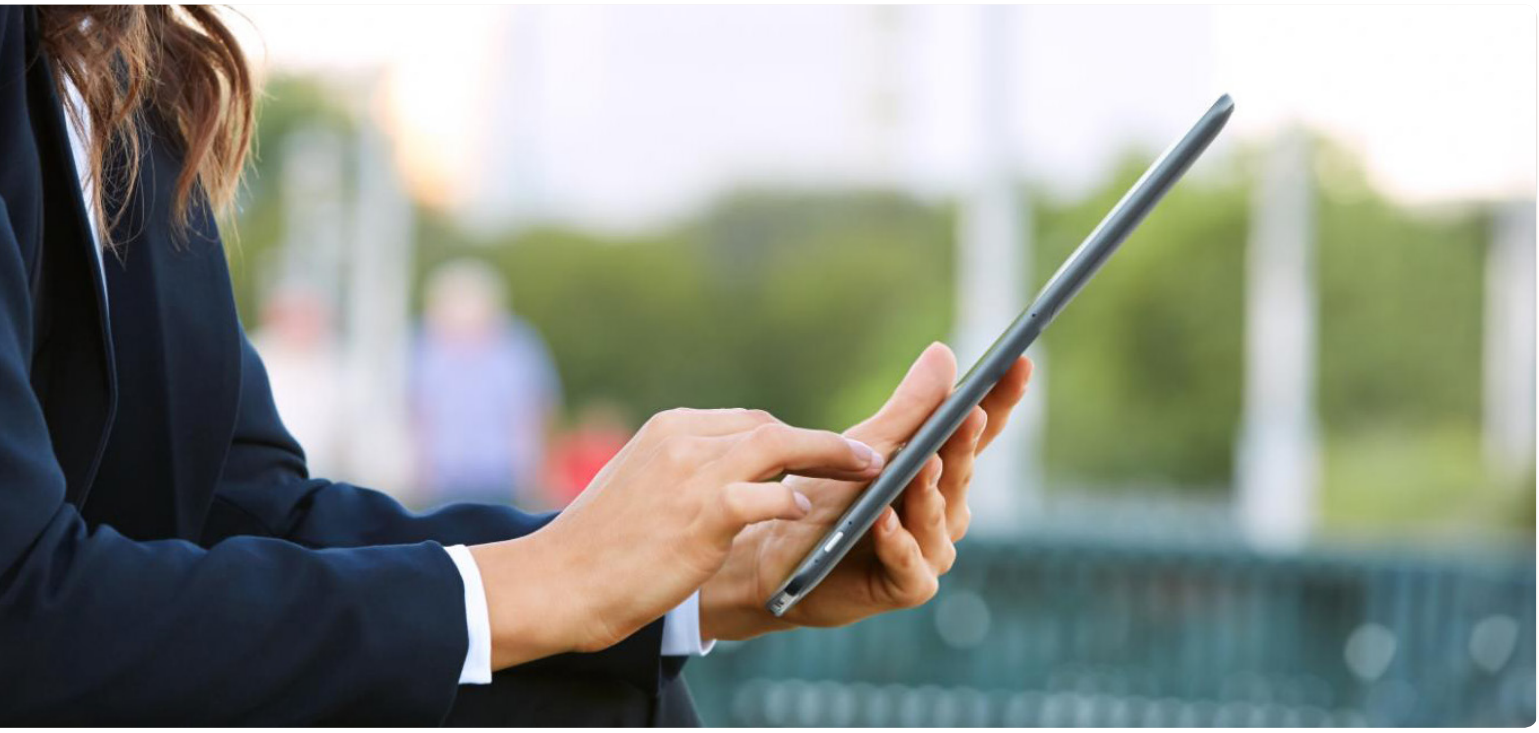
Protect, control and monitor data wherever it goes with Dell Data Guardian



Introduction

Insider threats are a serious and growing data security problem. New mobile, cloud and other technologies make it easier than ever for employees to transfer data beyond secure enterprise environments and share data with unauthorized individuals. Those technologies also make it difficult for IT administrators and security teams to retain control over sensitive data and monitor how data is accessed, by whom and where.

Intentional, malicious acts — such as stealing intellectual property or customer data — are only part of the problem. Employees are also putting data at risk and jeopardizing regulatory compliance through an array of other behaviors, including accessing data from personal devices, transferring files to external hard drives, sending documents to individual email accounts and sharing files through cloud collaboration services.

