CIO
Strategic Marketing Services

EXECUTIVE BRIEF

Three Steps to Achieving Comprehensive Data Protection from Endpoint to Cloud Apps

AS DIGITAL TRANSFORMATION TAKES HOLD, THE DATA LANDSCAPE IS RAPIDLY EVOLVING. AS A RESULT, IT NEEDS TO REASSESS HOW TO MANAGE DATA TO MAINTAIN COMPLIANCE.

AS THE WELL-KNOWN Bob Dylan song lyrics proclaim, *Times they are a changin'*. With digital transformation rippling through organizations of every size, these words have never been truer. And if organizations want to keep pace, it's time for IT to start marching to the beat.

Specifically, how businesses create and manage data has evolved significantly in recent years. The new corporate data landscape results in so much data residing on laptops, mobile devices, and in cloud applications that IT suffers a loss of visibility and control. And any effort to control that information requires the data to be protected to ensure business continuity, data governance, and employee productivity.

Unfortunately, most organizations – leaders included – often think at the very least they're backing up their most crucial data. However, when things fail and there is a need to restore data, too often they discover they were not backing up anything at all. Or even with some form of protection in place, organizations find that they were only backing up their endpoints, not realizing how much critical data resides in a growing number of cloud or SaaS apps.

For instance, when looking at CRM systems alone (i.e. Salesforce), it is estimated that half were deployed via SaaS as of 2015 and will rise as high as 85 percent by 2025, according to a Gartner study.[1] Likewise, Office 365 continues to add subscribers. According to financials released October 2015, Office 365 saw an impressive revenue growth of nearly 70 percent.[2] The reality is: Just because your data is in a SaaS app doesn't mean it is being backed up. When looking at how many businesses are utilizing SaaS applications, the numbers are not only significant, but the data stored in these SaaS apps are often the organization's most critical such as customer data, data repositories, and email.

With all of this data spread across endpoints and cloud apps, the chance of costly data exposures in the enterprise rises as well. Unfortunately, the lack of an adequate protection and backup strategy becomes strikingly clear when organizations suffer a failure or even fall victim to a ransomware attack. As such, enterprises need to take

[1] The Gartner CRM Guide, March 2014 https://www.gartner.com/doc/2679218/gartner-crm-vendor-guide-
[2] Microsoft 1Q Results, October 2015 http://www.winbeta.org/news/office-365-sees-revenue-growth-of-nearly-70

action to protect corporate data — wherever it resides— and ensure that it is recoverable to mitigate internal and external data risks. A unified data protection approach lets organizations address these challenges, bringing together availability and governance for end user data residing on laptops, smart devices, and cloud applications like Office 365, Google, or Box — in a single solution.

WHY DATA PROTECTION IN THE CLOUD?

Simply put, organizations have a responsibility to maintain and preserve their data, ensuring it can be accessible and auditable to meet data regulations or respond to legal inquiries. However, most traditional approaches fall short of protecting the enterprise, since they fail to provide IT with the seamless reach necessary to cover the entire realm of data creation points, whether they be on endpoints like laptops or in cloud apps like Office 365.

Trying to address this challenge with traditional approaches – including legacy infrastructure and technology stacks – means having to overcome the inherent issues of complexity and costs due to all the nuances of both managing and attempting to understand the data. However, cloud changes the model by providing a scale-out architecture accessible from wherever the endpoint resides to support massive ingestion of data. Its elasticity provides ways to scale indexing and scanning of the data in near real-time, removing a significant hurdle that would bottleneck the network and resources in a traditional model. Simply put, cloud provides a way to gather all this information efficiently, centralize it, and provide multiple data services on a single dataset on-demand.

Cloud also provides organizations with the on-demand ability to backup and ultimately recover endpoint and cloud data in the case of a breach, loss of a laptop, or a cloud failure or outage, to name a few. As organizations back up their data, they should have the opportunity to monitor and identify at-rest data risks (ex. PHI, PCI, PII). This allows organizations to ensure that unencrypted data residing on laptops does not contain sensitive information that could result in costly fines. It also helps prevent a data breach when devices are lost or stolen, by performing remote wipe to ensure that the laptop does not contain any confidential information.

By embracing technologies that leverage the cloud to aggregate business data efficiently, organizations realize scale-out storage architecture for unstructured information. Cloud in itself, like AWS, provides an infrastructure capable of hosting complex architectures. To make the cloud efficient for this use-case requires enabling the real-time ingestion and retrieval of data at any point in time where a snapshot of the state of the data was taken. Having this ability means it's also possible to run multiple services on the same dataset, ranging from backup and restore to data analytics or full-text search.

Essentially, this solution harnesses the efficiencies, global reach, and native technologies of industry-leading public cloud providers for unmatched storage flexibility. By leveraging cloud technology to provide data protection, it's possible to combine user data across laptops, mobile, as well as SaaS applications – meaning IT has the ability to enjoy centralized visibility, full-text search, and the type of controls needed to meet enterprise data governance needs.

Having that end-user data easily

By leveraging cloud technology to provide data protection, the opportunity exists to combine user data across laptops, mobile, as well as SaaS applications – meaning IT has the ability to enjoy centralized visibility, full-text search, and the type of controls needed to meet enterprise data governance needs.

visible and unified also means organizations can quickly respond to litigation and investigative requests without breaking the chain of custody. By bringing together disparate data sources — laptops, mobile, and cloud applications — both legal and compliance teams get a centralized and actionable view to monitor and search for risks, administer legal holds, and provide access for downstream eDiscovery processes — all without impacting employee productivity.

