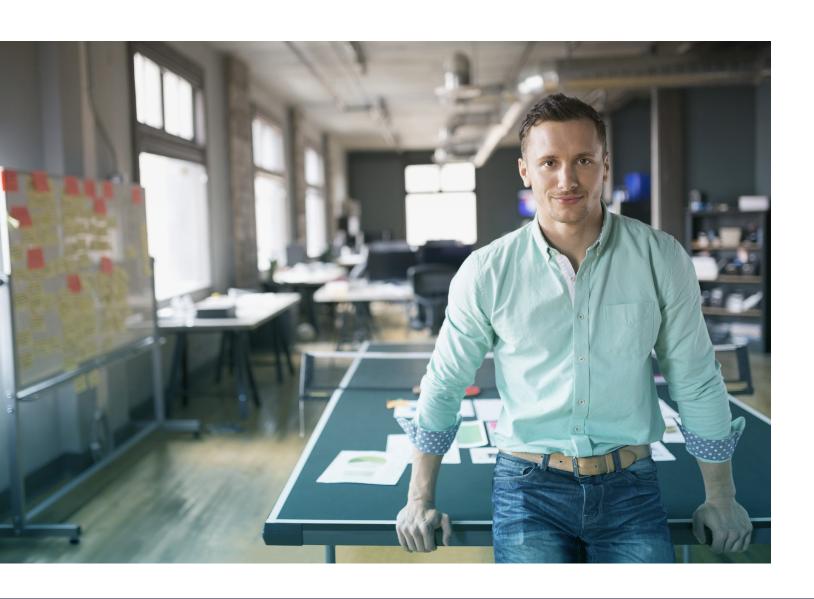# COMMVAULT®

▶ # CIO Spotlight: Controlling Data Risk in the BYOD Onslaught

The BYOD era is in full swing, posing a higher level of data security risk to enterprises. CIOs are faced with balancing the needs of workers to be more mobile and have more choice with the needs of the enterprise to protect its data regardless of the delivery channel. **Here are five areas that support risk mitigation and data protection, the solution to controlling data in the BYOD era.**

Data protection has always been a challenge, even when data flow was, more or less, confined to a closed network system. Now, we have the BYOD (Bring Your Own Device) era in which your employees and contractors basically feel they should be able to use whatever device they want to create information, share it and retrieve it at will. It makes previous risk mitigation issues look relatively simple. The challenge and potential for risk will only increase. IDC forecasted that by 2017, the number of global workers bringing their own smart phones to work will reach 328 million, up from the estimated 175 million workers doing so in 2014.[1] Company-purchased smart phones are also on the rise, with an anticipated 88 million in use by 2017, up from an estimated 69 million in 2014.

Tablets, too, are on a fast trajectory: Forrester Research reports that by 2017, nearly one in five tablet purchases will be made directly by companies. That equates to roughly 68 million tablets flooding the workplace.[2]

The numbers tell the story: BYOD and the flexibility it gives our highly mobile workers are here to stay. Happy as employees may be to use mobile devices, it presents an enormous challenge to CIOs who must set new standards and policies across the enterprise to protect data and mitigate risk. CIOs are working with their IT teams to put into place systems, rules and technology that will allow workers the computing freedom they desire, at the same time ensuring data is safe, retrievable and to the best possible extent, risk free.

Commvault® is at the forefront of offering solutions to reduce BYOD data security risks. Let's examine five key areas in which Commvault is addressing this evolving phenomenon of BYOD usage with its Commvault Edge® capabilities that provide file sharing, backup, search, retrieval, eDiscovery and access control across employee-owned mobile, desktop and laptop devices.

▶ ONE: ENABLING FILE SYNCHRONIZATION

Enterprises view BYOD as a way to increase productivity, and that means enabling work to continue without delay across the different devices used by employees. They need a file synchronization solution that meets data security objectives while enabling data access, whether the data was created at an office desktop, or on a laptop at a different location. While employees send files to the cloud or put them on USB drives, assumedly to work on later at home, often they may not be able to return to the file and wind up working on it again, back at the desktop or laptop. This creates risk because business data now resides in a potentially unsecured location and different versions of the files exist in different locations.

It's critical to managing risk to be able to pull different data sources into a single pool of protection, management and access. That is the principle Commvault Edge software is built upon as it answers customers' mobile worker data concerns by providing a secure, IT-owned alternative to data going outside their organization. Commvault Edge software enables automated file synchronization between PCs that can easily be setup via a web portal or natively in Microsoft Windows Explorer. It allows organizations to retain control over their data and information while empowering corporate employees to securely work on files no matter where they were created.

