COMMVAULT®

Stop the Bad Guys Cold: Securing Your Mobile Data

MOBILE DEVICES ARE LOST AND STOLEN EVERY DAY. DON'T LET YOUR CORPORATE DATA GO DOWN WITH THEM.

Protecting your company's mobile data is a business imperative. It's also a multi-functional process including backup and restore, safe file sharing, compliance and eDiscovery, analytics – **and strong security and data loss prevention that stops the bad guys cold**.

Apply encryption, IP address tracking, remote wiping, geo-location, access control – and do it all with centralized, policy-based management and auto-discovery.

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.

Look at the sheer number of remote and mobile devices that have access to corporate data. Whether company-issued or BYOD (Bring Your Own Device), employees average three mobile devices per user. That's a lot of traveling devices and a lot of insecurity. Laptops are the worst security offenders: users commonly keep work files on the hard drive, and losing a laptop is an invitation to anyone who cares to take a look at the data.

The result is a growing number of data breaches throughout the world, many of them thanks to lost or stolen laptops. A 2014 study by the Ponemon Institute surveyed enterprises located all over the world, revealing that the average cost to a company was $3.5 million in US dollars – 15% higher than in 2013.[1] The 2015 version of the study reported that in the United States, the average cost for each breached confidential record averaged $217 – and the average cost per breach soared to $6.5 million.[2] Not all of these data breaches occurred on mobile devices but many of them did.

Serious data breaches can happen to anyone, anywhere. In 2014, a disgruntled employee stole laptops from Coca-Cola's Atlanta headquarters. Among other data, the laptops contained unencrypted HR records containing personal information on over 70,000 people – suppliers, workers and contractors.[3]

The level of the breach was devastating. The records listed Social Security numbers, addresses, names, driver's license numbers, and many other details; all there for the taking.

Simply telling employees to keep tabs on their mobile devices in airports, hotels, homes and HQ is never going to be enough. Your company needs a way to let your employees do their work while you transparently protect their device against the bad guys.

Fortunately the technology is out there. Here's how to find it.

CIO Spotlight: Controlling Data Risk in the BYOD Onslaught[i]

Read about the five areas you need to know to mitigate risk and protect data in the BYOD era.

READ NOW

THE FEATURES YOU ABSOLUTELY, POSITIVELY MUST HAVE

Mobile and remote endpoint solutions are increasingly popular. They also have a spectrum of capabilities ranging from a simple solution set to a mobile protection platform. We prefer the latter, where capabilities from data protection to compliance to security work together to give you complete mobile protection.

Let's look at the critical security features that your solution set must have: granular file encryption to frustrate a would-be thief. Geo-location and IP address logging to find a lost or stolen laptop before the bad guys get to

1 Ponemon Institute, "Ponemon Institute Releases 2014 Cost of Data Breach: Global Analysis," 2014
2 Analyst Ponemon Institute, "Ponemon Institute Releases 2015 Cost of Data Breach: Global Analysis," 2015
3 InfoSecurity, "74,000 Data Records Breached on Stolen Coca-Cola Laptops," 2014

it. Remote wipe to delete files when you just can't find the device in time. Policies to automate security actions whenever and wherever needed. Let's take a closer look.

ONE. ENCRYPTION – KEEP THEM FROM READING STOLEN DATA

In 2014, the healthcare industry experienced a record number of HIPAA breaches. Almost 79% of these breaches occurred using lost or stolen computers and USB thumb drives – all of which were storing unencrypted data.[4]

Encryption is the beating heart of securing data wherever it resides. It is crucial for securing data that lives beyond the boundaries of the firewall. In this world, securing devices against theft is important, but some theft and loss will always occur. Encryption makes sure that even if a thief gains access to your data, they cannot understand it.

For top security, choose encryption products that follow industry and government regulations like HIPAA and SOX. The FIPS 140-2 security standard fits this bill. Also look for granular encryption features that work selectively at the folder and file levels, and that enable both IT-set policies and end-users to encrypt files.

TWO. ACCESS CONTROL - MAKE SURE THEY ARE WHO THEY SAY THEY ARE

Most employees set weak passwords, rarely change their passwords, and when they do change them they do it by adding a single digit. These passwords are easy to crack even by an aspiring password cracker. With two-factor authentication (2FA), or a layered login system like SSO, your mobile passwords will be a tougher nut to crack.

Improve data security with 2FA to be really certain that the person signing in is the person who is supposed to be. 2FA requires a user ID and password plus a second layer of authentication, such as a text code sent only to their cell phone or on a small authentication device that they carry.

