Protect, control and monitor your data wherever it goes

Dell Data Guardian

If your business is no longer restricted to an office, your data is at increased risk. Critical business data can be anywhere and everywhere. If employees mistakenly–or intentionally–send a file or link to the incorrect person or use a public network that is hacked, data can quickly fall into the wrong hands. The results can be devastating: loss of business, reputation risk and/or fines.

An increasingly mobile workforce enables higher risk. Organizations are enabling more anywhere, anytime workforces to increase worker flexibility and productivity. To be productive, many employees are using a wide variety of devices, from desktop computers and laptops to smartphones and tablets. They are also using external devices and cloud services to share information as part of increasingly collaborative work models.

A new approach to data protection will safeguard data wherever it goes and however it is shared. Data needs to be protected from the moment it is created on desktops, laptops, tablets and smartphones. Data protection must persist when in motion and in use as files are shared with personal email accounts or cloud-based collaboration services. Data should remain protected as it is accessed on a wide range of devices, in a variety of locations and on any type of network. You must ensure data stays secure even as it is shared among a broad array of colleagues, partners and customers. Through all of this data movement, you need ways to monitor who is accessing the data and to revoke access if necessary.

Comprehensive protection and management

Dell Data Guardian is advanced data security that ensures data is encrypted beyond the boundaries of your enterprise, usage is controlled and monitored, and visibility of data activity and location is simple and accessible. Strengthen your security posture without hindering workforce productivity.

- **Protect**: Secure your data wherever it goes. Your data is protected as it is shared via email, cloud services, FTP and portable storage devices by company employees, contractors, vendors and business partners.
- **Control**: Define parameters for access of your data. You can define who has access to specific data, when your data can be accessed and how your data can be used.
- **Monitor**: The Dell Security Management Server contains analytics on data access, activity and location. You now have the capability to see who is using your data and how it is being used. You can detect potential security risks and take action such as revoking file or user access where appropriate.

Encryption and enterprise digital rights management

With Dell Data Guardian, you can encrypt individual files and maintain that encryption throughout the file's lifecycle, wherever it travels or resides and however it is shared.

- Transparent operation ensures files are secured with encryption and enterprise digital rights management to ensure only approved access. This protection is transparent to authorized users.
- On screen watermarks can be applied to files showing registered email address for audit purposes.
- HTML 5.0-compatible Data Guardian Web Client: no need for full Data Guardian client install for external viewing and editing of files
- Streamlined pre sharing authorization process when sending files with Microsoft Outlook. Easy post sharing authorization request process for external users.
- The Data Guardian Mobile is a secure, encrypted container for your companion iOS and Android devices.
- For Windows users: Use Microsoft Word or Adobe Acrobat Reader DC for open, view and annotate .pdf documents.
- Centrally manage access control policies, events, alerts and compliance reporting.

Enterprise digital rights management (EDRM)

With Dell Data Guardian's enterprise digital rights management (EDRM), you have file access control capabilities.

- Control enterprise file sharing–create white-and black-lists of domains and individuals who can access specific files.
- Tailor file usage to your specific requirements, including read/write, copy/paste, printing, expiry and embargo restrictions.

Visibility and Monitoring

Which individuals are accessing sensitive files? What are they doing with those files? Where are files being accessed from? Dell Data Guardian provides insights to help you assess security risks with enterprise file sharing.

- Use these capabilities as a preventive measure, monitoring potentially troubling trends and identifying individuals who might be breaking rules for accessing or sharing sensitive information.
- Capitalize on these insights for applying forensics, determining policy abuse, data location and policy adherence.
- Use data monitoring reports to streamline audits, demonstrate regulatory compliance and take action such as revoking access rights.
- Revoke access rights for users or access to individual files right on Audit Events page.

Protection for mobile devices

Using the Dell Data Guardian Mobile app, you can create a secure file container on mobile devices–including ones on iOS and Android™ platforms–that lets employees securely view, request access or edit files and prevents any data leakage into their private email or phone storage.

- Secure mobile container for iOS and Android, downloadable from the app store.
- Extend your data protection beyond Data Loss Prevention (DLP) to data sync'd and shared with mobile devices.

Manage with ease

Dell Data Guardian helps reduce management complexity by incorporating your encryption on the go, EDRM and reporting capabilities into a single, integrated solution by incorporating data at rest and in motion protection into a single integrated solution with reporting capabilities

- Centrally managed policies, encryption keys and reporting.
- Fully integrated into the Dell Security Management Server for extensibility.
- Export Dell Data Guardian events to your security information and event management system (SIEM).
- Assess audit events with mapping and revoke file or user access if necessary.
- For organizations under EU GDPR specifications: Allows for admin to turn off data sent back to the Data Security Management Server.

Technical Specifications

File Types Protected:

- .docx, .docm, .xlsx, .xlsm, .pptx, .pptm, .pdf

Supported Operating Systems:

- Windows, 7, 8, 8.1, 10 - R1 (Threshold and Threshold 2, Redstone R1, R2)
- Mac OS X 10.10.5 (Yosemite), 10.11.6 (El Capitan), 10.12.6 (Sierra) and 10.13 (High Sierra)
- iOS 9, 10, 11
- Android 4.4+ (KitKat), 5.0+ (Lollipop), 6.0+ (Marshmellow), 7.0+ (Nougat)
- Chrome, Firefox, Edge, Mac Safari for Web Client

Dell Security Management Server:

- Version 9.9 for latest functionality

Learn more at Dell.com/DataSecurity