How StoneFly Solutions Ensure

Ransomware Protection

For your mission-critical workloads

Most enterprise systems are built to deliver the bare minimum, forcing customers to invest more in third party data protection services for mission-critical workloads. However, StoneFly solutions come preconfigured with enterprise data protection features delivering high availability, business continuity, and advanced ransomware protection without any extra costs.

With StoneFly solutions, users can run and store enterprise-scale workloads, scale out seamlessly, and brush off cyber-threats like ransomware effortlessly.

Data Protection Features

Included in StoneFly HCI & backup & DR solutions

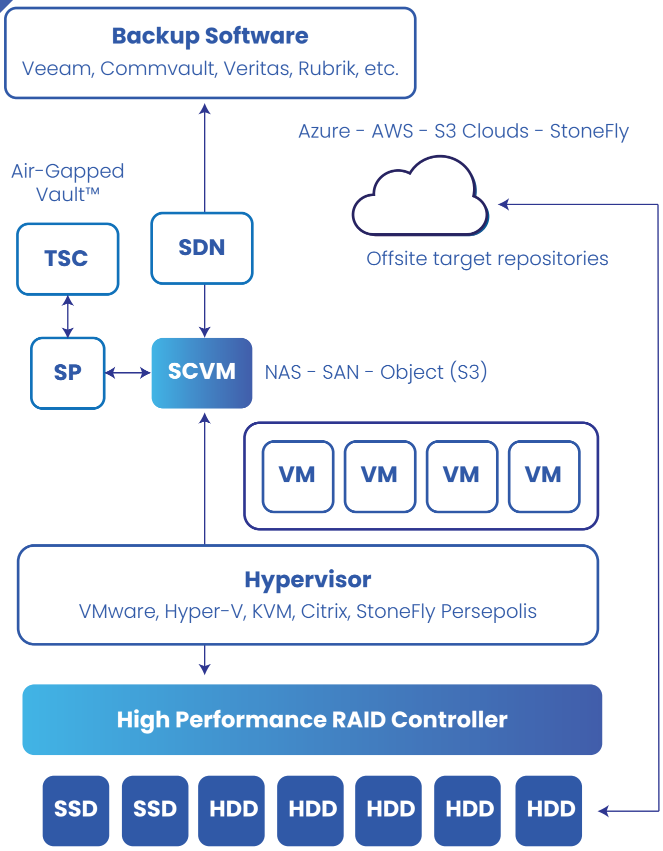
All StoneFly hyperconverged infrastructure (HCI) and backup and disaster recovery (DR) appliances come preconfigured with the following enterprise data protection features:

- Air-Gapped Vault™ & Air-Gapped Fabric™
- Backup Vault
- Immutable Delta-Based Snapshots
- Write-Once Read-Many (WORM) Repositories
- Threat Scan & Detection for Dormant Malware
- Anti-Virus & Anti-Ransomware for NAS Volumes
- S3 Object lockdown
- Advanced AES 256-bit Encryption

All data protection features are delivered using StoneFly's patented 8th gen storage OS (SCVM) which is pre-installed in all StoneFly appliances.

STONEFLY

Air-Gapped Vault™ & Air-Gapped Fabric™


Backup Software
Veeam, Commvault, Veritas, Rubrik, etc.
Azure - AWS - S3 Clouds - StoneFly
Air-Gapped Vault™
TSC
SDN
Offsite target repositories
SP
SCVM
NAS - SAN - Object (S3)
VM
VM
VM
VM
Hypervisor
VMware, Hyper-V, KVM, Citrix, StoneFly Persepolis
High Performance RAID Controller
SSD
SSD
HDD
HDD
HDD
HDD
HDD

