UNITRENDS

THE STATE OF CLOUD BACKUP & DATA PROTECTION 2017

SIX SIGNIFICANT FINDINGS FROM UNITRENDS ANNUAL CLOUD SURVEY

INTRODUCTION

KEY FINDINGS

Unitrends 2017 annual survey of IT professionals' cloud backup and business continuity programs shows data protection and recovery remains a significant challenge. Data centers are growing in complexity and the volumes of data requiring protection are adding to the pressure on IT teams to guarantee quicker recoveries. Many organizations are not even following minimal best practices, and at the opposite end of the spectrum leaders in DR are increasingly using the cloud to play a critical role in business continuity. See where your business stands against the very latest IT metrics including recovery times, DR testing frequency, and cloud usage.

Six major findings stand out from the survey responses. If this information leads you to research the cloud further, read the data sheet entitled How to Meet Compliance Requirements and Control Your Cloud Budget.

FINDING #1 – EXPONENTIAL DATA GROWTH

In one year, there has been a 54% growth in the number of companies reporting they are protecting more than 100 TB of data.

One challenge IT professionals of all industries face is the growing size and complexity of corporate IT environments. While a majority of respondents reported having both physical and virtual servers needing protection, the biggest challenge is the growing volume of data needing protection. With similar-sized organizations responding in both 2016 and 2017, 13% more respondents reported being tasked to protect data volumes between 26 and 100TB, and 54% more are mandated to protect volumes over 100TB. Without the right backup and recovery tools, growing data volumes makes the entire business continuity process longer, more complex and costly.

FINDING #2 – BROADENING PROTECTION REQUIREMENTS

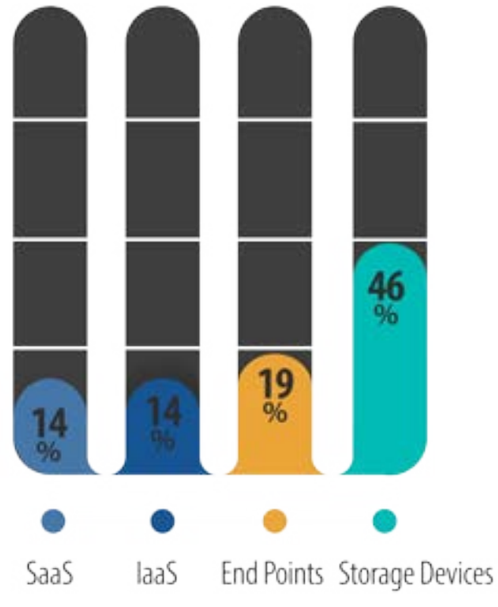
Contributing to the growth of data is the need to protect more types of computing devices. Today data protection and recovery programs have to account for much more than traditional servers and PCs.

46% Forty Six percent (46%) are required to protect storage devices such as SAN, NAS and DAS.

19% 19% need to protect “Other End Point Devices” such as smart phones, tablets, thin clients, printers or other specialized hardware such POS terminals and smart meters.

14% 14% are required to backup cloud-based servers (IaaS). This category will grow rapidly as analysts predict an 18 – 20% annual growth rate in cloud computing.

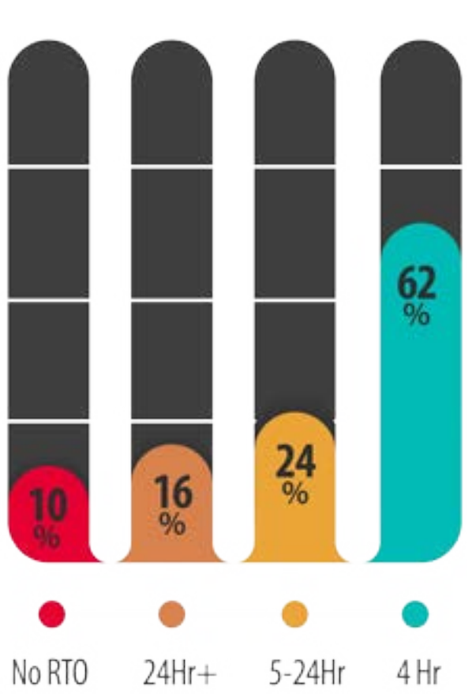
14% 14% currently protect SaaS applications such as Office 365 running in the cloud. This portion will rise as a major analyst firm says that 70 percent of their clients plan to deploy cloud Office 365 in the first six months of 2017.



