Cloud Storage Security Hardening Checklist

A comparison of key security hardening steps for OneDrive, Dropbox, and Google Drive.

Security Area	OneDrive	Dropbox	Google Drive
Multi-Factor Authentication	Use Microsoft Authenticator or a FIDO2 key. Enforce MFA for all users.	Use a TOTP app or FIDO2 key. Enforce 2FA for all accounts.	Use Google Prompt or Titan/FIDO2 key. Require 2-Step Verification for all users.
Encryption	AES-256-bit at rest and TLS in transit. Optional client-side encryption for highly sensitive files.	AES-256-bit at rest and TLS in transit. Pre-encrypt sensitive files with Cryptomator or Boxcryptor.	AES-256-bit at rest and TLS in transit. Client-Side Encryption available in Google Workspace Enterprise.
Sharing Controls	Default to 'Specific people'. Set link expirations and disable anonymous links.	Restrict public links. Password-protect and set expiration dates for shared files.	Limit sharing to specific users. Disable 'Anyone with the link' access.
Ransomware Protection	Supports version history, ransomware detection, and file restore.	Use Dropbox Rewind and version history to recover deleted or encrypted files.	Uses file versioning and Trash for recovery. Restore deleted or modified files easily.
App Integrations	Remove unused apps and restrict API access to trusted services only.	Audit connected apps regularly and remove unused ones.	Review OAuth app permissions and revoke unnecessary third-party access.
Admin & Audit Controls	Unified Audit Logs, Microsoft Purview DLP, and Defender for Endpoint integration.	Dropbox Insights logs and optional DLP integrations through the API.	Drive Audit Logs, Workspace DLP policies, and Security Center alerts.
Compliance & Retention	Use retention policies, legal hold, and Microsoft Information Protection.	Use Dropbox Backup and admin recovery options for compliance.	Use Google Vault for retention, eDiscovery, and legal hold management.