WHITEPAPER

Redmond MAGAZINE

HOW THIRD PARTIES FILL THE CRITICAL FUNCTIONAL GAPS LEFT BY CLOUD PROVIDERS

By Lee Pender

druva

www.druva.com

Just about everybody is investing in the cloud, but not everybody understands all the responsibilities that come with moving to the cloud. Sure, cloud providers offer a wide range of services, but companies are often left in charge of more than they realize—especially in the realm of data protection. In an age in which data is a company's most valuable resource and laws around compliance are becoming stricter, data integrity is critical. And while outsourcing some operations to cloud providers eases the burden on IT staffs and lowers costs, it also brings about a new set of challenges.

While cloud providers are responsible for functions such as network controls and host infrastructure, they generally do not provide comprehensive endpoint protection, asset management or data accountability. It's up to customers to cover those areas themselves in a new and unfamiliar setting.

That's where a partnership with the right third-party vendor can be critical to the success of a cloud migration—and to maintaining the integrity of a company's precious data. The cloud also enables companies to update old workflows with more secure processes, and here again, the right third-party partner can be crucial to helping an organization maximize its efficiency without sacrificing security.

THE CLOUD IS EVERYWHERE

Cloud-based applications are way beyond the hype stage. An ever-increasing number of mobile users, who demand secure access to data and applications from any location, are driving companies to implement cloud-based solutions, from productivity suites such as Office 365 to storage platforms such as Box and Google Drive.

CLOUD-BASED APPLICATIONS ARE WAY **BEYOND THE HYPE STAGE.**

The numbers are impressive. ZDNet reports that by mid-2017, 80 percent of IT budgets will be dedicated to cloud computing. Okta adds that most businesses offer users between 11 and 16 cloud apps, up 33 percent year-over-year.

Cover Image: Deepadesigns/Shutterstock.com

Statistics from Forrester Research further illustrate the growth of cloud-based solutions. The analyst firm reported in fall 2016 that 38 percent of enterprises in North America and Europe are building private clouds; 32 percent are using public cloud services; and 30 percent would implement some form of cloud technology over the next 12 months.

the responsibility of making sure that data is tracked, stored appropriately for compliance purposes and not corrupted or lost—falls entirely on the company implementing the cloud solution and not on the cloud provider.

This trips up a lot of companies, as Gartner recently noted: "Some IT organizations wrongly assume that high-availability and disaster recovery capabilities offered by SaaS providers can cover data loss by user errors or malicious attacks."

LEGACY METHODS OF DEALING WITH DATA-RELATED PROBLEMS **WON'T NECESSARILY WORK** IN THE CLOUD.

ASSUMPTIONS CAN BE DANGEROUS

Companies implementing cloud-based systems understand the benefits: lower maintenance costs, freeing IT staff to work on projects that are profit centers rather than cost centers, and ability to scale easily as the business grows. But many don't understand what else they're getting themselves into in the cloud.

Most cloud providers, as part of their service-level agreements, take responsibility for certain functions, including application control levels, network controls, host infrastructure and physical security, or the security of the cloud servers themselves.

But other responsibilities are shared between the cloud provider and the customer, including client and endpoint protection, and identity and access management. Perhaps most critically, data classification and accountability—

They can't, so companies need to be prepared to deal with, and preferably avoid, those problems themselves. But legacy methods of dealing with data-related problems won't necessarily work in the cloud, and the proliferation of compliance requirements in recent years further complicates cloud migrations.

These aren't isolated problems, either. Data protection vendor Druva recently found that **44 percent** of cloud malware contained ransomware and that **56 percent** of malware-infected files are easily shared in a cloud environment.

One common scenario for data corruption is very simple: A user downloads malware in email and unknowingly puts an infected

file in a company-sanctioned cloud application. Other users access the file, and the malware spreads via the cloud app. In that scenario, it's the company, not the cloud provider, that is responsible for detecting and removing the malware and recovering corrupted data.

"EVEN THOUGH THE CLOUD MAY INITIALLY PRESENT NEW CHALLENGES, ITS **FLEXIBILITY, SECURITY, AND SCALE** MAKE IT VERY MUCH **WORTH PURSUING.**"

Other factors that can lead to data loss or corruption in the cloud are also common in company environments. They include snafus such as sync errors, migration errors and third-party software errors. They also include damaging user actions, such as accidental file deletion, document override, or an exiting employee deleting files that need to be stored for legal or compliance purposes.

Of course, perhaps the greatest fear among security professionals dealing with cloud implementations is malicious activity, whether it's instigated by a disgruntled employee or comes from outside the organization in the form of ransomware, malware, a data breach or an attack.

THIRD PARTIES UNLOCK THE POTENTIAL OF THE CLOUD

Even though the cloud may initially present new challenges, its flexibility, security, and scale make it very much worth pursuing. as most companies clearly realize. The right third-party software can fill in the gaps cloud providers leave, enabling companies not only to protect their data but also to maximize the potential of their cloud migrations.

The key to finding the right third-party application is to consider not just breadth of services but also simplicity of deployment and support for multiple cloud applications and environments. Certain capabilities are critical: detecting and enabling IT to avert malware and ransomware attacks, backing up and restoring data, archiving data, providing search and audit features, and automating the process of holding data for compliance and legal purposes.

What's even more important is to find a third-party offering that will perform those functions across operating systems, including Windows, Linux, OSX, iOS and Android, and across cloud-based services, such as Office 365, Google G Suite, Box, Dropbox and Salesforce. Also critical is deploying an application that can cover all endpoints in a cloud setup.

