myworkdrive

COMPUGEN
Dream. Design. Deliver.

CASE STUDY · HEALTHCARE · MANAGED SERVICES

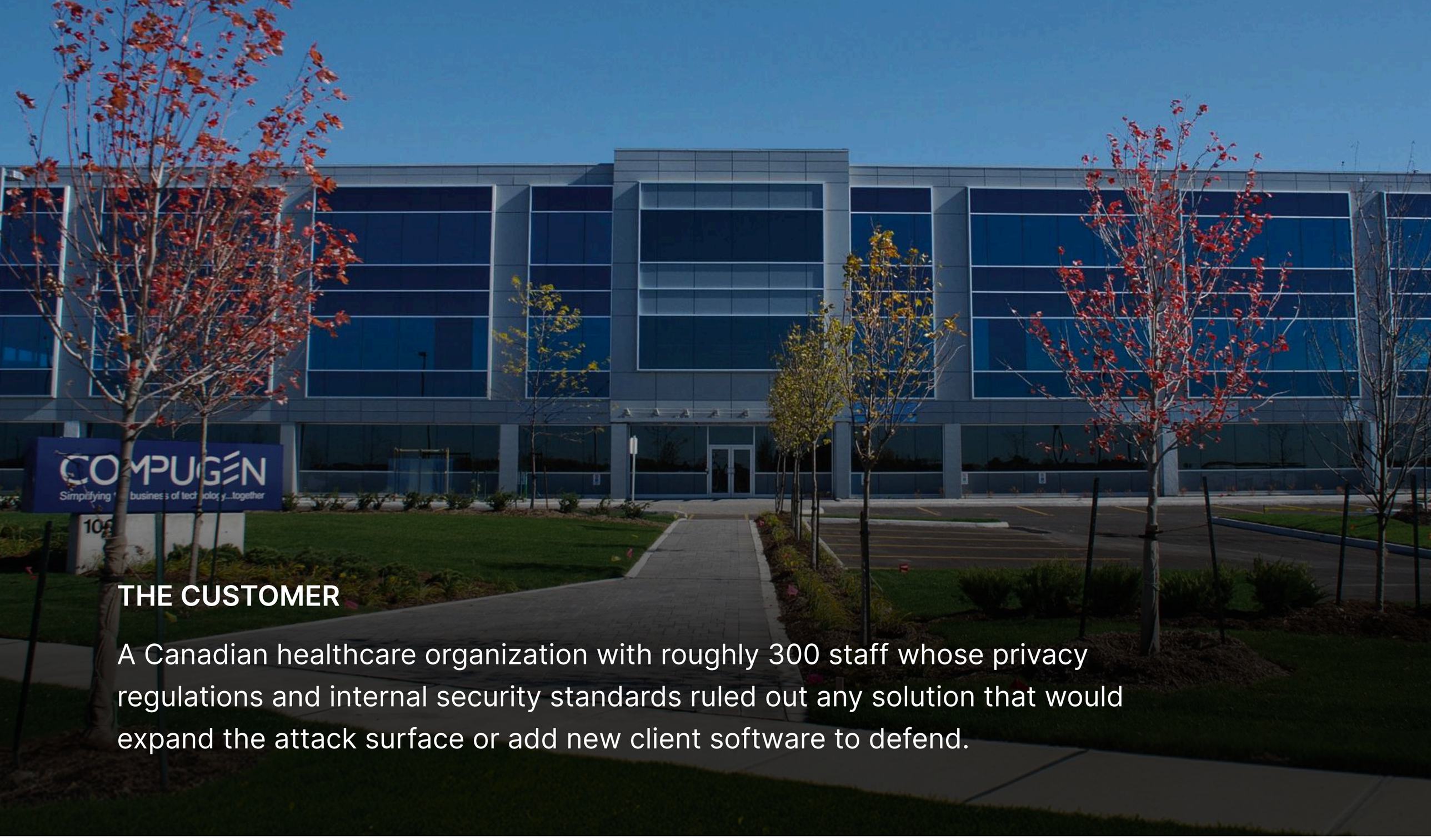
How Compugen Migrated To Azure Files Without A Single Moment Of Downtime.

