Offering Flexible Deployment

Storage Agnostic Tigris can utilise any storage environment, including DAS, SAN or NAS. Optional pre-configured Asigra TrueNAS and Asigra Zadara Cloud Appliances are also available.

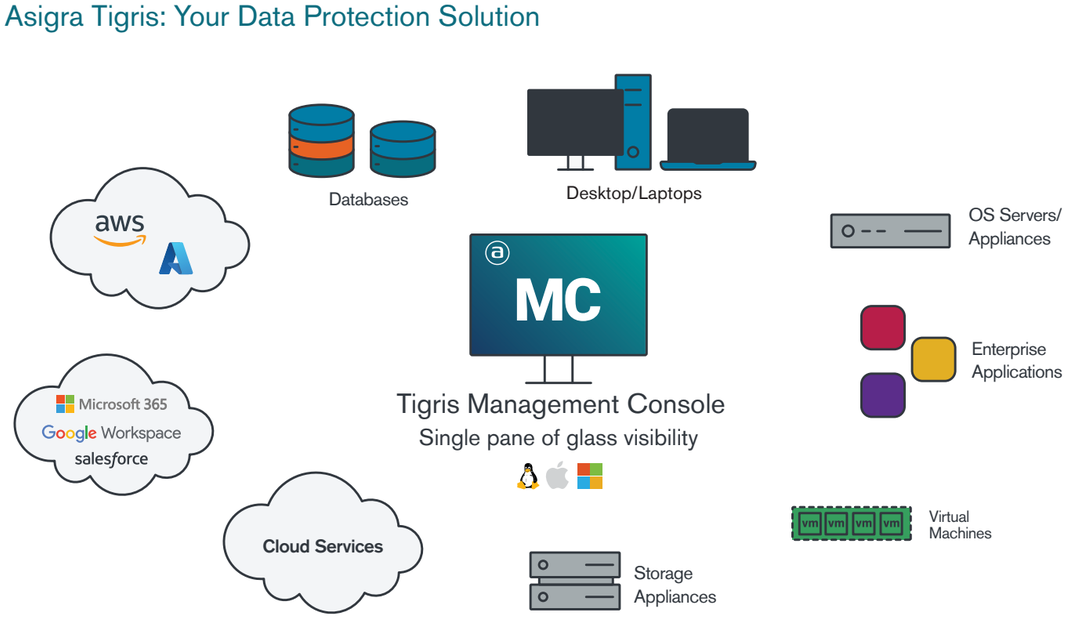
Location Agnostic The Asigra Secure Repository Manager (SRM) and backup storage can be deployed either in your own data centre or in the public cloud or service provider of your choice. Asigra's Management Console can be deployed in any location, while Asigra's agentless Data Security Modules (DSM) are installed on your LAN.

OS Agnostic Asigra is flexible enough to run on Windows, Linux, & Mac installations.

Highly Available & Fault Tolerant With options for stand-alone or N+1 deployment, Asigra Tigris can provide fault tolerance and load balancing.

Deployment Efficiency Asigra can be deployed quickly, as agents don't need to be deployed to hundreds or thousands of endpoints. The Tigris DSM is set up at the LAN level allowing deployments to be up and running in as little as one hour!

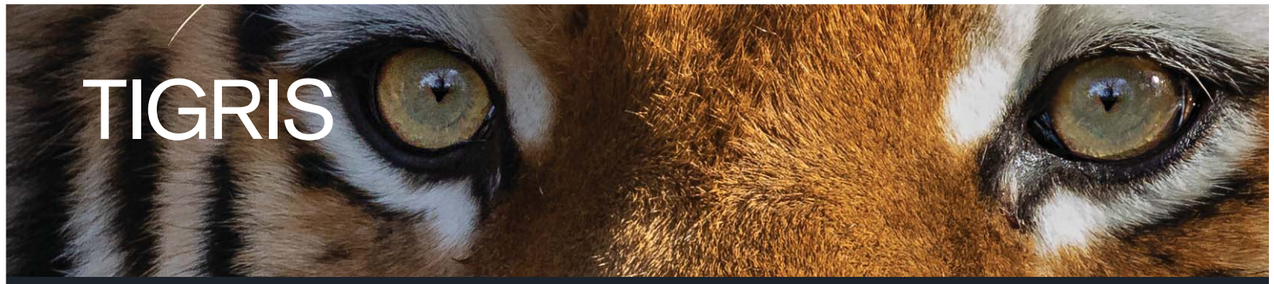
Asigra Tigris: Your Data Protection Solution



Are you looking to strengthen your data backup security?

Contact Data2Vault for more information www.data2vault.com

ULTRA SECURE BACKUP



Asigra Tigris is an award-winning agentless backup and recovery platform that proactively hunts ransomware.

Tigris is the world's most secure enterprise backup software platform protecting data centres, cloud, & SaaS with advanced anti-ransomware technologies that secure your last line of defence against hackers. Your backups.

Air-gapped & Immutable Backups Are No Longer Good Enough.

Attackers know that a clean backup foils ransomware paydays. As a result, the new generation of ransomware evades traditional backup strategies, like 3-2-1 air-gapped and immutable storage.

The Trojan Horse Strategy Sets Up the Attack-Loop™

The new breed of ransomware utilises trojan horse (sleeper) attacks with detonation delays of weeks or months. These strategies ensure that the dormant malware is implanted everywhere, including air-gapped and immutable backups. Unfortunately, immutability ensures that the backed-up ransomware can't be touched. Then ransomware detonates, and the IT team reaches for the backups, but the ransomware implanted from months ago is restored along with your corporate data, and you are caught in an Attack-Loop.

Using Stolen Credentials to Nullify Immutability

Another known attack utilises stolen credentials, allowing them to gain access and use the backup system against itself, circumventing immutability. The bad actors delete data directly or adjust the retention period from years to hours, triggering backup deletion just before a ransomware detonation.

2022 and the Massive Ransomware Ramp-Up

The volume of ransomware increased 148%* in 2021. *Sonicwall

Average ransom request grew from £4K ($5k) in 2018 to £220K ($228k) in 2022*.
*Coveware

Average downtime is 24 days*.
*Coveware

"Earlier this year, the firm Cybersecurity Ventures predicted, "There will be a new attack every two seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities."

https://www.nasdaq.com/articles/ransomware-is-the-greatest-business-threat-in-2022

Users Love Us · MES Matters 2022 · CRN Storage 100 2022 · CRN Storage 100 2021 · DCIG Top 5 2020-21 · SDC Awards 2020 Winner · Storage Magazine Products of the Year 2020 Finalist · CRN Storage 100 2020