Protect data stored and shared in public cloud storage.

Dell Data Protection | Cloud Edition

Today employees, vendors and partners routinely move, share and store files in cloud storage services like Box, Dropbox, Google Drive and Microsoft OneDrive. The sheer ease and convenience with which people can collaborate enhances productivity, allowing them to work the way they want using the devices they want.

Yet, as convenient as they are, public cloud storage services have also introduced a huge data security gap. As soon as users save files in a public cloud, IT immediately—and irretrievably—loses control over data security. From that point forward, users can share that data with whomever they want, whenever they want. They can continue to share information after they leave the company, or forget to stop sharing with a former partner, or their account can be hacked. In these all too common scenarios, data security suddenly relies on the tenuous hope that data will remain protected.

Dell Data Protection | Cloud Edition helps put IT back in control of data security, protecting data as it moves into and out of public clouds, with a transparent encryption and decryption process that lets people use cloud storage as they always have, without disruption. Cloud Edition is also reinforced by Dell Data Protection | Mobile Edition to secure data even when it is accessed on a smartphone or tablet.

The solutions are fully integrated with Dell Data Protection | Enterprise Edition, a comprehensive security platform that protects data across all endpoints, from personally and company owned computers, removable media devices, smartphones and tablets, to public and private clouds.

Comprehensive protection, simple management

Cloud Edition gives IT granular control over which users can view data, including shared files, as well as which endpoints users can employ to access the data, and how they can view the data. It also enables you to immediately revoke access, remotely enforce policies or remotely wipe stored content, monitor and audit as needed.

Cloud Edition enables IT administrators to:

- **Control File Sharing** - Create white lists of email addresses that users are allowed to use for file sharing
- **Monitor Usage** - Monitor all known IP addresses for cloud storage services and match them with the application process. Monitoring operates independently of a browser, and captures all traffic no matter what cloud storage application is in use
- **Protect** - Control data through transparent client-side encryption, encrypt traffic captured as it moves into the cloud, and decrypt traffic captured as it moves out of the cloud
- **Centrally Manage** - Centrally manage encryption, encryption keys, access recovery and remote wipe of content, policies and forensics
- **Audit Events and Create Reports** - Audit and report on file activity, files synced, files accessed by whom, where and when, and compile compliance reports
- **Support Mobile Devices** - Access encrypted data in the cloud from iOS and Android platforms
- **Enforce Policies** - Enforce policies for access to cloud services, public folders, applications, key expirations and polling periods using the Cloud Edition client

Enhanced end user productivity

Cloud Edition provides transparent encryption as files

move into the cloud, and transparent decryption as files move out of the cloud. Processes for file sharing, access and storage are also transparent to end-users, enabling workers to use cloud storage exactly as they always have.

When combined with Mobile Edition, the solutions help keep data protected when it is accessed on Android and iOS smartphones and tablets, both personally and company owned. Together, they enable end users to work when, where, and how they want while IT remains in control of data and compliance.

Efficient compliance

Currently, data stored in cloud storage services is vulnerable to account hacking, user control after termination, SSL weaknesses, or is left to the safeguards of the provider, since the provider is performing the actual encryption. Cloud Edition provides an additional encryption key, stored on your network and owned by you, so data is guarded even from the storage provider itself. This added layer of protection between your data and the cloud service provider helps you stay in compliance with data privacy regulations like HIPAA, HITECH, PCI, and others. It also enables you to review and analyze, to verify policy enforcement, and to make adjustments as demands dictate.

Because Cloud Edition is centrally managed through a single console, security teams gain increased visibility into access, usage and policy enforcement, greatly reducing the compliance workload.

Dell Data Protection | Enterprise Edition

Cloud Edition is part of the integrated Dell Data Protection | Enterprise Edition platform, which secures data across all physical and virtual endpoints, including:

- Desktops and laptops
- Smartphones and tablets
- Removable media
- Public and private clouds
- Self-encrypting drives
- BitLocker

Simple to install and easy to maintain, Enterprise Edition helps protect data wherever it goes.

Technical Specifications

DDP | Cloud Edition is available for mixed vendor environments that meet the below specifications.

Supported cloud services:

- **Box**
- **Dropbox, & Dropbox for Business**
- **Google Drive**
- **Microsoft OneDrive & OneDrive for Business**

Supported Client Platforms:

- **Windows 7, 8, 8.1, 10**
- **Mac OS X 10.8, 10.9, 10.10**
- **iOS 6.1.6+**
- **Android 4.0+**

Supported Encryption Algorithm:

- **AE 256**

Learn more at www.Dell.com/Datasecurity

11/2015