ACHIEVING COMPREHENSIVE DATA PROTECTION

Fortunately, there is a clear path for organizations to get back on track and provide the business with the data protection needed in case of an unplanned event.

Step 1: Assess where data resides. According to Forbes[3], SaaS business applications enjoy a compound annual growth rate of 19.5 percent, and there is a noticeable shift in where data resides – and it's not just on endpoints. Specifically, organizations are now storing data within this growing array of SaaS applications as well as leveraging storage services like Box. In some instances, organizations may not even realize that the user base is leveraging these solutions. Thus, it is important that organizations understand where data is and ensure that it's properly backed up.

Relying solely on a cloud-based SaaS provider to safeguard your critical data, whether it's in Office 365 or a CRM application like Salesforce, should never be an option. After all, the risks posed by outages, data loss, and potential litigation are too great. For true peace of mind, organizations need a backup plan in place; one that regularly backs up user data to satisfy company-specific data protection and retention needs.

Fortunately, there is a clear path for organizations to get back on track and provide the business with the data protection needed in case of an unplanned event.

Specifically, organizations should embrace a solution that can automate data protection policy, and address both availability and governance requirements by providing:

- Point-in-time snapshots for recovery of information in case of data loss or corruption issues;
- The ability to restore objects or individual records, files, and attachments including metadata, such as intellectual property research, financial information, or client records;
- Assurance that your data is archived and available for compliance, eDiscovery, and other legal requirements;
- The ability to scan over data on endpoints or in cloud apps and highlight any violations of an organization's compliance policies;
- Strict adherence to data privacy and data residency requirements.

Fortunately, once IT has an understanding of where its user base creates and stores data, it shines a spotlight on the importance of assessing options and ultimately taking action.

Step 2: Understand differences. Unfortunately, managing data across multiple sources makes holding and storing data for long-term archiving more complex, as each system has its unique nuances. Oftentimes, organizations will embrace a false sense of security, thinking they are adequately backing up their data – that is until a system is damaged, lost, or the organization has a ransomware attack, making it necessary to recover and restore. A solid data protection system will allow organizations to ensure all user data is retained for as long as it's needed to meet corporate governance obligations. Likewise, any strategic approach will minimize spoliation risks, avoid the need to copy data, and eliminate the chance of accidental deletion or purge when employees leave the company.

Organizations need to seek out solutions that enable them to centralize and retain data across sources – by user. Taking this approach helps ensure the retention of all user data for as long as

[3]Centaur Partners, 2014. http://www.forbes.com/sites/louiscolumbus/2015/01/24/roundup-of-cloud-computing-forecasts-and-market-estimates-2015/#7d1dc1d1740c

necessary to meet corporate governance obligations. It also allows the organization to search across data and audit trails historically to identify data necessary for compliance responses. Lastly, it keeps legally responsive data from accidentally being purged—legal holds preserve data even after employees depart.

Of course, accomplishing this means finding a solution capable of providing the organization with seamless integration into today's popular cloud apps so the enterprise has a single access point for viewing and managing end-user data while eliminating the need to scour multiple, disjointed systems. Organizations need a platform to track, hold, and monitor data, which aids in adhering to regulatory compliance obligations and offers a centralized conduit for managing dispersed data to meet corporate governance requirements.

Step 3: Build and embrace a strategy. With the rapid adoption of cloud apps like Microsoft Office 365 (OneDrive and Exchange Online), Google Apps for Work (Google Drive, Gmail, and Google Docs), Salesforce.com, and Box, IT's visibility has been reduced significantly. The burden remains on IT to facilitate a system and protocols where legal holds, eDiscovery, and data governance for compliance are never compromised – regardless of where users create and store their data.

This process begins with developing and deploying a backup strategy that looks at endpoints and cloud apps equally, one that ensures that extended metadata and logs are also maintained for chain of custody and compliance requirements. A solid strategy should include giving the organization the ability to monitor data to reduce risks, and enact strategies for legal holds. It's also important to

Organizations need a platform to track, hold, and monitor data, which aids in adhering to regulatory compliance obligations and offers a centralized conduit for managing dispersed data to meet corporate governance requirements.

embrace automated, time-indexed snapshot backups of data to further minimize the potentially crippling impact ransomware can have on an organization. Information can be restored back to its original state and an infected machine can be restored to any point in time prior to the attack. This ensures successful backups and restores, even with varying network speeds.

BOTTOM LINE

Now's the time to take a closer look at how well your current strategies and solutions protect your enterprise. Chances are the results fall significantly short of your needs. Fortunately, the protection you need is within reach. After all, no business can afford the often costly and sometimes crippling consequences of failing to protect data.

ABOUT THE SPONSOR

Druva provides unified data protection in the cloud, bringing data-center class availability and governance to the mobile and distributed enterprise. With a single dashboard for backup, availability and governance, Druva's award-winning solutions minimize network impact and are transparent to users. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations on over 4 million devices. Learn more at **www.druva.com** and join the conversation at **twitter.com/druvainc.**

druva

amazon web services™