N2WS

#1 AWS Backup

An MSP Guide to

Selling Managed Backup for AWS

Overview

Worldwide public cloud revenue is set to rise 17.% to $266.4 billion in 2020, according to research from Gartner, and Statistica research shows that 80% of companies are either planning or already running projects in AWS.

Taking this into account, the public cloud, and AWS in particular, represents a massive opportunity for MSPs. This guide will provide a roadmap for how MSPs can take advantage of this opportunity and successfully move or enhance their business offering in the cloud.

Table of Contents

SECTION 01

Introduction

Written by Nick Cavalancia

Managed service providers (MSPs) like you are always looking for ways to deliver services that are enterprise-caliber, low-cost, highly available, and fast. That's a pretty tall order, considering you need to rely on third-party vendors to actually create said service first, right?

But the explosion of the public cloud provides MSPs – regardless of whether you're already in the backup market or not – with the opportunity to engage in leveraging the cloud as a means to more efficiently offer services requiring storage, software, and infrastructure.

The rise of the public cloud provides those new to the cloud with an end-to-end set of services around Backup- and Disaster Recovery-as-a-Service. And, for those of you who are already doing (or considering) cloud backup (read: using it for storage) should be evolving your thinking to be focused on the bigger picture of cloud-based DR as well.

The public cloud brings enterprise-level service down to the smallest of your customers. It provides a huge opportunity for you and is definitely not a roadblock to new services. While simplifying the implementation, management, maintenance, and backup of a virtual infrastructure, the cloud still requires a level of expertise – the same expertise your customers require of you.

So, it's a natural fit for MSPs like you to begin to transform your business to one that leverages the cloud for nearly every aspect of your service offerings.

The public cloud solves a number of challenges you face as an MSP when looking to offer Backup or DR:

1. It Eliminates Big Investments

Roll the clock back 10 years or so and you'd be needing to purchase and maintain a ton of infrastructure.

2. You're Immediately Scalable

Cloud-based storage and infrastructure is, in essence, infinitely scalable, with more than enough flexibility to address any specific needs your customers may have.

3. Offering is Competitive

The best part of the cloud is the very same services offered to the largest of enterprises is also available to you (read: your customers). So, from day one, a Backup or DR offering is a mix of world-class cloud services and your expertise.

There are also a number of other benefits to you when leveraging cloud services for infrastructure, backup and recovery:

- You can focus your business efforts on keeping your customers running, rather than break/fix of server hardware
- You improve your ability to quickly address your customer's need anytime, anywhere, and from any device because their critical infrastructure is in the cloud
- The backup of data, applications, and systems is tightly integrated, reducing the risk of corruption and, therefore, bad restores
- Offering DR services becomes a natural extension to your business – the backups are already in the cloud; why not recover there and, possibly just stay there?

As you read through this guide and potentially look to build a managed Backup and DR service offering using the public cloud, consider how the cloud can also be used to lower management and maintenance costs, increase business availability, and improve service delivery.

Nick Cavalancia

Technical Evangelist & Bestselling Author

SECTION 02

What is the opportunity for you as an MSP?

Despite some early reservation and concerns around security, it's almost impossible to avoid the growth of public cloud adoption over the past few years. And it's showing no signs of letting up.

Research firm Gartner is forecasting that the worldwide public cloud services market is set to grow 17% in 2020 to $266.4 billion, from $227.8 billion in 2019. This means it's a matter of when, not if, you will have customers who need expert support for cloud environments.

Gartner is also predicting that despite still being in an early adoption phase, Infrastructure as a Service (IaaS) will grow by 24% to $50 billion in 2020. Fueling this growth is strong interest among enterprise IT organizations to increase use of public cloud IaaS, as the major providers continue to address barriers for large-scale public cloud adoption.

It also claims, Platform-as-a-Service (PaaS) will continue to grow but not as strongly as it has in the past few years. Emerging technologies like containers and server-less computing are changing the IT delivery and consumption model and driving much more value for companies adopting a PaaS model.

By 2022, the report predicts that 90% of enterprises purchasing public cloud IaaS will do so using integrated IaaS and PaaS, from the same provider.

How does this split over regions and providers?

Analysis from Synergy Research found that Amazon Web Services (AWS) leads the way ahead of Microsoft and Google – apart from in the Asia Pacific region where Alibaba is in second place.