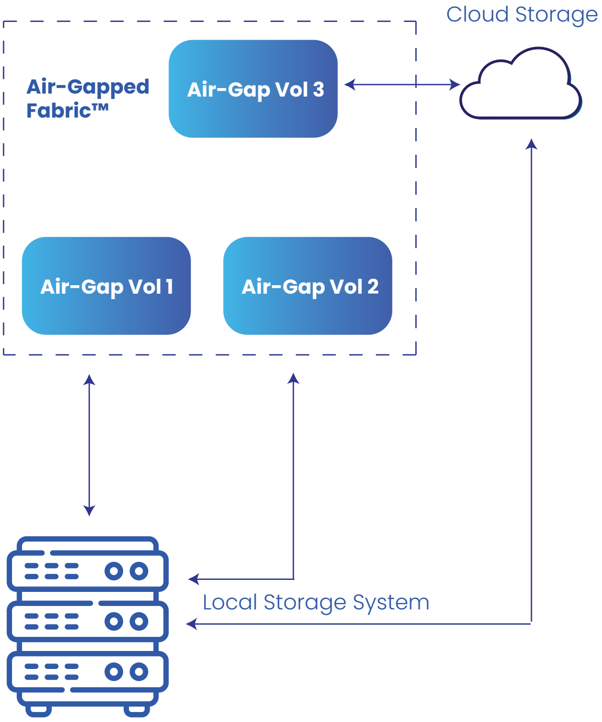
StoneFly SCVM enables users to provision detachable air-gapped vault volumes, on an isolated network. These highly secure target repositories run independently from the production network and can be turned “on” and “off” as per user defined policies.

In the event of data corruption or malicious encryption via ransomware, the Air-Gapped Vault ensures that users have another copy on a secure network available to recover data and restore operations effortlessly.

With StoneFly SCVM, users can choose to deploy air-gapped vault(s) locally, on an offsite storage, or in the cloud of their choice.

Air-Gapped Fabric unifies data management for air-gapped vaults and integrated data services deployed across multiple platforms.

The goal of air-gapped fabric is to provide seamless accessibility and control over air-gapped vaults - whether they’re deployed locally, in the cloud, or in a hybrid setup; simplifying data management and ensuring advanced data protection with minimum time and resource investments.



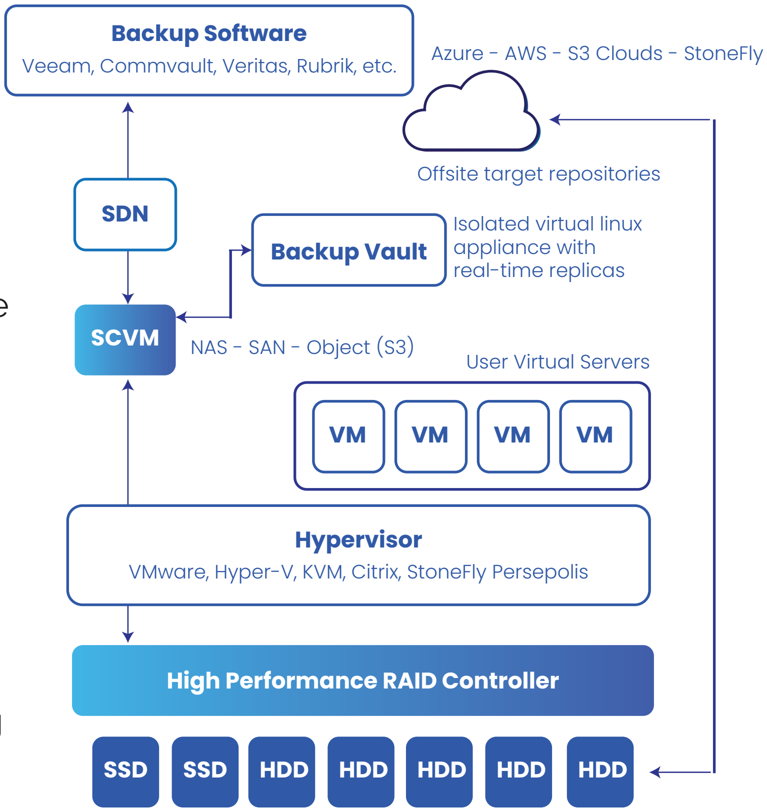
Backup Vault

With StoneFly SCVM, users can deploy an isolated virtual Linux appliance on a secure network independent of the production environment. When turned "on" the backup vault replicates and stores all preconfigured critical volumes.

