COMMVAULT®

▶ Commvault Secures Endpoint Data with Data Loss Prevention

▶ QUICK FACTS

As the global workforce continues to become more mobile, there is an increased risk of breach and data leakage from lost or stolen laptops. IT leaders want to keep corporate data secure and protected and out of the hands of unauthorized users, minimizing compliance and litigation risks while protecting intellectual property. They also want to minimize the hardware and resource costs of getting users working and productive again.

>$49,000
is the Average Cost of a lost laptop[1]

>7%
of laptops are lost over their lifetime[2]

80%
of the cost of a lost laptop is from data breach[3]

▶ Keeping the mobile workforce working efficiently means protecting their devices, while making it easy for them to access and recover lost or deleted files. Commvault protects your data wherever it lives with secure, efficient backup and recovery.

Commvault® software is a complete endpoint data protection solution that increases end user productivity by providing unparalleled access to protected content for users to search, sync, and share without compromise to security. Data resides in the ContentStore, a virtual repository for all Commvault software managed data that drives efficiency and enhances value from protected content, through access, security, governance, and analytics. Data Loss Prevention ensures critical business data is protected and secure in the event of an unforeseen incident. It reduces both the risks and costs associated with data breach.

▶ DATA ENCRYPTION

With Commvault software, files and folders can be encrypted by the administrator or end user, preventing unauthorized access in the event of a loss or breach. Without the user-defined pass-key, encrypted content from a lost or stolen endpoint cannot be accessed.

Data Encryption Features:

- Administrator managed policies that define what documents are locked (encrypted), encryption behavior, and how data can be unlocked
- User managed encryption using the Windows Explorer plug-in
- Pass-key is only required if a laptop is marked as lost or is unable to contact the server

▶ REMOTE WIPE

Commvault software provides remote wipe capabilities per administrator defined policy to prevent a breach of data from lost or stolen laptops.

Remote Wipe Features:

- Administrator managed policies that define a period of time, in days, when the client has not contacted the server, to initiate a secure erase of data
- Users can mark endpoint as lost or stolen from the web console or the administrator can perform the remote wipe from the admin console
- Ability to erase only protected content or the entire hard drive
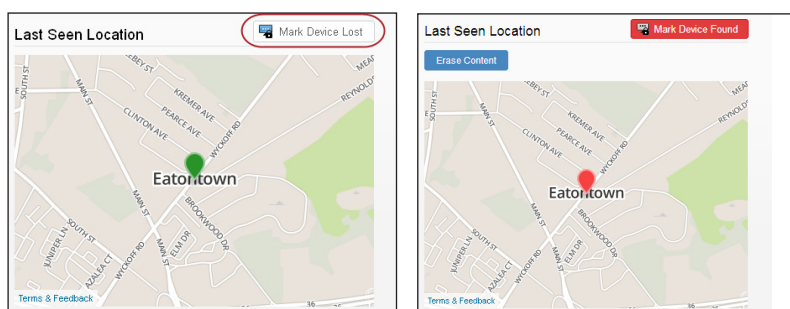- Content is erased and blocks are zeroed out

Figure 1: Users can mark their laptop as stolen and remotely wipe select content or the entire hard drive

▶ GEO-LOCATION

Commvault software provides the ability to track and record the location history of a laptop at the time of the last connection with the server. That information can then be used to track a device that has been lost or stolen.

Geo-Location Features:

- Location is identified based on the vector of endpoint IP address on the last connection
- Details such as street, city, state, and country are provided
- A map interface powered by Mapbox Streets provides a graphical representation for the location and device status
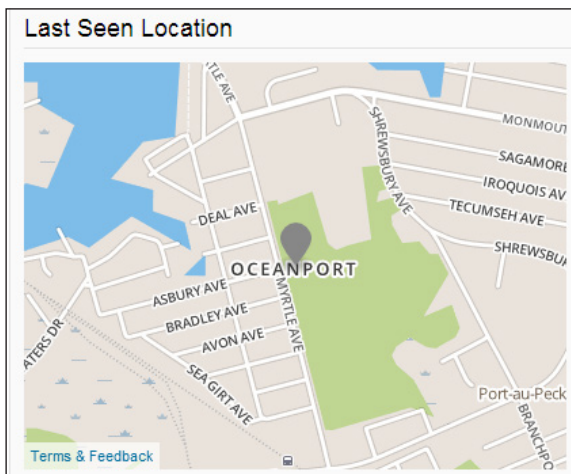

Figure 2: Map interface displays the location of the laptop

Converged Search of Endpoint, Email, Data Center and Cloud

Transform your tactical data protection and archiving tools into a unified strategic asset that alleviates your greatest information management burdens.

READ NOW

commvau.lt/2n6fVz8

▶ RESOURCES

123 Averages Based On The Billion Dollar Lost Laptop Problem Ponemon Institute, October 2010

▶ To learn more about the full benefits of Commvault Endpoint Data Protection software and the importance of endpoint data protection and access, visit **commvault.com/solutions/endpoint-data-protection**.

COMMVAULT