Research by Statistica also points to AWS continued dominance of the public cloud market, stating that 80% of enterprises are both running apps on or experimenting with Amazon Web Services (AWS) as their preferred cloud platform.

Azure follows behind with 67%, with Google's Cloud platform following even further behind with 18% of enterprises using it for applications today, and 23% evaluating the platform for future use.

Cloud-based BDR on the rise

Crucially, this massive increase in public cloud adoption, alongside the growing need to manage vast data sets, is also driving take-up of cloud-based backup and disaster recovery (BDR). On top of this, improvements in BDR technologies means functionality such as simple management and monitoring, real-time backup and recovery, simple integration of cloud backup with other applications in the enterprise and data de-duplication are increasingly available to organisations and managed service providers (MSPs) alike.

A survey by Market Research Future points to "remarkable" growth in the cloud backup market by 2023 with it set to reach a value of $5.66 billion, outstripping previous growth records with a compound annual growth rate (CAGR) of 21.4%.

What does this mean for you?

For the past few years the IT industry has been encouraging companies to move to the cloud because it will make life easier, providing them with scalable resources as well as removing the need to finance and maintain expensive on-premises data centres.

While companies are at last hearing this message, it is sparking a misplaced fear for many MSPs that once these companies have completed their migration to the cloud, they will dispense with their service providers as they no longer see a role for them.

The reality is that moving to the cloud is far from a one-off migration job for service providers, as many of the issues companies face with on-premises solutions still apply when they are in the cloud. For example, intrusion detection, security layers (disaster recovery being one of those security layers) and the ability to monitor and control what's happening to their data are still critical areas where you can provide support and expertise. We'll look in more depth at some of the recurring threats in the next section.

In fact, if you look at the areas where money is currently being invested in public cloud, they are all areas that are existing strongholds of the MSP. Spiceworks examined cloud/hosted service budgets, and found that online backup/recovery (15%) topped the spending list include, followed by email hosting (11%), and web hosting (9%).

Data protection is a shared responsibility in the cloud

On top of this, AWS' own shared responsibility model highlights the continued opportunities for you to provide holistic management and protection of your client's data through BDR.

It states that while AWS will ensure the integrity of the infrastructure, it's the responsibility of the company itself to understand the threats to their data and ensure they have the right defences in place to fully protect it. In short, this means that companies can't just move their data to the cloud and think that's the end of it, they will still need to have someone managing and overseeing their data and their environment.

To further reinforce the BDR opportunity for MSPs, AWS released a tool called AWS Backup. While this offers the ability to automate snapshots within the platform – the logical first step for any robust data protection strategy – it's currently a very rudimentary solution. Organisations need a fuller service that ensures data in AWS is safe and easily recoverable from any scenario. This is where you, the MSP, can step in.

Sources:

Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent in 2019

AWS leads across all geographies in public cloud – with Alibaba second in APAC

Current and planned usage of public cloud platform services running applications worldwide in 2018

Global Cloud Backup Market Research Report- Forecast 2023

The 2019 State of IT

SECTION 03

Why managed backup is essential in AWS

As we mentioned above, the IT services industry has spent a long time pushing the message about moving to the cloud, and until now that has been primarily focused on delivering cloud services and not cloud infrastructure or cloud databases.

The good news is that this change in focus means moving to the cloud is not a "migrate once and walk away" scenario. There's a huge amount of opportunity for you to continue to provide services.

Having a team of highly trained specialists means you can not only monitor and manage this environment for your customers, but also provide them with the ability to actually benefit from being in the cloud. By taking care of the infrastructure, you're enabling them to fully utilise the functionality.

Recovery in minutes… when you need it

The message for backup has been that the cloud forms a key part of a hybrid backup solution, which enables companies to not only easily store their backups offsite but also to move backups quickly and easily between different sites.

With AWS now offering the opportunity for companies to move their entire backup function to a public cloud solution, you need to reposition the way you sell your backup services.

Where traditionally many MSPs have used the cloud as the perfect way to move backups off site as part of a "grandfather, father, son" policy, now you are able to store data in a different account or region within the pubic cloud environment, meaning that if necessary you can recover in a matter of minutes or even seconds.