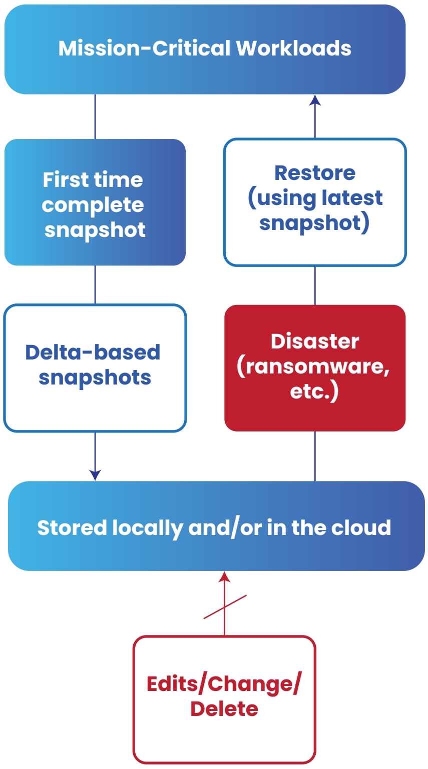
In the event of a disaster, users can spin up or turn "on" the backup vault to retrieve replicas and restore critical operations within minutes.

Similar to the air-gapped vault, the backup vault is detachable and can be turned "off" as per user defined policies.

By using the backup vault, users can effectively reduce Recovery Time and Point Objectives (RTPOs) while complying with industry regulations - all within their budgets.


Backup Software
Veeam, Commvault, Veritas, Rubrik, etc.
Azure - AWS - S3 Clouds - StoneFly
Offsite target repositories
SDN
Backup Vault
Isolated virtual linux appliance with real-time replicas
SCVM
NAS - SAN - Object (S3)
User Virtual Servers
VM
VM
VM
VM
Hypervisor
VMware, Hyper-V, KVM, Citrix, StoneFly Persepolis
High Performance RAID Controller
SSD
SSD
HDD
HDD
HDD
HDD
HDD

Immutable Delta-Based Snapshots


Mission-Critical Workloads
First time complete snapshot
Restore (using latest snapshot)
Delta-based snapshots
Disaster (ransomware, etc.)
Stored locally and/or in the cloud
Edits/Change/ Delete

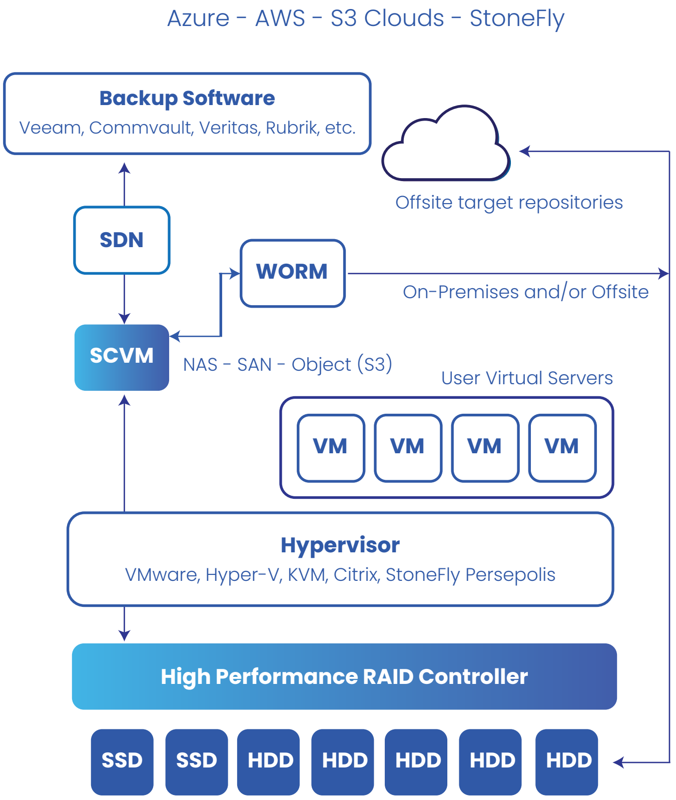
By using the immutable snapshots feature of StoneFly SCVM, users can secure mission-critical volumes from ransomware and other disasters like production hardware failure, human error, etc.