Transitioning from a departing service provider on a fixed contractual deadline while enabling secure browser-based access for 300 users from day one.

10 TB
Of Windows File Shares Migrated

~300
Users Onboarded

0
VPN Clients Deployed



THE CUSTOMER

A Canadian healthcare organization with roughly 300 staff whose privacy regulations and internal security standards ruled out any solution that would expand the attack surface or add new client software to defend.

THE PARTNER

Compugen, one of Canada's leading IT solutions providers and managed service providers

Compugen led the customer's transition to a new IT operating model and took on the role of ongoing service provider. The MyWorkDrive deployment was part of that engagement and ran as part of Compugen's managed service.

THE CHALLENGE

A Divestiture On A Deadline

The customer was in the middle of a major corporate divestiture, separating from a portion of the organization that had been sold. Every IT service running on the departing provider's infrastructure had to be cleanly extracted and stood up under new operations. A contractual deadline with significant financial penalties made the timeline non-negotiable.

At the heart of the transition sat a 10-terabyte estate of Windows file shares. The customer had to move that data off the previous provider, land it somewhere secure and economical, and keep roughly 300 users working throughout the cutover. The security posture a healthcare organization is required to maintain could not slip while any of that happened.

The obvious paths were closed. Keeping VPN in the picture meant supporting client software the customer did not want to operate and expanding a perimeter the security team did not want to expand. Migrating into SharePoint meant a re-formatting, re-permissioning, retraining project the timeline could not absorb.

WHAT THE SOLUTION HAD TO DO

- ✓ **Move 10 TB fast.**
  Get data off the previous provider before contractual deadlines triggered financial penalties.
- ✓ **Land somewhere economical and secure.**
  A modern storage target that didn't require buying and racking new infrastructure under deadline pressure.

WHAT THE SOLUTION HAD TO DO

- ✓ **Skip VPN entirely.**

  No VPN clients to deploy, no expanded tunnel infrastructure to defend.

- ✓ **Avoid a re-platforming project.**

  Keep files in native Windows format with existing NTFS permissions intact.

THE SOLUTION

Azure Files For Storage. MyWorkDrive For Access.

Compugen evaluated the market against the customer's requirements. The destination for the data was straightforward: Azure Files gave the customer a Microsoft-managed home for Windows file shares without the cost or delay of standing up new on-premises infrastructure. The harder question was how users would actually reach it.

Azure Files has no built-in remote access method other than VPN, and adding a VPN client across the user base was exactly what the customer was trying to avoid. Compugen searched the market for a way to put Azure Files in front of users without that overhead. MyWorkDrive came out at the top of the list.

> *"We were presented with the problem and searched the market. From what we could see, at least on paper, MyWorkDrive fit the bill. It allowed us to use the browser to start with. Then, once we got control of the laptops, we could deploy the client onto the laptops if we wanted to provide another access method.*
>
> **COMPUGEN**

A Two-Phase Access Strategy

The deployment ran in two phases that mirrored the customer's own transition. Phase one began while Compugen was still establishing control of the endpoint estate. During that period, users reached their files through the MyWorkDrive browser client. There was nothing to install on the endpoint, no VPN profile to configure, and authentication ran through the customer's existing identity provider. Azure Files appeared in the browser the way a Windows share appears in File Explorer.

Phase two came once Compugen had operational control of the endpoint fleet. The MyWorkDrive mapped drive client went out alongside browser access, giving users a familiar File Explorer experience for files that happened to live in Azure. Either path worked, both pointed at the same Azure Files back end, and the same permissions governed both.

Why It Worked Under Deadline Pressure

MyWorkDrive sat in front of the storage rather than replacing it. The 10 TB of Windows file shares moved into Azure Files in their native form, with NTFS-style permissions preserved. Nothing about the file structure changed, nothing had to be re-permissioned, and no files were converted into a different format. The migration project and the access project ran in parallel rather than stacking on top of each other.

End-user adoption was fast and usage was high from day one. The interface was either a browser or a mapped drive, both familiar, so users had nothing new to learn at a moment when plenty else about the IT environment was already changing.

