asigra

ULTRA SECURE BACKUP

TIGRIS

STOP HIDING FROM RANSOMWARE... START HUNTING IT!

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 physical and virtualized machines, cloud, data centers, applications, servers, appliances, and SaaS with advanced anti-ransomware, CDR and FIPS 140-2 encryption technologies that secure your last line of defense 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 utilizes 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 utilizes 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 $5k in 2018 to $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

asigra

Tigris Deep Six Security

Bidirectional Antimalware Scan & Quarantine Asigra uses advanced machine learning algorithms as well as heuristics-based and signature-based antimalware detection techniques to stop known and zero-day threats from reinfecting your environment. Our cutting-edge bidirectional antimalware scanning engine identifies malware during the backup process and quarantines infected files during the restore process. This step is critical for stopping sleeper attacks and the resulting Attack-Loop.

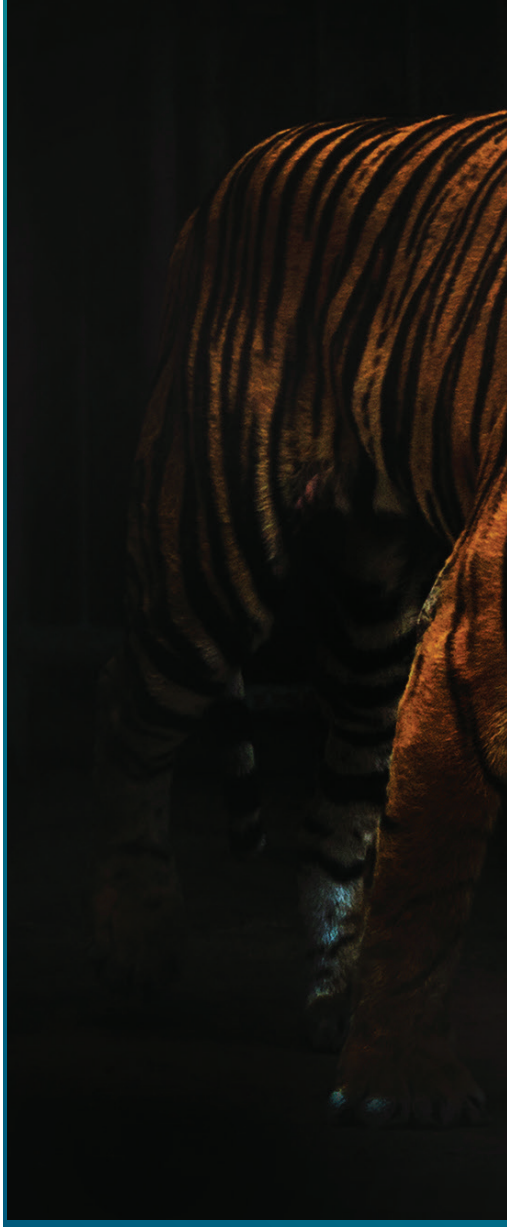
Content Disarm & Reconstruction (CDR) Another typical sleeper attack utilizes malware deeply embedded in a file to avoid antimalware detection software. With the addition of advanced CDR security, Asigra can scan files and filter, block, or remove potentially dangerous content, such as macros, scripts, and executables, based on predefined policies. This ensures the backed-up files are safe and free from potentially malicious or unauthorized content while still being usable during a restore. This enterprise-level security technology is unique in the backup industry and provides unparalleled protection against the newest ransomware strains.

Multiperson Approval (MPA) & Multifactor Authentication (MFA) Administrators can configure Multiperson Approval (MPA) for accounts so users require multiple people to approve a potentially destructive action that can result in data loss. Administrators can set a threshold to specify how many additional approvals are required and which actions require the approvals. When a user attempts to perform a task that requires approval, the approvers receive an email with the user's name and a description of the task and must approve or deny the request. The approval link expires after 30 minutes.

Soft Delete A hidden folder that holds deleted data, fooling attackers into thinking permanent data deletion has occurred. Soft Delete creates a 2-step deletion process and protects against accidental/malicious data deletions.

NIST FIPS 140-2 Certified Data Encryption AES 256-bit in-flight and at-rest data encryption protects your data at the highest level of security and compliance.

Variable Repository Naming Thwart attacks searching for specific naming conventions that may indicate the presence of backup data.



> “Immutable backups for ransomware defense may not be enough. “Sleeper attacks” that can be difficult to detect can attack backup environments, where malware infiltrates the environment and lays dormant until encrypting the data.”
>
> ~Krista Macomber
> Senior Analyst, SearchDataBackup, TechTarget

Unique Security–First Architecture

Agentless Architecture Traditional backup software requires compact endpoint agents. Asigra uses no agents but utilizes a software-based Data Security Module (DSM) on the network. The DSM is flexible and scalable, allowing the Asigra Tigris security stack to grow and evolve to keep pace with the ever-advancing cyber threats.

