druva

Business Brief

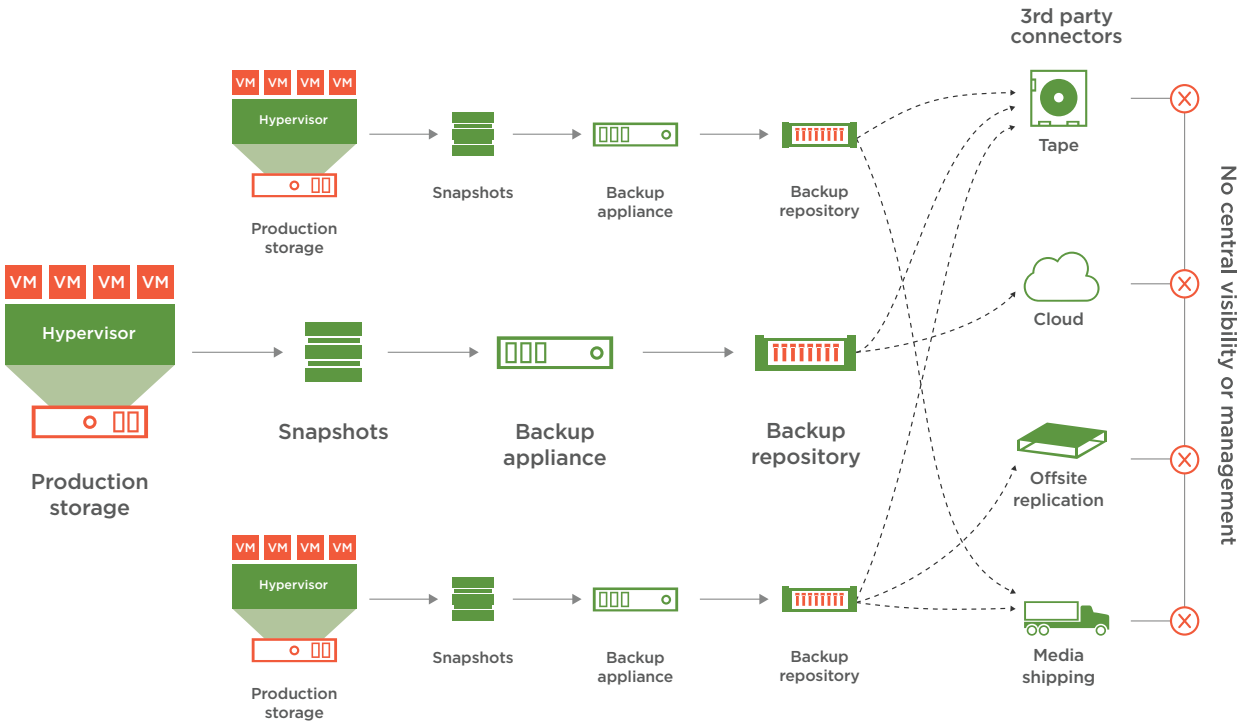
MAKING THE BUSINESS CASE FOR VMWARE CLOUD BACKUP

Q317-CON-10655

The Core Issues

The rise of virtualization as a business tool has dramatically enhanced server and primary storage utilization. Protecting these virtualized environments, however, as well as the ever-growing amount of structured and unstructured data being created, still requires a complex, on-prem secondary storage model that imposes heavy administrative overhead and infrastructure costs.