FINDING #3 –
AGGRESSIVE RECOVERY TIME OBJECTIVES

4 hour recover times are becoming the norm.

IT professionals understand that setting a Recovery Time Objective (RTO) is the first step to managing downtime. An RTO goal means that you at least have a recovery solution, measure your results and take steps to improve your performance. 62% of survey respondents reported having aggressive RTOs of 4 hours or less, with over half of those respondents reporting RTO times of 1 hour or less. These RTOs are coming at a time where IT professionals have less time and more budgetary pressure in their jobs. While some reported they weren't always able to meet those RTO objectives, at least setting a goal, measuring results and working towards improvement signal a commitment to protecting company assets.



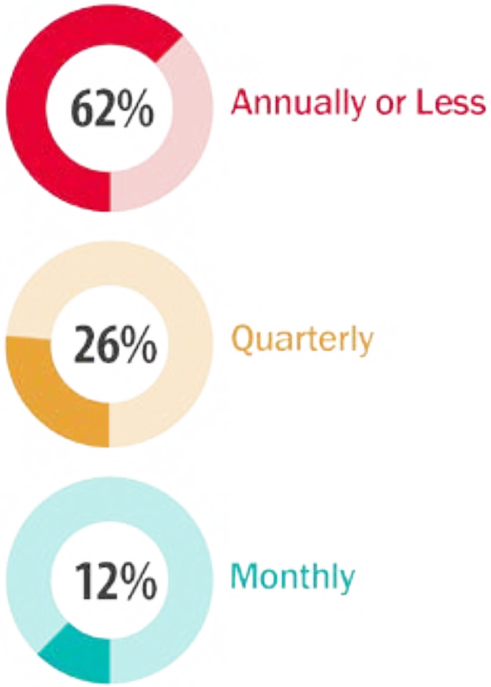
What is perhaps most surprising is that 16% of respondents reported they have RTO goals over 24 hours, which is a very long time for a business to be off-line. A whopping 10% reported having no RTO goals at all, which indicates a total lack of recovery planning and verification. With the growing threat of ransomware and the increasing complexity of virtualized environments, these organizations may be in for a rude surprise from which they have no quick way to recover.

FINDING #4 –
EXTREME EXPOSURE TO SITE–WIDE DISASTERS

A full 26% of respondents reported that their company has no secondary recovery site from which to launch recovery programs in the event of a site-wide event. There are multiple types of events that can affect an entire location such as an electrical failure, flood, hurricane or fire. With no secondary location recovering applications can take much longer since companies will be required to restore their basic infrastructure before they can even begin to recover data, reinstall software, run the network and get the business back up and running.

The cloud is especially well suited as a secondary recovery site for companies that conduct business out of a single location, especially if compared to creating and managing a full, remote data center. Cloud compute capacity and storage are not purchased outright but charged based on actual usage. Superior cloud providers will also offer a recovery Service Level Agreement guaranteeing that business applications will be available in a known time period after a disaster is declared.

FINDING #5 –
A FRIGHTENING LACK OF DR TESTING



A large majority (62%) of survey respondents reported they test their disaster recovery plans only once per year or not at all. Testing is the only way to know if you can truly recover from a downtime event.

