Comprehensive Malware Protection

For Your Microsoft Office 365 Cloud Data and Windows File System Backups

DATA2VAULT
SECURE DATA SERVICES

POWERED BY
Asigra.



Would You Survive a **Ransomware Attack on Your Backup?**

Ransomware is not a new phenomenon. However, technological advancements by savvy cybercriminals have totally changed the game. Attacks used to be random… criminals would send millions of malware infections (either via phishing emails or malicious links) to see which end user would open the file to encrypt an organisation's data. Trends show that while these types of attacks are still occurring, targeted attacks are becoming much more prevalent because organisations are more likely to pay the "ransom" to have their business critical data released.

There are currently three types of prevalent ransomware attacks today:

1

Data Encryption

These type of attacks (e.g. Locky, Petya and WannaCry) are large in scope and choose victims at random to see which end user will click on a malicious link to encrypt files.

The Solution: *Perform backups regularly so you can always revert to a previous version of your data that isn't encrypted. Test your recoveries.*

2

Deletion of Backup Repositories

These types of attacks (e.g. Samas) are typically deployed by Remote Desktop Protocols where cybercriminals steal domain credentials, look for unsecured servers, wipe all the files from the backup repository, and then proceed with file encryption.

The Solution: *Keep a recent offline version of your backups. Implement a backup solution that has Multi-factor Authentication (MFA) and allows you to change the names of the backup repositories. Asigra does both.*

3

Embedding Zero-Day Malware into Your Backup Repository

Regardless of whether you have the best backup solution, antivirus protection, or versions of your backup repositories, this next generation of ransomware is so advanced that your data is still at risk. These types of attacks embed time-delayed and undetected malware into your backup repositories sometimes months in advance. This makes file restoration pointless because as you recover your data the ransomware reignites and re-encrypts the data all over again. This is known as the **Attack-Loop™**.

The Solution: *Asigra – Your only solution against unknown threats, malware, and zero-day vulnerabilities in your backup and recovery stream.*



Introducing the Cyber-Generation of Data Protection

Powered by Asigra Attack-Loop™ Prevention Solution

Our comprehensive malware-in-your-backup(s) solution offers:

Attack-Loop™ Prevention for Microsoft Office 365 cloud data and Windows file systems

Our cyber-enabled data collector (DS-Client) protects your Microsoft Office 365 (SharePoint and OneDrive) cloud data and Windows file systems from malware attacks by performing real-time scans of your files during the backup and recovery process.

Three steps to ensure complete malware protection:

1. Ensure that your desktops and laptops are protected by running a corporate antivirus solution with up-to-date definitions.
2. Create a Microsoft Office 365 or Windows File system backup set that has been enabled with the cybersecurity scan. Any files on the protected Windows device or in your SharePoint or OneDrive data that are detected with malware are backed up to the DS-System repository in encrypted format and a warning message appears in the Event Log.
3. Perform a restore of a File System or Office 365 backup set that has been enabled with the cybersecurity scan. Any infected files will not be restored, but will instead by saved to a password protected zip file and copied to a quarantine folder.

Zero-day Exploit Protection:

Our signature-less technology checks and quarantines malicious code upon entry into the backup repository and prior to recovery into your environment.

Multi Factor Authentication (MFA)

This extra layer of security prevents the unauthorised deletion of backup repositories.

Variable File Naming Conventions:

Viruses looking for specific file names to attack will not find them. Our solution allows you to rename your file repositories in non-standard formats to prevent recognition and deletion of your backups.

Note: The cybersecurity feature is a licensed feature. The trial version includes five (5) free malware detections per DS-Client.

Our solution also includes…

Enterprise Data Protection

- Regardless of size or complexity, we ensure your organisation's data will be recovered back to any point-in-time and on any endpoint device.

Cloud SaaS Protection

- We protect and recover data within SaaS-based apps (e.g. Google G Suite, Salesforce.com, Office 365) regardless of where the data resides.