Legacy VM Data Protection Complexity



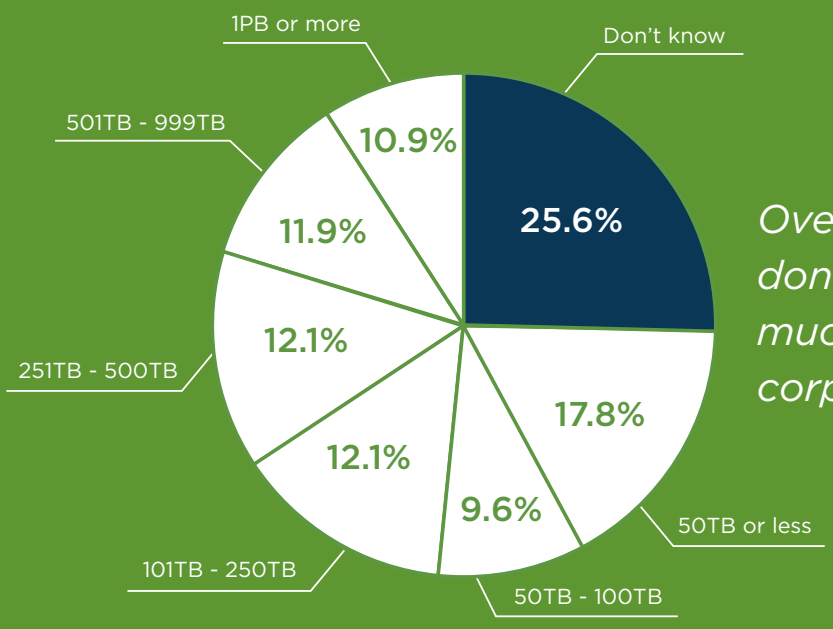
Lack of Mobility in the Virtualized Data Center

In many modern IT departments, the application, virtualization, and storage teams have become dissatisfied with traditional backup and now use the native point products available to them. They have, in effect, “gone rogue.”

Against this background, an organization's data protection strategy often consists of a half-dozen or more disparate backup and recovery "solutions," which may or (most likely) may not be compatible with each other. As a result, workloads are often siloed and unable to be migrated across systems or geographies, leaving companies at risk of losing business continuity and failing to meet data security needs.

Lack of Visibility in the Virtualized Data Center

With increasing complexity comes a lack of control and visibility, resulting in some IT teams not even knowing how much data resides on their servers. Without clear visibility into the volume of data, whether due to fragmented or inadequate protection solutions, effective management becomes much more difficult.



Over 25% of organizations don't actually know how much data resides on their corporate servers

ESG, 2017 Data Protection Modernization Survey, December 5, 2016

Cloud-Native Backup and Recovery for Virtual Environments

The increasing pressure on IT teams to maintain business continuity and information governance is changing how companies view infrastructure resiliency and long-term data retention. Organizations today are looking to the cloud to provide a viable, cost-effective alternative to traditional backup and disaster recovery (DR).

"By 2019, the percentage of enterprises using the cloud as a backup destination will double, up from 11% at the beginning of 2016."

–Gartner, Market Guide for Data Center Backup October, 2016

Here are five immediate, real-world business reasons that IT teams and company leaders should consider migrating their backup, archival, and DR to a single, cloud-native platform:

1. Offsite Infrastructure

Cloud-based backup and recovery infrastructure is hosted completely offsite—meaning there is no expensive hardware to requisition, and no software to license and keep updated. Reliable, durable, fast, and cost-effective data recovery can therefore be enabled by an enterprise-grade, multi-region, public cloud infrastructure. With virtual machines replicated offsite, system downtime (and its resulting impact on productivity) can be reduced to mere minutes.

2. Improved Business Agility

A cloud-native data management approach enables fast response times in the case of failover for DR with recovery time objective (RTO) in minutes. It also improves speeds when you're looking to replicate and move virtual machines (VMs) across regions for regulatory needs or for test/dev. Businesses can also backup VMs from the data center to the public cloud and recover entire VMs or individual files as needed. Savings, efficiency, and speed are achieved by minimizing the storage footprint through deduplication of data and optimizing storage tiers— with no extra infrastructure.

3. Dynamic DR & Workload Mobility

In the cloud, VMs can be configured for DR with immediate failover and replication as needed for production or test/dev purposes. Once in the cloud, workloads can be spread across geographies for easy replication and at-the-ready disaster recovery. Cloud-based DR eliminates the need for organizations to store complete copies of production systems at a secondary company-managed data center. Replicated virtual machines can be pushed to any global location, making spin-up in the event of disaster simple and efficient.

