

with clear success metrics

60–90 Minutes is the typical deployment time, provided there is proper access to DNS, certificates, and firewall management.