But the real value of a third-party system with all of those capabilities is one that provides management of the entire environment through a single pane of glass for simple but powerful management. Managing data in the cloud can become surprisingly fragmented and unwieldy when multiple operating systems and cloud services are involved in an implementation,

which is the case for most companies. Centralized management reduces security risks, eases maintenance and ultimately drives efficiency and lower costs.

Third-party applications working with cloud-based systems can also enable companies to complete critical processes more easily and securely. Consider the traditional workflow for e-discovery in legal processes. Companies have to reactively collect data from endpoints and applications through disparate solutions, risking data spoliation. There is no chain of data custody nor tracking and reports.

Then, companies have to transfer or ship data to legal counsel via FTP, email, disk or tape—sometimes literally in a truck—which opens huge security holes. When the legal entity receives the data, it has to move into its storage system before culling for relevant data can begin.

In a third-party enabled, cloud-based workflow, however, a single platform proactively collects all data. The third-party system offers automated legal holds, data preservation and chain-of-custody tracking and reporting. Companies can use the third-party application to search and cull data themselves, thereby reducing downstream e-discovery costs and maximizing security.

From there, the third party can facilitate secure data ingestion into any legal review platform or legal counsel's system. The process is more reliable, less expensive and far more secure. That's just one example of how third parties can unlock the power of the cloud for customers.

DRUVA **PROVIDES THE CAPABILITIES** COMPANIES NEED IN A **THIRD-PARTY APPLICATION.**

THE DRUVA APPROACH PROTECTS DATA AND DRIVES EFFICIENCIES

Druva meets the challenges of the cloud and maximizes its value for companies by taking a holistic approach to cloud data protection and information management. Druva provides the capabilities companies need in a third-party application to fill in the functionality gaps left by cloud providers.

Druva inSync backs up data from endpoints and collects data from disparate cloud applications. It provides a single pane of glass for control and policy management of all data running in all systems and on all endpoints, offering a critical management function.

inSync provides maximum security and reliability by backing up data to Amazon Web Services (AWS), Microsoft Azure or a combination of both. It performs cloud-to-cloud backup using API connectors with no impact on network bandwidth.

It also provides a comprehensive set of services around data, including backup and restore, archiving, search and audit, compliance, and legal hold. Access to and recovery of data are quick and easy, and companies can archive data for as long as they need to hold it for legal and compliance purposes.

DRUVA INSYNC **BACKS UP DATA** FROM ENDPOINTS AND **COLLECTS DATA** FROM DISPARATE CLOUD APPLICATIONS.

Granular controls make it easy for IT to manage backup schedules, storage quotas, data retention, and user access and privacy. In backing up user personas, inSync minimizes downtime by capturing user settings, enabling users to get quickly up and running after a cloud system migration or upgrade. And deployment is simple thanks to integrated mass deployment agents for Active Directory Group Policy, Systems Center Configuration Manager, and Casper.

As for the widespread problem of employees introducing ransomware and malware into cloud environments, Druva enables companies to avert this problem by recognizing possible unusual user activity and notifying IT that this could indicate ransomware. IT can then revert to a known last best snapshot for recovery. Companies can customize the frequency of their snapshots all the way to backing up data every five minutes.

Druva tackles legal and compliance issues by enabling companies to manage and place legal holds on data and capture forensic metadata. With inSync, companies can ensure legal admissibility of data, including providing chain of custody and auditing of users and administrators. And, critical to the process of e-discovery described previously, Druva provides data ingestion into e-discovery platforms.

Through its compliance management capabilities, Druva automates compliance management with reporting for sensitive and regulated information, full-text indexing, built-in support for common regulatory policies such as HIPAA, and customizable templates to search using keywords and regular expressions.

CONFIDENCE IS KEY IN THE CLOUD

For years, cloud adoption was held up by concerns about security and reliability, specifically regarding protection and recovery of data and compliance with evolving regulations. But market statistics indicate that companies are finally embracing the cloud for a growing number of critical business functions. While cloud providers offer a wide range of services, they can't cover everything. Companies themselves are responsible for data protection and information management, and that is where third

parties such as Druva play such an important role.

Aside from providing functionality critical to the success of cloud migrations, third parties offer customers a benefit that is less tangible but perhaps even more powerful: confidence. Armed with proof that vendors such as Druva can fill in gaps left by cloud providers, CIOs and IT professionals can push for cloud transitions with financial and business executives without having to worry about justifying data security. Druva has them covered.

Furthermore, IT leaders themselves can enter into agreements with cloud providers knowing which party is responsible for which function and how the company will cover the functions cloud providers can't. Users know that their data will be secure and protected, and that they have control of their personal profiles and can get up and running quickly after upgrades or migrations.

Certainly, anybody involved with a company's legal department will be relieved to know that the e-discovery process, among others, is both secure and simple. And financial leaders will like the lower cost of maintenance, e-discovery and data recovery that Druva provides.

Confidence to move forward in the cloud is a critical factor in any project, and it's a primary reason why the current wave of investment in cloud-based applications must be accompanied by investment in third-party systems that enable companies to get the most out of the cloud without compromising security. With the capabilities it provides, Druva is well positioned to enable its customers to unlock the full potential of the cloud without leaving any gaps in critical functionality.

CONFIDENCE TO MOVE FORWARD IN THE CLOUD IS A **CRITICAL FACTOR** IN ANY PROJECT.

Find out more

https://www.druva.com

druva

Lee Pender has been writing about the technology industry for 20 years. He formerly served as an editor for both Redmond and Redmond Channel Partner magazines and was also on the staffs of Computer Reseller News, eWeek and CIO magazine. Lee is now a freelance technology marketing writer.