Enable secure productivity for an increasingly mobile and collaborative workforce

Protect, control and monitor your data where and how it is used with Dell Data Guardian

Introduction

Keeping sensitive enterprise information safe has never been easy. But as organizations increasingly support and facilitate work beyond their physical walls, data is at even greater risk. Today, critical business data can be anywhere and everywhere. As a result, organizations must guard against a growing array of data security challenges, including insider threats.

Insider threats include not only malicious activities but also negligent and accidental behaviors. As employees increasingly use personal devices and access enterprise data through public networks, they put enterprise data at great risk. If employees mistakenly 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. Missing data caused by these and other insider threats can result in loss of intellectual property, new cases of fraud, a damaged company reputation, regulatory fines and more.

While most employees have a general awareness of security risks, one in five feel that protecting company data is not their responsibility.[1] Some take critical business data when they leave — with potentially catastrophic, headline-grabbing consequences. In other cases, data can be purposely transferred out of an enterprise environment. And employees are not the only possible threat. Only one in three companies is aware that on average, 89 vendors access their systems on a regular basis.[2]

Dell Data Guardian

- Robust encryption
- Enterprise digital rights management (EDRM)
- Protection for mobile devices
- File activity monitoring

In an era when work is more mobile and collaborative than ever before, organizations must refocus data security from securing devices to guarding data wherever it goes and however it is used. They need ways to control who can access data and in what circumstances, as well as ways to monitor how data is being accessed and used. They also require integrated security solutions that offer a full range of data protection capabilities through a single console.

Raising the data security bar

Organizations have already employed a range of data security solutions to address threats. For example, some have implemented advanced threat prevention solutions to help protect against a growing variety of malware and viruses. These technologies are critical, but to support today's mobile workstyles and open collaboration practices, organizations must do more. They need to protect data from theft, loss and unauthorized access as it is used by employees on the move and shared beyond the corporate perimeter.

How will your organization support flexible work models without risking data security? What does a complete, successful data protection strategy look like?

Implementing comprehensive protection and management of data as it traverses devices, services and geographies

As users continue to work in new ways, organizations should take a new approach to data security — an approach that guards data no matter how and where it is used. Once data is protected, it must stay protected.

You need to protect data from the moment it is created on desktops, laptops, tablets and smartphones. Data protection must then persist as your employees move files to personal email accounts or cloud-based services. Data should remain protected as employees access it on a wide range of devices, in a variety of locations and on any type of network. You must ensure data stays secure as employees collaborate, forwarding emails or sharing files among a broad array of coworkers, partners and customers. Through all of these actions and behaviors, you need ways to see who is accessing data and how.

Addressing the challenges of guarding data in motion has been a top priority for Dell Security. By listening to customers and drawing on its own deep security expertise, Dell has developed a data security solution that addresses the need to guard data as employees create, share and use it in a variety of ways.

Protecting data however it is used with Dell Data Guardian

Dell Data Guardian can help you protect data, control access to data and monitor data activity and location. With Data Guardian, data is protected throughout its lifecycle.

- **Protect data wherever it goes**
  Data Guardian keeps data protected while employees move it among different devices, services and geographies.
- **Control how data can be accessed**
  With Data Guardian, you can define who can access specific data, when that data can be accessed and how.
- **Monitor who is accessing data and from where**
  Data Guardian provides visibility into who is using data, how data is being used and from where data is being accessed. You can detect potential problems before they occur and identify miscreants when necessary.

Data Guardian offers all of the capabilities you need for comprehensive data protection, control and monitoring.

Encryption

Encryption is the foundation of data protection. With Data Guardian, you can encrypt individual files and maintain that encryption wherever files travel and however they are used.

Consider the case of an employee creating a new Microsoft® PowerPoint® presentation at work. Whether she emails the file to a colleague, uploads it to a cloud service or transfers it to her personal laptop using a USB key, the file remains encrypted at each step of the way. If her laptop is stolen or the cloud service is hacked, data is unreadable to unauthorized users. Encryption helps you avoid not only the loss of information but also the regulatory fines that might accompany data loss.

With Data Guardian, applying encryption to files is simple. Plug-ins for Microsoft Office run seamlessly in the background, automatically encrypting Word, Excel® and PowerPoint files, including macro-enabled files. Encryption extends to the cloud. Using Data Guardian, all files are encrypted when they are sent to the cloud.

You can prevent files from being readable by unauthorized individuals, even if employees transfer files out of your enterprise environment to personal environments or external devices. An advertising agency might decide, for example, to protect a spreadsheet that contains client contact information so a departing employee could not easily poach clients. Or an electronics manufacturer might want to protect intellectual property by keeping a patent document from being readable by unauthorized users, even if an employee were to send it to a competitor.

Enterprise digital rights management (EDRM)

With Data Guardian enterprise digital rights management (EDRM) capabilities, you can control who can access data, what they can access and in what circumstances. For example, you might set policies that restrict access to documents before a certain date. You could ensure sales and marketing materials prepared for an upcoming product release would be viewed only by internal marketing and product development teams before the product's official announcement.

Data Guardian gives you flexibility to tailor EDRM policies for your specific requirements. You might implement read/write, copy/paste or expiry/embargo, as well as sharing and printing policies.

Protection for mobile devices

You might decide that certain files can be accessed only within a secure environment. Using the Data Guardian Mobile app, you can create a secure file container on mobile devices — including ones on the iOS and Google Android™ platforms — that lets employees securely open and edit files.

It can also enable the use of personally owned devices without allowing employees to move enterprise data to personal environments. With this secure container, files synchronized to the smart device remain encrypted, helping you meet strict compliance rules by making files accessible only within that environment. Geofencing capabilities let you restrict data access to particular geographies. You can also enforce copy/paste and screen capture restrictions. If you want, you can enable secure use of cloud-based sync-and-share services from Box, Dropbox, Google and Microsoft.

Monitoring

Which employees are accessing sensitive files? What are they doing with those files? Data Guardian lets you monitor file access and usage. Use these capabilities as a preventive measure, spotting 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 how policies were abused or seeing how data files fell into the wrong hands. Or use detailed file monitoring to help streamline audits and demonstrate regulatory compliance.

Data Guardian helps reduce management complexity by incorporating these capabilities into a single, integrated solution. You can manage encryption, keys and access recovery; enforce policies; and conduct other management tasks from a central console.

Guard your data with comprehensive protection

Data Guardian is part of the Dell Data Security portfolio, which combines Dell innovation with technologies from RSA, VMware, Mozy and Cylance to offer a broad range of capabilities for preventing threats and maintaining secure productivity. Advanced threat prevention solutions help stop malware, ransomware and other threats before they can do serious harm. These solutions take a more proactive approach than traditional signature-based solutions, which attempt to detect and remediate behaviors that are already causing damage. Data Guardian and other data protection solutions are designed to maintain secure productivity, protecting the way your people work by securing data wherever it goes and however it is used.

Supporting new ways of working without compromising security

Organizations today need a new approach to data security — one that can guard data as it is used in a growing variety of ways. Data Guardian draws on powerful data protection capabilities to safeguard data as it is created, transferred, shared and stored. With Data Guardian, you can gain the confidence to support new, more flexible ways of working while minimizing risks.

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] Bomgar, “Vendor Vulnerability: How to Prevent the Security Risk of Third-Party Suppliers,” 2016, www.bomgar.com/assets/documents/Bomgar-Vendor-Vulnerability-Index-2016.pdf