▶ TWO: EFFICIENTLY PROTECTING DATA

As employees use as many as three devices a day, data governance takes on more complexity. Even less sensitive data needs to be governed as files move across devices, and outside the enterprise, to suppliers and customers. Commvault Edge software helps to prevent data loss by enabling efficient, rapid and transparent backup for business-critical data on laptops and desktops through source-side deduplication, opportunistic scheduling, bandwidth throttling, flexible policy definition, and the intelligence to run a backup only if a file has changed.

1 IDC, Worldwide Business Use Smartphone 2013–2017 Forecast Update
2 Forrester Research, Global Business and Consumer Tablet Forecast Update, 2013 To 2017

THREE: EASILY ACCESSING FILES WHILE MOBILE

Your employees will no doubt expect the same quick access to files while using a mobile device as they have from their laptop or desktop. Commvault Edge software delivers data portability and self-service access to a secure, personal data cloud. Employees can use the Commvault Edge mobile app to access their files from virtually anywhere, at any time, and also protect files from their tablet or phones with the upload feature. Integration with Microsoft Windows Explorer extends Commvault software's robust recovery features. Using a web portal, end users can quickly retrieve and view all of their protected files and e-mail in the Simpana® ContentStore, Commvault's virtual repository of all managed information. The Edge solution provides global access to distributed files and documents without having to resort to consumer-grade file sharing and cloud backup services, which are outside an IT department's awareness and control.

FOUR: FAST eDISCOVERY

Similarly, it's necessary to be able to access and retrieve documents that have legal and compliance relevance, regardless of where they reside, without having to spend a lot of resources retrieving laptops from far flung locations. Since all protected data is centrally located in the ContentStore single repository, Commvault software streamlines discovery across all ESI (electronically stored information). Your IT teams will benefit from the simplified administration and rapid finding of key documents. Chief Legal Officers (CLOs) will be able to leverage this rapid response to create legal holds and choose the best strategy earlier in the audit or litigation process while also containing costs.

FIVE: DEALING WITH DATA ON LOST OR STOLEN ENDPOINTS

Scary stats: In 2013, out of 1,460 cyber events, 325 were caused by a data governance failure. For example, in September 2013, an employee at the Georgia Department of Labor accidentally emailed an internal file containing names and Social Security numbers of 4,457 career center customers to 1,000 recipients. These types of data breaches are becoming more prevalent. Employees' increasing mobility only adds more probability to these types of incidences.

One of the major enterprise concerns is the incidence of lost or stolen laptops. File encryption is essential to preventing unauthorized access that can occur. Remote wipe can be used to delete files and geo-location is a valuable tool in tracking lost laptops. Commvault Edge software allows your administrators to set policies that define granular encryption rules

"As employees continue to demand the ability to use the devices of their choosing, and as enterprises begin to incorporate BYOD within their organization, it is critical to ensure the right policies and strategies are in place so both sides — employees and enterprise — reap the benefits of leveraging employee-liable mobile devices."

BEN HOFFMAN
Research Analyst With IDC's Mobile Enterprise Research Team

down to the file level. It also provides remote wipe capability for laptops that will initiate a secure data erase at the request of the user. IT can also initiate a remote wipe based on a specified period of time where there is no contact between the server and laptop. Lastly, IP address logging can be used to identify where a laptop or desktop is located to determine if it has been lost or to help recover it.

► BYOD'S NEXT FRONTIER

Like it or not, CIOs and IT teams are going to face even more complex challenges as the mobility and BYOD trends continue to accelerate. To further minimize data loss and breach risk, CIOs are looking at new ideas such as 'geo-fencing' in which an employee can only access certain data within a specified physical distance from a secure building. It is a critical time in BYOD's evolution as executives are examining ways to advance data protection solutions that work in a mobile environment. Commvault believes these challenges can be met and is developing the next generation of Commvault Edge software to provide enterprises with the best data protection and security possible.

> By 2017, more than 60% of workloads will run in a cloud-enabled data center.
>
> Source: Cisco Global Cloud Index: Forecast and Methodology, 2012-2017.

► RESOURCES

i   commvault.com/resource-library/54bfc12d6793542f4a000098/idc-critical-need-for-edge-data-protection-analyst-report.pdf

► IDC: Critical Need for Edge Data Protection[i]
Read why IDC believes the need to protect sensitive data residing on desktops, laptops, and mobile devices is more critical than ever and how Commvault software can meet end user demands by delivering a solution that is secure and allows users access to their data anywhere and at any time.

COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.
COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM
© 2015 COMMVAULT SYSTEMS, INC. ALL RIGHTS RESERVED.