STONEFLY

FAQs | Ransomware

Q & A about ransomware and how to protect critical data from them.

Inside this document:

- What is ransomware?
- How to prevent ransomware?
- What is the 3-2-1 backup rule?
- How to add air-gapping and immutability?
  And more!

What is Ransomware?

Ransomware is a malware that encrypts sensitive files, such as Personally Identifiable Information (PII), Protected Health Information (PHI), financial information, etc. and connected storage devices by infiltrating an organization's network using entry points such as phishing emails, operating system or software vulnerabilities, etc. Once the data is successfully encrypted, the cyber criminals demand ransom in return for a decryption key.

Most ransomware attacks today target production and backup files, encrypting them, leaving no choice for the organization but to pay the ransom.

How to Prevent Ransomware?

The best way to prevent ransomware is by being prepared before-hand. Having a solid defense helps with ransomware prevention. This includes having an automated air-gapped and immutable backup and disaster recovery (DR) strategy.

Data protection features such as immutable backups, air-gapped backups, delta-based snapshots, S3 object lockdown, file lockdown, and anti-ransomware ensure your backups are protected even if your production and network are compromised.

With StoneFly's Veeam-ready backup and DR solutions, you can get all of these features and instant recovery at-scale with features such as direct VM spin up and granular file-level recovery for any workload - which provides the much-needed diversity to the business in terms of ransomware protection and recovery from ransomware.

What is the 3-2-1 Backup Rule?

The 3-2-1 backup rule recommends that there should be at least 3 copies of data, stored on 2 different types of storage media with 1 copy stored offsite.

While the 3-2-1 backup rule is an old one, it still works as long as it's implemented properly. To add more reliability to it, you can improve it to the 3-2-1-1-0 rule which adds an air-gapped and immutable backup copy, and requires administrators to ensure that there are zero errors with the backup data.

For more information on the 3-2-1 backup rule, read StoneFly blog: https://stonefly.com/blog/maximize-data-protection-3-2-1-rule

How Does StoneFly Help You Protect Your Data and Backups from Ransomware Attacks?

StoneFly provides complete turnkey Veeam-ready backup and DR with automated air-gapping and immutable backups with integrated data services. The backup and DR solution allows you to automate ransomware protection for your physical/virtual servers and cloud workloads, and store backups, snapshots, and replicas on-prem, in a cluster, and/or in the cloud.

StoneFly DR365V allows users to host Veeam software on the same appliance enabling them to run agentless backups for virtual workloads reducing bottlenecks, ensuring security for backup jobs, and facilitating faster backups, replication, and snapshots.

The ability to automate backups, quickly recover data using these backups, and protect said backups from ransomware using air-gapping and immutability makes StoneFly backup and DR solutions the go-to choice for government departments such as US Navy, US department of homeland security, US department of defense, and market leaders such as Wells Fargo, Disney, and more.

How Exactly Does StoneFly Help You Recover from any Cyberattack in Minutes?

To ensure effective and seamless ransomware recovery, StoneFly provides:

- Automated air-gapped and immutable backups, with S3 object lockdown and file lockdown, on-premises and/or in the cloud protecting your critical backups, snapshots, and replicas from ransomware infection even if your production and backup server(s) are compromised.
- Built-in backup data integrity checks make sure that your backups and snapshots are not corrupted and can be used at any time to recover your critical workloads.
- Shorter recovery time objectives (RTOs) and recovery point objectives (RPOs) with data recovery features such as direct VM spin up, granular file-level recovery, and direct restore to cloud.
- Isolated virtual sandbox environment to restore backup data and scan for dormant malware (sleeper ransomware) without impacting production or backup server(s).
- Backup and DR orchestration to test and execute DR plans for physical/virtual servers, applications, and databases with a single click.

What Specific Ransomware Protection Features are a Must-Have?

Cyber criminals are continuously finding new ways to infiltrate corporate networks and maliciously encrypting important data. As a result, there's no "cure-all" for ransomware attacks. However, there are a number of features and best practices that can ensure effective ransomware protection and facilitate quick recovery from ransomware.

