



DATASHEET (DIGITAL GUARDIAN)

Data Protection for Citrix ShareFile

Secure File Sharing and Mobile Data Loss Prevention

The Challenge

Many IT organizations want a secure alternative to consumer-style file sharing services. Enterprises need full control over their data while maintaining productivity, by providing users with mobile access to information and synchronizing data across all devices.

Citrix ShareFile is an enterprise follow-me data solution that enables IT to deliver a secure and robust service that meets the mobility and collaboration needs of all users. The ShareFile StorageZones feature allows IT to store data both on and off premise. With customer-managed StorageZones, IT can store data within its data center to maintain complete control of enterprise content.

With ShareFile, users can receive comprehensive reports on file sharing activity within their workspaces. IT can track and log all user activity. In addition to encrypting data at rest and in transit, ShareFile allows IT to leverage mobile device encryption capabilities and enforce encryption for all ShareFile data on a device. With features like remote wipe, poison pill, jail-break detection, and passcode lock, IT can ensure corporate data remains secure across mobile devices.

Organizations also have advanced data security requirements and need to protect customer data, intellectual property (IP), classified government content, and other sensitive information. In particular, many organizations require end-to-end data protection between the secure ShareFile StorageZones servers, desktops, laptops, virtual environments, mobile devices, and removable media. They may require confinement of sensitive information in controlled environments to prevent data leakage via network upload, email, removable media, and printing. In this context, it is critical to protect the information without affecting user experience and productivity.

The Digital Guardian Solution

Fortra™'s Digital Guardian® is a data aware endpoint security platform that monitors, classifies, controls, and encrypts sensitive data on desktops, laptops, servers, and mobile devices. Digital Guardian extends the ShareFile security model with data classification, additional data usage monitoring, and data control on endpoints.

KEY BENEFITS

- Cover advanced data protection use cases for regulated and IP-centric industries and government organizations
- End-to-end data protection, from ShareFile StorageZones to IT-managed servers and user devices
- User-based policy controls define how data should be accessed and shared
- Data aware solution classifies documents and applies context-based policies to information access and movement
- Enforce information usage policy without negatively affecting business processes

Digital Guardian classifies data based on content, context, and/ or user input, and tags files accordingly. Using data classification enables a data aware approach to security that allows for differentiated policies. This provides effective controls without breaking business processes or affecting user productivity.

Digital Guardian endpoint agents use a number of controls, including user warnings, user operation blocking, and encryption, to enforce data access policies.

ShareFile and Digital Guardian 1+1 = 3

- Citrix ShareFile enables IT to deliver a secure follow-me data service to all users. Its advanced security features include remote wipe, device lock, and passcode protection. Data expiration policies ensure comprehensive control of enterprise data.
- Digital Guardian extends these security benefits by monitoring and restricting the use and transfer of data to unapproved destinations such as personal/ unsecure cloud storage (for example, Dropbox), USB devices, and removable media. In addition to blocking data transfers to unauthorized locations, Digital Guardian can automatically enforce the use of ShareFile for all data sharing activities.
- Digital Guardian ensures that classified information can only be placed in a permissible ShareFile location which has the appropriate level of access control for the sensitivity of the data.
- Digital Guardian enforces user-based policy controls and allows seamless access to encrypted files in many environments, including:
 - Microsoft Windows desktops, laptops, servers
 - XenApp-hosted shared desktops
 - XenDesktop-hosted VDI sessions
 - Apple iOS devices
- Digital Guardian provides detailed forensic logging of data usage on user devices for audit and legal purposes that complements the reporting capabilities of ShareFile. This includes:
 - Visibility of data movement in and out of ShareFile
 - Enterprise view across ShareFile and other platforms

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.