SCVM takes change-based snapshots to save up on storage consumption and speed up the process.

In the event of a disaster, users can restore data by using the latest snapshot.

As the snapshots are immutable, ransomware cannot edit, delete, or encrypt them - making them a reliable means of ransomware protection and data recovery.

Write-Once Read-Many (WORM) Repositories



Azure - AWS - S3 Clouds - StoneFly

Backup Software
Veeam, Commvault, Veritas, Rubrik, etc.

Offsite target repositories

SDN

WORM

On-Premises and/or Offsite

SCVM

NAS - SAN - Object (S3)

User Virtual Servers

VM VM VM VM

Hypervisor
VMware, Hyper-V, KVM, Citrix, StoneFly Persepolis

High Performance RAID Controller

SSD SSD HDD HDD HDD HDD HDD

In order to comply with industry regulations such as HIPAA, HITRUST, FedRAMP, and CJIS, data owners need to store critical data in secure volumes that limit access to approved usergroups. With StoneFly SCVM WORM feature, users can do just that.

WORM repositories, as the name suggests, are target storage volumes that enable reads but limit writes, edits, and deletion based on user-defined policies.

SCVM enables users to provision WORM locally on StoneFly appliances, in the cloud of their choosing, or in both (hybrid storage).

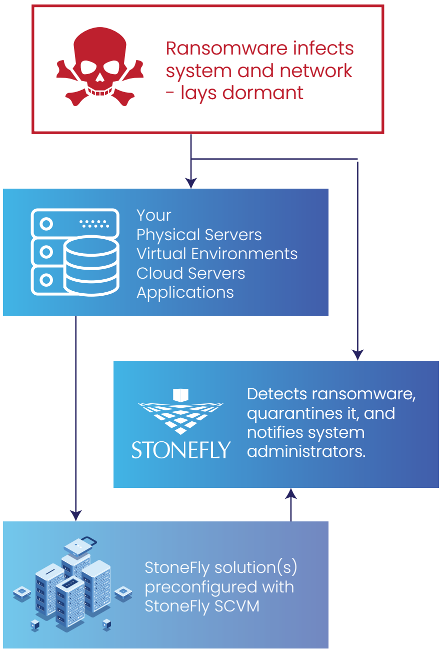
Data stored in these volumes is safe from ransomware attacks as it cannot be edited and therefore cannot be maliciously encrypted.

Threat Scan for Dormant Malware

Advanced ransomware threads are programmed to stay dormant, learn user behavior, and then "attack" when it has enough information. With information about target repositories and backups, such ransomware tend to be more devastating. However, StoneFly equips you with the means to detect and remove such dormant ransomware with ease.

Users can schedule regular threat scans which use advanced AI to detect any dormant malware threads. In the event of detection, the malicious software is quarantined and system administrators are notified.

Users can choose to schedule threat scans daily, weekly, or monthly.



Ransomware infects system and network - lays dormant

Your
Physical Servers
Virtual Environments
Cloud Servers
Applications

STONEFLY

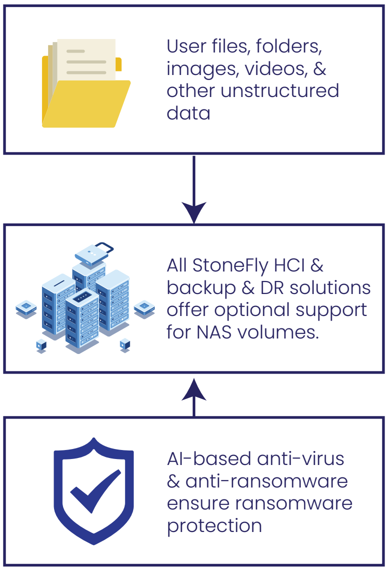
Detects ransomware, quarantines it, and notifies system administrators.

