TIGRIS

Ultra Secure Backup

STOP HIDING FROM RANSOMWARE & START HUNTING IT!

Asigra Tigris is an Award-winning Agentless Backup and Recovery Platform that Proactively Hunts Ransomware

Air-Gapped & Immutable Storage Are No Longer Good Enough

Attackers know that a clean backup foils ransomware paydays. As a result, the new generation of ransomware is designed to evade 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 strategies with detonation delays of weeks or months. These strategies ensure that the dormant malware is implanted in all backups, including air-gapped and immutable backups. Unfortunately, immutability ensures that the backed-up ransomware can't be touched.

Once the ransomware detonates and the IT team reaches for their backups, the implanted ransomware is restored along with your corporate data, and you are caught in an attack loop.

Using Stolen Credentials to Nullify Immutability

Once attackers gain network access via stolen credentials, they'll be able to use your backup system against you, circumventing immutable storage because the actions appear legitimate. They can exfiltrate or delete data directly or adjust the retention period from years to hours, triggering backup deletion just before a ransomware detonation.

Users Love Us

STORAGE MAGAZINE PRODUCTS OF THE YEAR 2020 FINALIST

SDC AWARDS 2020 WINNER

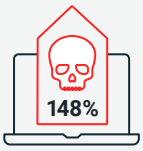
THE CHANNEL CO. CRN STORAGE 100 2021

THE CHANNEL CO. CRN STORAGE 100 2020

ENTERPRISE 2020-21 DCIG TOP 5 ANTI-RANSOMWARE BACKUP

2022 and the Massive Ransomware Ramp-Up

The volume of ransomware increased 148%* in 2021 and the impending impact of the log4shell vulnerability, puts every businesses' data at risk.



*Sonicwall

Average ransom request grew from $5k in 2018 to $237k in 2020
(National Security Institute)

28% of breaches affected SMBs
(Verizon)

Average downtime is 21 days
(Coveware)

A ransomware attack occurred every 11 seconds in 2021
(Cybercrime Magazine)

The Impact of log4shell vulnerability

LOG4J

> It could be a while before we see the real impact… if you are a ransomware affiliate or operator right now, you suddenly have access to all these new systems. You've got more work on your hands than you know what to do with right now.
>
> ~Sean Gallagher, Sophos Labs

asigra

Tigris Deep Six Security

Asigra Tigris Bidirectional, Anti-Ransomware Scanning

Backup Scanning & Quarantine

Asigra utilizes cutting-edge AI-powered antimalware scanning, featuring ransomware-focused heuristics and machine learning to catch even zero-day threats. Asigra scans at the LAN level within the Asigra Security Module to complement existing endpoint antimalware.

Regardless of where the data originates in the network, Asigra utilizes the backup stream as a centralized chokepoint, scanning all data before it's backed up.

Restore Scanning & Quarantine

If a ransomware attack occurs and the production environment is encrypted, restoring a clean version of the data is critical. Tigris performs a second ransomware scan during the restore process. This second scan catches and quarantines ransomware that had been previously dormant before it has a chance to re-infect the production environment.

Deep MFA

Once credentials are compromised, attackers can use a backup software against itself to delete data or change data retention periods from years to hours. Tigris' Deep MFA defends against stolen credential attacks using passwordless, multiperson, biometric authentication on the authorized people's phone (fingerprint/facial recognition) to neutralize the threat of password theft via phishing, keylogging, or credential stuffing.

Soft Delete

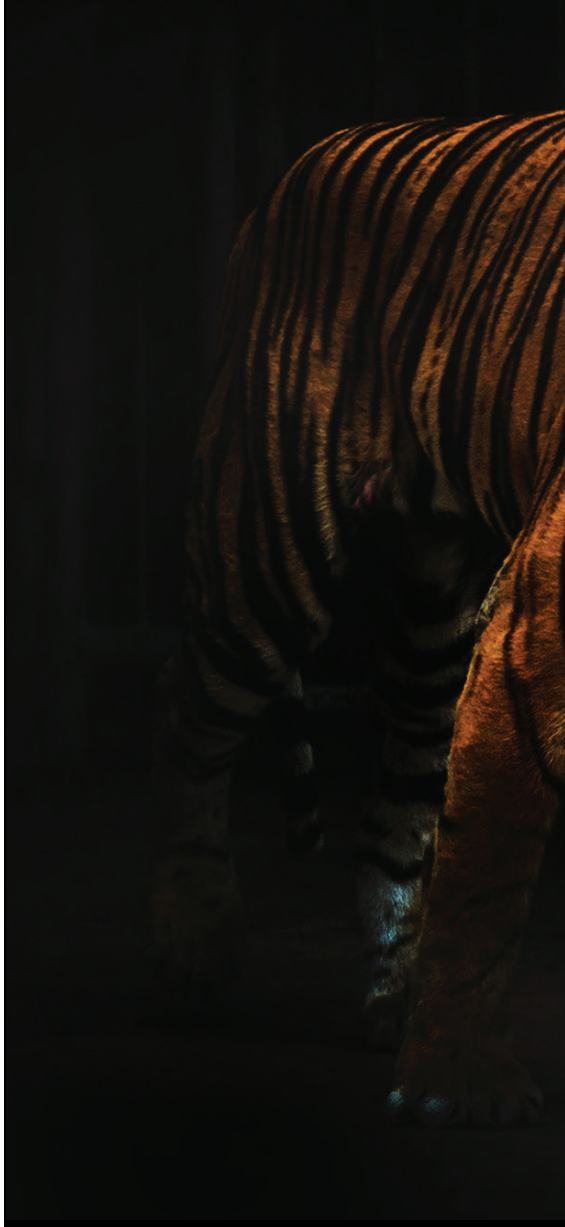
A hidden folder that holds deleted data for a designated period, fooling attackers into thinking permanent data deletion has occurred. Soft Delete creates a 2-step deletion process and protects against accidental/malicious data deletions. Deep MFA can also be applied to Soft Delete, requiring biometric authentication to delete data permanently.

