Secure Backup & Recovery

by People Who Study Cyber Criminals.

REQUEST A TECHNICAL WALK-THRU

SOLUTION OVERVIEW

asigra

Secure Recovery is Everything™

Table of Contents

Solution Overview

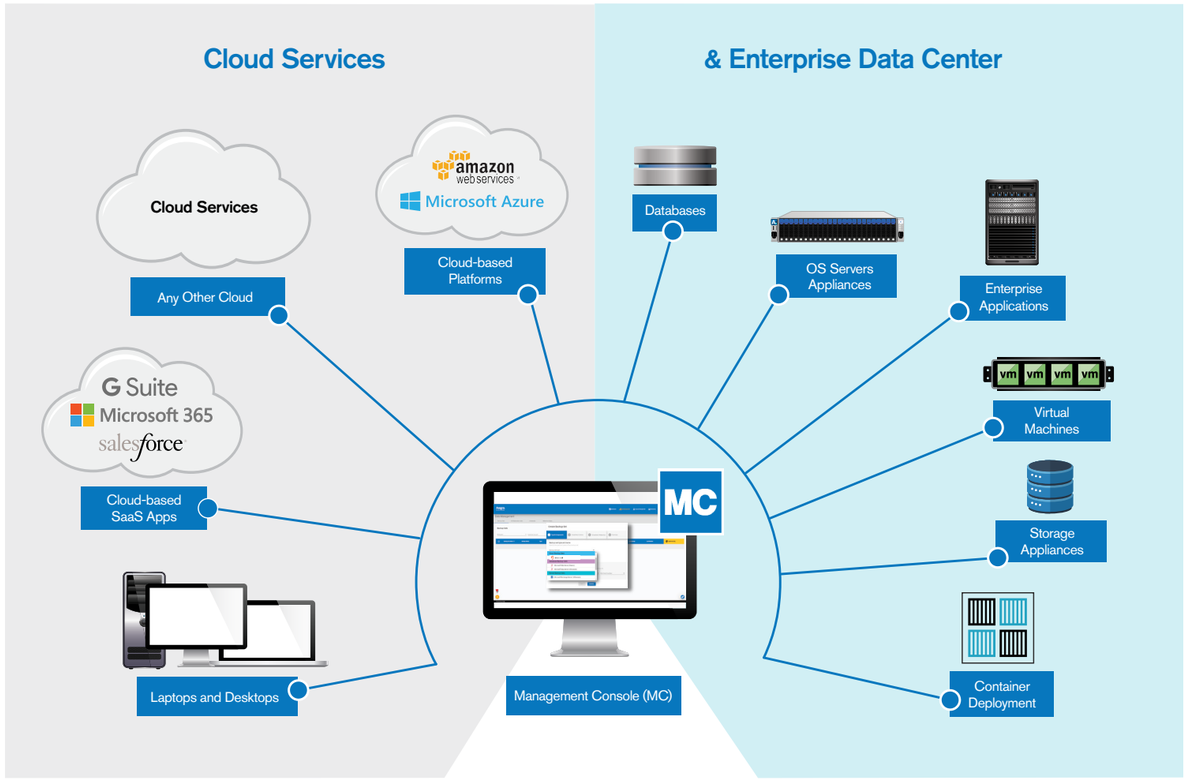
Asigra Cloud Backup is the most secure backup platform on the market today, making it extremely difficult for bad actors to attack or delete your data, while our intelligent software and deployment flexibility address the diverse backup needs of a real-world, working Managed Service Provider.

For Users – it offers a simple low-touch, secure and fully compliant backup experience – ready for disaster recovery and never worry about exposure. It protects all enterprise data resources, whether on-premise or in the cloud.

For Backup Admins – it offers so much more than file backup. It's VM backup, container backup, physical host backup, cyber security, compliance management, simplified data management and accessibility, cloud SaaS protection and the choice between Incremental Forever and Changed Block tracking.

For MSPs – it offers a cost effective, low-touch and re-source efficient solution to operate and support both modern and legacy infrastructure and applications, deployed on-premise or in the cloud.

