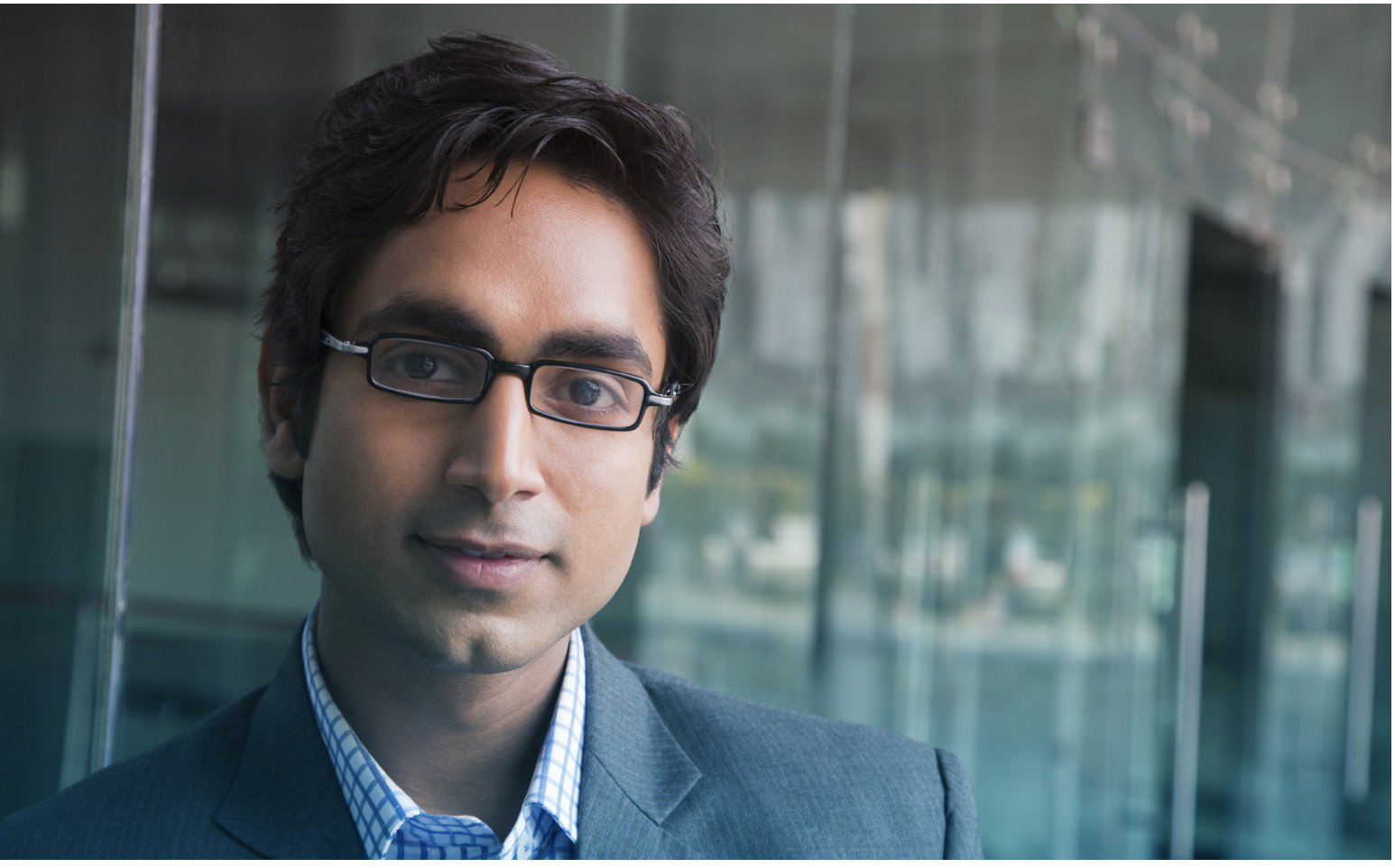
COMMVAULT®

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, eDiscovery, analytics – and strong security and data loss prevention that stops the bad guys cold.

Ally 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 worldwide, many of them thanks to lost or stolen laptops. The average cost varies by region, but it's safe to say that no one is immune from this problem. The Ponemon Institute compared the total average cost for a data breach in 2017 to the four-year average. The biggest increase in the average yearly costs was seen in the Middle East (+.83), United States (+.66) and Japan (+.52).[1] In this 2017 study, organizations in the United States had the highest total average cost at $7.35 million, followed by the Middle East at $4.94 million.[2]

Serious data breaches can happen to anyone, anywhere, and under some strange circumstances. A hard drive containing the personal information of approximately one million people was stolen in 2017 from a Washington State University storage unit in Olympia, WA. Information on the personal hard drive was part of the research the university had conducted for school districts, government offices, and other outside agencies; Social Security numbers and health history were among the personal details stolen. The university has sent letters to individuals who may have been affected and will be offering them a free year of credit monitoring.[3]

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.

"Carefree attitudes towards data protection in the workplace, combined with the blending of our work and personal information on devices, an actively mobile workforce and the growing use of cloud services, has seen traditional network perimeters dissolve and data visibility diminish."

GUY EILON
Forcepoint[5]

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 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.

1 Ponemon Institute, "2017 Cost of Data Breach Study," June 2017
2 Ibid
3 IdentityForce.com, "2017 Data Breaches – The Worst So Far," December 2017
5 Forcepoint, "How Data Protection Will Drive ROI in 2018," March 6, 2018

ONE: ENCRYPTION – KEEP THEM FROM READING STOLEN DATA

Although security improvements have helped in reducing HIPAA breaches in 2017, as seen in the reduction of breaches with hundreds of thousands of records, breaches of more than 10,000 records have remained fairly constant year over year. In 2015, there were 52 breaches of 10,000 or more records. That figure jumped to 82 in 2016. There were 78 healthcare data breaches in 2017 involving more than 10,000 records.[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, GDPR 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, or 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-knowing 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 Director or other access services, and them 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 that enables selective wiping. IT can set policies to automatically start a

4 HIPAA Journal, "Largest Healthcare Data Breaches of 2017," January 2018

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 control 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 the 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 now a fact of life, company-owned or not. It's hard to believe that CIOs were once told to try and get rid 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?

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

READ NOW

http://bit.ly/1pmf8b3

COMMVAULT ENDPOINT DATA PROTECTION

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.
- Mitigate the risk of data breaches and data exposure across the enterprise.
- Efficiently secure user access with SSO based on Active Director 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, Commvault endpoint data protection provides complete end-user data management with security, protection, visibility, and productivity advantages that safeguard business continuity – with on premises, cloud/hybrid, and SaaS solutions. Advanced search and secure file sharing options bring even more functionality.

Regain control and effectively manage company data – even outside the data center.

To learn more about protecting endpoint and mobile devices with Commvault software, visit **commvault.com/endpoint**.

COMMVAULT

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