For example, if your customer has a Wordpress website hosted in AWS you can use managed backup to recover a customer's infrastructure and data to another secure account within seconds in the event of an attack.

In this situation, your customers are not paying for the technology behind this, they are paying for the fact that you are providing them with a business continuity solution that gives them an uptime as close to 100% as possible.

Imran Sadiq
AWS APN Ambassador

"Not having a backup is something you cannot recover from. Cloud services are highly redundant but at the end of the day, your data is still sitting on a physical hard drive which like everything else physical can fail at anytime.

Customers often do not want to know if and how their data is backed up. They only want an assurance that their business will keep going regardless of any hardware failure - regardless if it is in the Cloud or on-premise. Having a managed backup solution with redundant checks provides that assurance."

The public cloud is not risk free

Ensuring the safety of your customers' data is paramount. And it's important to make customers aware that the cloud is not completely fail-safe and many of the problems that exist on-premises still apply. This is where your skill set adds value for customers,

Here are nine key stats that could make your customers think again if they believe that they have no need for an MSP when they are in the cloud.

1. Only **7%** of businesses have good visibility of all critical data; **58%** say they only have slight control. (ForcePoint)
2. **24%** of organizations have hosts missing high-severity patches in public cloud. (RedLock)
3. **80%** of security breaches involve privileged credentials. (Forrester)
4. **49%** of databases are not encrypted. (RedLock)
5. Through 2022, at least **95%** of cloud security failures are predicted to be the customer's fault. (Gartner)
6. In 2017/2018, an average of **51%** of organisations publicly exposed at least one cloud storage service. (RedLock)
7. **25%** of organisations have cryptojacking activity within their environments. (RedLock)
8. **84%** of organisations say traditional security solutions don't work in cloud
9. Public cloud account compromises are fueling new attack vectors, causing **27%** of organisations to have users whose accounts are potentially compromised. (RedLock)

4 ways the cloud is still vulnerable

While AWS may offer security at a level most companies wouldn't be able to afford, there are still very real risks that your customer needs to understand, and that you as an MSP can help them manage:

1. People are their weakest link

Human error is far and away the most common threat to companies' data. For example, it's easy to accidentally terminate an instance. While it is possible to set a protection in AWS that warns the user when they're about to delete an instance, if a company manages thousands of instances things can get missed and instances terminated by mistake.

If this does happen, companies have to be able to recover, which they may not be able to do if they are just managing their backups natively with AWS.

2. On-premises threats still exist in the cloud

Even though your customer's data is in the cloud it's still subject to the same threats as in the on-premises world. While AWS takes every reasonable step to put protections in place, cloud servers are still vulnerable to attack from ransomware and malware.

Not to mention the threat from natural disasters such as floods, earthquakes or fires – while rare, the likelihood of natural disasters impacting a business can vary depending on where the company is based.

3. Downtime does happen

While AWS claims it makes "commercially reasonable efforts" to guarantee at least 99.99% uptime, outages do happen. In the past year we have seen entire AWS regions being down for around five hours. If a company's whole production environment is running all instances in this region, they're left praying for it to come back online. With a dedicated team managing this environment for them and the ability to switch between regions, this issue is mitigated.

4. Even a cloud account can be compromised

As with any type of online account – even with different levels of protection in place – companies are still vulnerable to compromise; passwords can be stolen and individual admins can be targeted by sophisticated social engineering.

The reality is that companies can go out of business if their AWS account is compromised. Even Amazon itself recommends the use of multiple accounts to ensure users' resources are stored in multiple places in case of compromise.

All these are areas where you can add value. By building your own disaster recovery as a service (DRaaS) and Backup as a Service (BaaS) provision around N2WS Backup & Recovery you can confidently advise and provide your customers with the best-in-class solution as the cornerstone of your business offering.

This alongside the fact that you are armed with a team of highly trained technicians, means you are capable of solving anything your customer might encounter.

SECTION 04

Defining your offering

Once you've established where the opportunities exist in AWS, you need to set about defining exactly how you're going to sell your services to potential customers.

When we speak to MSPs who are already using N2WS Backup & Recovery – or even just starting to use it – their primary focus is on building out tiered service levels. Normally these will be split out over three tiers (so, entry level, standard and premium or bronze, silver and gold), with each tier adding different services to create more value for the customer.

