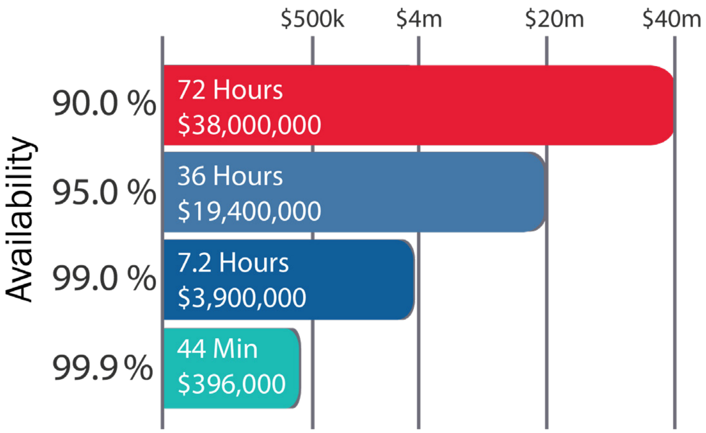
UNITRENDS

9 WAYS TO STAY UNDEFEATED AGAINST DISASTERS

INTRODUCTION

Downtime is expensive. So high, in fact that IT managers need to do everything they can to increase uptime. Even if you are happy with your existing approach to backup and recovery, **taking these nine steps could increase uptime.** Even just a 1% increase in uptime can save your company millions in negative business impacts.

Average Cost of Downtime Per Month



Most people think of backup as a defensive strategy. We don't have that luxury any more. Take the offense. While a good defense is important, any sports fan knows that a solid offense is just as critical. If you sit back and wait until a downtime event happens, you won't know how your recovery plans will respond until it is too late.

Here are nine highly effective steps you can take to be better prepared for any downtime opponent and ensure you recover faster with less data loss.

KNOW YOUR OPPONENT

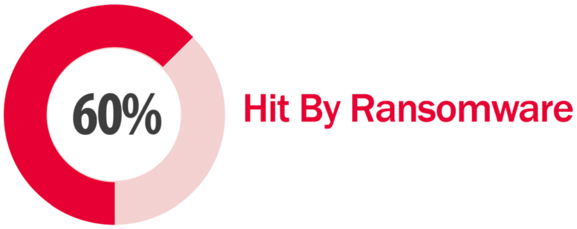
RANSOMWARE

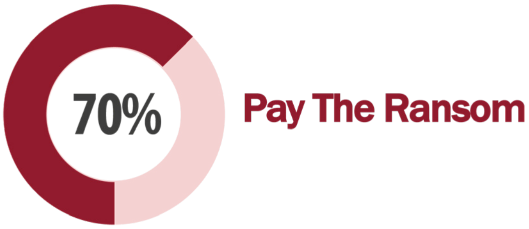
Ransomware is your scariest opponent.

The rate of ransomware infection is rising rapidly affecting every industry and company of all sizes. Last year 60% of organizations report being hit, with 70% of them paying the ransom.

Having antivirus protection in place and training employees is critical, but not enough - threats still slip through. That's why it's imperative that your backup solution can detect ransomware activity. Today's ransomware variants delay announcing their presence so they can infect the maximum number of files and better ensure a ransom is paid.

Your backup and recovery solution should actively inspect for ransomware infections during every backup. It should look for things like too many changed files, system files changing that shouldn't change, and inappropriate rates of change. Upon detection, your backup system should use AI and machine learning to minimize false positives, recognize an active infection and notify administrators so recovery procedures can begin immediately.





Don't wait for the red screen!