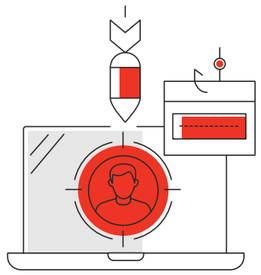
As a result, Asigra can be ubiquitously deployed across all business systems and applications to support all data pro-tection and disaster recovery use-cases. And for MSPs that are not ready to go all in with a single solution from day one, Asigra offers a gradual migration path and the ability to leverage the backup infrastructure of Asigra's international partner network.



Rethinking Secure Backup & Recovery

The data you manage has value to you and your customers.
That's why you're a target. But ask yourself, is my backup **protected** or **secured**?

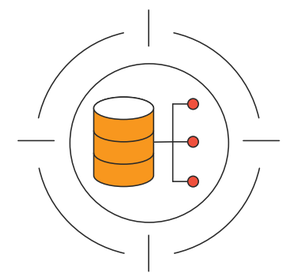
Many people use the terms **Protection** and **Secured** interchangeably, but while they share some similarities, in the digital world Data Protection refers to the mechanism of making copies of your data to restore in the event of loss or corruption, aka Standard Backup. Whereas **Secured Data** comprises the additional mechanism of keeping your backup data safe from ransomware, unauthorized access and deletion. We believe, you need both!



Assume your customers are already in a hacker's sights

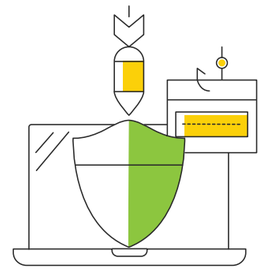
Because they are. Somewhere on the dark web or from a competitor's back office, someone's looking for a way in.

You can do nothing for your customers and hope the cyberthieves don't find a weak spot, or you can plug the holes before they're breached.



#1 and #2 Target

With advanced ransomware the primary target is now the Operating System and Backups, since backup data is the last line of defense when responding to these attacks. Your data might be protected, but is it secured?



Give cybercriminals every reason to move on

A constant among cyber thieves is their short attention span. Make your customers difficult to infiltrate and the hackers will find someone new. That's what we can do for you.