Business Continuity/Disaster Recovery Solutions

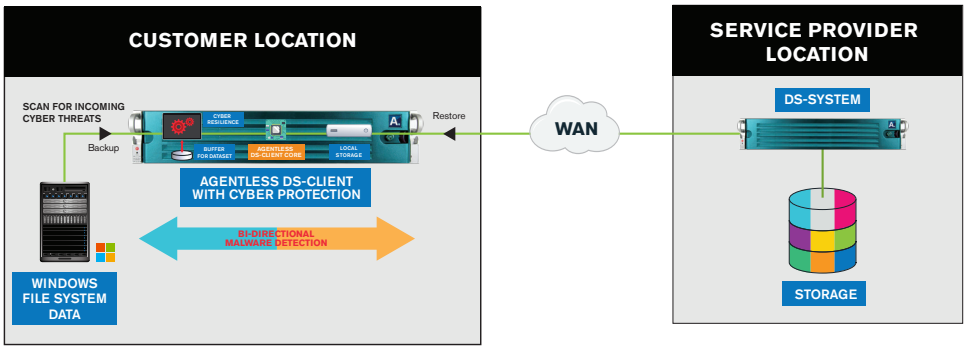
- Our disaster recovery solution reduces downtime from hours to minutes ensuring business continuity across all organisational units.

Compliance Management

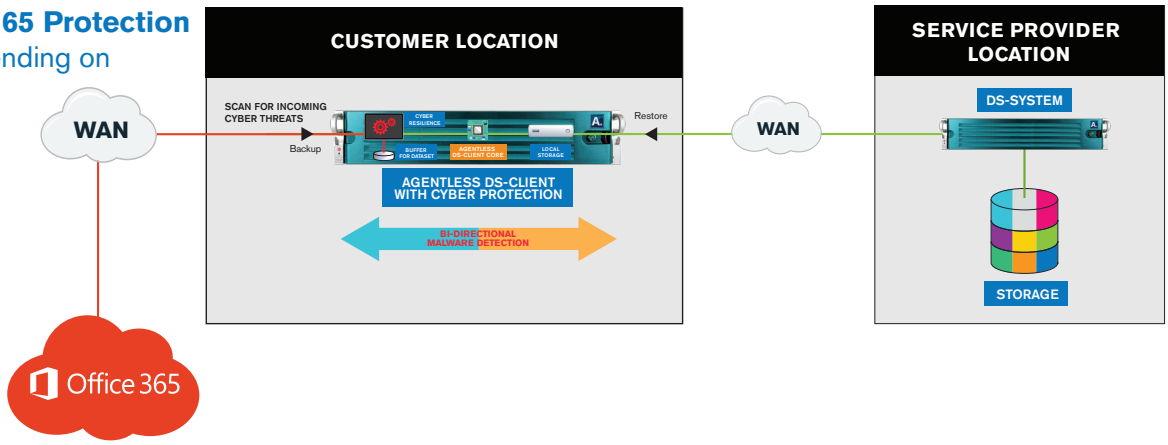
- Being NIST FIPS 140-2 validated allows you to efficiently archive, restore, and wipe data to ensure you are adhering to regulatory compliance.