Creating multi-tiered security packages

It may seem obvious, but you need to remember that you can't add any additional services if you give everything to your customers from day one as part of your basic package.

So instead, start light and build from there. For example, your entry-level option could offer your customers a basic backup and recovery service, say recovery within four hours of a disaster. On top of this you could offer additional security services.

At each level you can add additional services, so eventually your premium level would include everything that the lower tiers offer, plus a whole raft of additional features such as antivirus, a full security solution, intrusion detection etc.

Backup is an essential part of all MSP services, so it should be a given in all levels of your bundles. The powerful thing about cloud-based backup is that you can differentiate your backup services by the speed at which you recover.

Moving the conversation to continuity

So, for example, you could offer recovery within one hour as part of your top-level offering. What's dictating that change in time for the recovery isn't the product itself, it's the Service Level Agreement (SLA) that you set up with your customer.

The actual service itself hasn't changed, how quickly you respond to a ticket or respond to servers going down will dictate the cost of the package. And that should be based on the impact and costs to the customer's business of down time. This way the discussion becomes less about backup and more about providing a business continuity service.

There are other key features that can be added as part of your backup package such as layering in things like cross-region recovery, cross account recovery, infrastructure recovery, reporting, auditing, and data management from a GDPR perspective to help with compliance.

Not so hidden benefits

If you are already using N2WS Backup & Recovery, these are all core functions that are all available to you within your license fee.

Adding them in for the customer doesn't change the cost to you, but they can be used to add real value to the customer and you can generate more recurring revenue. The message here for you as the MSP is: you thought you could just do backup but actually there are different levels of service you can offer, and it's up to you as a business how you package and offer these services to your customers.

By using packages like this, you're not saying to your customers that backup and disaster recovery costs X, security costs Y and data management costs Z. You're saying "these are our services, which cost x amount per month as part of a 12-month contract, you can choose the level of service that best suits your own business needs."

You know how much the monthly services cost you and you can just add on your business overheads. This makes the whole process easier to cost out and potentially more profitable for you. In addition, by taking advantage of the N2WS partner program, you can enhance your existing service and increase the number of profit-making opportunities.

Peter Jackson
Cloud Engineer - Deloitte

We're using the backup solution for almost anything that could go wrong and something is always going to go wrong. Recently, a developer went into one of our instances, a linux instance and decided to pretty much wipe everything out with a stupid command but we were able to bring everything back. The backup systems we got there takes away all the problems we have.

Saving time and money

Ultimately, in a competitive market place, you need to not just offer your expertise and services, you need to offer real tangible benefits for the customer.

N2WS Backup & Recovery allows you to go into a customer and look at what they're doing: how they are backing up data; how frequently they actually need to backup data; how much data change there is between each backup; and the cost implication of all that data being stored in the EBS snapshots in AWS (which is currently how you would be storing snapshots in AWS today).

With N2WS Backup & Recovery, you can then look at the value that they can bring by optimising their backup processes and also moving that data into cheaper forms of storage. Currently that is S3 buckets. By using this you will be able to save your customers as much as 60% on their AWS storage costs, for data stored for longer terms.

You also have the ability to help your customers manage their infrastructure costs with automated server scheduling for non-critical instances, bringing even greater cost-savings.

This means that as an MSP you're not only improving your customers IT, helping admins save time, you're also helping the finance decision maker by saving money on their AWS costs.

How does N2WS S3 storage work?

At $0.05 per gigabyte of stored data per month, EBS snapshots may seem inexpensive, however if you have hundreds (or even thousands) of instances and a long backup retention policy the costs quickly start to mount.

In this case N2WS Backup & Recovery offers a powerful way to optimize costs and improve data lifecycle management by archiving snapshots to Amazon S3 and Glacier.

You still create a snapshot but N2WS enables you to copy this to S3 for archiving. It does this by saving your incremental snapshots in a pre-configured repository on Amazon S3 and Glacier.

This allows you to have a short retention period on your snapshots, while maintaining S3 copies for far longer – for months or even years, as required. This costs you far less than keeping monthly backups as a snapshot.

SECTION 05

How to sell your services and identify your target market

Before you actually go to market with any packages or "products", you need to decide exactly which segment of the market you want to target with your services.