NIST FIPS 140-2 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 looking 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 the malware infiltrates the environment and lays dormant until encrypting the data."
>
> ~Krista Macomber
>
> Senior Analyst, SearchDataBackup, TechTarget

Expansive Data Protection

Asigra Tigris enables you to protect your entire organization with one comprehensive solution. Tigris supports all major operating systems, servers, databases, and virtual machines, including:

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

Protecting SaaS data is crucial, and Tigris provides backup for the most popular SaaS apps, including:

- MS 365
- Salesforce
- Google Workspace

Maximum Manageability. Minimum Effort.

- **Agentless** – Truly agentless architecture reduces attack vectors and eliminates the downtime and disruption of deploying, updating and managing hundreds or thousands of endpoint agents.
- **Single pane of glass** – A management console to control complex environments, including multi-tenant deployments.
- **Granular Recovery** – This allows you to instantly recover specific files or systems from any point in time.
- **Granular Policies** – Each backup set can have its own retention rules.
- **Container Friendly** – Tigris data collector can run in Windows or Linux Docker containers (saving OS costs).
- **Automated Notification** – Email notifications for backup issues and status.
- **Customized Reporting** – Easy to create and schedule.
- **RESTful APIs** – Easy integration into monitoring tools, ticketing systems, etc.
- **Regulatory Compliance** – Ensures your backup data is fully compliant with all significant regulations, including GDPR.
- **File Level Control** – Targeted file-level restores to meet compliance audit (no need to mount multiple images).

Recovery Reliability

- **Autonomic Healing** – Constantly monitors the integrity of backup data and repairs it automatically if degraded or corrupted.
- **Continuous Data Protection** – Critical system data automatically backs up data in near real-time and recovers back to any point in time.
- **Restore validation** (MD5 Check) – Simulates recovery operations in memory to ensure restores will succeed when needed most.
- **Replication** – Data repository replication maintains several versions of files in a secure off-site location to protect against accidental and malicious data corruption.
- **BLM** – Backup Lifecycle Management allows lower-cost backup for noncritical (inactive) data with the option to archive to S3 compatible storage or Azure BLOB storage.
- **Instant recovery** (recovery in place) – Reduces downtime and keeps end users productive by restoring file systems, DBs and VMs to secondary systems in minutes.
- **VMware replication** – Protects virtual machines from partial or complete site failures by replicating to a disaster recovery data center.

Simple To Deploy

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

Preconfigured Appliances

For companies that need a backup appliance, Asigra offers three pre-configured options.

Asigra TrueNAS Appliance

With the Asigra TrueNAS Backup Appliance, your backup software is deployed as a simple integrated service natively on TrueNAS.

- Simultaneously supports Asigra Backup service, file (NFS, SMB), and block (iSCSI, FC).
- 99.999% uptime
- Includes RAID-Z, data scrubbing, and full-tree checksum
- High performance architecture, includes thin provisioning, snapshots, storage optimization, replication, and encryption.

TrueNAS Core Plug-In

Asigra teamed up with iXsystems to offer an easy to install and manage Asigra Plug-In. The Asigra DS-System repository software runs natively on the TrueNAS controller – freeing up resources by not requiring the backup software to run on an external host.

Asigra Cloud Appliance

The Asigra Cloud Appliance is integrated with the Zadara Storage VPSA technology which looks, performs and behaves like an Enterprise NAS appliance. It's offered as a service on-premise, at your chosen colocation, or at public cloud providers (AWS and Azure).

To learn more about Asigra Tigris, contact us at 1-877-736-9901, or by email info@asigra.com.