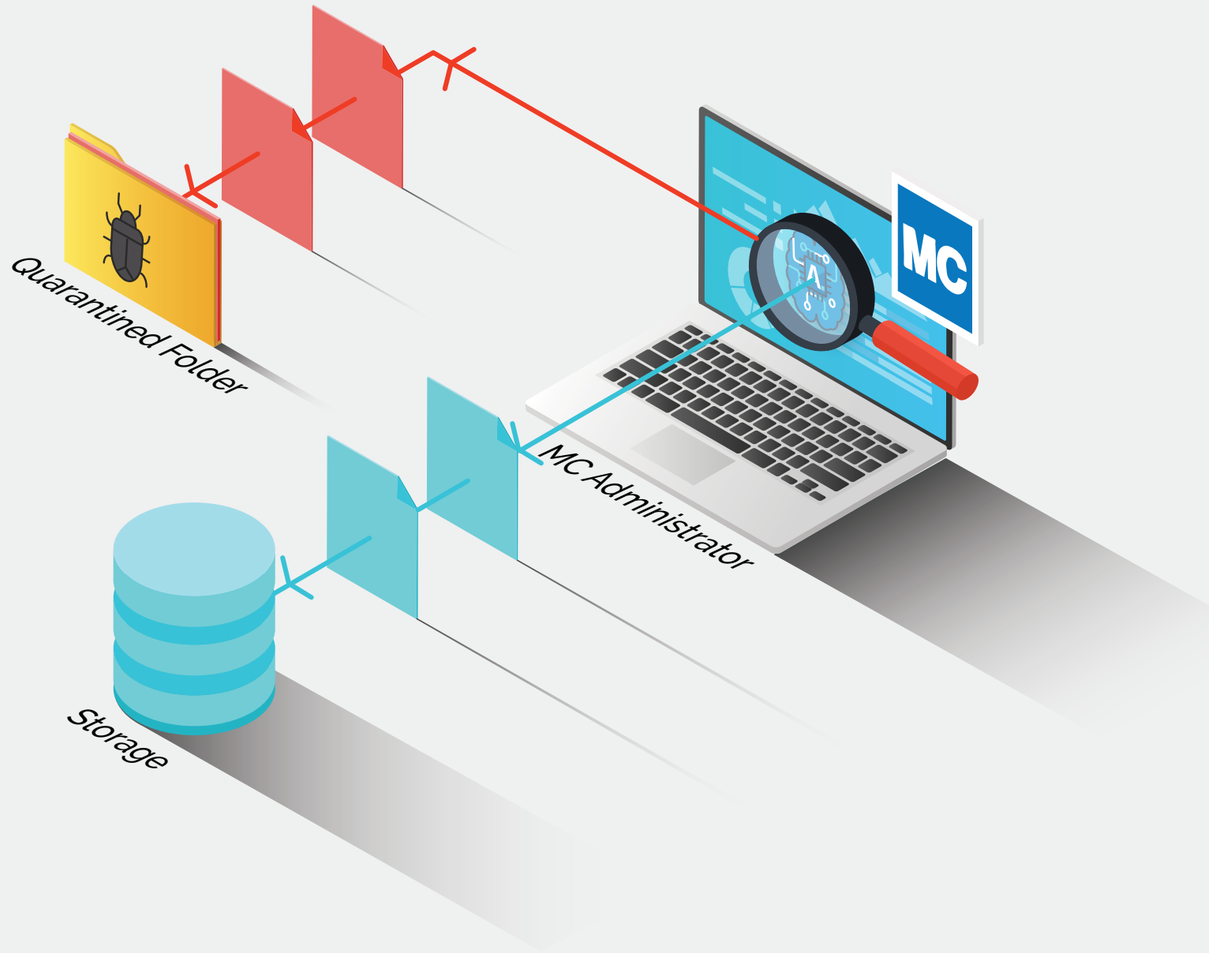
How We Protect You and Your Customers

Discover the Power of Asigra's Hybrid Data Protection

Traditional MSP backup tools are simply not designed to meet the cyberthreats posed by today's always evolving attack vector. Yes, modern backup tools protect the data of your customers, but ask yourself…does it secure it? As an MSP you are just as big a target as your customers, if not bigger. Gaining access to an MSPs inner sanctum grants Cybercriminals a VIP-Pass to cause maximum damage and increased potential for numerous payouts.

Asigra's Secure Backup changes the game by integrating data protection with cybersecurity. This hybrid solution makes security the focus point of your backup solution, keeping your client's data protected and your costs down. With our AI powered anti-malware protection and comprehensive Deep-MFA (multifactor authentication), Asigra Secure Backup intelligently combats advanced cyberthreats by inspecting, quarantining or removing suspect packages during the backup and restore process. Service providers can rest assured that the data they protect is secured from malicious encryption, deletions or loss from human error. Asigra Secure Backup doesn't just protect data, we protect your reputation as a service provider while you generate new revenue and decrease churn.

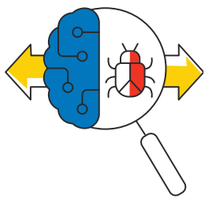
Our software protects your backup data with the highest levels of security and compliance



How We Protect Data

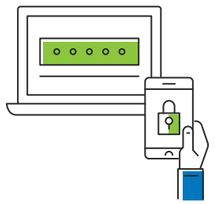
Feel secure. All the time.

Does your current backup and recovery solution reinforce the most popular entry points for cyber-criminals so your customers can wake up every morning knowing they won't go to bed that evening in full crisis mode?



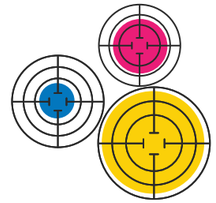
Bi-Directional Malware Detection

Real-time AI-Powered malware prevention scans backups and restores, isolating malicious code and alerts administrators of infections.



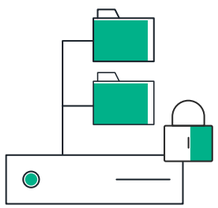
Deep MFA

Built-in, passwordless Step-up Multi-Factor Authentication protecting both users and backup tasks vulnerable to attacks.



Variable Repository Naming

Avoid your backups being a sitting duck. Simply creating a moving target gives you the upper-hand. If it can't find them, it can't delete them, nor does it know what storage volumes, file systems, or buckets to delete.



Admin Only Access

Prevent unauthorized users from deleting backup data from the DS-System (primary backup repository).

