White paper

Featuring

5 key data protection trends and challenges

Questions and answers featuring Forrester Research

Introduction

Modern businesses face multiple IT challenges with protecting and managing data across their infrastructure, including increasing data volumes, growing ransomware and malware threats, data loss due to unforeseen disasters, evolving transitions to public cloud, and the need to meet stringent compliance and data governance requirements. As a result, many businesses are seeking comprehensive technologies like cloud-based backup and recovery — thus improving overall data protection and enabling significant cost and time savings.

> *"Naveen's vision for technology leaders is to develop a dependable and reliable technology infrastructure. Naveen leads the research on enterprise storage, hyperconverged infrastructure, data protection, and disaster recovery technologies and practices.*

Naveen Chhabra, Senior Analyst at Forrester, serving infrastructure and operations professionals, was the guest speaker at a Druva webinar entitled, "Data resiliency moves to the cloud featuring Forrester." As a followup to the webinar, he was able to address some thought-provoking questions that are top-of-mind for numerous businesses. Throughout this white paper, you'll learn the top data protection trends that Naveen Chhabra is closely watching, and the most common challenges IT teams are navigating in 2020.

1. What are the major factors driving cost and complexity in delivering business resilience and how have customers changed them in the last year?

Business resilience is a resultant of many factors including choice of technology, organization structure, practices and policies surrounding the use of technology. From an IT resilience standpoint, there are several issues facing the I&O pros like a wide swathe of IT operations tools that don't integrate well, and incomplete & immature automation. For example, a reasonably sized organization uses multiple (ranging from 3 to 6) data protection and disaster recovery tools to achieve complete protection of all data sources. While these tools may offer similar technical capabilities to provide a complete coverage of all data sources, each tool brings its own architecture, deployment model, operational model, and operator experience. For different tools to work together, I&O pros resort to integrations that are time-consuming, costly, complex and fragile.

Business leaders have moved away from the unnerving complexity that slowed the innovation and reduced the speed at which business could respond to the internal and external forces. Technology leaders are increasingly looking at options that unshackle the otherwise binding architectures which slowed progress.

2. How does cloud-backup reduce the costs and complexity of meeting compliance requirements for the long-term retention of backup data?

Organizations use public cloud to increase the agility, innovation and speed of service delivery while optimizing the overall cost of technology services. According to the Forrester 2018 Infrastructure survey, 58 percent of respondents said they have either implemented or are implementing the use of public cloud storage to store backup and archive data. Firms want to reduce their overall cost of storing exponentially growing data and that is pushing them to consume public cloud. A benefit of concentrating the data sources is the possibility of building a single view into all business data and draw meaningful insights to drive a stronger business strategy.

From an operational standpoint, firms are looking to increase the reliability, availability and dependability of their own data sources by consuming the public cloud services. There is another group of companies that aim to use public cloud for disaster recovery purposes. The differences in technologies and underlying architectures of data center and public cloud infrastructure mandates the use of orchestrated DR capability.

3. What are the management challenges that backup and IT administrators face on a daily and weekly basis (and ways to solve them)?

I&O pros continue to be burdened by the increasing volume, variety and velocity of data sources that they must protect. Some of the operational challenges they face include:

1. **No view into recoverability.** Firms continue to backup the data sources, but there is no visibility into whether those backup copies are recoverable. It is worth noting that "A backup is as good as it can recover." So, if you don't know what can be recovered, you are pushing yourself to the other side of confidence.
2. **No feedback on backup plan relevance.** An ideal backup plan must be contemporary and at best looking into future needs. In the current environment, however, a plan/policy once established is as good as being set in stone. I&O pros must understand if the business objectives like SLA and security are being met with the established policies or not.
3. **Secure backups and backup infrastructure.** A pertinent challenge for firms is to secure the backup infrastructure from ransomware attacks. The ability of firms to weather attacks vary. Industry examples tell us that the bad actors go after the backup software, backup copies and destroy both to remove the victim's last line of defense.