Are you going to be targeting SMBs, enterprises, or both? While they may have a lot of similarities, there are some major differences that you need to consider carefully, as they may heavily influence your decision and your ability to make a healthy profit margin.

Understanding what the pain points are for both will be your starting point.

Who are you selling to?

Also, beyond simply looking at the types of business you're targeting you need to look at the types of buyer, and how that will change your approach.

Basically, there are two distinct buyer tracks: the business buyer (who is more focused on the business impact of your services); and the technical buyer (who will be more inclined to focus on the technology side). In general you're more likely to be selling to a business buyer when you're targeting enterprise customers and the technical buyer for SMBs. Although in smaller businesses you may get a cross over where you will likely be speaking directly with the owner who is also in charge of the budget.

Also, remember, with enterprise clients, you are likely to have many more people involved in the procurement process – so this isn't always cut and dried.

This means you need to think about what value you are bringing to both sides – the business and technical side – the challenges you may face are the technical people, certainly at enterprise level, thinking they have a team in place so why do they need to outsource anything.

Whereas a business focused buyer is more likely to think if an MSP costs X, but they can save Y, they have already achieve a net zero from a cost perspective plus they get the added benefit of additional technical experience.

So what are the key differences between the two business sectors?

Imran Sadiq
AWS APN Ambassador

"As an MSP, you primarily need to explain to customers where and how their data is stored in the Cloud. Get rid of may misconceptions that if they are in the Cloud, they don't need to backup their systems.

Secondly, remind them the cost of being down. Let them quantify how much it costs the business if their systems are down per hour/per minute."

The SMB

- ### SMBs need more direct support

  Smaller businesses will need a lot of handholding and your technical experience will be vital. In many ways this makes managed services a more obvious sell into the SMB sector.

- ### Regulation is still important

  SMBs will still care about many of the same issues: having quick recovery; knowing where their data is being stored and managed; and being compliant with the various data regulations (although at a different level to the enterprise, but we will touch on that in the next section).

- ### Your value lies in your experience and your team

  When targeting the SMB, the biggest thing you can bring to the table is a combination of your experience, time and your team of engineers. The SMB is just not going to have this. By nature of having more technicians, you will have a far wider breadth of experience across an array of different solutions, especially when it comes to managing AWS environments.

  Your message to the SMB is, “We're going to take away the pain points of managing your AWS environment, which is going to allow you to fully exploit the power of having a scalable solution and at the same time to focus on your business”.

- ### They just want things to work

  SMBs do not want to be focussing on infrastructure, they don’t want to be focused on what platform to host their website on, what security to use, what backup and disaster recovery solution to deploy or how they are we going to manage their data. They just want these things to work.

The Enterprise

- ### Take a consultative approach

  With an enterprise, you still bring the same experience, but the difference is an enterprise is more likely to have a larger team of IT admins, all with specific tasks. This means they will be more interested in your consultancy skills. This may make the enterprise a more profitable sector than SMBs as they require less direct hand-holding and so are not as much drain on time and resources.

- **Compliance means more focus on security, BDR and data management**

  The focus on security, backup and disaster recovery, data management, and infrastructure management in the cloud are heightened in the enterprise space as compliance is much more of a concern.

  If they get hit by a fine for non-compliance the financial risk is significantly higher than for an SMB, a look at what happened to Marriott International last year (2018) clearly demonstrates this.

  So, failure to be compliant across the board becomes a significant cost for the enterprise – and thanks to GDPR this is now formalised. Your key message here is that paying a modest monthly fee for your service to ensure compliance is a very worthwhile investment compared with potentially paying a massive fine for non-compliance that could destabilise the business.

- **Everything boils down to cost**

  Cost becomes a big issue for the enterprise, because there is a misconception that when you move to the cloud your costs are going to go down. The reality is that the direct recurring costs probably actually go up, because you have that always-on ability alongside the best technology possible.

  If you can go in and say, "hey, we can save you 20 to 30% on your AWS storage bill with our tool set and our expertise", this is a big deal.