Deployment Models

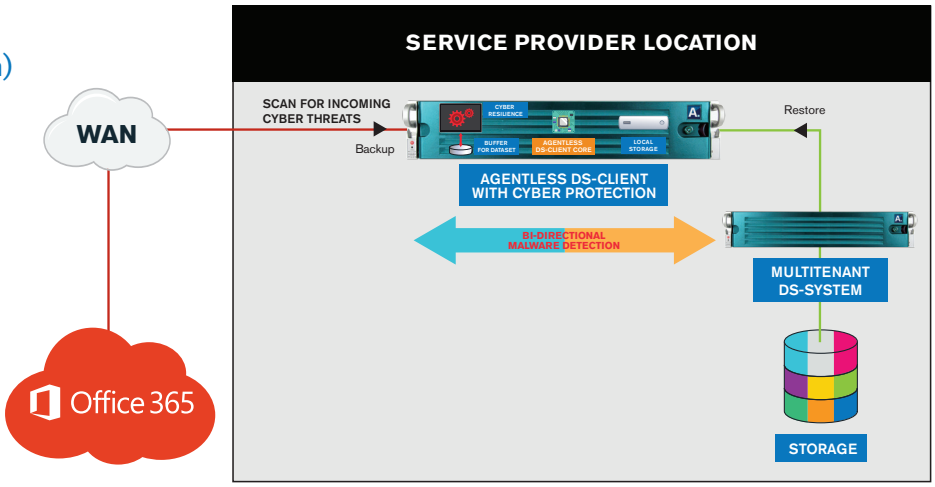
Windows File System Protection



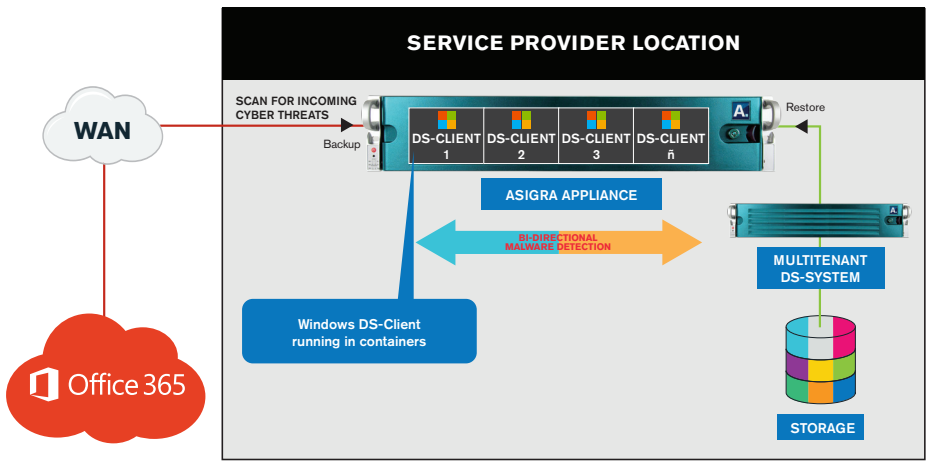
Microsoft Office 365 Protection
(50–100 users depending on configuration)



Microsoft Office 365 Protection
(Collocated DS-Client and DS-System)

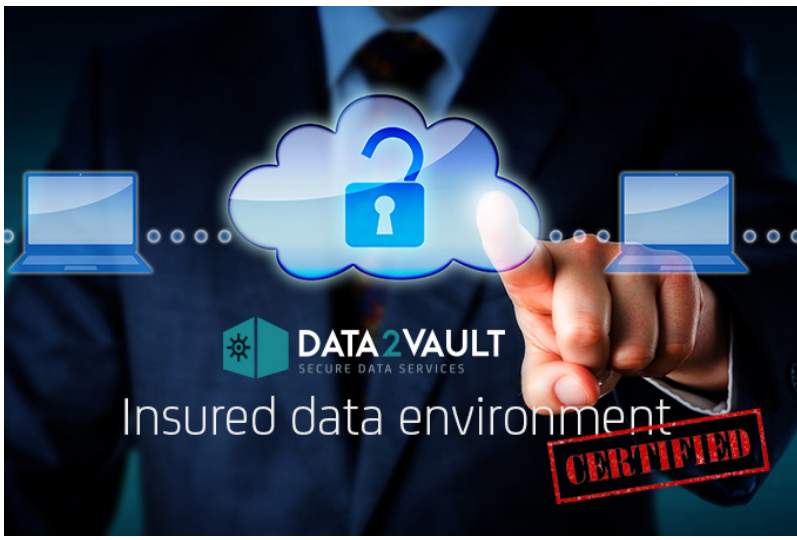


Microsoft Office 365 Protection
(Collocated DS-Clients in Docker Containers and DS-System)



Mitigate your Risk

Advanced Data Protection is about applying layers of safeguards to combat existing and emerging threats. To complement the **Attack-Loop**™ solution we can offer a unique Data Loss Insurance service, provided by authorised brokers and underwritten by Allianz. For more information visit us at www.data2vault.



About Data2Vault

Data2Vault executives and staff have been involved in the secure data protection market since before 2005 as a certified Asigra Service Provider throughout this time. Our philosophy is simple, security must be at the core of the data protection services we offer, and no one size service fits all.

Our objective is to always deliver the data protection services that your organisation needs, securely and in the way that you need it provided. As those needs evolve, then so must our service delivery models, while always retaining a consistent focus on security and management of risk wrapped up in a high quality service.

We operate from a number of UK Data Centres providing high availability and continuity of service. The Data Centres are all ISO9001, ISO27001 and ISO14001 certified, the Internet services we use are highly resilient and can scale as required to ensure we have no single point of failure.

To find out more about our solution, visit us at www.data2vault.com.

About Asigra

Trusted since 1986, Asigra technology is proudly developed in and supported from North America, providing organisations 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 recognised 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.

MALWARE-IN-YOUR-BACKUP
Attack-Loop™
Prevention.

DATA2VAULT
SECURE DATA SERVICES

POWERED BY Asigra.