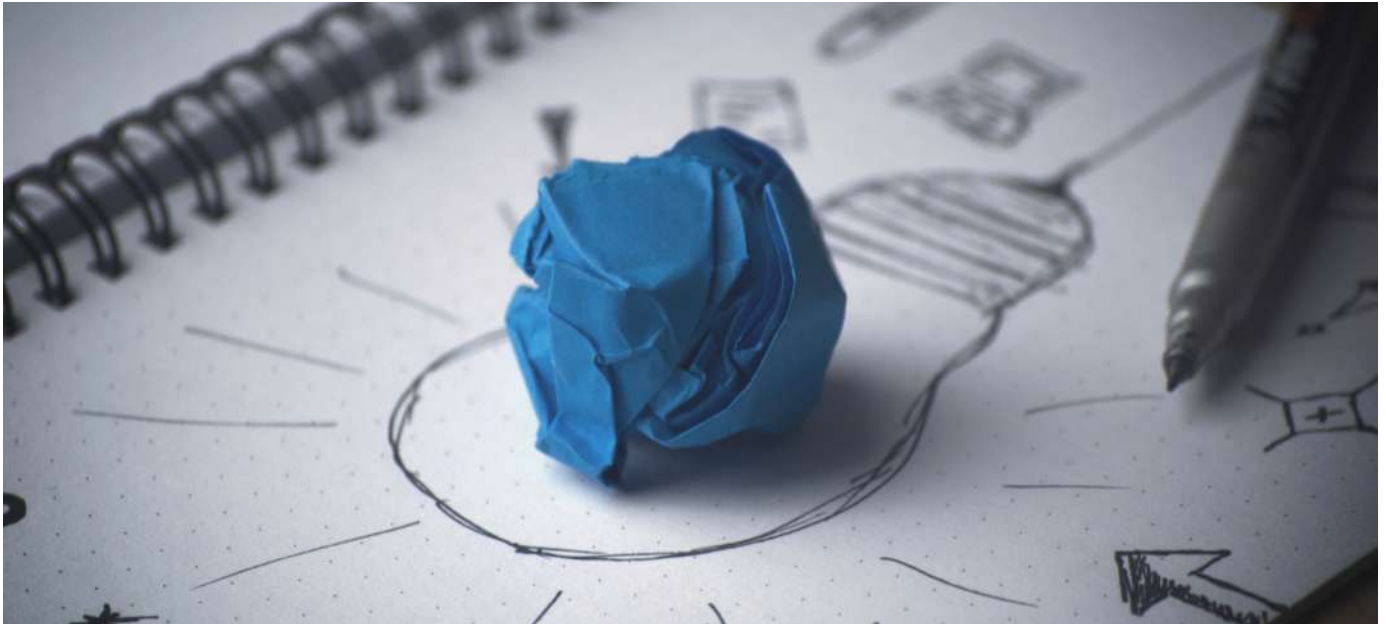# StoneFly DR365V Protects Engineering Manufacturer from Ransomware

ORGANIZATION

A US-based manufacturer and fabricator of engineered material solutions established in 1951 with 11 locations in the United States, Canada, Mexico, and China.

INDUSTRY

Engineering and Manufacturing

Challenges

In order to protect their business-critical data and multiple locations from ransomware attacks, the engineering company was looking for a solution that was able to support their large-scale VMware deployment, terabytes of data, and multiple locations.

The task of securing multiple endpoints, reducing Recovery Time Objectives (RTOs), and minimizing Recovery Point Objectives (RPOs) is challenging to say the least. Furthermore, building an infrastructure that can do all of the above and still be in the desired budget adds to the challenge.

"We knew we needed a solution that could support virtualization-at-scale, meet performance requirements, and make sure our data was safe from ransomware, hackers, and data breaches" said Jose, the data center administrator of the engineering company.

Solution

StoneFly Veeam-ready backup and disaster recovery (DR) appliance (DR365V) was selected by the company after verifying that it fulfilled their performance requirements, provided data protection capabilities their business could depend-on and was within their budget.

"What stood out to us was the air-gapped and immutable storage capabilities in addition to the Veeam backup support. And the fact that we could custom-build it to our needs within our budget made it the obvious choice" noted Jose.

In addition to ensuring ransomware protection, the engineering company can also run their high performance VMware workloads on the DR365V, set up failover clusters for instant recovery, and leverage storage optimization capabilities such as deduplication, thin provisioning, automated hot/cool storage tiering, and more.
"The capabilities that came with DR365V as part of the standard license were a pleasant surprise. We definitely got great value for money and are happy that we made the decision to choose DR365V" said Diana, the Chief Technology Officer of the company.

Challenges

The engineering company was looking for a reliable ransomware protection that can protect their large-scale VMware environment and multiple locations and ensure business continuity seamlessly.