Enable Soft-Deletes

Instead of actually deleting the record, soft-delete moves the data to a hidden folder for a set period of time pre-determined by the admin, deceiving the malware into thinking it has eliminated the backups.

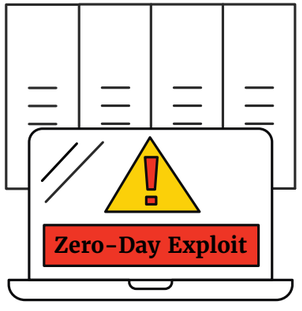
NIST FIPS 140-2 Certification

AES 256-bit in-flight and at-rest data encryption protects your data to the highest level of security and compliance.

Attack-Loop™ Ransomware Protection

Reinforcement for the back door.

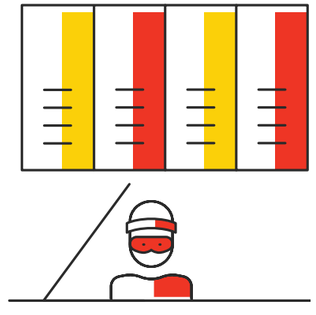
Modern cyber security puts a lot of emphasis on keeping hackers from breaching your customers' environments head on. The industrious criminal found a workaround.



Zero-Day Exploit Protection

A zero-day exploit is a cyber attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator.

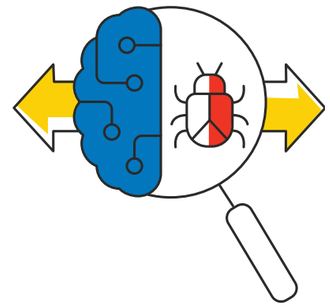
Our signature-free technology doesn't rely on a database of known malware to identify unauthorized code. It knows your code and so can spot and identify anything that seems off.



Today, hackers get in through the back door.

They implant their virus in your customers' backup repository, which slowly and stealthily infects their files until no clean data exists in the entire backup environment. Then they strike with a silly diversion, pushing you to do a full or partial back up, which pulls their hidden viral code into your customers' live environment. Then they hit you or your client again and again, until they're drained of funds by ransom after ransom.

And then the hacker leaves and moves on to the next target.



Attack-loop™ bi-directional ransomware protection is like a back-door bouncer.

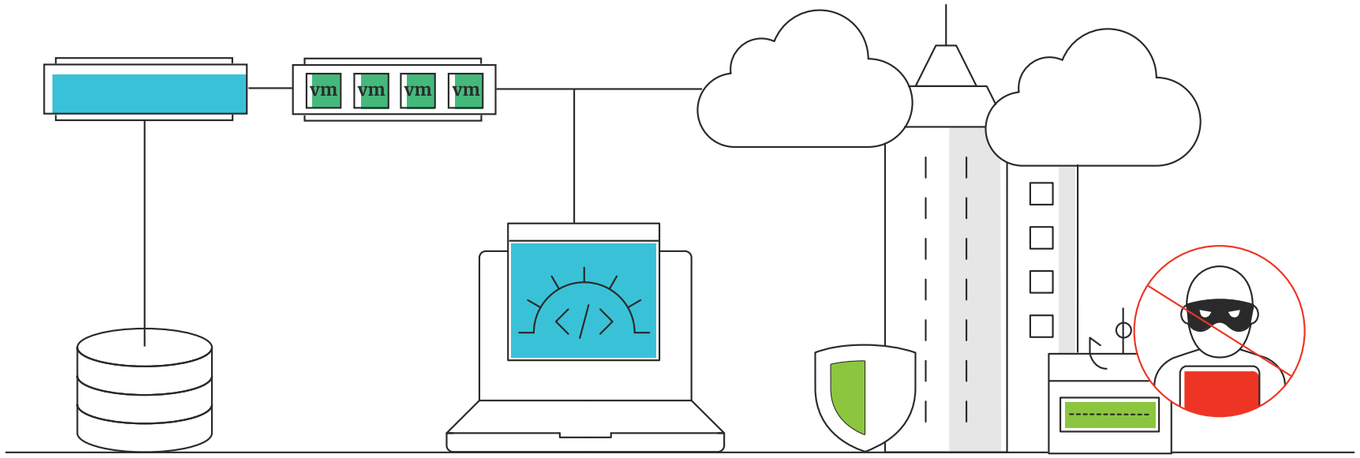
It keeps unauthorized code from penetrating your customers' backup repository and scrubs their existing backup for malware before they (or you) have a chance to recover it back into their live data sets.

