BACKUP SECURITY BRIEF

November 2020

Asigra.
Recovery is Everything™

Cybercriminals aren't breaking into my backup. I set it up with multi-factor authentication and immutable storage."

Hackers love hearing stuff like that. It gets them excited. But above all that, it gives them a big, juicy target they can exploit without breaking a sweat.

The Asigra Way

The Asigra approach to backup & recovery is to acknowledge that there is no 100% guarantee against attacks. The strategy we advocate is to always be ready for the inevitable but at the same time raise the "costs" to the Threat Actors. Raise their costs in terms of effort, time, skill, and minimize their likelihood of success. If the cost is too high, they'll move on.

You'll never be immune to cybercriminals. But you can cost too much to crack.

When I started Asigra back in the 80's the goal was clear, build a solution that can reliably copy and store data so that these additional copies may be restored in case of a data loss accident. With forces of nature and hardware failure accounting to 95% and human error the rest of all data "accidents". Fast-forward 10 years and we had to meet the demand for faster RTOs and RPOs fueled on by the evolution of computer technologies and data volumes expansion. The biggest culprits at the time, you guessed it… still the same three forces. But fast-forward another couple of decades and backups has a new enemy, and it runs a monopoly. The #1 culprit, Ransomware and in a close second place, hackers and neither are showing any signs of slowing down.

As these new threats and their solutions appear, backup methods and technologies become more complex. The term loosely used is "Modern Backup". But it got me thinking, which cumulative set of features make a backup and recovery solution truly "modern"? In my humble opinion, a solution that can still perform the original tasks it was designed for but has evolved to cater for the modern threats it faces. There is only one problem with this statement… In the past several years, Threat Actors have identified that backup software is a worthwhile attack vector because it is so poorly protected. And there are many reasons for this, most notably is that more of an organization's budget is spent securing the front door that there is nothing left to spend on protecting the backdoor protecting your last resort, the insurance policy, aka your backups. The other is that Backup professionals and stakeholders are mostly not working with their organization's security team and vice versa. It is this gap in coordination which permits the Threat Actors to take advantage and attacks on backup are mostly easy, with a quick route to payouts.

It is with this in mind that I tasked my team to put together this Backup Security Brief to share with you our latest practices on securing backups and provide information about how to mitigate risk.

I hope you find it helpful.

Regards,

David Farajun

Founder, CEO

What is multi-factor authentication?

It's a protective layer that forces a user to demonstrate their identity in at least two ways, generally from one or a combination of these categories:

A physical key like a USB stick or a card

A personalized number like a PIN

A biological identifier like a fingerprint or a voice

A specific location like a network or GPS coordinates

Why multi-factor authentication?

Because the best cybersecurity approach is layered and hard enough to crack that the threat actors give up and move on.

MFA worked for a while. Then it didn't.

How are hackers busting MFA?

Spoofed websites that copy keystrokes, PINs and personal info, or network malware that capture voice commands, long distance card-data readers are a few. And every time the threat actors come up with a new way to break down the front door, the industry responded with another obstacle.

So the hackers changed their approach angle.

Instead of banging their heads against the front door for hours, they went around back and walked right in because of the flippant approach way too many IT teams take to securing their backup software and data .

Companies discount the value of their backup data to a hacker, and the damage a compromise can cause.

We know this because the level of security on the back end isn't nearly as robust as it is up front, which seems counter-intuitive because a company's most important data lives in the backup.

Hackers know this too. They walk right in and they're gone before you know it, but not before crippling your system and setting themselves up to:

make **you pay** to get your clean data back

make **you pay** to not have your data leaked to the public

sell **your data** on the dark web and maybe blackmail you for fun

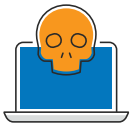
The experts thought they had a winner with WORM storage

WORM stands for "write once, read many" and it prevents files from being altered in any way by anyone but the network administrator, so even if a threat actor successfully breached a system, they couldn't touch the backup. It's also known as Immutable Storage.