4. Simplified Management

Managing a cloud-based backup strategy is considerably easier than with on-prem systems:

- Server backup and DR policies can be coordinated and monitored globally, from anywhere in the world, removing the burden of complex storage, compute, or networking management
- Data tiering ensures that VMs are always stored cost-efficiently for long-term archival to address compliance requirements, without the need for manual processes. Data is sorted into hot, warm, and cold tiers to optimize availability without adding unnecessary expense
- Cloud-native content analysis capabilities provide VMware administrators with a greater understanding of potential data and compliance risks across multiple data sources

5. Radically Lower Overall Costs

Not only does a cloud-based model eliminate costly hardware appliances, data centers, and reduce administration needs, it can also provide a unified approach to backup, disaster recovery, archiving, and analytics on a single data set, significantly lowering the costs created by data silos. Coupled with auto-tiered storage, it provides a highly efficient collection of data in an ever-incremental backup model, avoiding the large volume of information stored by legacy models.

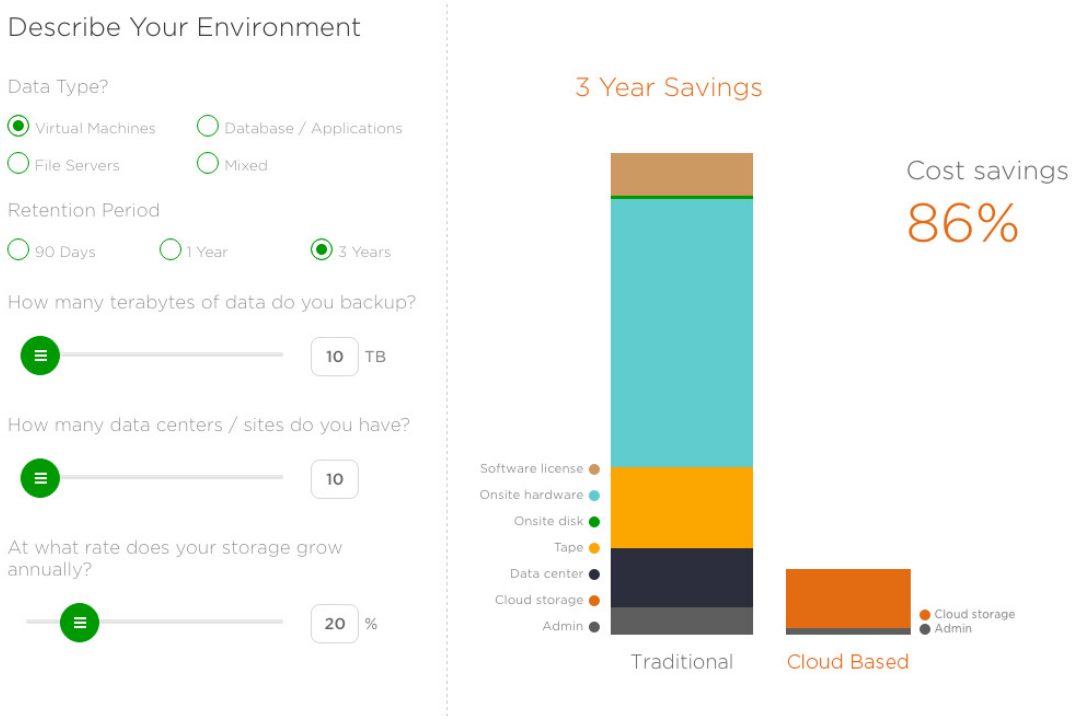
Calculating the Return On Investment (ROI)

Operationally, the success of a data protection solution is measured by how quickly the company can recover (RTO) and by how little worker productivity is impacted (otherwise known as recovery point objective, or RPO) during an outage. By demonstrating how an investment in cloud-native solutions could produce profitability through operational costs savings, compared to the current legacy model, managers can make a strong case that resonates with company leadership and also aligns with the fiscal needs of the business. By illustrating the business benefits along with a solid ROI justification, you can be in a much stronger position to negotiate for the budget necessary to make the transition.

In order to begin estimating the full capital expenditure (CAPEX) and operational expenditure (OPEX) costs of continuing with the curing data protection model, as opposed to moving to a cloud-native subscription service, you need to fully outline each cost center.

Here are the cost centers and considerations that need to be used in your comparison.

