Three Considerations for Modern Data Protection

WHITE PAPER

Today's digital data deluge has heralded changes in enterprise workloads, with data analytics, artificial intelligence, and machine learning all taking advantage of—and ultimately creating more—data throughout the enterprise. As organizations shift away from legacy relational databases toward new open source and cloud-based platforms, the very nature of applications and data is constantly shifting, making data protection increasingly challenging.

This paper discusses strategies for protecting all workloads across the enterprise and suggests three key considerations when modernizing data protection to encompass across-the-board data types and workloads.

Introduction: Data deluge to information explosion

"There's an app for that" has percolated throughout the enterprise, in part thanks to the consumerization of IT. A Cloud Security Alliance report found that the average enterprise has more than 450 custom applications alone.[1] As users increasingly demand new functionality, often created with new open source development platforms and delivered at least in part via the cloud, those workloads bring new data types and mounds of new data that IT needs to store and protect—wherever it resides.

As more workloads and data move to the cloud, many organizations find that the on-premises budget for IT-related expenses suffers at the cloud's expense. Businesses pressured to take advantage of

1 "New Skyhigh, Cloud Security Alliance Report Reveals Growing Security, Compliance Challenges in Face of Increasing Cloud Services Adoption," Skyhigh Networks, Feb. 12, 2017

VERITAS™ The truth in information.

TechTarget® | Custom Media

cloud platforms, whether for financial or technology reasons, may leave legacy data centers and the data within them behind. The results can be catastrophic: In IT's mad dash to deliver on user needs, the growing number and diversity of workloads—legacy, virtualized and hyper-converged—may not all be properly protected.

Pressure on data protection intensifies

Data protection professionals face many other challenges. For one, administrative headaches abound, especially in light of top management's constant push for IT to reduce staffing and increase employee efficiency. For many organizations, the age of highly specialized storage administrators is coming to an end or changing dramatically.

There is also an overall skill shortage in IT, especially as businesses seek data scientists to help meet analytics demands and cybersecurity professionals to help thwart the growing number of malware and phishing attacks on unsuspecting businesses. As a result, when IT resources are doled out, data management may be pushed aside.

Then there are the challenges of traditional IT infrastructure. Legacy servers, storage and other hardware require precious time to provision, set up, operate and maintain. Hardware lifecycle management, patches and service calls all take resources away from the new workloads and applications that generate bottom-line enhancing results, such as competitive analyses and product trending reports.

However, the need for data protection is constantly increasing. For example, data protection may be the only defense against ransomware attacks, which are steadily growing in both frequency and intensity.

Complexity increases daily

New applications also bring more people in contact with data and workloads. Data- and workload-specific administrators and end users all want their data protected. However, having more people in the mix can lead to struggles for control. Complicated political dynamics can lead to data protection tasks falling through the cracks, resulting in data loss and subsequent finger-pointing.

Then there is the complexity of data protection solutions in use today. Legacy backup, the proliferation of point protection products for certain applications and clouds, and existing backup scripts are often disconnected, which can lead to duplication of effort, mounds of wasted storage capacity, and data protection inefficiencies throughout the enterprise.

Finally, workload diversity itself drives complexity. Gone are the days when Oracle, SQL and VMware were where the applications and data lived. Today, there are many more specialized application platforms with even more coming, and container technology like Docker resides shoulder to shoulder with other virtualization platforms.

Why modernize at all?

Increasing complexity and unprecedented data growth often lead to data being either unprotected or under-protected in certain areas. Complexity also often means there is no central control or monitoring of data protection throughout the enterprise.

As workloads shift, so too do the backup requirements, and often the legacy tools in place just can't meet the needs of new applications. As budgets continue to shift away from traditional or legacy infrastructure to cloud and analytics projects, IT increasingly needs to drive efficiencies and productivity improvements in the traditional on-premises data center.

Key considerations

As organizations plan to modernize data protection, they should keep these three considerations in mind:

1. **Workloads:** Can the chosen solution protect all workloads in a non-disruptive manner, that meets users' recovery time objectives (RTO) and recovery point objectives (RPO)?
2. **Storage:** What is your overall storage RPO strategy? Tiered? Tape? Cloud? Servers? How and why are you storing backup data? How long do you need to retain historical data, and what can you do to mitigate storage growth?
3. **Admin and process:** How intuitive is the user experience? What kind of reporting is available? How can day-to-day tasks be automated? What's the support for software-defined...everything?

Introducing Veritas NetBackup 8.1.2

With the latest release of Veritas NetBackup, IT organizations can help make their on-premises data center more like the cloud, simplifying data protection in the process. NetBackup 8.1.2 enables users to perform self-service workload data protection, and powerful automation reduces the amount of people, time and effort needed, helping to reduce the stresses caused by workload proliferation.

A comprehensive API suite enables users to deploy rich functionality, such as:

- Automatic creation of trouble tickets when data protection issues arise
- Provisioning that automatically spins up a protection plan when virtual machines are created
- Custom Integration with a broad range of enterprise applications

NetBackup 8.1.2 delivers one solution for all enterprise data protection needs, eliminating the array of point products that clutter IT data management. Scalable to the largest enterprises, it is also low maintenance, which lets IT free up both workload and backup admins to do more, transforming them from specialists to versatilists with a broader portfolio of responsibilities. The result? Better efficiency from scarce human resources.

NetBackup 8.1.2 is the modern way to ensure enterprise-wide data protection, regardless of workload or data type.

Next step: Click here to find out more about NetBackup 8.1.2.