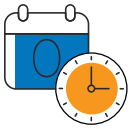
WORM worked for a while. Then it didn't.

Hackers figured out how to steal network administrator credentials and disable the WORM file retention settings. Then, they:

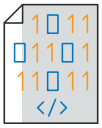
corrupt the data without anyone knowing



plant their ransomware



reset the retention parameters



take off with the clean data

& detonate the ransomware when they know you don't have a recoverable backup

Right now, the industry is working on a way of thwarting that kind of credential theft. But by the time they do the threat actors will have developed another way in.

So where does that leave you?

That depends on how wide open you choose to leave your back door. And make no mistake, it's a choice you have, because Deep MFA is available for backups.

What is Deep MFA?

It's a more robust approach to MFA that gates access across a software stack to protect sensitive data at multiple levels in the backup process. So even if a threat actor manages to steal credentials and get in the front or back door, they can't do anything except stay there.

Think of a hacker facing Deep MFA like a prisoner standing in a round room with 20 doors and who can only get out by opening the right doors in the right order with some doors needing to be opened multiple times.

A backup equipped with Deep MFA sends hackers on their way

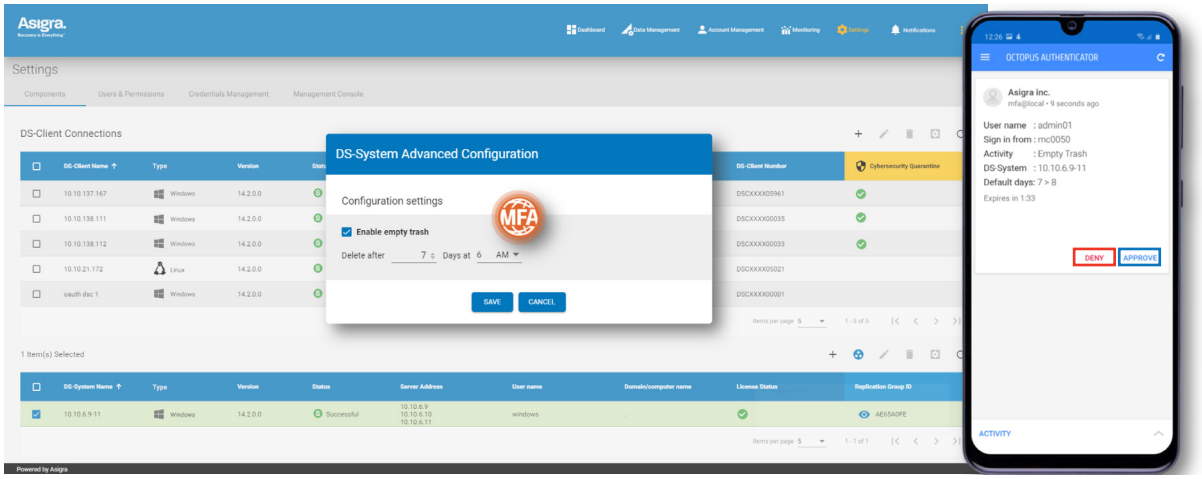
That's why security people are so bullish on the principle of it and why they're adopting it more and more. But they're not implementing on their back ends and they're paying the price — along with whatever money they spent to poorly upgrade their security.

Asigra 14.2 creates such a secure backup

As a leading provider of the most secure cloud-based backup software, we looked at where the cat-and-mouse between hackers and data pros was, and we jumped ahead.

- We built Deep MFA into the backup software around any task that could affect data.
- We eliminated the possibility of theft by integrating the facial/thumb print recognition already built into smart-phones.

For the first time, backup software has built-in, password-free, deep multi-factor authentication across its entirety.



For the first time, your back door can be just as secure as your front door. And you can be twice as confident in the security of your data.

FIND OUT MORE ABOUT HOW ASIGRA PROTECTS YOUR BACK END.

Request a Demo

Asigra.
Recovery is Everything™