	Legacy Model	Cost ($)	Cloud Model	Cost ($)
Software (to be depreciated)	Software Agent	Per Server	No upfront capital costs for customer	No Cost
	Additional add-ons or plug-ins	Per Server	Annual or monthly subscription	Per User
Hardware (to be depreciated)	Storage hardware, tape drives, network capacity, autoloaders, and extra server memory	As Needed	Service provider bears all costs	No Cost
	Hardware maintenance fee	Per Year	Service provider bears all costs	No Cost
	Tape Media	Per Year	Service provider bears all costs	No Cost
Software implementation, maintenance, and tech support (to be depreciated)	Server support	Per Server	Immediate implementation if desired	As Needed
	Internal, fully burdened, hourly cost or contractor hourly rate	As Needed	Service provider bears all costs	No Cost
	Software maintenance fees	Per Year	Service provider bears all costs	No Cost
	Productivity ("soft") costs during maintenance down time	Varies	Service provider bears all costs (with high SLA)	No Cost
Hardware maintenance/ support costs/ media + shipping (to be depreciated)	Hardware refresh, tape drives, network capacity, autoloaders, and extra server memory	Per Year	Service provider bears all costs	No Cost
	Hardware maintenance fee	Per Year	Service provider bears all costs	No Cost
	Tape media	Per Year	Service provider bears all costs	No Cost
Labor (in-house and contracted)	Internal, fully burdened, hourly cost or contractor hourly rate	As Needed	Service provider bears all costs	No Cost
	Labor - daily backup tasks	As Needed	Service provider bears all costs	No Cost
	Labor - data recovery from tape	As Needed	Service provider bears all costs	No Cost
	Labor - server migration	As Needed	Service provider bears all costs	No Cost
Offsite storage and maintenance	Storage service performing pickup, moving data offsite, storing, and maintaining data	Per Year	Service provider bears all costs	No Cost



Typical costs savings based on the Druva TCO Calculator here.

Additional Cloud Considerations

Governance and Compliance

Central auditability, legal admissibility, and long-term retention make compelling cases for easier governance and compliance around data within virtual images. Since data is stored in the cloud, it is readily available for mining, legal, and compliance needs. Enterprises can analyze backed-up information to understand the risks and challenges around dormant data, storage growth, and data classification. A cloud storage model can therefore increase visibility into existing data, which can then be better leveraged for additional business value.

Test and Development

Cloud storage allows for test/dev replicated systems to be instantly spun-up as needed with no additional hardware or software, for greater flexibility and speed. By leveraging a copy of a virtual machine in the cloud, tests and validation can be run against a copy of the production data with no interference with critical production environments. A single replicated virtual machine can be centrally managed and replicated as often as needed, even across geographies, so test/dev can be easily handled around the clock. There is no need for separate test/dev systems, as available virtual machines can be repurposed at any time.

"An IT operations team spends over 70% of its time on day-to-day IT management operations—monitoring, troubleshooting, patching, updating, and configuring resources."

–Converged and Integrated Datacenter Systems: Creating Operational Efficiencies - IDC

Conclusion

Managing the backup and restoration of virtual machines in a distributed environment is typically an expensive and convoluted process involving multiple staff members supporting a complex architecture. Any reduction in new hardware, software, or administrative burden, therefore, improves business agility and radically lowers overall total cost of ownership (TCO).

Adopting a cloud-native approach to backup, archival, and disaster recovery offers companies many benefits, including eliminating the need for expensive on-prem hardware and simplifying the implementation and administration of backup systems. It also ensures that mission-critical data will always be globally available in the event of disaster recovery, for test/dev purposes, or to meet legal and data retention needs.

To learn more about how to achieve cost and time savings by managing your VMware environments from within a single, centralized console, visit www.druva.com/phoenix and try backup, disaster recovery, and archival in the cloud.

Or, get started right away by calculating the cost savings using our TCO calculator.

About Druva

Druva is the leader in cloud data protection and information management, leveraging the public cloud to offer a single pane of glass to protect, preserve and discover information—dramatically increasing the availability and visibility of business critical information, while reducing the risk, cost and complexity of managing and protecting it.

Druva's award-winning solutions intelligently collect data, and unify backup, disaster recovery, archival and governance capabilities onto a single, optimized data set. As the industry's fastest growing data protection provider, Druva is trusted by over 4,000 global organizations and protects over 25 PB of data. Learn more at http://www.druva.com and join the conversation at twitter.com/druvainc.

Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com