Asigra.

Recovery is Everything™

DATASHEET

Don't Rely on a False Sense of Security.

Hard to by-pass, easy to use integrated Step-Up MFA for Backup.

Security professionals have known for years that the best cyber defense is layered making it harder for the cyber criminals to penetrate the IT organization. It has been an ongoing race of offense versus defense. To prevent modern ransomware attacks requires better backup defenses. The irony of it all is that while cybersecurity teams have been spending most of their efforts securing the priority applications and systems, their backups remain the soft-underbelly to their security stack. Backup applications are notoriously unprotected. Most data protection solutions in use today have no integrated Multi Factor Authentication, while the handful that have MFA only have front door protection, leaving the back door exposed.

Step-up MFA means deeply imbedding MFA to every single backup task that affects the data within the application. Tasks such as backup schedules, retention time, backup location, replicating the backups, etc.

> **"WHY DO I NEED IT? I HAVE DATA IMMUTABILITY"**
>
> CYBERCRIMINALS LOVE KNOWING YOU THINK THIS.

When ransomware has encrypted the data, applications, and systems, recovery from backup has been the last line of defense for many organizations. Cyber criminals recognized that and changed their attack by simply going after backups by deleting replicas, backups, snapshots, everything they could find and then detonated their malware. It can be quite disturbing to be hit by a massive ransomware attack and find all the backups simply gone.

To counter this, backup and storage vendors have been implementing storage immutability which would stop the ransomware attack of deleting the backups. Immutability is tied to the retention period of the data being stored and as long as that data is within its retention period of days, weeks, months, or years, it cannot be changed, erased, or encrypted in any way. And for a very brief period of time, it did.

Circumventing Data Immutability

To counter this, threat actors have now modified their attack by using targeted phishing and vishing aimed at the backup administrator, operators, and other users. They steal the credentials and change the retention period without anyone being the wiser. Instead of a 30-day, 60-day, 6 months, etc. retention period, they change it to

Asigra.

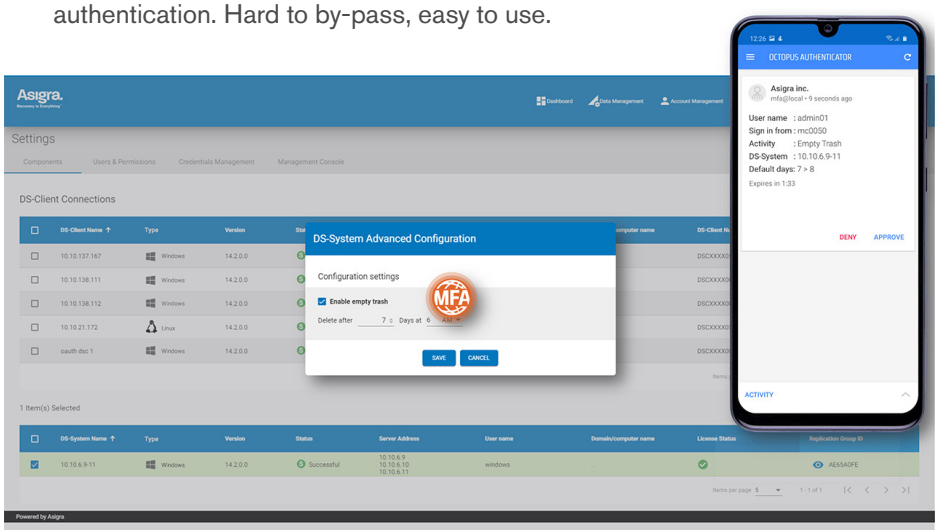
hours or just long enough for the software to report a successful backup. And then the data disappears. The ransomware detonates and there are no backups to recover from. But that's not all, the twist to this new ransomware variation is the use of those privileged credentials to also steal valuable data by copying or redirecting backups to another location using it to extort victims by first applying pressure threatening to release damaging data to the public. The second is to further apply pressure by releasing some of the most damaging data into the public (which triggers litigation costs). The third is to sell that valuable data on the dark web whether the organization victim pays the ransom or not.

HOW IT WORKS

SECURING THE LAST LINE OF DEFENSE

Asigra, the leading provider of the most secure cloud-based backup software, recognized these problems and added Deep MFA for any task that could affect the data. It's built into the backup software. None of the data affecting tasks can be done without MFA.

Being Deep MFA Secured, doesn't have to mean time painstakingly cumbersome or time-consuming. Asigra went much further by making it convenient with passwordless authentication utilizing the biometric facial recognition or thumb print identification already built-into smart phones. For the first time, backup software has built-in passwordless setup-up multi-factor authentication. Hard to by-pass, easy to use.



This is modern warfare. Gear up, layer up...It's you against the hackers.

Interested in learning more about Deep MFA?

To request a demo or for more information, call **1-877-736-9901** or **416-736-8111** or **email** info@asigra.com.

Deep MFA Key Benefits

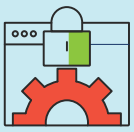
Integrated MFA

App-centric Multi-Factor-Authentication enabled passwordless sign-in available throughout the software stack to protect sensitive data at multiple levels in the system. Once logged in via MFA, administrators will be able to configure access to control which users can sign into the Asigra Management Console and other mission critical areas of the application without using a password.

Immutable Retention Protection

Unifies immutable retention and application credential protection to prevent any unauthorized source from deleting or modifying backup data on the storage repository.

Secure Setup Wizard



The Secure Setup Wizard provides management console users with a guided tour through the initial setup process, including configuration of security settings, DS-System and DS-Client connections, users and permissions, and email/alert settings.

Credentials Management

Asigra Management Console users can now configure and manage their credentials from one location. Once the credentials are saved, users simply select them when creating a backup set rather than manually entering them each time.

MS365 Credentials Management

Implementation of Modern authentication has been designed for ease of use, it requires only one click and no additional configuration from the user.