Solution

StoneFly Veeam-Ready backup and DR appliance (DR365V) with built-in air-gapping, immutable WORM, anti-ransomware, and clustering with automated failover and failback.

The Results

- Reliable and compliant ransomware protection for multiple locations.
- Ability to quickly restore data after any disaster such as ransomware attack, hardware failure, human error, etc.
- Automated failover to secondary appliance in the event of a disaster.
- Manage backup and DR for all locations using a centralized management interface.

The Results

Quick Recovery from Ransomware Attack

Earlier in October 2021, the engineering company's hypervisor was maliciously encrypted by a ransomware attack. As a result, terabytes of critical business data and virtual machines (VMs) running on it were rendered inaccessible.

However, the company did not lose any data and was able to quickly recover from the ransomware. Even though the primary production data and backups were encrypted, the air-gapped backups were safe and untouched.

After restoring their VMware hypervisor, StoneFly's technical team worked with the engineering company to restore their emails and all their data seamlessly.


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.

Write-Once Read-Many (WORM) Volumes

With features such as file lockdown and S3 object lockdown, the engineering company is able to set up immutable WORM storage volumes on-premises and/or in the cloud. The data stored in these volumes cannot be edited, deleted, or overwritten for a user-defined period of time. This also makes these volumes ransomware-proof as the malware cannot access and encrypt data stored in them – in turn helping compliance.

Delta-Based Immutable Snapshots

In addition to the ability to go back in time and restore previous system state, the delta-based snapshots are quicker, require less performance resources, and consume less storage capacity. Furthermore, immutable snapshots, similar to WORM volumes, cannot be edited, deleted, or overwritten for a user-defined period of time.

Moreover, StoneFly DR365V enables users to set up storage snapshots in addition to granular file-level snapshots – delivering more control to data center administrators and helping them build a customized data protection strategy.

Ransomware-Proof Data Storage

The engineering company is able to leverage the DR365V appliances deployed at different locations to set up failover clusters. If the primary appliance is offline, due to a hardware failure; maintenance; or natural disaster, the system automatically failover to the secondary appliance so that the business continues to operate.

Each DR365V appliance also supports hardware RAID and erasure coding which enhance performance and add another layer of fault-tolerance to each node.
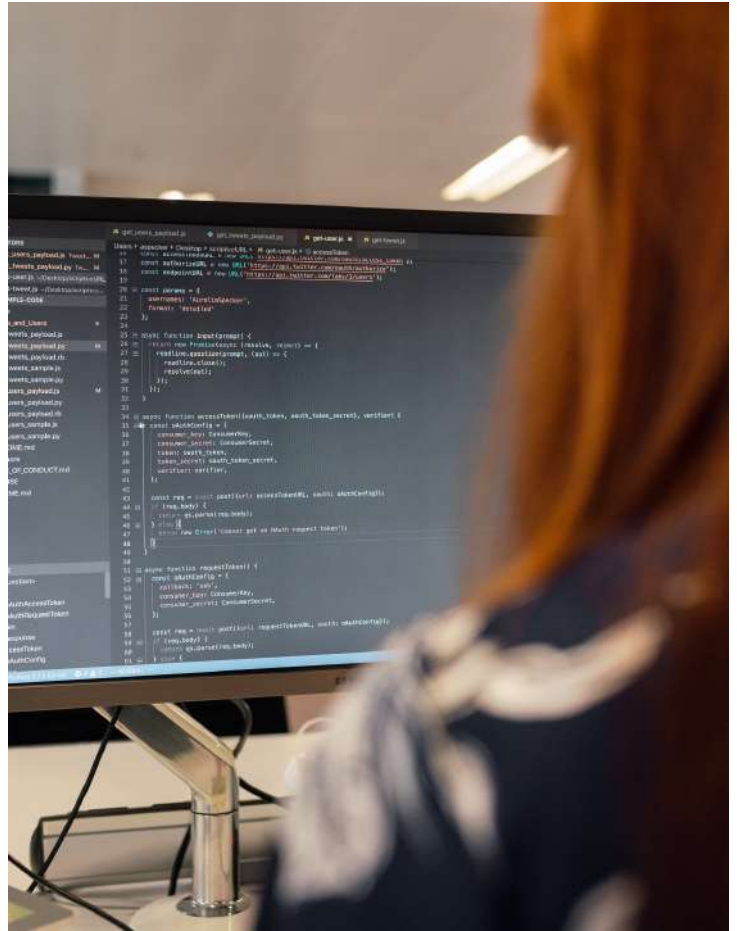
Looking to set up reliable ransomware protection? Contact Us!

Email: sales@stonefly.com

Phone: +1 510 265-1616