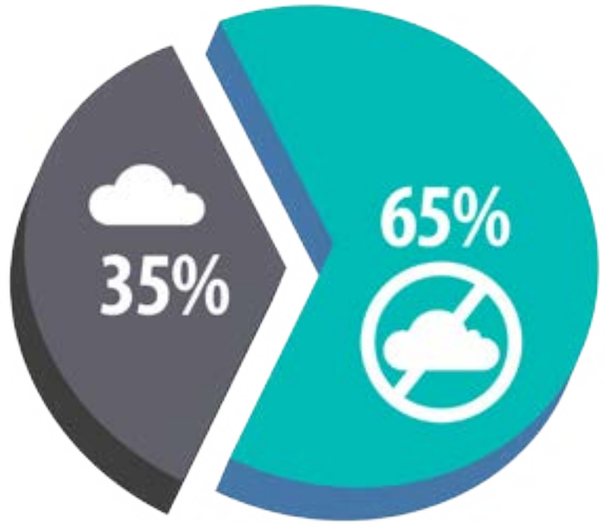
Servers, operating systems, settings, data and software need to be aligned before a business application can be brought back on-line. If any one piece is out of step the entire process will fail and critical business applications will remain down.

The good news is that there are strong tools to make recovery testing automatic and easy, with high quality reports to identify what part of the process is not ready to recover. Many industries such as healthcare require all companies to know and document their recovery times. Only 12% of respondents reported testing their DR plans at least once a month so they can be sure they will recover from a downtime event. Most backup professionals would recommend DR testing much more frequently.

What do the other 90% tell their managers if asked how long it will take to recover from a downtime event such as a ransomware attack or flood?

FINDING #6 –
CONTINUED RESISTANCE TO USING THE CLOUD

45% of responding companies are not currently using cloud and have no plans to do so in the next year.



The top four reasons given were cost (52%), security (45%), loss of control (39%) and data privacy (31%).

Cloud providers have come a long way in enabling their products to meet the highest security requirements as many are already certified to handle medical (HIPAA), financial (SOX) and personal information. In addition data can be encrypted with military grade AES-256 security for in-transit or at rest data protection. Many cloud providers also have SSAE 16 certification for physical security. WAN optimization features reduce the impact of clouds on data networks.

Even if you can't get your management to accept including the cloud in your infrastructure today you can take some steps to make this easier when they do. Isolate recovery servers and storage in your data center to make it easier to relocate these services to the cloud later. Use recovery testing tools to ensure you can recover from a downtime event as these services can be outsourced to leading cloud providers in the future.

The cloud is an underrated tool for data protection. To learn more about the cost of the cloud please use Unitrends Cloud Cost Calculator.

CONCLUSIONS

It is more and more likely you will experience an outage. As the volumes of data requiring protection increase and the complexity of datacenters grow the chances of a fast recovery diminish unless you are prepared, equipped and trained in recovery. This includes following industry best practices of establishing recovery goals, conducting regular backups, replicating data to remote locations, and regularly testing backup procedures. Unitrends 2017 survey shows that a large percentage of enterprises are highly unprepared to recovery quickly from a downtime event.

The survey also shows that leaders in disaster recovery are using the cloud as a truly cost effective and efficient tool in their data protection and business continuity program. They are using cloud services to speed recovery and ensure that they can meet aggressive RTOs 100% of the time to protect their business against the high cost of downtime. If the experiences of your peers leads you to want to learn more about the role cloud can play in data protection and disaster recovery watch How to Choose the Right Cloud for Continuity.

Interested in seeing exactly how much it will cost for you to implement cloud in your environment for data protection and disaster recovery? Compare prices across Amazon AWS, Azure, and Unitrends by visiting the Cloud Cost Calculator.

CLOUD COST CALCULATOR

Unitrends increases uptime and confidence in a world in which IT professionals must do more with less. Unitrends leverages high-availability hardware and software engineering, cloud economics, enterprise power with consumer-grade design, and customer-obsessed support to natively provide all-in-one enterprise backup and continuity. The result is a “one throat to choke” set of offerings that allow customers to focus on their business rather than backup. Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.