4. What are the new challenges that IT and backup teams face around security and governance and what steps should those teams consider to address them?

Near vertical growth in the number of cyberattacks, especially ransomware attacks, has made it particularly hard for all firms. Meanwhile, business leaders expect the I&O pros to rise to the occasion and recover production systems, but it is easier said than done. Why? Because, I&O pros need to work through several issues like:

1. How can you ensure you are recovering from the clean and uninfected backup instance? Because if you are not, you are risking the recovered systems one more time.
2. To identify the clean data copies, security teams need to provide clearances. Without a security clearance, you can't push systems back into production.
3. Security team can provide a green signal only after they have performed the forensics around the ransomware infections, tracing its path and performing sanitizing operations.
4. If for any reason, you must recover from old data archives because your active backup copies are destroyed, you need to have clearances from your business peers because recovering from an older data copy means losing transaction records — an hour, a day, a week — depending on the last clean backup copy. This data loss means untenable business liabilities.
5. A technology decision quickly balloons into a business decision. Recovering from a ransomware attack is not just an IT decision, multiple stakeholders need to come to a common platform to make the best decisions for the firm.
6. Besides making such hard decisions, firms also lack coordinated plans across different constituents within a company. Forrester research studies tell us that ~30 percent of respondents mentioned that I&O and security teams have developed commonly agreed upon plans for such operational recoveries.

The recent examples in the industry show that recovery post ransomware attacks can be a multi-month endeavor with no guarantee of complete data recovery. Firms need to proactively identify the risks, situations, develop remediation strategy, and periodically test those plans.

5. What problems are organizations seeking to solve through direct-to-cloud backup or storing backup data in the cloud?

Firms aim at improving the:

1. Cost equation by moving the backup and archive copies to the public cloud. Additionally, firms get the ability to shift from capital expenditure to operational expenses.
2. Reliability of the technology services by consuming public cloud infrastructure services that have higher inbuilt resilience. This provides higher availability and data durability SLA's than the legacy data center infrastructure.
3. Ability to improve the disaster recovery posture by consuming public cloud infrastructure that inherently can be used to recover virtual machines and applications since the data resides in the public cloud storage.
4. Improved service levels. A derivative of the availability of backup data in the public cloud is that I&O pros can spin up virtual machines faster and on-demand. Firms aim at improving the service level achievements in order to better serve service level agreements.

Discover more ways to tackle data protection challenges at www.druva.com

About Naveen Chhabra

Senior Analyst Serving Infrastructure & Operations Professionals

Naveen serves infrastructure and operations (I&O) professionals, delivering strategic guidance to Forrester's vendor and end user clients. Naveen's vision for technology leaders is to develop a dependable and reliable technology infrastructure. Naveen leads the research on enterprise storage, hyperconverged infrastructure, data protection, and disaster recovery technologies and practices. Naveen guides tech leaders across his coverage and helps them navigate their path as these leaders face a myriad of factors affecting them, including the use of multiple cloud services, containers, expanding storage technology options, increasing ransomware-induced outages, and the like. Naveen researches the ways technology leaders can proactively prepare themselves to improve their recoverability posture.

druva

Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976	Japan: +81-3-6890-8667
Europe: +44 (0) 20-3750-9440	Singapore: +65 3158-4985
India: +91 (0) 20 6726-3300	Australia: +61 1300-312-729

Druva™ delivers data protection and management for the cloud era. Druva Cloud Platform is built on AWS and offered as-a-Service; customers drive down costs by up to 50 percent by freeing themselves from the burden of unnecessary hardware, capacity planning, and software management. Druva is trusted worldwide by over 4,000 companies at the forefront of embracing cloud. Druva is a privately held company headquartered in Sunnyvale, California and is funded by Sequoia Capital, Tenaya Capital, Riverwood Capital, Viking Global Investors, and Nexus Partners. Visit Druva and follow us @druvainc.