Your customer can store an unlimited version of their backed-up files, take advantage of short RTOs and RPOs, and easily roll back to unencrypted versions if an attack does occur. And you both can be one firm and confident step ahead of the hackers.

Agentless Architecture

Make points of attack disappear.

Reduce points of failure through a lightweight, agentless backup solution. Asigra's agentless architecture reduces resource consumption, simplifies installation and ongoing operations by eliminating the downtime and disruption of deploying and maintaining agents.



Close ports. Secure ships.

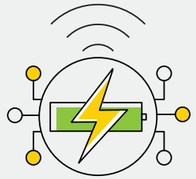
On an agent-based architecture, all machines connected to an open port on your customers' networks are vulnerable to a breach. Depending on how many employees a customer has and how many you or your customer don't trust to see a phish attempt, that could be a problem.

Our solution puts the software right on the connected machines. This cuts out vulnerable-to-attack long-running processes on the target host.

Other benefits of agentless architecture

No process to manage

Devices and machines across your customers' networks are connected to the platform using the standard protocols on those devices. All they'll have to do is decide how they want their data backed up and recovered.



Less pinging. Less power.

Communication is established only when a backup needs to be performed. This differs from agent-based platforms that continuously ping servers to request tasks. Depending on your customer's size, this could slow core function and increase downtime.

Lower costs

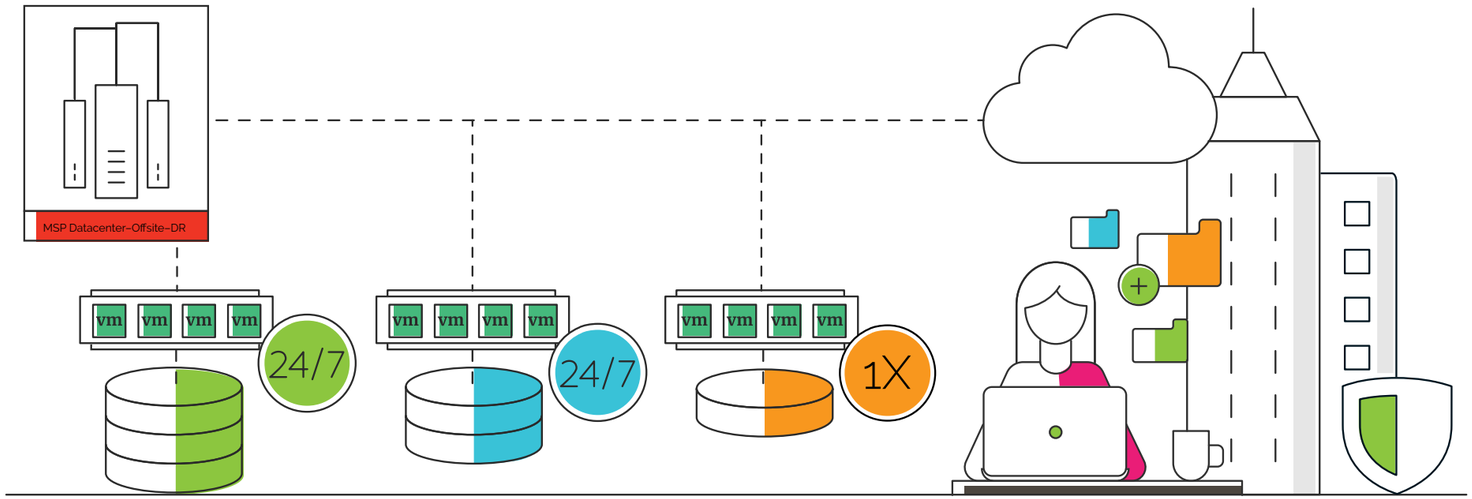
No modifications are required for your current on-prem or cloud environments. We talk directly to the underlying platform through APIs to control security. This will save you or your customer from spending money on tech and losing time modifying.

Customizable Storage

Rules set. Goals met.

We're a single data protection solution for an entire enterprise, but we don't force "one-size-fits-all" protection.