ARCHITECTURE

How It Fits Together

STORAGE	Azure Files. 10 TB of Windows file shares migrated in native format. Permissions preserved. No re-platforming.
ACCESS LAYER	MyWorkDrive. Deployed as the secure HTTPS gateway in front of Azure Files. Browser, mapped drive (Windows File Explorer integration), and mobile clients.
IDENTITY	Customer’s existing identity provider with SSO and MFA. No separate user database, no parallel credential store.
PERMISSIONS	NTFS-style permissions on Azure Files remain authoritative. MyWorkDrive cannot elevate access beyond what storage and identity already grant.
VPN FOOTPRINT	Zero. No VPN clients deployed for file access. No tunnel infrastructure to scale or defend.
OPERATIONS	Deployed and operated by Compugen as part of the managed service engagement. The same platform Compugen uses across its practice, which is to say they eat their own dog food.

Why Microsoft refers Azure Files customers to MyWorkDrive

Azure Files gives organizations a Microsoft-managed home for Windows file shares. Microsoft does not, however, provide a built-in way to reach those files remotely without VPN. That is the gap MyWorkDrive fills. The Azure Files program team at Microsoft regularly directs customers to MyWorkDrive when the requirement is secure remote access without expanding VPN or migrating to SharePoint.

THE RESULTS

The Deadline Held. The VPN Stayed Out.

10 TB
Migrated
to Azure Files

Zero
VPN Clients
Deployed

High
Day-One Adoption
Across ~300 Users

A Deadline Met Without a Re-Platforming Project

The customer cleared its contractual divestiture deadline. 10 TB of Windows file shares moved off the departing service provider's environment, landed in Azure Files in native format, and stayed accessible to roughly 300 users throughout the cutover.

Zero VPN Clients Deployed

No VPN client was deployed for file access during or after the transition. Remote access got simpler at the moment when added complexity would have been hardest to absorb.

Fast, Sustained User Adoption

Users took to the platform quickly. Browser access required no software install. The mapped drive client looked and behaved like Windows File Explorer. Both paths reached the same data under the same permissions, so there was no wrong way to work. Usage has stayed high since rollout.

An Operating Model Compugen Can Stand Behind

MyWorkDrive is part of Compugen's broader managed service practice, and the team operates it across its customer base. That hands-on familiarity with the product, the deployment patterns, and the things that can go wrong is part of why the platform performed under live operations during this engagement.

> *We wanted to make sure whatever we deployed was something we were comfortable with and could operate. It is a little bit like eating your own dog food.*
>
> **COMPUGEN**

WHY MYWORKDRIVE

The Right Layer For Cloud File Access

Compugen selected MyWorkDrive after a market evaluation against a clear set of requirements. The platform offered the right combination of speed, simplicity, and security for a customer whose timeline left no margin for either added complexity or schedule slippage.

AZURE FILES NATIVE	Built specifically to provide secure remote access to Azure Files and on-premises SMB shares without VPN. Microsoft's own Azure Files program team refers customers to MyWorkDrive for this scenario.
BROWSER-FIRST, CLIENT-OPTIONAL	Start with the browser when endpoints aren't under management yet. Roll out the mapped drive client when they are. Both paths to the same data.
NO RE-PLATFORMING	Files stay in native Windows format with NTFS-style permissions intact. No SharePoint migration. No re-permissioning. No file conversion.
IDENTITY-NATIVE SECURITY	Built on the customer's existing identity provider. SSO and MFA enforced upstream. MyWorkDrive cannot elevate permissions.
FAST ADOPTION	Browser and File Explorer are interfaces every user already knows. No training curve during a period of operational change.
MSP-OPERABLE	Built for managed service providers to deploy, monitor, and run day-to-day. Compugen operates the same platform across its practice.

READY TO EVALUATE

Azure Files Without VPN. On Your Timeline.

MyWorkDrive gives your users secure HTTPS access to Azure Files and on-premises SMB shares, with SSO and MFA, on browser, mapped drive, and mobile. No VPN to deploy. No migration to plan.

Start a free 14-day trial at myworkdrive.com