Getting your messaging right

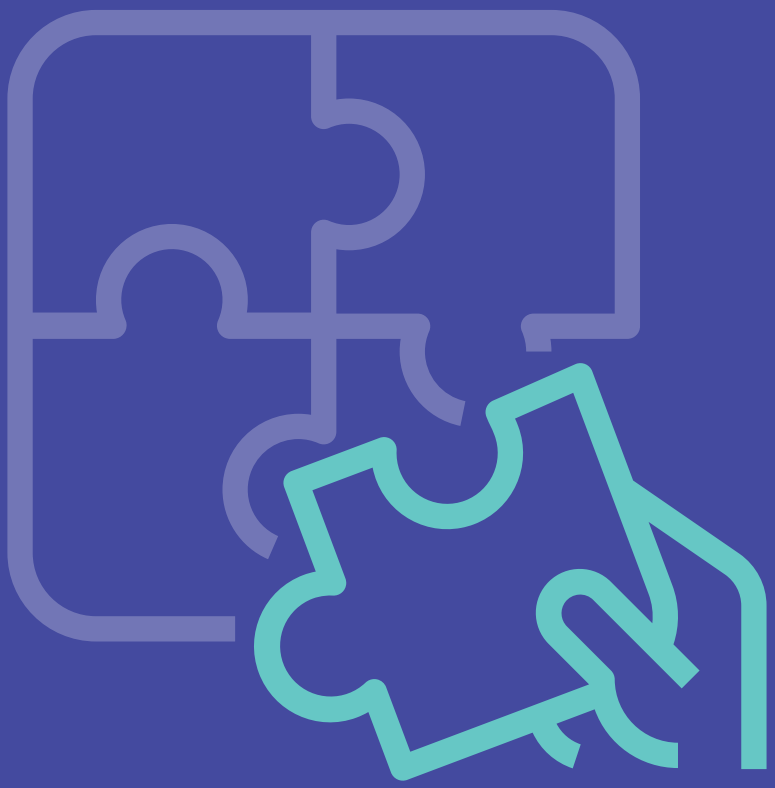
Once you understand who your audience is and what their pain points are you can talk to them in the right way.

Getting your message right at the start prevents you from sending out confusing signals to the marketplace about who you are and what you are selling. Your messaging should clearly set out why and how you're unique and exactly what your value proposition is.

Focus on how your customer can benefit, not what you can do. Most buyers don't really care about the technology, they do, however, care about how it will help their businesses.

SECTION 06

The N2WS Solution



In this section we'll look at how the N2WS Backup & Recovery can form the cornerstone of your offering to customers within AWS, and the benefits it offers.

Today, you'd be hard pushed to find an MSP that doesn't already offer some form of backup and disaster recovery to their on-premises customers. Just because you've moved to the cloud, that shouldn't change – Backup as a Service (BaaS) should be one of the key components of your offering.

How do we help you do that?

Ken Weinreich
Cloud Manager - 2ndWatch

We've been one of the earliest partners with Veeam and N2WS, we've been using CPM for quite a long time. 2ndwatch is about 9 years old, we've been working in AWS from very beginning, and as soon as N2WS and CPM came around as a product we saw the need for our customers to have a reliable backup solution and we've been using them ever since. My team is personally responsible for number of our very large customers, I'm talking about hundreds and thousands of snapshots everyday, and it's just reliable, it gets the job done.

A growth plan tailored to your business

We want to help our MSP partners grow, because when you grow, we grow. The core of our offering is built around creating a plan that grows with your business.

Our growth plan will offer you a simple invoice that's based around the usage that you and your customers have. What you use is what you pay for. Here are two examples of what that means in practice:

1. If you decide that you're going to target customers that are server-less only, we're not going to charge you for server-based backup and disaster recovery. Your pricing is going to be fully based around those server-less environments. So you're going to pay on a per-gigabyte pricing model for unattached data volumes in AWS.

2. Alternatively, if you're only going to focus on customers who have SAP environments, you're going to have a per instance charge on a monthly basis.

This way, you have a plan that's tailored to the target market you want to go after. If you want to structure your business around AWS, we can create a plan to help you do that – from targeting start-ups with lots of accounts but low incidence number, to enterprises with large multi-tenancy environments.

On top of this, the more your business grows and the more customers you bring on board, the cost per instance or per gigabyte comes down. Not only do you benefit from the additional revenue of more customers, but also your profitability for each customer improves.

So there's an incentive to go and acquire new customers to continue to boost your own profitability.

