PARALLEL IMPLEMENTATION

Protection starts on day one. Migration happens in parallel.

When a new firm comes on board, the instinct is to get everything moved first and then worry about security. FCI reverses that order. We deploy endpoint protection and security controls immediately — before the file server migration is complete, before users have transitioned to Microsoft 365, before anything else changes. The firm is protected from the moment we begin.

Day 1
endpoint protection deployed

2 Tracks
security & migration run simultaneously

Zero
days the firm is left unprotected

THE CHALLENGE

Every new engagement starts with the same question.

A firm is ready to move forward with FCI. There is a local file server — possibly in a closet, possibly at a data center — that everyone depends on. Users log in through a firewall to access shared files. The firm also needs to transition to Microsoft 365, deploy OneDrive, and modernize how people work. Where do you start?

The traditional approach is sequential: migrate first, secure later. The problem is that during migration — which can take weeks or months — the firm is exposed. Endpoints are unprotected. Communications are unencrypted. The firm is at its most vulnerable exactly when nobody is paying attention to security.

> THE QUESTION
>
> *If migration takes weeks, who is protecting the firm's endpoints during that time?*

THE APPROACH

Two tracks running at the same time.

FCI runs two parallel workstreams from the start of every engagement. Track one is security: endpoint protection, always-on VPN, and security controls are deployed to every device immediately. Track two is migration: the file server transfer to Microsoft 365 and OneDrive begins at the same time. Neither track waits for the other.

TRACK 1 — SECURITY

Protect every endpoint immediately

Endpoint protection is deployed on day one. Always-on VPN is installed on every device, encrypting all communications from the start. Security controls are enforced before a single file is migrated. The firm is protected from the moment FCI begins work.

TRACK 2 — MIGRATION

Transfer the file server to Microsoft 365

In parallel, FCI begins migrating the firm's file server to Microsoft 365. Files move to OneDrive and SharePoint. This takes time — the volume of data, the folder structure, and the firm's operational needs all affect the timeline. But users are already protected while it happens.

> "We don't wait for migration to finish before we protect the firm. We protect the firm first and migrate in parallel."

THE TRANSITION

From local file server to Microsoft 365 — without disruption.

The transition is not a single event — it is a gradual process with a clear beginning, middle, and end. During the overlap period, users can access files through both the local file server and OneDrive. This flexibility eliminates the risk of a hard cutover and gives the firm time to verify that everything has transferred correctly.

● **Phase 1 — Coexistence**

Users continue to access the local file server through the firewall while FCI migrates data to Microsoft 365. Once OneDrive is installed on each device, users begin to see their files in both places. Nothing changes about how they work — they just gain a second path to the same data.

◆ **Phase 2 — Overlap & Verification**

For a period, both systems run side by side. Users work primarily from OneDrive but can still log into the office to access the local file server if something is missing or not working as expected. This is a safety net — not a permanent state. FCI monitors the transition and confirms that all files are accessible and intact.

■ **Phase 3 — Cutover & Decommission**

When FCI confirms that the migration is complete and users are working successfully from Microsoft 365, the local file server access is cut. The firewall is reconfigured to stop accepting remote connections to the file server. The file server itself is decommissioned. From this point, all file access runs through OneDrive — protected, encrypted, and backed up.

Security deployed | Both systems active | Migration complete

DAY ONE

What FCI deploys before migration begins.

Security does not wait for migration. The following controls are deployed to every endpoint at the start of the engagement — regardless of where the firm's files currently live or how users are currently accessing them.

01 **Endpoint Protection**
Advanced endpoint detection and response is deployed to every device. FCI's SOC monitors all endpoints around the clock from this point forward.

02 **Always-On VPN**
An always-on VPN is installed on every device, encrypting all communications — whether the user is in the office, at home, or on the road. This is active from day one and remains in place permanently.

03 **Security Controls Enforcement**
MFA, full-disk encryption, and access controls are enforced across all users. The firm's compliance posture is established before a single file has been moved.

04 **CISO Portal Visibility**
The firm gains access to the CISO Portal — a real-time dashboard showing the compliance status of every device, every user, and every control. Visibility begins on day one.

THE CUTOVER

When the old system goes away.

The cutover happens only when FCI has confirmed that the migration is complete and that users are working successfully from Microsoft 365. This is not a deadline — it is a decision based on evidence. Once the firm is ready, FCI executes three final steps.

Firewall Reconfigured

Remote connections to the local file server are blocked. The firewall no longer accepts inbound access for file sharing.

File Server Decommissioned

The local file server is taken offline and retired. The firm's data now lives exclusively in Microsoft 365.

OneDrive as Primary

Every user accesses files through OneDrive — synced, backed up, and accessible from any device, anywhere.

Always-On VPN Remains

The VPN installed on day one stays in place permanently, encrypting all communication regardless of how or where users connect.

THE RESULT

The firm is fully protected, fully migrated, and fully modern — and at no point during the process was there a gap in security coverage.

WHY THIS MATTERS

The risk of doing things in the wrong order.

Firms that migrate first and secure later accept a window of exposure that can last weeks or months. During that time, endpoints are unprotected, communications are unencrypted, and the firm has no visibility into what is happening on its devices. If something goes wrong during migration, there is no security infrastructure in place to detect it, contain it, or produce evidence for regulators.

FCI's parallel implementation eliminates that window entirely. From the moment we begin, every endpoint is monitored, every communication is encrypted, and the firm has full visibility into its security posture through the CISO Portal.

> "The most dangerous moment for a firm is the transition. That is exactly when you need security in place — not after."

Ready to discuss implementation for your firm?

FCI works with broker-dealers & branch offices, insurance carriers & agencies, and RIAs. Every engagement begins with security — and migration runs in parallel from day one.

PHONE

973-227-8878

WEB

fcicyber.com