StoneFly solution(s) preconfigured with StoneFly SCVM

Anti-Virus & Anti-Ransomware for NAS Volumes

Protect your files, folders, and other unstructured workloads stored on StoneFly appliances with built-in anti-virus and anti-ransomware.

The anti-virus and anti-ransomware in StoneFly appliances is regularly updated with information about latest virus and ransomware threads making it capable of detecting and neutralizing advanced threads before they "attack".

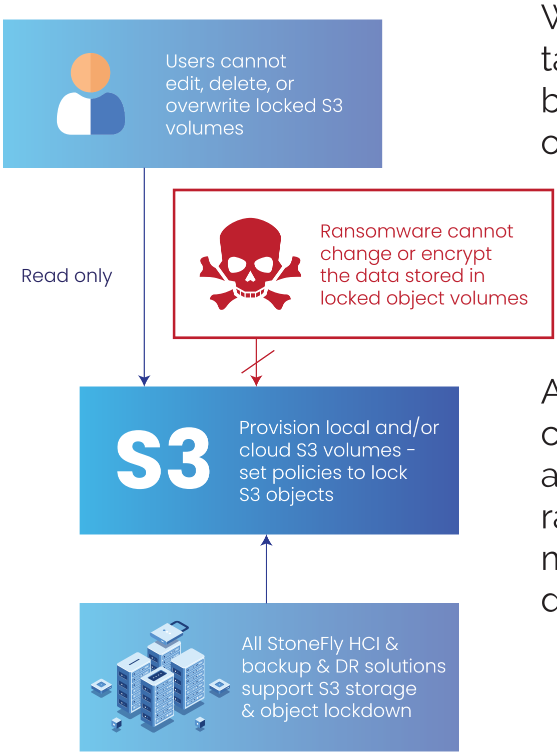


User files, folders, images, videos, & other unstructured data

All StoneFly HCI & backup & DR solutions offer optional support for NAS volumes.

AI-based anti-virus & anti-ransomware ensure ransomware protection

S3 Object Lockdown



Users cannot edit, delete, or overwrite locked S3 volumes

Read only

Ransomware cannot change or encrypt the data stored in locked object volumes

Provision local and/or cloud S3 volumes - set policies to lock S3 objects

All StoneFly HCI & backup & DR solutions support S3 storage & object lockdown

With StoneFly SCVM, users can provision S3 object target repositories and "lock" them so that they cannot be edited, deleted, or overwritten for a specified period of time.

Similar to the WORM model, S3 object lockdown especially helpful for organizations looking for compliance.

Additionally, as S3 objects, when locked, cannot be changed - they also provide a line of defense against threats like ransomware, human error, malicious deletion, and other disasters.

Advanced AES **256**-bit Encryption

All StoneFly appliances offer military-grade AES 256-bit encryption capabilities. By using StoneFly solutions, enterprise customers can rest assured that their mission-critical workloads are safe from unauthorized access and from cyber-threats such as ransomware, etc.

Get Solutions You Can Rely On

Contact us to schedule a demo or to learn more about our HCI and backup & DR solutions:

Email:	sales@stonefly.com
Phone:	+1 (510) 265-1616

About StoneFly, Inc.

StoneFly Inc., headquartered in California, was founded to deliver upon the vision of simple and affordable storage optimization and disaster recovery protection through IP SAN solutions. StoneFly is a leading manufacturer of high-performance network-attached storage (NAS), storage area networks (SAN) – iSCSI systems, hyperconverged systems, and RAID systems.

StoneFly's range of enterprise products also includes cloud storage solutions, cloud storage gateway solutions, and data migration services for enterprise workloads.

STONEFLY