While organizations want to enable more flexible ways of working and support new collaboration technologies, they need to guard their data. They must secure data at rest, in motion and in use. They need ways to control data access, ensuring it cannot be accessed by unauthorized individuals. And they need to monitor file activity and report on how data is being used to spot troubling trends, stop malicious acts, identify miscreants and streamline compliance activities.

74% of breaches originate within the extended enterprise[1]

At the same time, many organizations want solutions that can help simplify management. The quest to implement best-of-breed capabilities has led some organizations to acquire multiple, discrete data security solutions. Organizations want to reduce the sprawl of software, limit the need for additional hardware infrastructure and minimize the number of management consoles administrators must navigate.

Dell Data Guardian can help your organization protect data, control data access and monitor data usage while reducing infrastructure complexity. The solution combines encryption and enterprise digital rights management (EDRM) with file activity monitoring, data visualization and reporting — all in one integrated package from a single vendor.

Protect data however it is used with robust encryption

Encryption is the foundation of data protection — it helps ensure sensitive data cannot be read even if it falls into the wrong hands. Data Guardian offers robust encryption capabilities that keep data protected at rest and in motion. It also provides additional layers of security to keep encryption keys safe and minimize potential damage that could be caused by an encryption hack.

Data in motion

Traditional encryption solutions simply encrypt a device's hard drive. This approach can help prevent data from being read if the device is lost or stolen. But what happens when an employee emails a file to a partner, moves it to an external USB drive or shares it with colleagues through a cloud sync-and-share service? The file is unencrypted and vulnerable to theft or loss.

Protecting data in motion — as it moves from one device, medium or environment to another — is critical to safeguarding information. However, not all approaches designed to protect data in motion offer complete security.

One approach to protecting data in motion involves encrypting the communication channel through which data is traveling. This approach — which might use Transport Layer Security (TLS)/https technology — focuses on protecting data from being intercepted in transit. But what happens when data sent through an encrypted channel is received by its intended recipient? Typically, that data is unencrypted, and it remains that way, which would become a problem if, for example, the recipient forwards an unencrypted file to a colleague. Though it was protected during its initial journey, the data is once again at risk for theft or loss.

Data Guardian takes an alternative approach. It provides persistent encryption that protects files from the moment they are created and maintains that protection no matter where they travel or reside. Plug-ins for Microsoft® Office automatically encrypt new Word, Excel® and PowerPoint® files, including macro-enabled files.[2] Data Guardian can also conduct a sweep of a device to encrypt any unencrypted Word (.docx, .docm), Excel (.xlxx, .xlxm) and PowerPoint (.pptx, .pptm) files. Each file remains encrypted whether an employee sends it to a colleague by email, moves a file to a network file share, transfers it to an external drive or shares it with colleagues through a cloud service from Box, Dropbox, Google or Microsoft.

When a file encrypted by Data Guardian is sent over a secure communication channel, that file benefits from both layers of protection. In the event of a "man-in-the-middle" attack on the TLS communication channel, the Data Guardian protection would keep the file secure — the file would require authentication before it could be read.

External user registration

Data protection solutions should not restrict collaboration with trusted partners, or curtail productivity. With Data

Guardian, you can enable external users to access encrypted files through a simple registration process.

When an encrypted file is sent to or shared with an external user, the recipient sees a cover page noting that the file is encrypted. The page provides instructions on how the recipient can authenticate himself or herself to decrypt the file. If your organization decides to allow access, the external user can open the file. That external user does not need to purchase any new software. You can extend secure access to partners, colleagues, customers and others without adding costs or excessive complexity to the workflow.

Per-file encryption
Data Guardian uses per-file encryption to add an extra layer of protection. Most data-at-rest solution providers use a single key to encrypt a large number of files, such as all the files stored on a device. By contrast, Data Guardian provides a unique encryption key for each file.

Data Guardian also helps keep encryption keys protected. You retain control of the encryption keys. Keys reside on your premises and on your hardware, not in a cloud share that could be hacked or subpoenaed.

Policy-based management
Data Guardian offers policy-based encryption management to give your administrators the greatest control and flexibility over how encryption is applied. For example, administrators can force all Word, Excel and PowerPoint files to be encrypted or allow users to opt-in into encryption for those file types. You can apply a single policy across the entire enterprise or create distinct policies for particular devices and/or workgroups.

Control data access

With Data Guardian, you control who can access enterprise data and in what circumstances. You can keep files encrypted at all times and make sure data is accessed only when you permit it.

