UNITRENDS

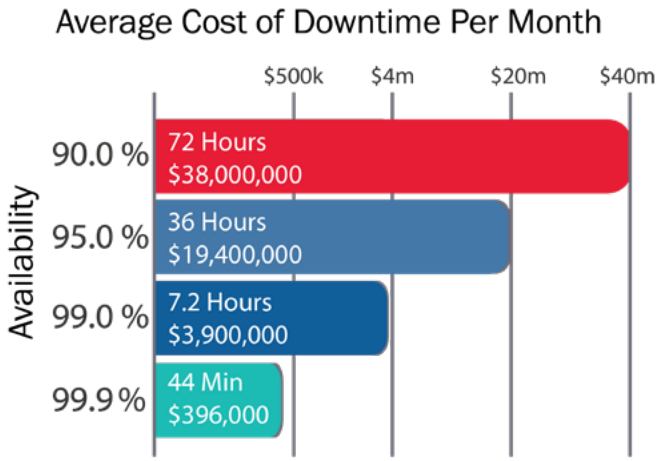
THRIVING IN THREATENING TIMES WITH IT RESILIENCE

FIVE STEPS YOU CAN TAKE TO BUILD IT RESILIENCE TODAY.

INTRODUCTION

IT Administrators are responsible for the technology that keeps the world's businesses running. Every day they are faced with circumstances threatening to bring down your applications, servers, and even communication. IT is forced to recover from catastrophic weather events, hardware failures, advanced ransomware infiltrations, and hundreds of other potential disasters. Even a minor event in just one of the millions of components in a modern datacenter can ripple out of control and cause enterprise-wide problems.

The cost of failure is high. Failing to recover or deflect the attacks results in application downtime. While the cost downtime on your business varies dramatically across industries, an average for all organizations is about $9,000 per minute. While 99.9% uptime is great, shortening that to 99.99% saves the average organization about $350,000 per month. This level of uptime is only possible if data protection and business continuity systems are automatically able to identify an issue and take near-instantaneous action without waiting for human directions.



*Average Cost of Downtime - $9,000 per minute Source: Ponemon Institute© Research Report

In the past, the gold standard of protection was tape backup; it was good enough just to preserve your data.

"The future is already here — it's just not very evenly distributed."

- William Gibson

Today backup has evolved to include the rapid recovery of not just the data but the applications and server software used to conduct business operations. Backup and continuity solutions have evolved to include virtualization, cloud, deduplication, orchestration, replication, and local and remote storage devices. And the evolution is continuing.

The next step in the journey is for systems to self-diagnose and resolve threats with minimal human involvement. Humans have become the weak link in the chain; no longer can mission critical applications wait for humans to identify an issue, devise a recovery plan and initiate action before business can continue. This takes too long and errors can occur. The next stage of the business continuity evolution is called IT Resilience (ITR). ITR includes building smart, self-directing capabilities into applications as well as the IT infrastructure.

> ITR needs to be in your plans and your data center.

Many of the elements of IT Resilience are available today if you know where to look. Many vendors are selling data protection and business continuity products but just a few have begun to integrate ITR capabilities into their offerings. Here are five ITR-enabled technologies on the market today that are playing increasingly important roles in building the bridge to near instantaneous and automated recovery.

IT Resilience Technology #1 Automatic Ransomware Detection and Notification

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 and recovery solutions automatically 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. ITR-enabled backup and recovery solutions actively inspect every file during every backup for ransomware infections. They look for things like too many changed files, system files changing that shouldn't change, and inappropriate rates of change. Files believed to have been corrupted are then automatically flagged so they are not used for recovery. Upon detection, the solution will automatically notify administrators through email and notices on their dashboard so recovery can begin immediately.

IT Resilience Technology #2 Orchestration of Instant Recovery

Not all applications have the same importance to a business. In a recovery scenario, business critical applications need to be prioritized ahead of general purpose apps. Also today's applications can be required to run on multiple servers. A client–server architecture is one where presentation, application processing, and data management functions are running on physically separated hardware. There needs to be recovery boot sequence to ensure software dependencies are established in the right order. ITR is especially effective in ensuring the right order and recovery technologies are used for each client's specific requirements. ITR is playing an increasingly important role in instant recovery technologies.

> Instant recovery is one of the fastest ways to recover critical applications. Instant recovery enables a recovery of a failed or corrupted physical or virtual machine at a remote site without having to wait for the production issues to be resolved.

ITR can provide measurable, trustworthy and repeatable RPO and RTO metrics since the technology is automated and requires little to no human involvement. In fact we are approaching a day when only ITR will be able to handle the full complexity of recovering modern data centers.

Instant recovery for physical servers virtualizes the full Windows environment on a backup appliance or on a remote server at a secondary site. In the event of a disaster

the virtualized instance is spun up as a virtual machine on an embedded hypervisor. Windows instant recovery means there is no need to restore the original hardware before the application is again available for business production. This saves the need for quick ordering from hardware vendors, the need for like-hardware or for stockpiling of spare equipment to be swapped in the event of a local or site-wide disaster.

