TOP CRITERIA TO REALIZE EFFICIENT DATA PROTECTION IN TODAY’S MULTI-CLOUD ENVIRONMENT

As CIOs take a step back and consider a strategy for operationalizing their cloud environment, they face a greater level of complexity than ever before. In order to overcome this complexity and achieve the efficiencies they desire, IT organizations need to take a unified approach to data management in the cloud. To help, consider these buyer checklist requirements for a cloud data management solution that enables IT efficiency.
TOP REQUIREMENTS FOR EFFICIENT CLOUD DATA PROTECTION

Migration of data into the cloud drives the need for data management and protection processes that are as equally seamless and easy in the cloud as they are on-premises. This can be achieved, but it requires looking at data management and protection in a whole new way. Because of the increasing complexity of the IT environment, incremental improvements are quickly overshadowed. IT organizations need a solution that works hard under the covers to truly transform how IT manages and protects corporate data retained in cloud infrastructure. To achieve this, select a solution that provides all of the following features and capabilities in a single, unified data management solution:

- **END-TO-END AUTOMATION**
  Data protection tasks like backup, archive and disaster recovery should all be automated, regardless of where the data resides. Any need for scripting or human intervention requires resources and introduces risk. A data management solution optimized for the cloud should be capable of orchestrating complex end-to-end processes with pre-built and custom workflow automation engines.

- **CONVERGED BACKUP, ARCHIVE AND REPORTING**
  A cloud-enabled data protection solution must bring convergence to data management tasks, eliminating the need for multiple point solutions. Convergence requires a common infrastructure through which tasks are performed in a single, efficient step across the entire IT environment, thus reducing operational overhead and IT investments.

- **SNAPSHOT TECHNOLOGY TO SPEED DATA PROTECTION**
  When linked to backup processes, hardware array-based snapshot technology can increase the speed of data protection. However, not just any snapshot tool will do. The provider’s snapshot technology should combine deep application, hypervisor and cloud awareness with broad hardware compatibility in a single console.

- **COMPREHENSIVE REPORTING AND ANALYTICS**
  Access to actionable information gives IT organizations the insight they need to make informed decisions about their data management processes. Any data management and protection solution selected to support cloud infrastructure should provide built-in, comprehensive reporting and analytics, which enable IT to identify opportunities to further improve efficiencies.
A VARIETY OF OPTIONS FOR GETTING DATA OUT OF THE CLOUD

Ideal solutions for cloud data protection should allow IT to choose the technology or tool that best supports business requirements for any given workload, rather than forcing all workloads into a one-size-fits-all approach. This means having access to array-based replication, VM replication, host-based block-level replication and WAN-optimized deduplication – all from a single platform. Moreover, the solution should be able to intelligently apply the appropriate technology based on the business requirements defined by IT.

SELF-SERVICE CAPABILITIES

Thanks to the consumerization of IT, employees are more willing than ever to do for themselves. A cloud-based data protection solution should take advantage of this trend to enable users to more quickly have their needs met. Today's solutions must provide a web-based self-service management console via which users can manage their own cloud resources and access archived data. However, to prevent increased complexity, help desk strain and security concerns, the solution must also give IT the appropriate control, security and discovery capabilities.

DEEP INTEGRATION WITH CLOUD PLATFORMS

A solution that features native integration into major cloud compute platforms such as Amazon Web Services and Microsoft Azure, and cloud storage platforms like OneDrive and Dropbox, can normalize the management of those platforms. As a result, IT can gain visibility into these environments and manage all of them from a centralized tool.

CLOUD VENDOR AGNOSTIC

A solution that integrates across numerous cloud compute platforms, cloud storage platforms and hypervisors helps reduce complexity, thereby increasing IT efficiency. A vendor-agnostic solution also frees IT and employees to use the cloud platforms that best meet security, application, cost and reliability requirements – without risk of vendor lock-in.

A SINGLE POINT OF CONTROL

Finally, the best cloud data protection solutions provide a single point of control that serves as IT’s command center for protecting and managing data regardless of where it resides – a common cloud framework from which to manage all of your cloud data protection operations. The cloud framework should simplify tasks and enable IT to focus on business requirements, while the complexity of choosing technologies and translating those requirements into automated processes is handled under the covers, decoupling the IT admin from the complexity of the environment and eliminating the need to learn to operate separate consoles.

45% of IT organizations have had cloud-related projects that originated outside of the IT organization come back into IT ownership.

IDG ENTERPRISE
Cloud Computing Research, 2014
WHAT TO LOOK FOR IN A CLOUD DATA MANAGEMENT PROVIDER

Achieving data management efficiencies in a multi-cloud environment is nothing short of impossible. But automating, orchestrating and integrating tools and technologies is no easy feat, either. IT organizations must find a data protection and information management provider that has deep roots in the cloud and an established track record for protecting on-premises data. This will help allay concerns regarding the maturity of the provider as well as the robustness of the solution.

IT organizations should also seek a provider that makes data protection and recovery operations as easy and seamless in the cloud as they are in a traditional, on-premises infrastructure. Look for a provider that made early efforts to integrate across cloud storage platforms and offer cloud orchestration and provisioning capabilities designed to streamline the management of the cloud infrastructure. These efforts are proof that the provider understands the value of the cloud as well as its impact on data management processes.

More than a quarter of IT organizations use at least three different archiving solutions.

FORRESTER RESEARCH
Market Overview: Information Archiving Q2 2015, May 2015

RESOURCES

http://commvault.com/1ZFPs7X

To learn more about Unified Cloud Data Protection with Commvault software, visit commvault.com/cloud.