Must-have ransomware protection features:

- Air-gapped backups: Isolated and detachable target storage volumes that are on a separate and secure network, inaccessible via the primary production network.
- Immutable storage: Target storage volumes that leverage the Write-Once Read-Many (WORM) model to prevent overwriting, editing, and deletion for a user-defined period of time. Immutable storage features include S3 object lockdown and file lockdown.
- Delta-based immutable snapshots: Scheduled change-based volume-level snapshots that are stored in air-gapped and immutable volumes so that they cannot be maliciously encrypted and can be used to recover operations when/if all else fails. Delta-based snapshots are faster as they create incremental snapshots of the changes rather than the complete volume.
- Anti-ransomware: Automated AI-based detection and removal of dormant malware (sleeper ransomware).
- Backup Data Integrity Checks: Regular automated backup data integrity checks that orchestrate backup and DR to ensure backups are not corrupted/encrypted and can be used at any time to recover your critical workloads.

Best practices to prevent ransomware infection and downtime:

- Multi-Factor authentication (MFA): Protect your admin access from brute-force attacks by leveraging MFA.
- Backup Strategy: To effectively utilize your backup and DR solution(s) make sure that they follow a backup strategy such as 3-2-1, 3-2-1-1-0, or 4-3-2.

To differentiate between 3-2-1, 3-2-1-1-0, and 4-3-2 backup strategies read StoneFly blog:
https://stonefly.com/blog/3-2-1-vs-3-2-1-1-0-vs-4-3-2-backup-strategies

Is a Ransomware Attack as Disastrous as a Flood or Fire? Are There Any Additional Protective Measures that Could Help Protect Business/ Employee/Customer Data?

Natural disasters, such as floods, earthquakes, hurricanes, etc. are capable of taking out your production, on-prem backup server(s), and connected/shared storage devices. While ransomware does not affect the hardware directly, it has the ability to cause similarly devastating disruption and downtime.

StoneFly, together with Veeam, provide you an array of disaster recovery capabilities that enable you to reduce downtime to near-zero and minimize data loss. The built-in DR features include:

- **Data recovery:** Instant VM recovery, granular file-level recovery, and direct restore to cloud.
- **DR testing:** Orchestrate and test DR plans to ensure faster recovery in the event of a (real) disaster.
- **Clustering:** Leverage dual-node clustering with automated failover and failback for high availability and near-zero downtime.

Do I Need to Protect Microsoft Office 365 Environments from Ransomware?

Microsoft makes sure that your office 365 data is highly available. However, protecting your data from ransomware, data corruption, virus, and human error is your responsibility. This is what Microsoft calls the "shared responsibility" model.

High availability means that regardless of what "state" your office 365 data is in, Microsoft will make sure that you can access it anytime and from anywhere. In order to do so, they use geo-replication across servers and regions.

To make sure that you do not lose your important emails, files, and documents, it's necessary to set up backup and DR for office 365 which follows a backup strategy such as 3-2-1, 3-2-1-1-0, or 4-3-2.

Is Cloud Technology Safe from Ransomware? If Not, How to Keep it Safe?

Just because it's in a highly available cloud storage, does not mean your data is safe from ransomware. Cyber criminals attempt to steal admin credentials to your cloud accounts with brute force attacks and ransomware are programmed to infect not just your production but also connected storage repositories; which includes integrated cloud storage.

With StoneFly's solutions, you can choose to set up backups for your cloud storage volumes and store backups, snapshots, and replicas on-prem and/or in the cloud in a hybrid or multi-cloud environment. StoneFly solutions are vendor agnostic and work with Windows/Linux servers, SAN, NAS appliances, VMware, Hyper-V, KVM, and Citrix (formerly XenServer) virtual environments, and Azure and AWS public clouds.

How to Add Air-Gapping and Immutability to Existing Environment(s)?

StoneFly offers vendor-agnostic physical, virtual, and cloud-based air-gapped and immutable storage solutions that provide a "plug and play" experience. In addition to easy integration, our customers can choose to set up double or triple layered immutability which helps with data security, compliance, and cyber insurance requirements.