Key features of N2WS

N2WS Backup & Recovery puts you in complete control, because the software can run either in your environment or in your customer's environment.

It's not SaaS based, and sits within a walled off area that you've created in the environment you are running it in. So you have complete control, not just of the data but also of the solution running the data, which means it has all the benefits of being in the cloud without any of the risk.

Also, because you can white label the solution as your own, you can build your service around that and then you're not selling a specific product you're selling your MSP service.

The key benefits N2WS Backup & Recovery include:

- **Multi-tenancy with a single pane of glass**

  You can support multiple AWS accounts so you can on-board and manage as many customers as you want in one single backup application.

- **Low RTO**

  Recover anything in seconds – from a single file to your entire AWS environment.

- **Disaster recovery across regions and accounts**

  You can quickly restore workloads to another region/account in case of disaster (including VPC).

- **Resource Control**

  N2WS Backup & Recovery allows you to turn instances on/off on demand, saving customers money on infrastructure costs.

- **Data Lifecycle Management**

  Having the ability to backup to Amazon S3 and Glacier can reduce your customers' AWS storage costs and help them choose the most appropriate long-term storage tier.

- **Reporting**

  Show granular details to your customers with an efficient reporting suite.

- **API integration**

  The N2WS RESTful or CLI APIs can be used to integrate with any application that support APIs.

- **Compliant solution**

  Helping you to meet regulatory compliance requirements via DR plans, reporting, auditing, logs and much more.

- **Recovery Orchestration**

  Bring customers' workloads back to production in seconds. Orchestrate recovery for entire applications and services.

Manik Anand

Cloud Architect - Tata Consultancy Services

I'm a cloud architect and we migrate servers to AWS. The Backup solution is straightforward and it helps us keep up to date backups. We tend to migrate servers, they don't turn out fine and the backup solution helps us bring back the servers that we have lost for one reason or another. We usually install it on the production servers but we have recently started doing it for the dev boxes.

There was this instance where the customer asked us at some point to roll back the server and decommission the one in AWS. As it turned out, someone had already removed the server from VMWare and we had lost the AWS server as well. So that's where N2WS really came in. We were able to bring back the server in AWS, we took an image and spinned it on to VMWare. So it's pretty straight forward, it's build for the cloud, for native cloud applications and it works very smoothly.

N2WS Backup & Recovery

#1 AWS Backup

Built for scale. Built for simplicity. Built for AWS.

As more companies move to the public cloud, they need a way to ensure their critical data is always available. The first step is finding a solution that provides easy, automated backups and a giant instant recovery button to protect your data from any outage any time. The next step, after automation, is optimization —making sure your environment is set up for cost-effectiveness (and compliance). We help you on both counts.

Top Rated Backup & Recovery solution in AWS Marketplace

Automated Backup + Instant Recovery = No Downtime + No Worries

- Automate backups and get 1-click recovery for Amazon EC2 instances and EBS volumes
- Recover only what you need in 30 seconds (from individual files to full volumes or instances)
- Perform Disaster Recovery to any AWS region or account

Your Database Protection Plan: Always Available, Application-Consistent

- Capture the most complete database picture with application-consistent backups for Amazon RDS databases engines: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle, MSQL
- Enjoy complete support for NoSQL databases: Cassandra, DynamoDB, Mongo DB

Savvy Data Lifecycle Management to Save Your AWS (and Your Budget)

- Save up to 60% on long-term retention costs by decoupling and transferring your EBS snapshots to the N2WS S3 repository, with the ability to recover to any region or account
- Start, stop and hibernate groups of Amazon EC2 or Amazon RDS instances and save on computing costs with N2WS Resource Control

About N2WS

N2WS Backup & Recovery is a cloud-native data protection solution built specifically for the AWS platform. Our solution gives you the flexibility and control to move data around your AWS environment, providing backup and disaster recovery functionality across regions and accounts. N2WS is an independent worker-owned IT company.

Become a Partner ›

AUSTRALIA
+61 2 8294 9490

FRANCE
+33 1 86 26 52 56

GERMANY
+49 89 4120 7337

MALAYSIA
+60 1 6299 4494

SPAIN
+34 91 901 7644

UK
+44 1315 601551

USA
+1 888 426 4329

info@n2ws.com
www.n2ws.com
www.n2ws.com/partners