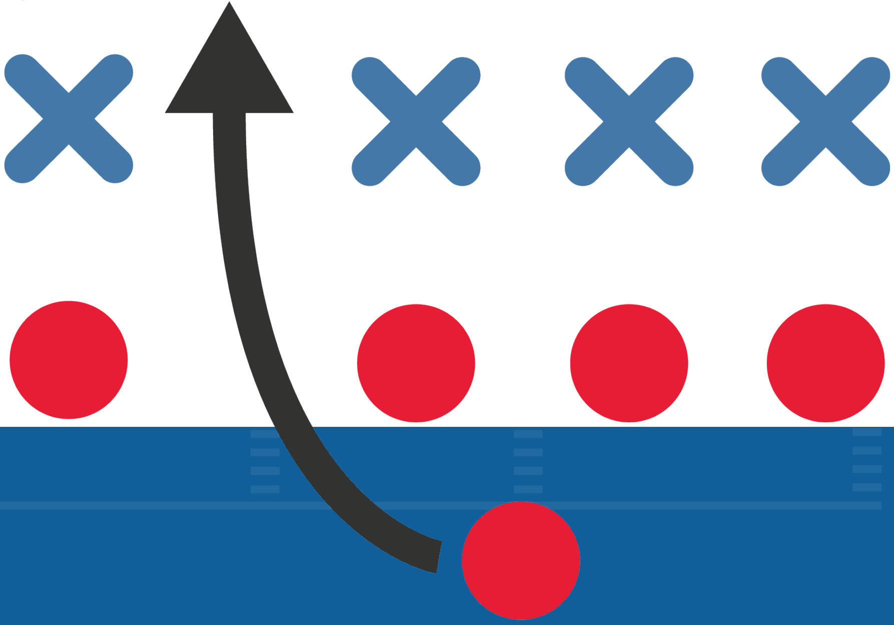
MAKE EVERY PLAY COUNT

DON’T MISS A BACKUP

You don’t know when a downtime event will occur and a missed backup can cause you to lose data. However this should not come at the cost of requiring hours and hours of your attention each week.

You should not have to spend more than 1 hour each week managing backups. If everything is running smoothly you should know. If there are issues, you should be appraised with easy to understand reports directing you to exactly what needs repair.

Your backup solution should constantly keep you appraised via email and your admin dashboard. The dashboard of the appliance should be customizable to allow you to organize the data just as you want. A full collection of backups is essential to fast recoveries that can deliver your RPO and RTO goals.



3

EASILY SET UP YOUR PLAYBOOK

FLEXIBILITY IN BACKUP

Your backup schedule is your playbook. Some plays are easy to setup and others are more complicated. You need to have flexibility when it comes to defining your backup schedules and ensure that they can support your business goals.

Your backup and recovery solution should offer multiple ways to schedule backups. The traditional way allows you to manually designate times, locations, targets and storage assets. However, new methods allow backups to be scheduled based on business objectives.

Just tell the system your RPO goals, identify the targets, and where you want the backups stored and the system calculates the rest of the variables required to meet that RPO requirements.

This ensures your backups can indeed support your business requirement.

LET THE EXPERTS DO THEIR JOB

ROLE-BASED MANAGEMENT

The enterprise collection of backups can get quite large and IT should let the designated departmental admins handle the data in their area of expertise. Your users know their data best so let them manage as much of it as possible.

Backup and recovery solutions that support role-based access gives designated department admins control of their data with no visibility to the data for other groups.

Administrators given role-based access can recover their own lost files, schedule backups that meet their production requirements and manage their own accounts. This gives users self-service rather than having to open IT tickets and interrupting your day. Let departments manage their own backups.

5

PRACTICE, PRACTICE, PRACTICE

AUTOMATED TESTING

Testing is how you practice recovery, and automated testing is practicing smart. The only way you know you will recover is to test it regularly, automatically and after every change to your infrastructure.

Recoveries seem simple but are often complex due to the fact that many applications have multiple tiers spread across different virtual and physical machines. You want to test how you would recover not just individual machines, but how ALL the machines in an application are recovered together. You need to know that all dependencies and the application components running on them can be brought up, in the correct order, with no fatal recovery issues.

6 IDENTIFY KEY PLAYERS

TRIAGE YOUR APPLICATIONS

Not all applications are equal. Triage you applications by their importance to your business so critical apps can be recovered first. Applications that manage customer orders are far more important than, for example those that enable employee expense reimbursement.

Your backup and recovery solution should allow you to set the recovery order for applications. This is a requirement for local recovery within the data center as well as cloud-based DRaaS recovery services. You decide the order of what recovers when.