With Asigra, you or your customer can easily establish granular rules to achieve individual data protection objectives.



Uncompromising Security

Some virtual machines may only need to be backed up once while others may require daily backups. Other VMs running mission critical apps may need to be replicated hourly to a warm standby for fast failover and disaster recovery.

You can set protocols as your customer needs them, and you can change them at will so the protection you offer customers is always on point.

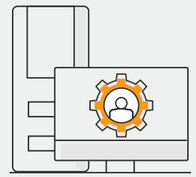
Other benefits of customizable storage

Easier to take on sensitive projects

When you can set your customers' data storage rules as you see fit, you can adjust as needed as new opportunities present themselves.

Respond to threats before they threaten

If you hear of a situation brewing in your region or industry, you can preemptively set new protection protocols for your customers.



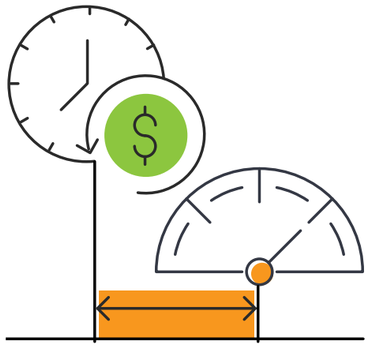
Support individuals differently

If some people in your customers' offices are given more access to sensitive information than others, you can adjust their backup protocols to protect what they have.

Feel confident.

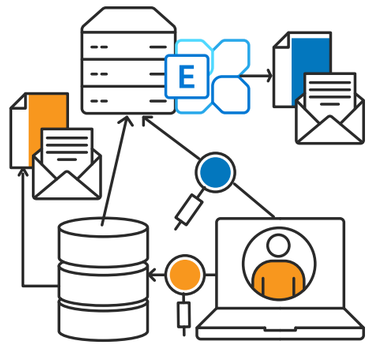
You always have help.

Asigra takes the burden of data-related inconvenience off your shoulders, and removes the possibility of data-related disasters for your customers. It's liberating and empowering.



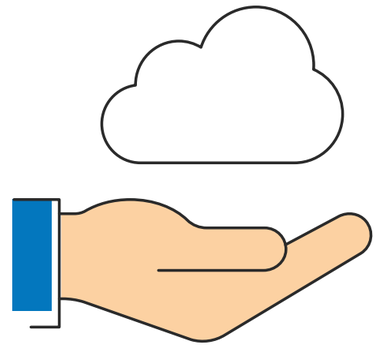
Recovery Time Customization

Set and meet any RPO or RTO with considered options for both.



Granular Recovery

Be able to get singular data elements as needed from your backup.



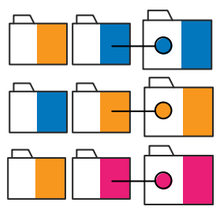
Maximum Manageability

Have continuous, low-touch control of your networks and devices.

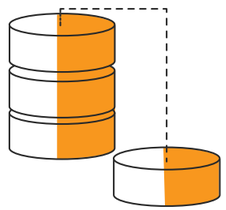
Cloud Backup Built for the MSP

Protect your customer data with a suite of manageability and reliability features

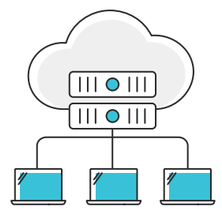
Block-Level Incremental Forever



Deduplication

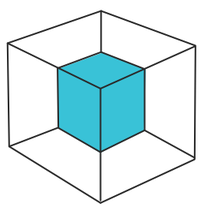


Compression



Hybrid Cloud

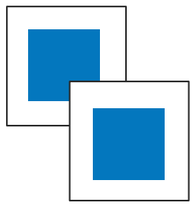
Retention Rules



Extensible Storage

SaaS/PaaS

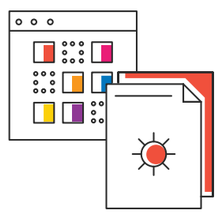
Global Privacy Regulatory Compliance



Replication

Restore Validation

Autonomic Healing



Reporting and RESTful APIs

Recovery Time Customization

What do you need to get back to work?