There is also instant recovery for VMware environments. This technology is best for large numbers of VMs or very large VMs, configurations not ideal for hosting on recovery appliances. Replicas are maintained at a remote site and kept up to date through the normal backup process. Replica recovery times can also be confirmed with the normal testing that organizations should be using for the rest of the DR program.

IT Resilience Technology #3 Automated Testing

The only way to know if you can recover in an emergency is to test regularly and each time you make a change to your infrastructure.

> New, intelligent tools are now available that can greatly ease your concerns by automatically testing to ensure all components are in place and capable of recovering or telling you what is broken so it can be fixed.

Additionally, you get an easy to read, formal report certifying that your disaster recovery solutions have been tested and showing the RPO and RTO results. These tools automate testing so you know exactly how fast and to what point your data and applications are protected without requiring any manual work on your part.

IT Resilience Technology #4 Cloud

Cloud is an ideal way to ensure geographic resilience for smaller companies, especially those that need a remote presence to protect copies of their data. Purpose-built DR clouds are incorporating ITR capabilities into many of their offerings to increase the speed and success of recovery. Two advanced Cloud-based ITR technologies that are not usually thought of as being automated are:

Cloud Seeding

Cloud Seeding is an important part of speeding the cloud recovery process. It can take months to move 100TB over 1GB WAN connection. Cloud seeding services use hardware devices to move data into and out of the cloud. You load your data on tape, removable drives, disks or even servers and ship them to the cloud location overnight. Then incremental updates are all that is needed to ensure an exact copy of your files are located in the cloud. The process is reversed for restoring your on-premises data after a disaster. The cloud provider uses automated processes to physically load the files on hardware and ship it to your data center for high speed replication. Cloud seeding should be part of the services offered by your cloud providers. Without it, gaining the advantages of cloud recovery are slowed considerably.

Compliance Reporting

Almost every industry has legal requirements on how they must protect their IT infrastructure and their data. HIPAA, for example, is the one of the widest compliance mandates affecting every hospital, medical practice, lab, dental office and all the companies that do business with them. HIPAA requires that medical organizations have a disaster recovery plan and prove that it is regularly tested. Leading cloud providers have automated testing applications so well that the resulting performance reports can be used to pass compliance audits. These reports are generated automatically each month or whenever there is special need to test, such as when there has been a change to the infrastructure. No human actually launches or performs the tests, they are just part of an ITR-enabled environment.

Today's ransomware variants delay announcing their presence so they can infect the maximum number of files and better ensure a ransom is paid.

"Maybe the most important result of this deployment is that I now have faith in our failover strategy. If I had an outage at our primary site, I am very comfortable that a failover would be successful."
Steve Crocker, CIO Magna Bank

IT Resilience Step #5 Disaster Recovery-as-a-Service (DRaaS)

One especially critical area where ITR can make a large difference is DRaaS. Adding DRaaS to a corporate disaster recovery plan need not take a large amount of IT time and budget. DRaaS can be contracted for just business critical applications or entire suites of apps. Be sure and request a recovery SLA (Service Level Agreement) to insure the DRaaS provider will stand behind their recovery service results. A one hour SLA means that even in the event of a site-wide disaster, computing applications will be available to the enterprise in less than 60 minutes – a very speedy recovery. ITR is what makes a one hour SLA possible.

DRaaS provides high levels of recovery confidence. Contracting for DRaaS services also means that the corporate IT resources are freed from having to manage and monitor this activity, allowing them to focus on projects only they can perform – working with their business partners. They can sleep better at night knowing that their disaster recovery operations are in the hands of professionals equipped with ITR-enabled tools.

CONCLUSION

IT organizations that adopt todays forward looking IT Resilience technologies are setting themselves up for success. IT Resilience will become a more-widely supported concept over the next few years. It holds the promise of near-instant recovery from any failure or disaster with little human involvement.

Now that you have heard about ITR-based technologies that are currently available, it is time to begin integrating them into your IT infrastructure. You may be interested in seeing how Unitrends is deploying these capabilities for Simpler, Smarter IT.

Think you have ITR? Take the quiz and test your IT Resilience!

Other Items that May Interest You:

5 Minute Disaster Recovery Checkup

Get a personalized disaster recovery report for your environment.

Read More

Anatomy of a DRaaS Event: A True Story from Hurricane Irma.

Irma had just destroyed much of the Caribbean, and Safety Products Inc did not want their company operations to be part of the toll.

Read More

Get Your DR Plan in Shape for 2018

Five Questions, Four Calculators, and One Test to prepare you for the new year.

Read More

GET YOUR FREE TRIAL

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.

unitrends.com
PART# WP-2070-ENG-A-syndicate Thriving

UNITRENDS