COMMVAULT®

# Why Laptop Security Cannot Wait

Laptop theft can strike at the heart of a company's reputation and revenue. Consider the sheer number of laptops that store corporate data, much of it highly confidential. In fact, whether the device is company-issued or a personal BYOD (Bring Your Own Device), employees average three mobile devices per user.[1] That's a lot of traveling devices and a lot of insecurity. If these devices contain unprotected and sensitive information, then the consequences can get very ugly, very fast.

Serious data breaches from stolen laptops can happen to any company, regardless of its size. In 2014, an unhappy employee stole over 55 laptops from two locations: Coca-Cola's Atlanta headquarters and a local bottling plant. The theft netted tens of thousands of unencrypted HR records, which stored personal information on over 74,000 employees and contractors.[2] The records contained massive amounts of personally identifiable information (PII) including 18,000 Social Security numbers and many more addresses, names, and driver's license numbers. An employee filed a class action suit against Coca Cola on behalf of everyone whose PII was breached.

1 Forrester Research, Market Trends: Secure File Sharing and Collaboration In The Enterprise, Q1 2014
2 InfoSecurity, "74,000 Data Records Breached on Stolen Coca-Cola Laptops," 2014

In April 2015, a US Healthworks employee left his laptop in his car where it was stolen during the night.[3] The loss extended far beyond a single individual. The laptop was protected by a password but the data on it was not encrypted even though it contained PII including customer names, addresses, dates of birth, job titles, and Social Security numbers. The healthcare firm offered employees free enrollment in identity protection services for one year – frankly, the least they could do.

## SECURING THE ENTERPRISE

Although the majority of user devices will not be seriously compromised, they are all at risk for serious data loss and exposure. There are six critical functions that work together to efficiently secure endpoint data.

1. Controlled access secures data against fake user credentials. The first line of computer security is user password. End-users find it difficult to manually generate and remember passwords, so often use the same weak password for most of their applications and web services. Secure single sign-on (SSO) or two-factor authentication (2FA) adds a strong layer of access control to mobile devices.
2. File-level encryption defeats data breaches on desktops and laptops. Although many high-profile data breaches are network attacks, many of them are from stolen computers. With encryption, you can be sure that even if a thief steals a laptop its data is useless to them.
3. Geo-tracking lets you narrow down a missing laptop's location by country, state, city, and zip code; some geo-tracking software narrows it as far as a street. If the laptop appears miles away from its location, you can initiate a remote wipe.
4. Remote wiping turns the loss of a laptop into an annoyance instead of a disaster. Full or selective wipes will zero out blocks so that even a data recovery tool will not help the thief.
5. Policy-driven automation lets IT efficiently manage security and protection for mobile devices. When it's time to make changes, IT only makes changes to the governing policy.
6. Secure data transfer protects moving data over HTTPS without the added cost of a VPN. Built-in SSL certificates and strong data encryption protects data-in-transit just as encryption protects data on device hard drives.

## COMMVAULT ENDPOINT DATA PROTECTION

Filling these security needs usually takes multiple point products. Now you can secure corporate information wherever it resides with Commvault Endpoint Data Protection. You and your end-users will be confident that even if a device is breached, your corporate data will stay secure.

**Stop the Bad Guys Cold: Securing Your Mobile Data**[i]

Mobile devices are inherently at risk for loss and theft. Managing that risk is the heart of mobile security, but without the right tools it's a losing game. Read how to protect your mobile data with the strong security and data loss prevention that stops the bad guys cold.

READ NOW

PDF



3 pymnt.com, "Stolen, Unencrypted Laptop Leads To US HealthWorks Data Breach," 2015

Endpoint Data Protection does not only secure endpoint devices; it also backs up and restores remote data, enables compliance and eDiscovery, and grants secure file sharing. It also increases productivity with policy-based administration and end-user self-service. All of these operate securely within IT's control.

- Access to files from virtually anywhere and any device including automated sync of files and folders. Automated file and folder sync across desktops and laptops keep all files immediate and available and secure file sharing enables smooth collaboration.
- Commvault Endpoint data protection software administers policy-driven security. It encrypts files and folders to prevent unauthorized access in the event of a laptop loss or breach, and provides remote wipe capabilities of entire drives or protected data sets so that data will not fall into the wrong hands. IP address monitoring and geo-location identify a laptop's last server sign-on location down to the street level.
- Efficiently secure user access with Single Sign-on based on Active Directory and roles-based access controls (RBAC). Auto-discovery works with Active Directory to automatically discover and deploy new clients.
- Commvault centralizes data in ContentStore for unified compliance and eDiscovery, no matter where your employees are located. Run compliance and eDiscovery on ContentStore and email archives, and set legal holds.

Even with this breadth of endpoint services, Commvault does not stop there. Endpoint Data Protection exists as a standalone solution, or you can seamlessly integrate it with the Commvault software platform for complete enterprise protection, security, file sharing, eDiscovery and analytics.

The majority of information workers use three or more devices

**FORRESTER RESEARCH,**
*Market Trends: Secure File Sharing and Collaboration In The Enterprise, Q1 2014*

## RESOURCES

i http://commvau.lt/1M1pSA0

To learn more about protecting endpoint and mobile devices with Commvault® software, visit comvault.com/solutions/endpoint-data-protection.



COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM