probax

Most MSPs have inadequate disaster recovery solutions

Is your MSP one of them?

A Probax White Paper

Table of contents

probax

“Historically data protection was thought of as backup. But simply backing up business data with extra copies is no longer sufficient in today’s market. Simply having copies of data to fail back to after an unexpected outage usually means slow manual processes need to be completed.

The worst part? There is a significant cost attached to this. It results in unacceptable revenue losses due to the business not being able to keep operations running during those periods.

Disaster Recovery as a Service means MSPs can ensure business continuity for their customers, and rapidly fail back from outages to minimize impact to operations.

When it comes to data protection, Disaster Recovery as a Service needs to be the main game for MSPs.”

- Tim Smith, Probax CEO

SOME END CUSTOMERS HAVE INADEQUATE DISASTER RECOVERY SOLUTIONS

Business data is the lifeblood of every organization. As a result, uptime is one of the most important necessities in the digital world—and perhaps its most fragile as well.

When that data can't be accessed due to an outage, cyberattack, human error or for some other reason, unplanned downtime has a range of negative impacts to businesses of all sizes.

It's common for businesses to engage a Managed Service Provider (MSP) for managing their IT infrastructure, offering technical support to staff, managing user accounts and licenses, hardware procurement, as well as to support backup and recovery.

When it comes to recovering from a disaster, many businesses don't understand that their MSP is relying on backup-based recovery. But backups alone are inadequate as a true disaster recovery solution. Similarly, third-party disaster recovery solutions which are not fully independent of backup data are also inadequate.

MSPs that fail to understand this concept are leaving their clients exposed to unnecessary risk when recovering from downtime

Even worse, the consequences of this approach may even result in unacceptable revenue loss due to the financial impact. For the MSP, this may result in a compensation claim for damages and losses suffered by their client.

The purpose of this white paper is to show that MSPs need to offer true disaster recovery based on replication to protect their own MSP business and ensure that the businesses they support can recover from downtime rapidly.

Disaster Recovery as a Service, or DRaaS, based on replication is the only solution that will deliver the protection businesses need.

Businesses are demanding true disaster recovery to minimize downtime

The sentiment in the IT world about disaster recovery is clear — 65% of organizations' key IT decision-makers are not confident that data critical to business operations will be recoverable in case of a cyberattack.[1]

In response, 41% of these decision-makers are prioritizing Disaster-Recovery-as a-Service (DRaaS) as the solution to their concerns.

By 2023, 51% of organizations plan to adopt DRaaS to improve their resiliency to downtime.

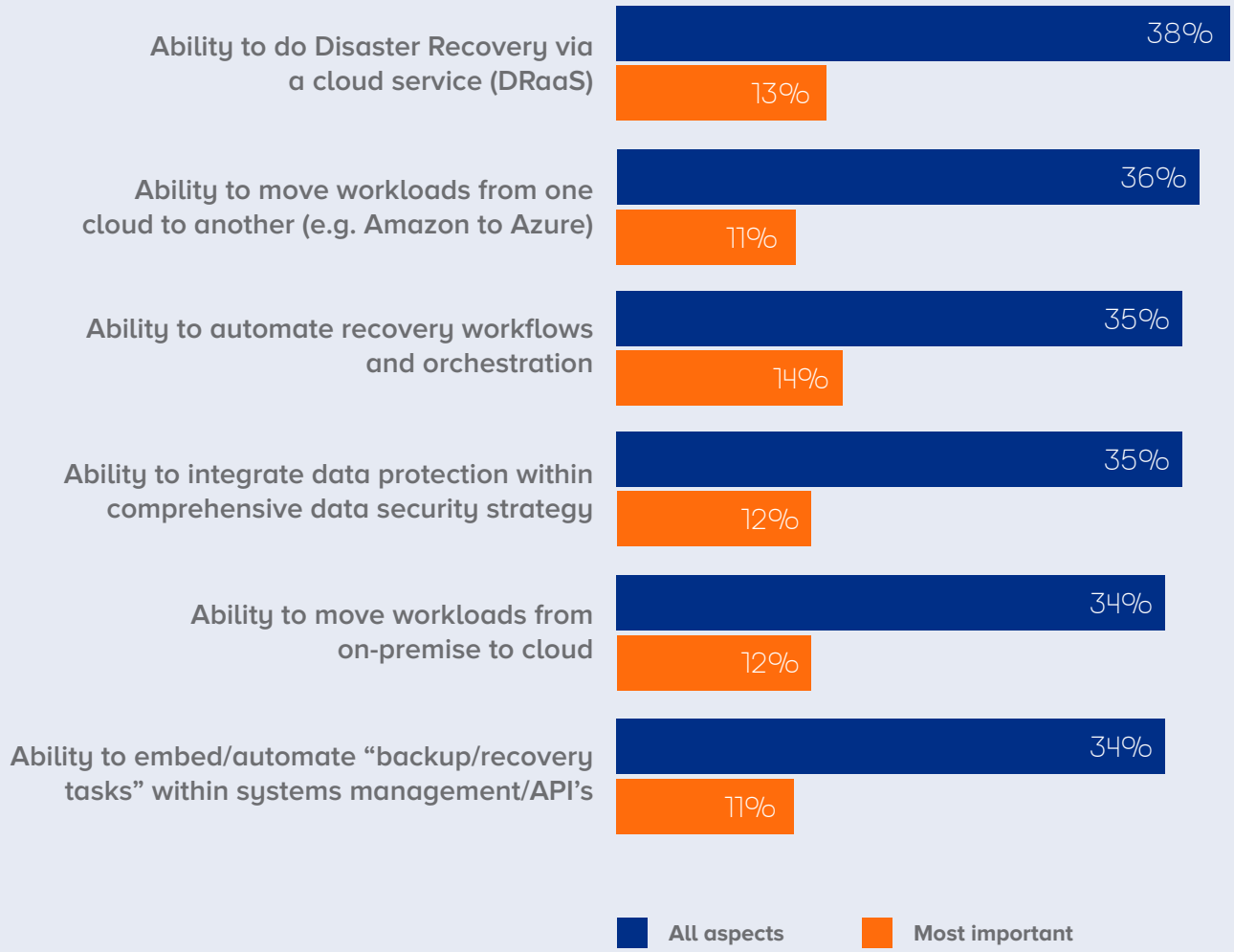
Today's organizations need data protection that gives them the ability to respond to an outage as quickly as possible, fail over and fail back to production rapidly while minimizing impact to operations.

Replication-based DRaaS represents the next generation of data protection and business continuity assurance. Plus, the ability to recover applications in the cloud, when needed, slashes the cost and complexity of traditional recovery capabilities.

probax

Cloud-based disaster recovery already represents a critical business priority

According to the 3,000 global organizations who took part in Veeam's 2021 industry research, integrated data protection and security, cloud workload portability, and the ability to do disaster recovery via a cloud service (DRaaS) represent top priorities for leadership teams.[2]



probax

Cloud-based disaster recovery represents cost savings

Infrastructure & Operations (I&O) leaders are increasingly looking to DRaaS for a variety of reasons, including faster implementation, increased business resiliency and reduced costs.

Fiscally speaking, it is not uncommon for DRaaS prices to be 30% to 50% of what it would otherwise cost to build out, operate and maintain similar capabilities.[3]

When it comes to cloud-based DR, MSPs also benefit from cost savings in that they don't need to build or maintain their own platform.

Outsourcing infrastructure, storage, networking and facility needs to vendors like Probax and Veeam results in an ability to consolidate and integrate costs, reduce capital and operational expenditure, minimize technical engineer time and focus on higher revenue earning opportunities.

Probax also offers its partners a multi-tenant platform for centralized management, automation and enhanced reporting.

Types of threats and causes of downtime

Downtime can be the result of one or even multiple factors and just over half of these are caused by equipment failure and natural disasters.

A large part of the downtime equation has human root causes—whether through error or malicious intent.

Because these causes are so diverse and varied, businesses need a DR strategy that can protect against all of these causes. A robust continuity strategy should also be established to minimize downtime and reduce the impact of service outages.

What's causing all of this downtime?

UPS SYSTEM FAILURE	25%
DISTRIBUTED DENIAL OF SERVICE ATTACKS	22%
HUMAN ERROR	22%
WATER, HEAT, CRAC FAILURE	11%
WEATHER	10%
GENERATOR FAILURE	6%
IT EQUIPMENT FAILURE	4%

https://www.vertiv.com/globalassets/documents/reports/2016-cost-of-data-center-outages-11-11_51190_1.pdf

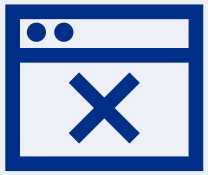
probax

What's causing all of this downtime?

Accidental/Human Error

Cyber Attack System Failure

Cloud Outage



Software Failure

System Failure

Natural Disaster

MEASURING DOWNTIME

To better understand and plan how downtime impacts an organization, you need to set two critical metrics—Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Recovery Point Objective (RPO)

Recovery Point Objective describes the maximum amount of data that can be lost in an incident before there is an unacceptable impact on business. The RPO is described as a function of time because it is based on the regular intervals when your data is backed up. For example, if the last available copy of data comes from 18 hours ago and your business continuity plan allows for a recovery time period no greater than 20, then you're still within your RPO.

RPO also describes the worst-case scenario data loss associated with downtime. If you backup your data every 12 hours, then you will lose a maximum of the last 12 hours of data.

The RPO should be as low as possible in order to minimize the amount of damage caused by an incident. You should also set up notifications that warn you when your RPO is reaching critical levels, and set individualized RPO targets for each application based on the thresholds set in your service-level agreements—not just having a single shared RPO for your entire business.

Of course, reducing RPO means increasing the frequency of backups, which in turn increases the data and bandwidth requirements over time.

Recovery Time Objective (RTO)

In contrast, Recovery Time Objective (RTO) is the duration of time and service level within which a business process must be restored after notification to avoid unacceptable consequences associated with interruption.

Essentially, it's the answer to the question in your recovery plan: "How long will it take before we're back in business after a service outage or downtime?"

Just like RPO, RTO must be reduced to as low a figure as possible. Every minute of downtime represents thousands of dollars in lost revenue.

Failover and failback

Failover is the ability to switch automatically and seamlessly from one system of operation to another with minimal or no downtime for users.

To achieve redundancy upon the abnormal failure or termination of a formerly active version, it is imperative that standby hardware components always stand ready to automatically switch into action.

All backup and recovery services must themselves be resistant to failure because disaster recovery relies on failover being successful.

probax

Up to a $26,000 loss per hour: Measuring the cost impact of downtime

Downtime can affect many facets of your customers' businesses. These costs accumulate from loss of revenue, lost employee productivity, damage to reputation and more. For small-to-medium sized businesses, downtime and data loss can even have catastrophic consequences.

What would downtime cost your customer?

Quantify the impact of downtime to gauge the impact of a potential IT disaster. Use our Downtime Calculator at: https://www.probax.io/the-cost-of-downtime#calculator

THE LONGER THE DOWNTIME, THE GREATER THE IMPACT.

1 MINUTE	>$137–$427 FOR SMALL BUSINESSES
1 HOUR	>$8,000–$26,000 FOR SMALL BUSINESSES
YEARLY AVERAGE DOWNTIME	65 minutes 5-10 TIMES A YEAR ON AVERAGE
MAXIMUM DOWNTIME AN AVERAGE BUSINESS CAN TOLERATE FOR **MISSION CRITICAL APPS**	2 hours
MAXIMUM DOWNTIME AN AVERAGE BUSINESS CAN TOLERATE FOR **OPERATIONS CRITICAL APPS**	3 hours

COMPARING BACKUP AND DISASTER RECOVERY

The terms ‘backup’ and ‘disaster recovery’ are often discussed as interchangeable. However, while the two are related and overlapping concepts, they do not mean the same thing. Indeed, traditional backups may not even be appropriate solutions for disaster recovery in mission-critical and business-critical environments.

Backup

Backup is the process of making full copies or snapshots of an organization’s business data and storing it in secondary and tertiary locations to protect it from loss. Upon data loss, the latest restore point snapshots are restored to the live environment.

Backups are often completed at Virtual Machine (VM) level or at storage level and are completed at fixed intervals, usually daily, weekly, monthly or a combination of all three.

Best practice for backups is to follow what Veeam calls the **3-2-1-1-0 rule**.

3-2-1-1-0 RULE STAGES EXPLAINED

3 different copies of data on → **2** different media → **1** copy of which is kept offsite, and → **1** of which is offline air-gapped or immutable, while ensuring → **0** errors after automated backup testing and recoverability verification.

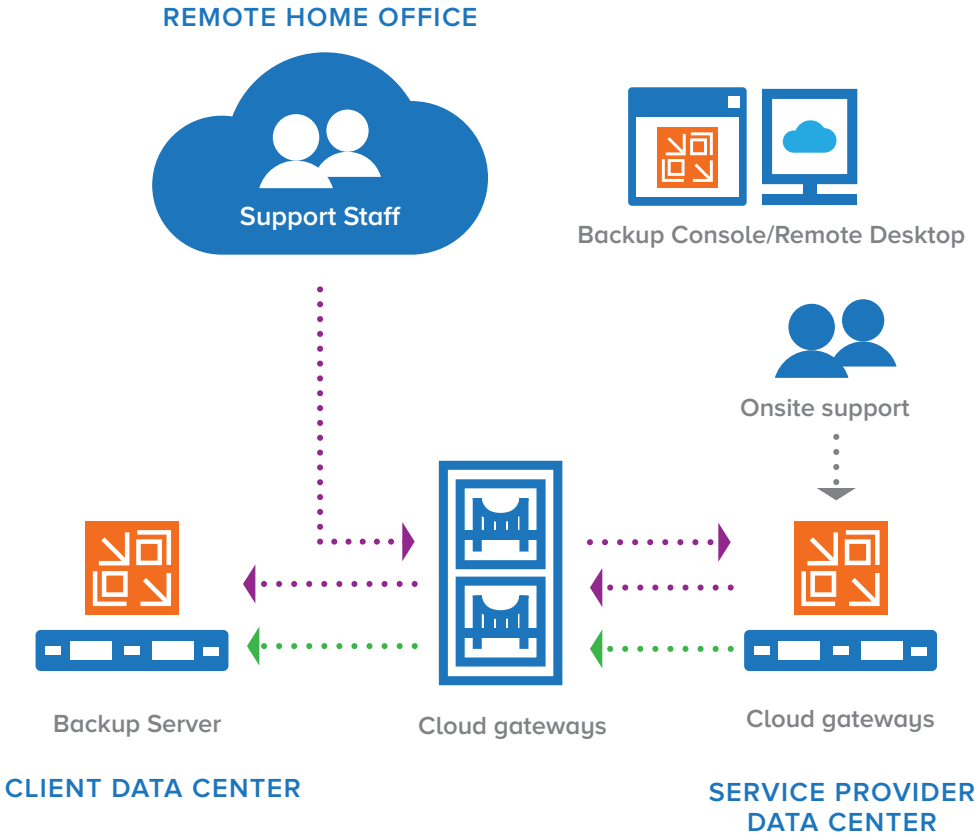
When backup is delivered as a service, the responsibility for capturing and maintaining a company's backups falls on the MSP who takes over from an on-premises IT team. The MSP manages, maintains, and hosts these backups, and can restore them to their end user client upon request.

In general, Backup-as-a-Service (BaaS) does not include helping avoid downtime. Customers will still need to manually restore backup data and in some cases source new hardware infrastructure.

When completed manually, failing back to production requires an unacceptable amount of time. The MSP usually needs to set up temporary hardware infrastructure and then restore data back to the point in time of the last image-based backup.

Depending on the complexity of the environment and data structure, this manual process can be lengthy.

The revenue loss impact could be significant, exposing the MSP to a compensation claim for damages and losses suffered by their client.



Disaster Recovery

On the other hand, disaster recovery refers to the processes and solutions in place that allow you to rapidly restore access to your services, applications, and IT infrastructure after an outage-causing incident. It may also include the ability to keep critical functions working even in the immediate aftermath of a disaster, as in the case of failover systems.

Disaster recovery based on replication ensures data is regularly replicated to one or more, highly available data centers on redundant, high-performance infrastructure.

Where a backup snapshot represents a single point in time, replication utilizes change-block tracking at the hypervisor layer to constantly replicate data to storage, as it is written. The performance and network impact is negligible since only changes to data are replicated continuously, rather than the whole VM, host or array.

'Disaster', despite the term, does not automatically refer to a significant event — it may refer to any unplanned system outage that prevents access to your infrastructure, applications, or business data for any amount of time.

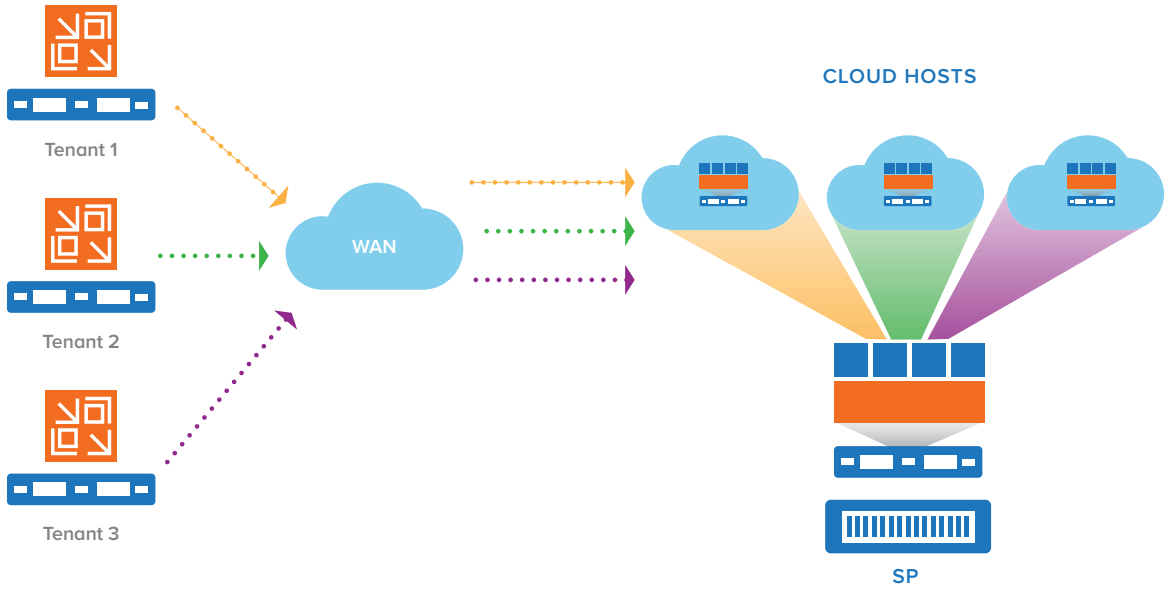
When disaster recovery is delivered as a service, the MSP handles all the data replication, synchronization, maintenance, and continuity requirements that a business may need in the event of a disaster. Alternatively, they may choose to outsource these functions to a 3rd party solutions provider like Probax.

Disaster Recovery-as-a-Service (DRaaS) maintains one or more recovery sites to which their client data is replicated.

When failover is required, pre-configured virtual machines are spun up to restore user access to systems, applications and/or business data with minimal or no downtime.

Critical to a failover plan is sufficient network infrastructure to handle the failover and failback.

Each critical element of the LAN, WAN, SD-WAN or other infrastructure services contributes to the network connectivity in the event of a workload failover and failback.



DR from backups vs DR based on replication

There continues to be a misperception that backup-based DR is an adequate disaster recovery solution for end user businesses, compared with replication-based DR.

The reality couldn't be further from the truth.

MSPs that offer backup-based DRaaS solutions ultimately need to recover their customer's environment in the cloud using backup images. When a MSP is using a vendor's backup-based DRaaS solution, the manual recovery process is usually performed by the vendor.

Either way, this has enormous consequences on the end user business and may have revenue loss consequences. That's because it takes considerably longer to fail over and fail back from image-based backups compared to a true DRaaS solution that regularly replicates an environment to a provider's cloud.

This means that MSPs providing replication-based DR are providing a significantly better business outcome than providers who only offer backups and/or DR solutions based on backups.

A reputable DRaaS provider will offer a solution that makes both failover and failback frictionless, usually by leveraging market leading technology from vendors like Probax and Veeam.

"If you're unsure whether your MSP offers backup-based or replication-based DR, ask!"

Tim Smith

BACKUP VS REPLICATION

DEFINITION

Backup involves making a copy or copies of data.
Replication is the act of synchronizing systems and data between a company's production and recovery sites - the latter usually being in the cloud. It is typically measured with RTO and RPO.

PURPOSE

Backup focuses on compliance and granular recovery, and is a snapshot of data at a point in time.
Replication and recovery focus on delivering adequate Disaster Recovery, minimizing RTO and enabling fast failover and failback to resume operations after an outage.

USES

Backup is typically used for everything in the enterprise, from critical production servers to SaaS applications.
Replication is often used for mission-critical applications that must always be up and running.

REQUIREMENTS

Backup requires an external storage repository or appliance for onsite backups (usually a Server, NAS or SAN). Offsite backups are usually stored in the cloud or on tape.
Replication requires investment in secondary infrastructure in order to enable recovery and continued business operations.

HOW IT WORKS

Backup typically relies on snapshots which are copies of the data set taken at a pre-determined point-in-time.
Replication can be Synchronous, Asynchonous or Near-Synchronous and may use Continuous Data Protection to enable users to access historic data.

BOTTOM LINE

Backup is a relatively inexpensive way to avoid complete data loss. Valuable for non urgent data recovery and compliance. Does not ensure continuity of operations.
Replication is focused on ensuring that business applications and business-critical data are always available, even after a disaster. DRaaS is 30-50% of the cost of traditional DR and a fraction of the cost of the cost of downtime (up to $26,000 per hour).

Top reasons why legacy backup alone is NOT a viable disaster recovery method

Data protection based on backup alone is unable to keep pace with the demands of most end user organizations, posing a threat to business continuity, and potentially leading to severe consequences for both business reputation and performance.

1. Backups only protect data at a point in time

The principal reason why backup alone isn't sufficient is that backing up copies of data only protects the data itself at a specific point in time and is better suited for longer-term data retention. Data replication is focused on uninterrupted operation of mission-critical and customer facing applications.

2. Lengthy RPOs and RTOs

If backup copies are only made weekly or daily, the RPOs are relatively high. This means that for an outage, any updated or additional data produced since the last backup was taken, will be lost. Additionally, since the backups are just copies of data, the system recovery is manual, meaning the RTOs are much higher. The higher RPOs and RTOs alone make backup an inadequate DR solution.

3. Exposure to unacceptable downtime

It's all too common for MSPs and some DRaaS vendors to focus on the RTO/RPO of the failover only. Failing back and restoring full backups during incidents can be extremely time-consuming depending on the size of the environment, the backup storage medium used and the process of manual restoration of data and services to bring the production environment back online. The consequence of neglecting the RTO/RPO of failback is unacceptable as the impact can result in significant downtime and revenue loss

4. Limited snapshots or recovery points

Traditional backups can take a long time to create and save an entire snapshot or state of data. Combine this with the impact of shorter backup intervals on RPO, and you will find only a limited granularity of backup snapshots to select from when initiating recovery. This can be dangerous if the data at the time of the latest backup was corrupted and you need to restore to a different earlier time—potentially one outside your RPO window.

5. Poor recovery automation

Starting the process of rebuilding from a backup can be automated, but there is a limit to how much efficiency you can derive from it due to the sheer time it takes to carry out a full backup recovery. If you want a more automated recovery system that can help you get your systems back up and running, you need a disaster recovery solution that offer quick and seamless failover and failback.

6. Data retention

If an outage were to occur, failing back to a backup will take your environment back to the point of that backup. Any data generated by users since the last backup was taken will be lost. A disaster recovery solution will ensure all user data is protected no matter when you failover or failback.

The case for DR based on replication

Given the problems of automation, poor RPO/RTO targets, and limitations in recovery points, what would be a superior DR alternative to backups that address these issues? For many businesses, the answer is replication, the process of replicating and then transferring data across one or more recovery sites, such as a dedicated DR site or cloud infrastructure.

Replication is a blanket term for a variety of methodologies, but they all have in common the ability to capture your system's data, detect changes to data as they happen, and reproduce these changes at recovery sites. This allows for several benefits over traditional backups for DR purposes.

Better backup and recovery performance

Because replication doesn't capture all your data at once, but rather only synchronizes what has been changed, it takes up less storage and CPU resources than initiating a backup.

It also allows you to maintain continuity in case of a disaster—if one site fails, your system may automatically failover to the next replication site with little to no downtime.

Improved granularity of backup snapshots

As mentioned, increasing the interval of backup snapshots can exert a significant strain on your processing capacity and contribute to reduced performance. This is why in most cases, you may only select from 12-24 hour intervals. Meanwhile, replication allows for a vastly increased granularity of restoration points because they are created at the file or even block level, depending on the technology used. This helps you meet much tighter RPO metrics, oftentimes in the order of minutes or even seconds.

For Tier 1 mission critical applications, RTO/RPOs can be less than 15 minutes with Veeam replication.

CRITICAL INCLUSIONS FOR DISASTER RECOVERY PLANNING

Planning for disaster recovery involves far more than simply the process of recovery itself. You need to ensure that you consider these inclusions before you deploy your plan.

1. Roles and responsibilities

It is imperative that all stakeholders in the disaster recovery plan are aware of the roles and responsibilities they have in carrying out the plan. They should have their contact information and everything they need to perform their tasks laid out in detail.

This is not only so that they can be reached in the event of a disaster, but also for accountability and evaluation of the plan itself after execution. There should also be backup personnel for important decision-making roles.

2. Storage considerations

You must identify the cost and storage utilization of the disaster recovery solution you plan to implement. These will allow you to set aside the necessary resources to have the plan run as smoothly as possible. For example, snapshot-based replication incurs an average overhead of 20-30% of total storage, whereas journal-based continuous data protection only requires 7-10%.

3. RPO/RTO

Your RPO and RPO targets must be set based on your SLAs and the total costs associated with your downtime. They must also be reasonable based on your disaster recovery needs—if you're inadvisably running backup-based DR for high-availability systems, you need to be aware that tighter RPOs mean significantly higher overhead.

4. Login management

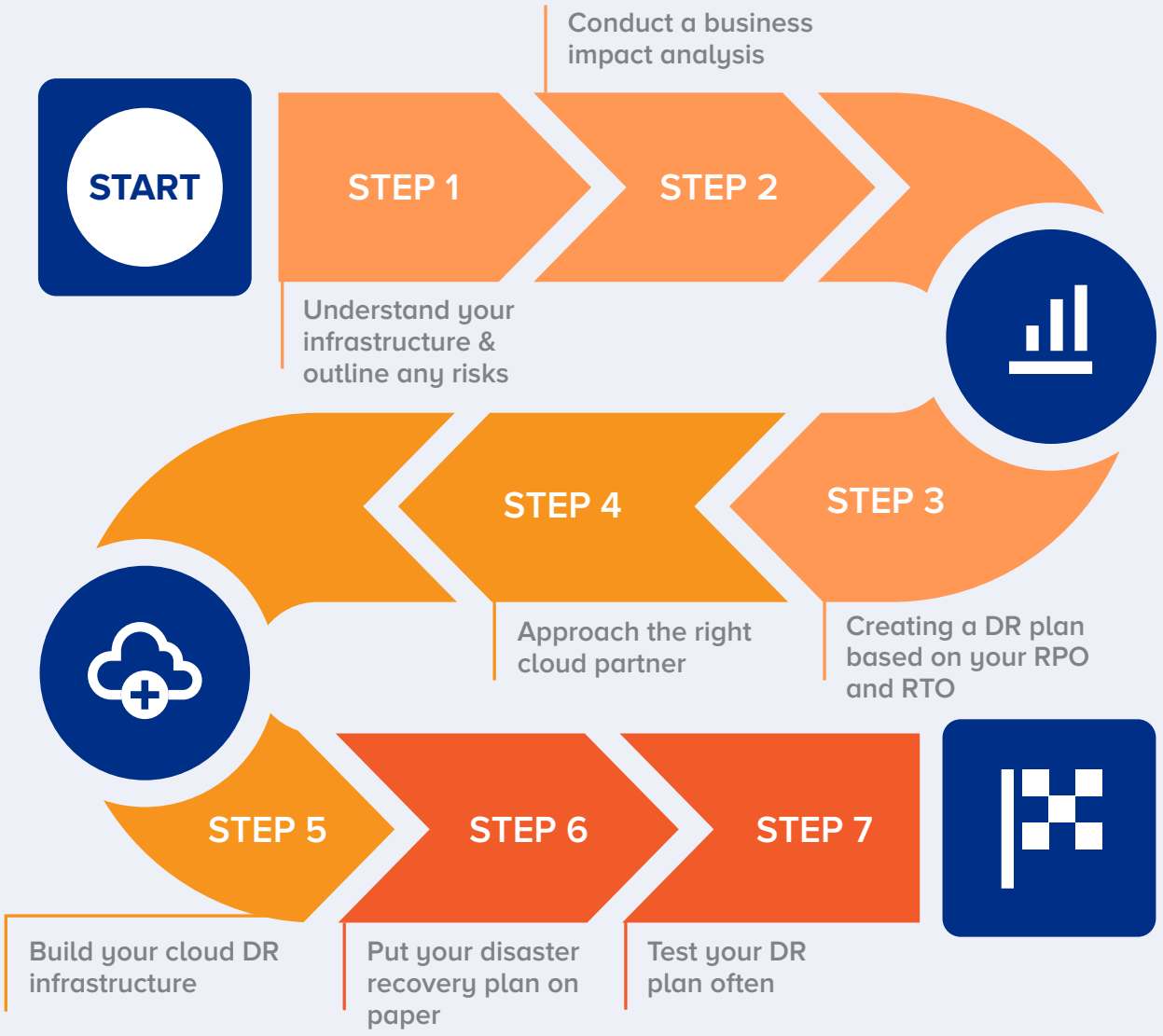
Disaster recovery requires access to very sensitive parts of your system, so having it be highly secure is imperative. However, it's equally important for the secure login information to be accessible even if a key stakeholder is on vacation or otherwise unavailable. Make sure that there are several backup personnel who have the necessary logins to initiate your disaster recovery plan.

5. Testing schedule

You need to set a regular testing schedule of at least once a year to ensure that your failover and other DR capabilities are working as planned. Perform complete training drills that test your DR team's performance and make sure they match your RPO. This will also help them practice their roles and perform their jobs better in the event of an actual disaster.

6. Compliance documentation

Ensure that the status and location of sensitive information, essential documents, and other data required for compliance are all recorded and easily accessible by your DR team. This will help you prioritize how your DR plan is executed and helps meet compliance requirements in case of a disaster.


START
STEP 1
Understand your infrastructure & outline any risks
STEP 2
Conduct a business impact analysis
STEP 3
Creating a DR plan based on your RPO and RTO
STEP 4
Approach the right cloud partner
STEP 5
Build your cloud DR infrastructure
STEP 6
Put your disaster recovery plan on paper
STEP 7
Test your DR plan often

THE UNDENIABLE DRAAS OPPORTUNITY FOR MSPS

A $23.3 billion DRaaS market for MSPs

By 2027, the DRaaS space is expected to become a $23.3 billion market, growing at a remarkable 23.3% Compound Annual Growth Rate (CAGR). Of this, it is projected that MSPs will constitute almost half of the total market by 2027.[5]

The market size forecasts are only getting bigger with every passing year, and the number of companies with plans to adopt DRaaS methods continues to grow.

MSPs have a clear, growing market in which to enter and provide new managed services, as companies become more and more aware of the dangers of not having DR—as well as the savings and benefits associated with having a third party manage their disaster recovery initiatives.

The main drivers for DRaaS adoption

According to survey respondents, main drivers for DRaaS adoption had an equal weighting across diverse reasons. The following six main drivers are:

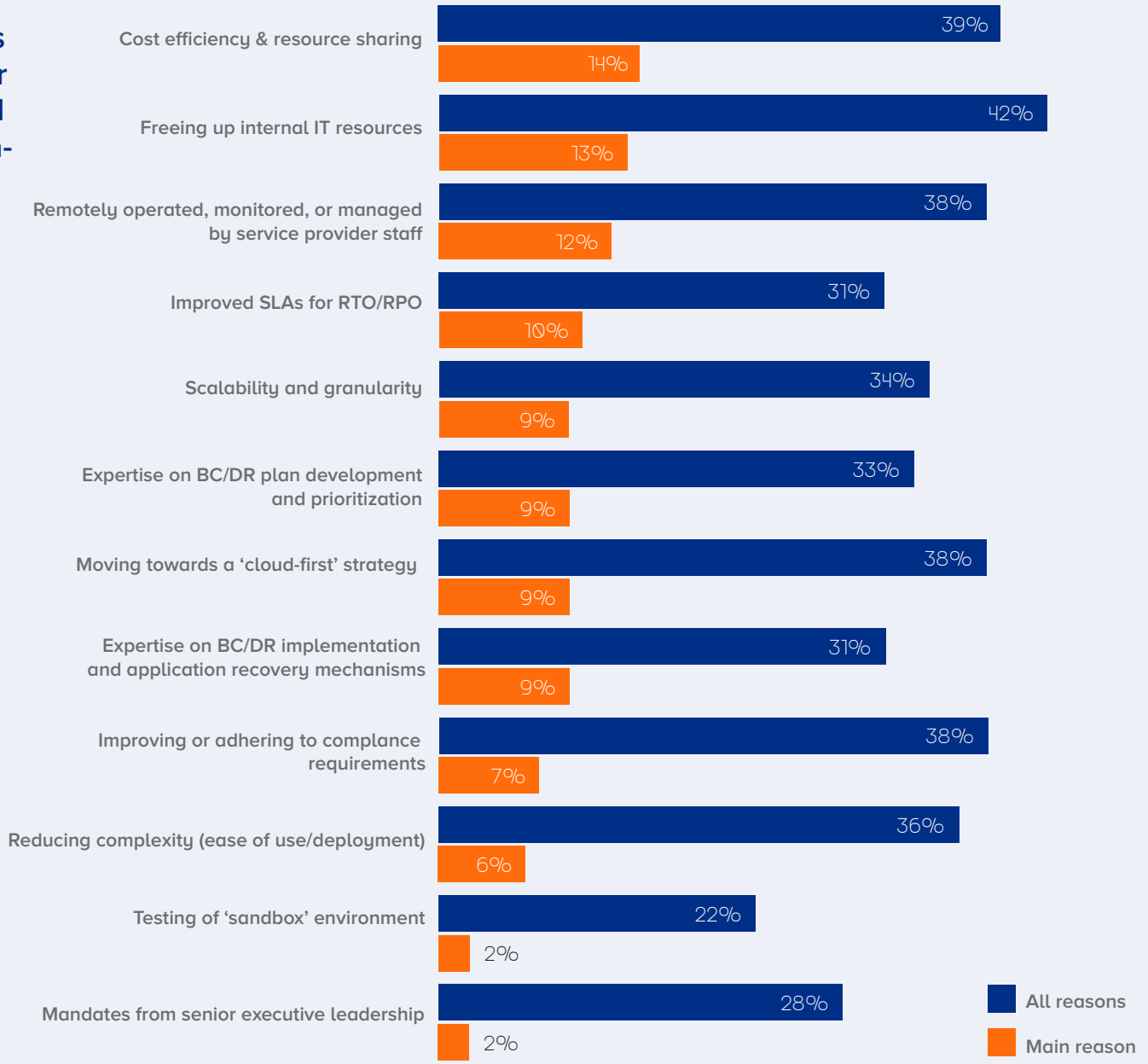
1. Cost efficiency & resource sharing
2. Freeing up internal IT resources
3. Remote monitoring
4. Adhering to a cloud first strategy
5. Improving compliance
6. Reducing complexity.[6]

This means the reasons that organizations use DRaaS in lieu of a secondary data center has a broader variety of appeal and recognized value beyond just survivability and economics.

Out of these, the primary reason for DRaaS adoption is for operational efficiencies, including cost efficiency, resource sharing of internal resources as well as better outcomes delivered through remote monitoring and improved SLAs.

probax

Which of the following best describes why your organization uses Disaster Recovery as-a-Service (DRaaS), instead of managing your own secondary data-center? What is the main reason?



Veeam Data Protection as a Service Report 2021

probax

What do customers consume from their DRaaS provider?

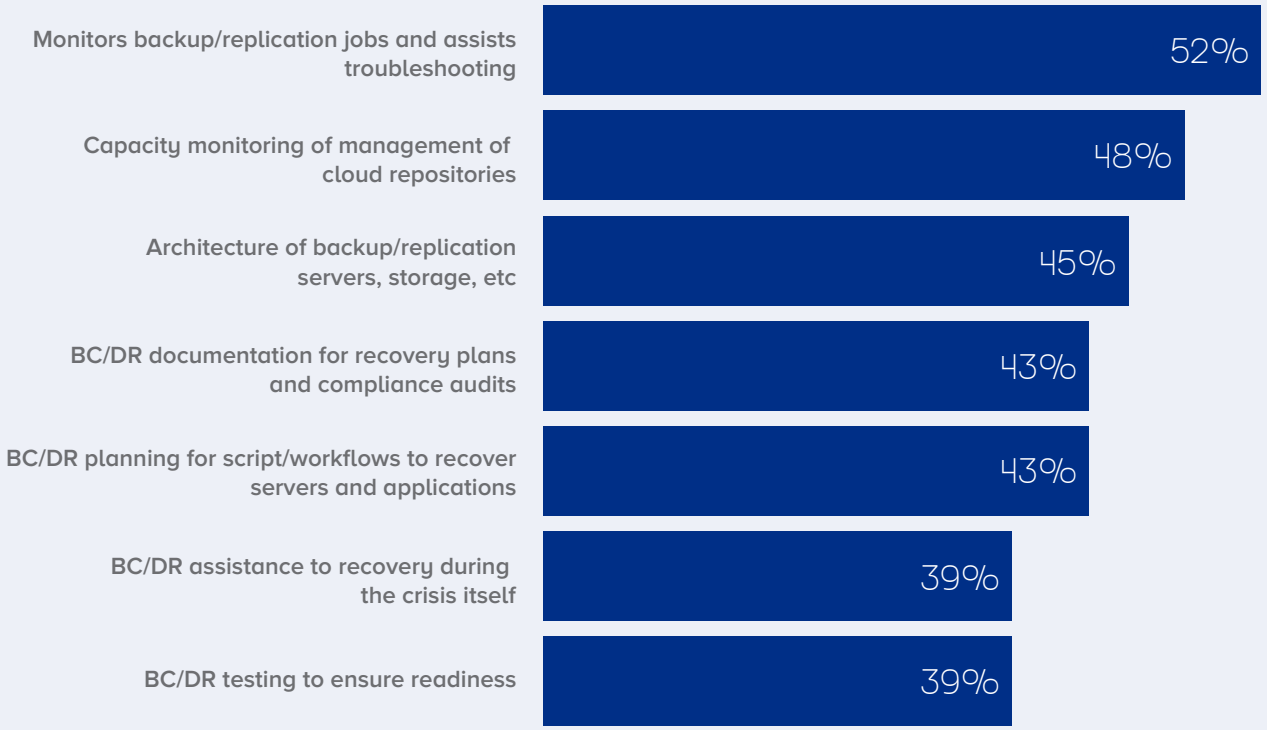
There are a range of functions customers look to their DRaaS provider for, including monitoring backup/replication jobs and assisting with troubleshooting, capacity monitoring or management of cloud repositories, and architecture of backup/replication servers and storage.

These functions which organizations mostly consume from their DRaaS provider can be seen as two main categories, which are:

1. **The operational management of the secondary infrastructure including monitoring and architecture, and**
2. **Business Continuity / Disaster Recovery (BC/DR) expertise including documentation, planning, testing and the actual recovery itself.**

It will be beneficial for MSPs who are taking a DRaaS offering to market or who are looking to expand the reach of their DRaaS offering to position and articulate their offering in the context of these two key categories.

What functions does your DRaaS provider deliver to your organization in regard to data protection?



Veeam Data Protection as a Service Report 2021

probax

MSPs need to address end user DRaaS concerns

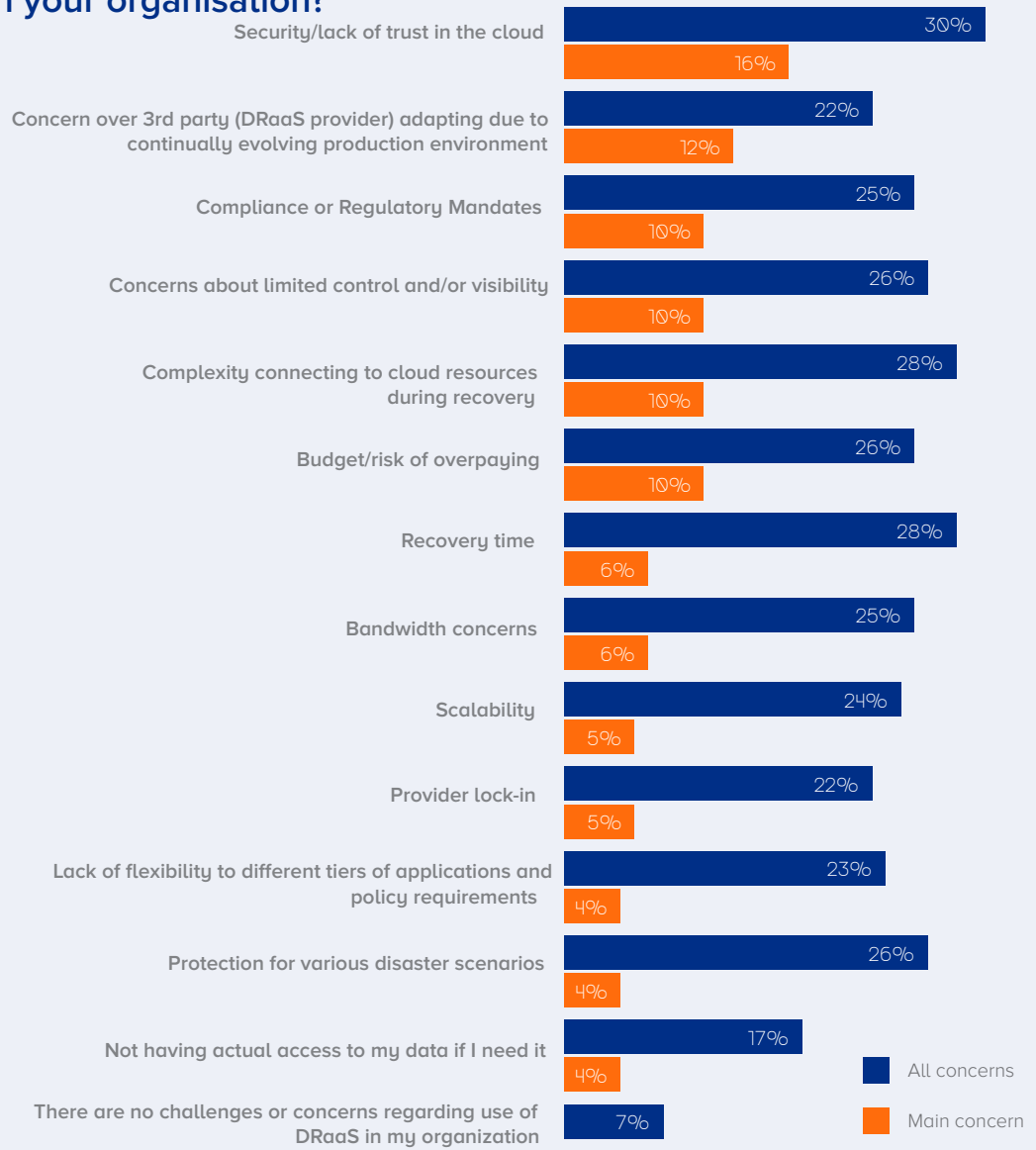
While there are main drivers encouraging DRaaS adoption, there are also concerns inhibiting certain cohorts to adopt DRaaS.

Business leaders surveyed had two top concerns with adopting DRaaS data protection solutions. They were concerns regarding security and lack of trust in the cloud, and questions around trusting 3rd party DRaaS providers to adapt due to continually evolving production environments.

There are four concerns tied for third according to survey respondents. These are concerns about compliance or regulatory mandates, concerns about limited control and/or visibility, complexity connecting to cloud resources during recovery, and concerns over budget and/or overpaying for DRaaS.

MSPs will need to strategically address these specific concerns that are inhibiting end user adoption of cloud-based DRaaS solutions.

What challenges or concerns do you have or have you had regarding use of DRaaS in your organisation?



Veeam Data Protection as a Service Report 2021

MSPs urgently need to remove the complexity from DR

Disaster recovery is a complex process that may require its own infrastructure considerations, cost implications, and practically an entire department's worth of personnel needs on standby.

DRaaS takes many of these out of the equation and reduces the complexity of managing DR.

Successful MSPs will remove the complexity by realizing the following three end user client benefits.

1. Simple, predictable costs

Understanding the storage costs of DR can be difficult due to the variability of requirements. MSPs need to simplify these costs and condense things down to a simple and predicable fee based on client disaster recovery needs.

2. Offloading recovery site and maintenance

Rather than clients having to maintain their own recovery site in parallel with their production environment, MSPs need to make this straightforward. In addition, MSPs need to ensure they are taking over all maintenance so that their clients can focus on their business. Alternatively, MSPs can outsource all maintenance and management tasks to a third-party provider like Probax.

3. Achieving better compliance

Maintaining compliance can be a difficult task during a disaster. MSPs need to ensure their clients are meeting all regulatory and compliance requirements. The more efficient this can be delivered by the MSP, the better.

YOUR MSP + PROBAX + VEEAM = BETTER TOGETHER

Your clients may not be adequately protected unless they have replication-based DRaaS. The next step is to have the right partner in place to help you get your DRaaS offerings off the ground.

Don’t learn the hard way...

The idea that all DRaaS solutions are the same is a common misconception. The truth is, picking the wrong solution and/or provider can have truly catastrophic consequences.

Probax DR is powered by certified, award-winning Veeam solutions, giving you access to some of the best disaster recovery platforms available.

We help you set up off-site data protection, Office 365 backup, and other services all in turnkey, out-of-the-box packages.

Probax CEO Tim Smith sat down with Robin Robins, Founder and CEO at Technology Marketing Toolkit to discuss what MSPs should consider when choosing their data protection and disaster recovery provider.

Simply click below to watch

Probax is the #1 choice for MSPs delivering data protection

Probax is at the forefront of innovation in data protection. We help you solve complex data protection problems that you and your clients face, providing you with an award-winning platform and a single pane of glass view of all the data protection solutions you have deployed at each of your clients' sites.

We also work with you and your specific needs to help you discover new solutions to your current problems, as well as proactively identify data protection and compliance needs as new devices come in.

1 VEEAM PARTNER OF THE YEAR & INNOVATION AWARD WINNER	2 MSP-READY DRAAS FOR VMWARE / HYPER-V	3 ACCESS TO VEEAM CERTIFIED EXPERTS
4 PSA INTEGRATION	5 MULTIPLE AVAILABILITY CENTERS GLOBALLY	6 INDUSTRY LEADING CUSTOMER SERVICE

READY TO EXPERIENCE THE POWER OF PROBAX? TRY FOR FREE!

Discover how your MSP can benefit with Probax and Veeam by experiencing the power of Hive and Scout for a no-obligation and free trial.

Get 10TB of Hot Storage, 10TB of Cold Storage + unlimited SaaS Protection for free for 14 days. You'll be set up in minutes, no payment details required.

>>> Active your free trial now!

ENDNOTES

1. “Global Data Protection Index 2021”, Dell Technologies https://www.dell-technologies.com/asset/enin/products/data-protection/industry-market/global-data-protection-index-key-findings.pdf

2. “Data Protection Report 2021”, Veeam https://www.veeam.com/wp-2021-data-protectiontrends.html

3. “Market Guide for DRaaS 2021”, Gartner https://www.recoverypoint.com/2021-gartner-marketguide- for-draas/

4. Data Protection Report 2021”, Veeam (n2)

5. “Global Disaster Recovery as a Service (DRaaS) Market Share, Size, Trends, Industry Analysis Report, By Solution (Backup & Recovery, Real-time Replication, Data Protection, Professional); By Service Provider; By Deployment Model (Public, Private, Hybrid Cloud); By Vertical; By Regions; Segment Forecast, 2020 – 2027”, Polaris Market Research https://www.polarismarketresearch.com/industry-analysis/disaster-recover-service-market

6. “Data Protection as a Service Report 2021”, Veeam https://go.veeam.com/report-data-protectionas- a-service-2021

Your data is there when you need it.
We're here when you need us.

probax

probax.io
sales@probax.io

USA
(888) 8-PROBAX
434 West 33rd Street, 7th Floor
New York, NY 10013

AUSTRALIA
1300 776 229
Level 33, 250 St Georges Terrace
Perth, Western Australia 6000