Another method of controlling access without also requiring 2FA is a secure Single Sign-on (SSO). SSO is a concept that developers implement using different specs; SAML is one of the best-known on the web. The SAML configuration does not pass a browser user's credentials immediately to the user's requested service provider, but first runs it through a separate identity provider. The IdP checks the credentials using Active Directory or other access services, and then passes it on to the service provider, who checks it again. Only then is the user allowed in.

THREE. REMOTE WIPES - DELETE THE DATA BEFORE THEY SEE IT

The risk of lost and stolen laptops is always present. Lower that risk by selectively wiping corporate data on missing laptops. Automatic remote wipes are not highly popular with device owners, so go with a toolset

> "New threats, vulnerabilities and gaps in business processes are being discovered constantly that add layers of complexity, while new solutions are being proposed with almost the same breakneck frequency. There's never a dull day in the world of security, especially when enterprise mobility architecture must also enable balanced BYOD programs that equip professionals with the tools necessary to respond, collaborate and produce at a more efficient clip."
>
> **ISRAEL LIFSHITZ**
> *"Reducing Risk: How to Make BYOD Safer" Security Magazine, 2015*

4 PrecyseSource, "The Cause of a Data Breach – Lost/Stolen Laptops or a Security Design Flaw," 2014

that enables selecting wiping. IT can set policies to automatically start a remote wipe based on a set period of time between the laptop and its last server connection.

Ideally users can initiate their own secure data erase without calling IT. In any case, the remote wipe should not only delete content but also zero out blocks, so a thief cannot use a data recovery tool to view deleted content.

FOUR. GEO-LOCATION - FIND THE LAPTOP BEFORE THEY DO

Geo-location helps to identify the laptop's location. For example, security software automatically logs in IP addresses to create server access records, while geo-location features locate the laptop's geographic location.

When a laptop is reported lost or stolen, administrators can identify the last known location. Look for a geo-location software that can narrow down a laptop's identification closer than a zip code, which is not by itself very helpful for finding the missing laptop. The software will provide the location and a marked map.

FIVE. POLICY-BASED AUTOMATION – SECURE DATA IN YOUR SLEEP

Automation is critical to maintaining control and scalability over mobile security. Security automation includes options like setting baseline responses based on server access times, selective or full remote wipes, and encryption based on users, roles and data priority.

Instead of making security changes to individual mobile devices – clearly the impossible dream – IT makes simple changes to controlling policies.

Another handy automated tool is automated device discovery. It is not at all uncommon for remote users to own three or more devices: simply owning a laptop, tablet and smartphone will do the trick. Multiply these two to four devices per employee by number of employees at your company, and you easily have hundreds to thousands of remote devices to secure. This is a manual impossibility, so make sure that the solution's automation tools include reliable auto-discovery.

WHERE DO WE GO FROM HERE?

Remote devices are a fact of life, company-owned or not. Some corporate advice tells CIOs to rid the company of BYOD devices.

This advice is short-sighted and ultimately futile. Employees already meld their work and personal lives, and every well-meaning corporate intention will not change that. Having said this, companies must be able to secure mobile devices whether they are company-owned or not.

The right mobile security tools will allow you to do this. The best mobile protection tools will do even more.

Is Your Data Secure?[ii]

View this infographic to see the 9 points you need to consider as your refine your BYOD strategy.

VIEW NOW

PDF

"More and more content is being created, edited, and shared at the edge on mobile devices such as laptops, tablets, and smartphones, raising accessibility, security, and protection concerns. Much of this data is confidential or otherwise sensitive corporate information. As a result, data protection requirements are rapidly evolving to include endpoint protection as a must-have."

ERIC BURGENER
IDC[5]

4 51 Research, "Backup to the Future," April 2014
5 Gartner, "Magic Quadrant for x86 Server Virtualization Infrastructure," July 2015

COMMVAULT ENDPOINT DATA PROTECTION

On the security and DLP side, Commvault Endpoint security features encrypt files and folders to prevent unauthorized access in the event of a laptop loss or breach. The software 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.

- Reduce security costs and risks by using policies to effectively manage global mobile security.
- Repel data breaches and exposure across the enterprise.
- Efficiently secure user access with Single Sign-on based on Active Directory and roles-based access controls (RBAC).
- Encrypt data without impacting backup or tiering performance, and rely on policies to selectively encrypt files and folders.

Finally, extend mobile protection with Commvault's full Endpoint platform. Security is a critical feature in the comprehensive platform that also provides endpoint backup and recovery, eDiscovery and compliance, secure file sharing and collaboration, and visual analysis.

RESOURCES

i http://commvau.lt/1LmGFn2
ii http://commvau.lt/1M4qh5e

5 IDC, "The Critical Need for Data Protection," 2014

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