Continuous protection
Data Guardian lets you guard sensitive data no matter where it goes. For example, you can protect a document with design specifications for a new technology product, even if a member of your product development team attempts to email it to the press or a competitor.

Data Guardian also protects data in the cloud. It encrypts all data as it is sent to cloud services. In addition, administrators can prevent unapproved cloud sync-and-share applications from uploading data to the cloud.

Secure environments for mobile devices
To guard data in mobile device environments, Dell offers the Data Guardian Mobile app. The app creates a secure file container on iOS and Google Android™ mobile devices that lets employees safely create, open and edit files in a protected space. Files synchronized to the mobile device remain encrypted, helping you meet strict compliance rules by making files accessible only within that environment. The app also enables secure use of cloud-based sync-and-share services. Geofencing capabilities let you restrict data access to particular geographies. With the Data Guardian Mobile app, you can support new ways of working without compromising data security.

EDRM
Policy-based EDRM capabilities let you control who can access data, what they can access and in what circumstances. For example, administrators can set per-machine policies for controlling printing and export.

In addition, administrators — and users — can apply embargos and expiration dates for particular files. Your organization might enable contract workers to access files only for the duration of their contract. They wouldn't be able to access sensitive information after their projects are complete.

With Dell Data Guardian, you control who can access enterprise data and in what circumstances. EDRM capabilities help ensure data is accessed only when you permit it.

Conversely, your organization might embargo certain files, preventing them from being accessed until a specified amount of time has passed. You could decide that a press release announcing a new product or a document with quarterly earnings information should not be opened until a particular date. With Data Guardian, IT administrators can enable content creators to set these time-based parameters.

Monitor how data is used

In addition to protecting data and controlling data access, Data Guardian lets you monitor who is using data and how. With file activity monitoring, visualization and reporting capabilities delivered through an easy-to-use dashboard, Data Guardian can help you spot potential issues, improve forensics and streamline audits.

File activity monitoring

Data Guardian uses metadata to monitor what data is accessed, by whom, when and where. That metadata might help you determine that a particular spreadsheet was sent by an employee to an external user, who then opened the file on a specific date in another country.

With this visibility into the file's journey, you might decide to turn off access for certain individuals. This visibility also helps streamline forensics if sensitive information is leaked; you can easily identify the individuals and pathways responsible for the leak.

Data visualization

Data Guardian provides data visualization through a dashboard so you can understand data usage and easily monitor trends at a glance. The dashboard gives a snapshot of information and also enables you to drill down into details. You can also conduct SQL queries on the metadata to find additional information.

Reporting

Data Guardian lets you quickly generate reports that draw on the raw metadata. Reporting lets you streamline the processes of satisfying audit requests and demonstrating regulatory compliance.

Choose an integrated solution from a single vendor

Data Guardian lets you capitalize on critical data protection capabilities in a single, integrated solution. You deal with only one vendor and avoid having to piece together multiple, distinct solutions.

With Data Guardian, all of the key data protection capabilities are managed from a single, centralized console — the same console provided by other Dell Data Security solutions. Whether you are integrating Data Guardian into your existing Dell Data Security environment or adding Dell Data Security solutions after implementing Data Guardian, your administrators do not need to learn new skills or juggle new interfaces.

Choosing Data Guardian also lets you seamlessly integrate additional data security capabilities from Dell for comprehensive data security. For example, by combining Data Guardian with Dell Endpoint Security Suite Enterprise, you can supplement data protection with robust advanced threat prevention. And you can manage all capabilities from a single console.

Conclusion

To address the growing prevalence of insider threats, organizations need innovative methods to protect data. With Dell Data Guardian, your organization can safeguard data across a full range of employee activities — including emailing files beyond enterprise firewalls, transferring files to personal devices or external storage, and sharing files through cloud services. Data Guardian brings together robust encryption and EDRM capabilities with file activity monitoring, visualization and reporting in a single, integrated solution. You can facilitate secure productivity while making sure your enterprise data stays accessible only to authorized people.

Learn More

To learn more about Dell Data Guardian, contact your Dell representative or visit: Dell.com/DataSecurity

[1] Clearswift, "Clearswift Insider Threat Index (CITI)," 2015, http://pages.clearswift.com/rs/591-QHZ-135/images/Clearswift_Insider_Threat_Index_2015_US.pdf

[2] Dell Data Guardian currently offers plug-ins for Microsoft Office that support Word (.docx, .docm); Excel (.xlsx, .xlsm); and PowerPoint (.pptx, .pptm) files. Support for additional file types will be available in the future. For the latest product support information, visit: support.dell.com