7 BUILD YOUR GAME PLAN

COMMIT TO SLAS

Now that you understand which apps are critical you can set SLAs for different classes of applications. This communicates to your stakeholders how fast you will recover which applications and the maximum amount of data that could be lost in a downtime event.

Your testing procedures should compare your projected recovery times against your committed SLAs. Testing should be performed at least once per month and after any changes to your infrastructure such as adding new applications or servers. The test recovery report should be shared with and easily understandable by management.

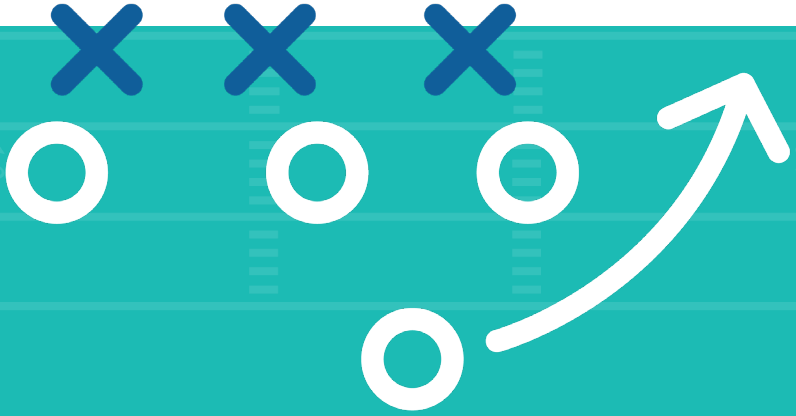
KNOW THE FIELD OF PLAY

SECONDARY RECOVERY SITES

No recovery plan located exclusively at a single site can be successful. Site level disasters such as floods, electrical outages and earthquakes will equally affect production and recovery assets.

A secondary backup location is needed to host application recoveries. For organizations doing business at a single location the cloud can be more cost effective than funding a second site or colo.

While hyperscale clouds such as Azure and AWS can meet this need you should consider the advantages of a purpose-built DRaaS cloud. These are built to optimize DRaaS performance and offer specialized services such as cloud seeding. With this type of cloud you are outsourcing your DRaaS requirements to experts. This frees you to focus on other tasks that only you can do. Some even offer recovery SLAs to increase your confidence that failovers will be executed correctly and on time during a downtime event.



9 CHOOSE THE RIGHT ASSISTANT COACH

LEADING CUSTOMER SERVICE

There will be issues with your backup and recovery solutions that you cannot handle. You may not understand how to set up a new feature or your recovery solution may need service.

Make sure your service provider uses advanced tools such as predictive analytics to identify hardware and software failures before they affect your backups. Ask to see their customer service satisfaction rating to see what others think.

You should look for a single vendor solution so you don’t have to figure out where a performance issue resides. Since disaster can strike at any time, you need to have your solution supported by a team available by phone, chat, and email—24 hours a day, 7 days a week, 365 days a year.

CHECK LIST

○ RANSOMWARE AWARENESS

○ DON’T MISS A BACKUP

○ FLEXIBILITY IN BACKUP SCHEDULING

○ ROLE-BASED MANAGEMENT

○ AUTOMATED TESTING

○ TRIAGE YOUR APPLICATIONS

○ COMMIT TO SLAS

○ SECONDARY RECOVERY SITES

○ LEADING CUSTOMER SERVICE`

CONCLUSIONS

You need to be 100% sure. You can't afford to just hope your backup and recovery solution will work correctly when you have a downtime event. Hope is not a strategy.

We have outlined 9 things you can do right away to reduce downtime to an absolute minimum. You should use the checklist included to verify that your backup and recovery solution can support these features and provide the highest levels of uptime possible.

Employing these tactics will protect you from all sorts of downtime events, malicious attacks, employee sabotage, accidental deletions and other unforeseen potentially destructive events.

Can't do everything on the list? You may be interested in seeing how Unitrends supports the features described in this report.

COST OF DOWNTIME 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.