The DSM gathers all data from the network. It then dedupes, compresses, scans (antimalware and CDR), and encrypts all data inline before sending it back to the repository. During the restore process, the DSM scans and quarantines (antimalware and CDR) to catch advanced ransomware attacks.

Maximum Manageability. Minimum Effort.

- Simple Agentless Deployment
- Single Pane of Glass Management Console
- Container Friendly
- Automated Notifications
- Customized Reporting
- RESTful APIs
- File Level Control
- GDPR Regulatory Compliance
- Autodiscovery automatically creates new backup sets for items added to a Microsoft 365 domain.

Recovery Reliability

Autonomic Healing Nearly 50% of all backup recovery jobs fail due to everyday data corruption. Asigra maximizes recoverability by proactively monitoring the integrity of backup data and repairing it automatically if degraded or corrupted.

Restore Validation Most backups are never tested due to the need to perform a test restore on physical infrastructure. Asigra's restore validation simulates recovery operations in memory, making it fast and easy to test backups, ensuring they will succeed when needed.

Additional Recoverability Features

- Continuous Data Protection
- Granular Recovery
- Granular File Retention Policies
- Backup Lifecycle Management
- Replication

Expansive Data Protection

Asigra Tigris backup software allows you to simply and securely back up data to any location you choose, including public cloud, private cloud cloud or on premise. Tigris supports all major operating systems, servers, databases, and virtual machines, including:

- Windows & Mac
- Unix/Linux OSs
- Hyper V and VMware VMs

Protecting SaaS data is crucial, and Tigris provides backup for the most popular SaaS apps, including Microsoft 365, Salesforce, and Google Workspace.

Offering Flexible Deployment

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

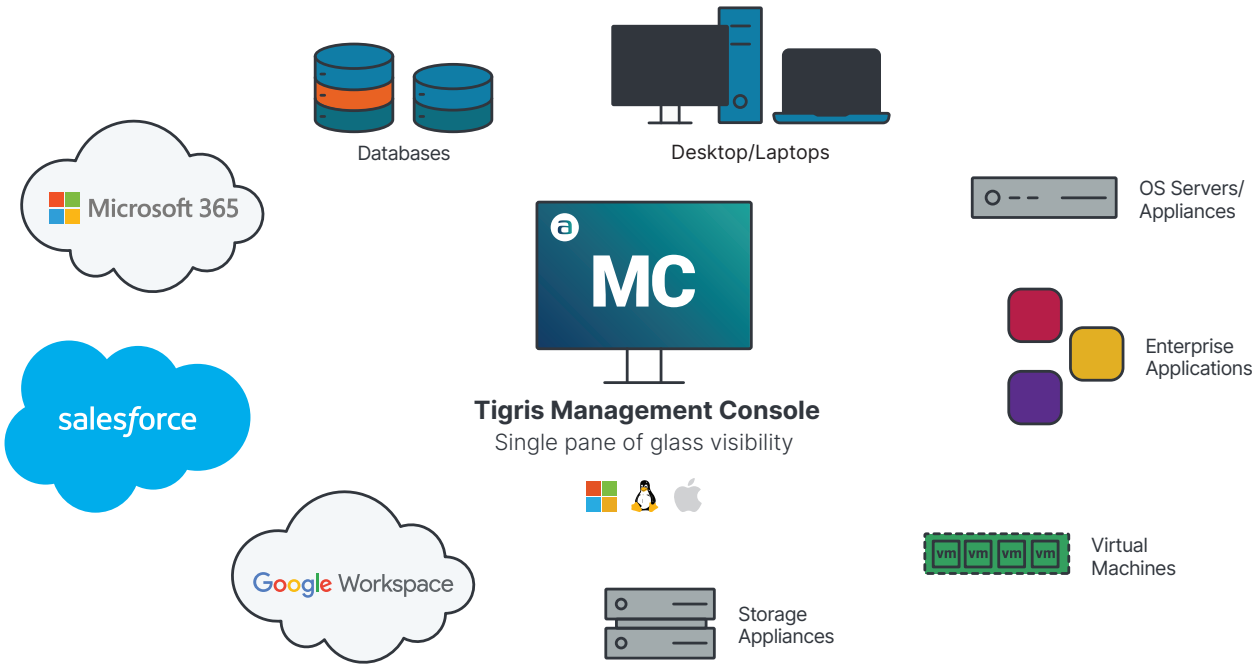
Location Agnostic The Asigra Secure Repository Manager (SRM) and backup storage can be deployed either in your own data centre or in the public cloud or service provider of your choice. Asigra's Management Console can be deployed in any location, while Asigra's agentless Data Security Modules (DSM) are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



For more information about Asigra Tigris, contact us by email: **sales@asigra.com**.

asigra