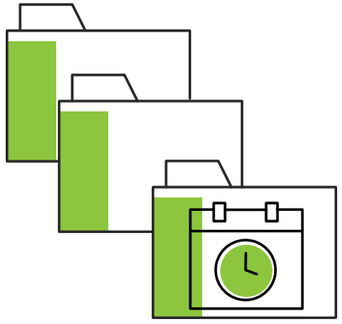
Depending on a customer's RTO and/or RPO requirements, you may need near-instant recovery for some mission-critical applications and data. **No problem.**

We'll protect the availability of any digital point in time so you can get your customers there and back faster.

Did you know?

MSPs using Asigra can restore in a few minutes rather than several hours.

Three places to start.

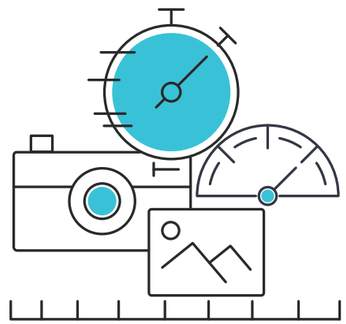


Continuous Data Protection (CDP)

For specific backup sets to ensure your customers can be up and running quickly with minimal data loss.

Incremental Backup

Your customers can back up VMs by retrieving only the changed blocks from the server and incremental pieces from the source.



Snapshot Capability

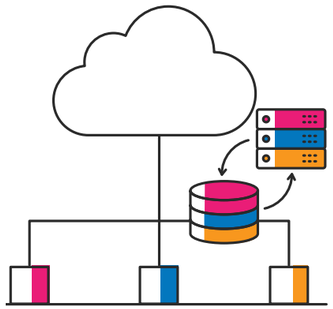
Set and exceed ultra-aggressive RPO and RTO goals for customers with large data sets.

SaaS/PaaS Data Backup and Recovery

Fully manage protect critical cloud-based app data

It's their cloud, but your customer's business data. Ensure your backup strategy includes data residing in third-party cloud applications, platforms, and services.

Reclaim control of customer data residing outside your data centers.

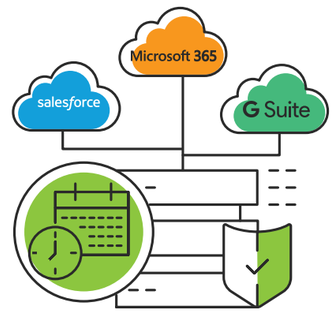


Deploy with Ease

Mass deploy backup configurations to hundreds of cloud application users at once. New users are automatically detected for inclusion.

Define your own Frequency and Retention

Be there for your customer when they need you most. Ensure that data is protected as often and for as long as required, while retaining access to data at all times, even during those downtimes.



Cloud-to-Cloud Data Protection

Easily schedule the creation of point-in-time backup copies of Microsoft 365, Google Workspace, Salesforce, and many more!

Why Backup SaaS?

Most SaaS vendors suggest the use of a third-party service to backup customer data and we agree. There are a lot of good reasons to backup SaaS Data; data will be easier to use, safer from hackers and rogue admins, and might even cost less than the alternatives, once the extra storage requirements of using retention periods and retention locks are considered. But most importantly, recoveries can be at any level of granularity (e.g. email, file, folder, user, site, or subsite) and they come with a durability guarantee not of-fered by SaaS providers.

Granular Recovery

Eliminate the haystack.

Most companies want to backup an entire data source for full protection but will usually only need to recover individual items or files.

We make that easy for your customers to do from VMs, Microsoft Exchange and SharePoint servers and SaaS based databases. Recover quickly and get back to work faster.

