Kiteworks

SOLUTION BRIEF

FOR IT AND SECURITY LEADERS

Top 5 Reasons to Move Off ShareFile

How Consolidating Onto One Hardened Appliance Ends the Storage Zone Controller Exposure

On July 10, 2026, Progress Software told every customer running a ShareFile Storage Zone Controller — the on-premises Windows server that connects ShareFile's cloud login to an organization's own file storage — to shut that server down over a "credible external security threat." As of July 13, Progress is gradually restoring general ShareFile cloud access, but Storage Zone Controllers remain instructed offline, no patch is available, and no root cause has been confirmed. Online discussion has pointed to a previously disclosed vulnerability chain — a pre-authentication remote-code-execution pair (CVE-2026-2699, CVE-2026-2701) that watchTowr Labs disclosed on April 2, 2026 — as a possible explanation, though Progress has not confirmed this.

This is the second time in five years the same component has forced a shutdown-grade response: a 2021 authentication-bypass flaw (CVE-2021-22941), confirmed exploited in the wild, was added to CISA's Known Exploited Vulnerabilities catalog under Citrix, the product's previous owner. Kiteworks was not part of this incident. But the exposure it illustrates — a customer-run, internet-facing storage server that only a vendor patch can fix — is precisely what a hardened, vendor-maintained appliance is built to remove.

1 Stop Waiting on a Patch That Isn't Coming

When Storage Zone Controller has no available fix, the only option is to power the server down and wait — as customers were told to do on July 10. Kiteworks replaces that dependency with a Kiteworks-maintained hardened appliance, one-click full-system updates that patch the application, runtime, operating system, and libraries together in a single coordinated cycle, and continuous penetration testing backed by a standing bug-bounty program — so a new disclosure is a routine update pushed by Kiteworks, not a customer-side emergency shutdown with no fix in sight.

2 Retire the Customer-Managed Storage Server

Storage Zone Controller is a Windows server the customer configures, patches, hardens, and exposes to the internet by design — security depends entirely on getting that configuration right, every time, on every server. Kiteworks removes that server from the equation. It deploys as a hardened virtual appliance with an embedded network firewall, an embedded web application firewall, and multiple layers of intrusion and anomaly detection built directly into the appliance — maintained by Kiteworks, with no separate security stack, patch schedule, or admin-port exposure for the customer to manage.

3 Eliminate the Single Point of Failure With Single-Tenant Isolation

One compromised Storage Zone Controller can expose every file that passed through it. Kiteworks supports single-tenant deployment, so an organization's databases, file systems, and application runtime never mix with any other customer's — there is no shared infrastructure for a single exploit to cross into. That isolation is reinforced by FIPS 140-3 validated encryption, customer-owned keys with HSM integration, and tamper-evident audit logging, aligning with the controls regulators already expect under HIPAA, CMMC Level 2, PCI DSS, and GDPR Article 32.

4 Unify Fragmented Logs Into One Audit Trail

A separate file-sharing platform running alongside managed file transfer, secure email, and SFTP means separate vendor relationships, separate policies, and separate logs to reconcile in the middle of an incident like this one. The Kiteworks Data Security and Compliance Risk: 2025 MFT Survey Report found 62% of organizations run fragmented systems across MFT, email, file-sharing, and web-form channels, and 63% haven't integrated MFT with their SIEM. Kiteworks unifies every channel under one policy engine and feeds a single, complete, real-time audit log to SIEM tools — never sampled, never throttled, and never delayed.

5 Move Without Rebuilding Your Workflows

Migrating off ShareFile is a planning exercise, not a forklift replacement. Kiteworks provides a structured migration path that preserves partner endpoints, folder structures, permissions, and encryption requirements, and maintains audit trail continuity from day one — so external partners and internal teams keep working the way they already do. The next file-sharing security notice becomes a routine patch cycle instead of an all-hands emergency shutdown.

Ready to Leave ShareFile Behind?

www.kiteworks.com

Kiteworks' mission is to empower organizations to effectively manage risk in every send, share, receive, and use of private data. The Kiteworks platform provides customers with a secure data exchange that delivers data governance, compliance, and protection in a unified control plane. Kiteworks unifies, tracks, controls, and secures sensitive data moving within, into, and out of their organization, significantly improving risk management and ensuring regulatory compliance on all private data exchanges. Headquartered in Silicon Valley, Kiteworks protects over 100 million end-users and thousands of global enterprises and government agencies.

in X f ig yt