Securing the data lifecycle

Protect data wherever it goes and however it is used

Introduction

The way people work is changing. Organizations are enabling more anywhere, anytime work as a way to increase worker flexibility and boost productivity. To get that work done, 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.

As a result of these changes, critical business data is accessed and stored anywhere and everywhere — including places that put data at increased risk. Studies show that 35 percent of employees spend an average of two hours each week working in public places,[1] and 87 percent of senior managers upload business information on personal email or cloud accounts.[2] You need to protect data not only at rest but also in motion as it's accessed through the wireless network of a local coffee shop, uploaded to a cloud service or sent from an enterprise email account to a personal one.

Reality check

New modes of working are changing data realities. How should you respond?

Reality: Data is accessed on a variety of devices, locations and networks.
Response: Control access to data based on *who*, *what*, *where* and *when*.

Reality: Data is created on endpoints and moved through email and cloud.
Response: Keep critical business files encrypted at rest and in motion.

Reality: Colleagues use your data, in whole or in part, and can share it with others you might not know.
Response: Empower secure collaboration by controlling how data is used — including copying, pasting and printing.

Reality: You must prove to auditors, clients and other stakeholders that tight data security is in place to protect files.
Response: Track file access activity for compliance, forensics and policy effectiveness.

Insider threats are also an increasing possibility and a growing concern for organizations everywhere. One in five employees feel that company data is not their responsibility.[3] Some even take critical business data when they leave — with potentially catastrophic consequences, as evidenced by the recent "Panama Papers" incident in which 11.5 million files of secret bank accounts were leaked to the press. 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.[4]

Shortcomings of existing security solutions

Available solutions fail to meet the full range of challenges organizations now face across the data lifecycle.

No protection for data in motion
Many data security solutions focus on data at rest and are unable to protect data once it leaves the premises or certain devices. Organizations need ways to support an increasingly mobile workforce that uses a variety of means to create, access and share information.

Lack of visibility
The absence of any data monitoring creates blind spots for organizations about how the lost or leaked data is being used.

Absence of integrated solutions
The traditional approach has been to purchase point solutions as specific needs arise. Many organizations end up purchasing separate products for data loss prevention (DLP), digital rights management (DRM), file access control and analytics — each with a separate management console. As a result, IT has no way to easily administer end-to-end policies.

What does it take to secure data across its lifecycle?

Keeping data safe across its lifecycle requires a comprehensive solution — one that can secure, maintain authority and provide visibility.

Security: Protect data on the go
Organizations need to safeguard data not only as it resides on PCs and mobile devices but also as it moves between them. Data must remain secure when employees share it in cloud storage, send it to a personal email account or transfer it to an external device. Encryption is often the best way to protect data in motion as it traverses devices, cloud services and geographies.

Authority: Define how data can be accessed
Data loss prevention and digital rights management are needed to define who can access specific data, when and for what purposes. Capabilities such as setting policies for copy/paste and printing are essential.

Visibility: Track who is accessing data and how data is used
Tapping into detailed information on file usage can help you detect potential problems before they inflict serious damage on the business. Visibility into data usage can also help with forensics. Forensics based on file access helps to quickly contain the damage, minimize the impact on an organization and identify miscreants.

Instead of acquiring these capabilities by collecting point solutions, choose an integrated solution that can offer a full range of data protection features across devices and operating systems. With an integrated solution, you can simplify and centralize administration by managing all of these data protection capabilities through a single console.

Protect data wherever it goes with Dell Data Protection | Secure Lifecycle

Dell Data Protection | Secure Lifecycle is an integrated solution that can help you secure data, maintain authority over how data is used and gain visibility into data use. The solution works with Dell and non-Dell devices as well as different operating systems.

Encryption capabilities protect data wherever it goes — including mobile devices and cloud services — without interfering with workflows and worker productivity. DLP and DRM enable you to control the who, what, when, where and how of data usage. And visibility into data usage helps identify any deviant behavior to prevent loss of critical information.

Made for today's security realities

Today, data spends more and more time in areas that lack the physical security of the corporate data center. With expanding groups of mobile and remote employees accessing data, emailing it from place to place and sharing or storing it in public clouds, organizations are reassessing their approach to data protection. These realities require a solution that covers the entire lifecycle of data, and includes ways to control how data is used and to track its use.

Now you can have always-on protection for your critical data, wherever it is used, with Dell Data Protection | Secure Lifecycle. Gain the capabilities you need in an integrated solution that is simple to deploy and manage.

Learn More

To learn more about Dell Data Protection | Secure Lifecycle, contact your Dell representative or visit: Dell.com/DataSecurity

[1] "Dell and Intel Study Uncovers Truth Behind Technology and the Workforce," February 2014, http://www.dell.com/learn/hr/en/hrcorp1/press-releases/2014-12-02-dell-intel-study-uncovers-truth-behind-technology

[2] Stroz Friedberg, "On the Pulse: Information Security Risk in American Business," 2013, https://www.strozfriedberg.com/wp-content/uploads/2014/01/Stroz-Friedberg_On-the-Pulse_Information-Security-in-American-Business.pdf

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

[4] 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