For example…

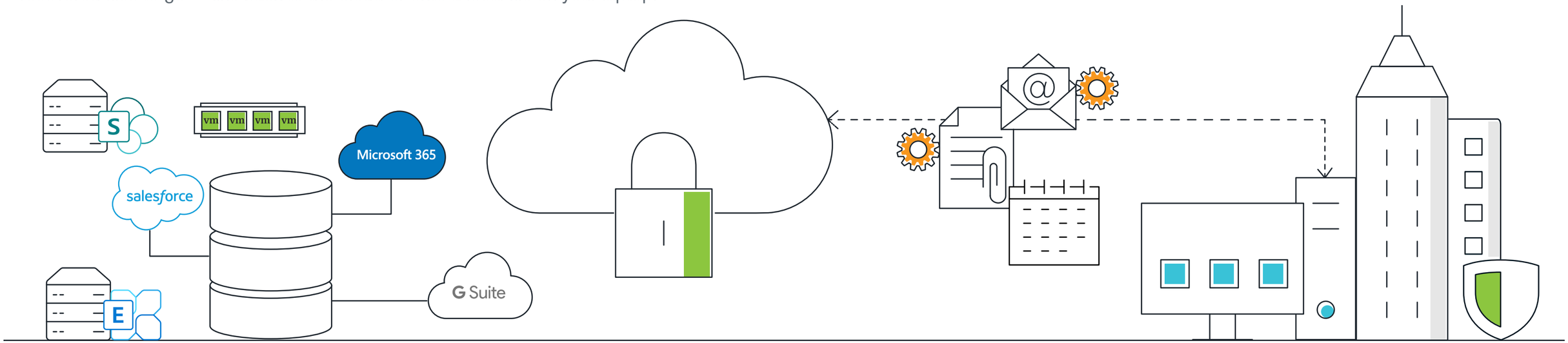
A convenient feature enables the backup of hundreds of mailboxes from a Microsoft 365 domain to one backup set.

No customer of yours could recover something as specific as an attachment or calendar entry without having to take all data in the domain. And they can choose where you want the recovered files to go — like back to the cloud or onto a local file on your laptop.

Our favourite customer review…

> *I was able to prove that one of my business partners was deleting important emails to get me removed. And he wound up getting removed. Karma."*

~ J.P., Tech Founder
Toronto, Canada

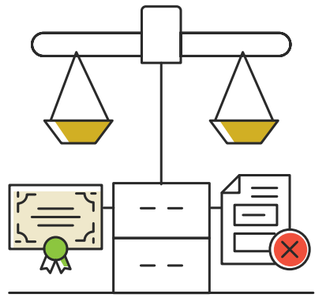


Maximum Manageability

Relax. It's all easy.

We've simplified data compliance and capacity management. This makes having a comprehensive, unified, organization-wide view of your systems, users and devices easy.

Some of our more popular features



Granular Backup File Deletion

Comply with "Right to Erasure" regulations, such as GDPR Article 17. Asigra enables organizations to find and wipe personally identifiable information (PII) from backup archive data and produces a certificate to prove it.

Single Consolidated Repository

Organize data currently backed up in silos scattered across the enterprise in one easy-to-recover place.

Management Console View

Manage from an intuitive web-based dashboard with cross-enterprise visibility for the most complex disaster recovery and business continuity strategies. Could include modules for branch locations, local/remote backup and data centres.

Support for Private, Hybrid and Public Cloud

Choose the cloud architecture or deployment model that best suits your business needs. Easily migrate as your needs evolve.

World-class Service from Our Global Partners

Minimize your spend on backup and recovery and have the confidence that what you spend is worth the investment.

It’s you against the cyber thieves.

Take the upper hand.

Our approach to backup and recovery, combined with a unique perspective of the enemy, makes our data protection solution a wise choice for complete data protection. We focus on one thing: being the absolute best at backing up and recovering your data.

REQUEST A DEMO

This is the ideal.

“Thanks to Asigra we have shaved off the number of hours spent on backup significantly and substantially improved our ability to recover from a data loss event regardless of where the data was originally located.”

~ Scott Reid, VP of Operations
PacMoore

Contact us for more info about improving recoverability.

Please call us at 1-877-736-9901 or 416-736-8111, or email us at **info@asigra.com**.

About Asigra

Trusted since 1986, Asigra technology is proudly developed in and supported from North America, providing organizations around the world the ability to quickly recover their data from anywhere through a global network of IT service providers. As the industry’s most comprehensive data protection platform for servers, virtual machines, endpoint devices, databases and applications, SaaS and IaaS based applications, Asigra lowers the total cost of ownership, reduces recovery time objectives, and eliminates silos of backup data by providing a single consolidated repository with 100% recovery assurance and anti-ransomware defense. The company has been recognized as a three-time Product of the Year Gold winner by TechTarget for Enterprise Backup and Recovery Software and positioned well in the market by analysts.

More information on Asigra can be found at www.asigra.com.

Secure Recovery is Everything™