Air-gapped and immutable storage solutions by StoneFly:

- **DR365 Veeam-Immutable Veeam-Air-Gapped (VIVA) Nodes:** Physical air-gapped and immutable nodes with automated network and power management purpose-built for Veeam with optional support for popular backup software such as Commvault, Rubrik, Zerto, Quest, and more.
- **StoneFly SCVM™:** Our 8th gen patented storage controller enables you to reclaim and repurpose unused storage resources and provision virtual air-gapped and immutable storage volumes on-prem. StoneFly SCVM is compatible with VMware, Hyper-V, KVM, Citrix (formerly XenServer), and Nutanix AHV.

- **Cloud storage in Azure:** Integrate air-gapped and immutable cloud storage in Azure with your backup software, applications, databases, servers, SAN and NAS appliances. Protect your critical data with automated policy-based air-gapping and immutable storage features such as S3 object lockdown and file lockdown, on-prem and/or in the cloud.

Regardless of which solution you choose, StoneFly experts work with you to customize it for your environment so that you can get the best ransomware protection, high availability, scalability, ease-of-use, and affordability.

What does Veeam Ready Mean?

The Veeam Ready Program provides a solution qualification process to help Veeam Alliance Program partners meet Veeam functional and performance standards.

By attaining Veeam Ready status, customers are assured that storage solutions are compatible with Veeam Backup & Replication features.

Which Veeam Ready Qualifications do StoneFly Solutions Have?

StoneFly backup and DR solutions have been tested by Veeam and validated as:

- **Veeam-Ready repository:** All Veeam backup, replication, & restore features supported. (Listed on Veeam ready database: https://www.veeam.com/kb3241)
- **Veeam-Ready object:** S3-object compatible target storage for Veeam backups. (Listed on Veeam ready database: https://www.veeam.com/kb4052)
- **Veeam-Ready Object with Immutability:** Object storage immutability for critical Veeam backups. (Listed on Veeam ready database: https://www.veeam.com/sys321)

Which StoneFly Product(s) Should I Explore to Protect my Data from Ransomware?

StoneFly offers a diverse portfolio of affordable, secure, highly available, and scalable backup and DR solutions including physical, virtual, and in the public/private cloud.

Our pre-sales engineers work with you to custom-build a solution that works for your requirements and is within your budget.

Physical ransomware protection solutions include:

- **StoneFly DR365V:** 4 to 60-bay Fully automated Veeam-ready backup and DR physical appliance with air-gapping, immutable backups, S3 object lockdown, file lockdown, integrated data services and SAN, NAS, cloud-native S3 object storage.
- **StoneFly DR365VIVA:** 4 to 60-bay Purpose-built fully automated immutable and air-gapped backup and disaster recovery node for Veeam backup environments with integrated policy-based network and power management.
- **StoneFly miniBackup:** Affordable plug and play backup and DR appliance with terabytes of storage on-prem with RAID, optional cloud support, and optional round robin backups for air-gapping and ransomware protection. Best fit for small businesses with 10-20 VMs and/or desktops, remote branches, and employees working from home.

Virtual ransomware protection solution:

- **StoneFly SCVM ™:** Reclaim and repurpose unused storage resources to air-gapped and immutable storage using our patented 8th gen storage controller compatible with VMware, Hyper-V, KVM, Citrix (formerly XenServer) and with optional cloud support for Azure, AWS, StoneFly private cloud, and other S3-compatible public cloud(s).

Cloud-based ransomware protection solutions include:

- **Veeam cloud connect backup to Azure:** Leverage automated backups with Veeam and store backup data in StoneFly's air-gapped and immutable storage in Azure using built-in management server and secure encrypted tunnel. In the event of a disaster, restore directly to the cloud for shorter RTOs and RPOs.

- **Veeam cloud connect backup and replication to StoneFly cloud:** Automate backup and replication to air-gapped and immutable repositories in StoneFly private cloud using built-in management server and secure encrypted tunnel. Directly spin up VMs in StoneFly private cloud for cloud disaster recovery and/or directly restore to StoneFly cloud in the event of primary hardware failure.

- **StoneFly CDR365:** Automated cloud backup and restore with centralized browser-based management for virtually unlimited remote users. Store backups on-prem and/or in the cloud and restore remotely to similar/dissimilar hardware. Best fit for managed service providers (MSPs), small businesses, and remote teams.

To choose which one is right for your business, contact StoneFly pre-sales engineers at sales@stonefly.com.

About StoneFly, Inc.

StoneFly, Inc 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, backup and disaster recovery solutions 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.