Save millions - Protect your mission-critical workloads Effectively

Ransomware is a real threat - Setup Data Protection before not after an attack

While ransomware is acknowledged as a real threat globally - many enterprises large and small, government agencies and even entire cities are ill-prepared to fend off a ransomware attack. Without appropriate means to recover their mission-critical workloads, IT environments rack up huge recovery costs in the event of a ransomware attack.

Security experts advise not to pay the ransom, when data is compromised due to a ransomware attack. That's because more than 50% victims who pay up don't recover their data anyway; often because the malware authors botch the decryption code. In other words, the only way to ensure that mission-critical workloads are always recoverable is to setup enterprise-level backup and disaster recovery (DR) solutions before a ransomware attack.

Why StoneFly

Simply because we're the best at what we do. StoneFly's enterprise-level products have been deployed in all Microsoft commercial and government datacenters worldwide. StoneFly's products have also been deployed in US Navy Littoral Combat Ships (LCS) and Virginia Class Nuclear Submarines.

Ransomware Attack - Costs Atlanta over $10M

In April 2018, the city of Atlanta, Georgia, USA ended up being a victim to "SamSam" ransomware. The city decided not to pay the $51, 000 ransom in bitcoin and decided to recover their data. Unfortunately, the city of Atlanta was ill-equipped to effectively recover their data. This attack has delivered a terrible to the city of Atlanta.

According to Atlanta's chief of Information Management, more than third of the city's 424 essential applications were affected by the attack while 30 percent of those supporting vital municipal functions like the court system and police department ended up as victims. Reports suggest that the City's Attorney office lost most of their computers (71/77) and an estimated 10 years worth of documents. While the police department lost all of their stored dash cam recordings.

This could've been avoided if Atlanta had DR365™

It's estimated that Atlanta will have to spend over $9.5 million over the next year to recover and an additional $2 million in recovery cost outlays from the first weeks after the attack. The totaly cost may even increase further as the city completes its cleanup and post-mortem analysis.

The disruption, data loss and the cost implications could've been avoided if Atlanta had chosen to setup their backups in StoneFly's innovative backup and disaster recovery appliance - DR365™.

StoneFly's proven expertise make it the primary choice for data protection of mission-critical workloads. DR365™ is a purpose-built appliance that ensures recoverability in the event of a ransomware attack, natural disaster, accidental/malicious deletion and other similar threats.

With DR365™ businesses can:

- ✔ Effectively ensure recoverability and high availability of mission-critical workloads

- ✔ Setup data protection on-premises and data redundancy on Microsoft Azure or AWS cloud(s)

- ✔ Scale-out or scale-up effortlessly and infinitely

- ✔ Reduce CapEx and OpEx costs of backup and DR overall

- ✔ Ensure data security with advanced encryption technology

- ✔ Setup backup and DR that is compliant to a number of industry regulations

- ✔ Ensure business continuity with reduced RTOs and RPOs

- ✔ Easily access and manage on-premises infrastructure and backup resources setup in the cloud with a simple to use and user-friendly software

DR365™ enables IT environments to setup backups in Azure datacenters worldwide

StoneFly's solutions are trusted by 500, 000 businesses worldwide

DR365™ delivers immutable snapshots and encryption making ransomware attacks - a mere inconvenience

Easy advanced Data Protection for Enterprise Workloads

Data protection hasn't always been simple. Ten years ago it was nothing short of a nightmare - rebuilding servers and restoring lost data. It was difficult, time-consume and prone-to-errors even for IT experts. In that time, backups used to be measured in MBs and companies could go for hours or even days without data.

Today, it's a lot different. Data volumes are increasing at an exponential rate while businesses require recovery times to be reduced to minutes. Legacy infrastructure might be working today but can they really keep up with the growing demands of enterprise IT environments? No, they can't keep up; they're struggling as it is.

Now with the large volumes of data, simplicity, speed and scalability are very important. IT environments simply cannot waste time and availability gaps are far more dangerous to businesses now. StoneFly has designed DR365™ with these requirements in mind. That makes the backup and DR appliance capable of delivering a number of benefits to the enterprise IT environment, some of them are:

Easy setup - DR365™ is a plug and play device. It's fully-featured and is easy to setup and deploy. With the user friendly guide and manual, IT environments can have their DR365™ appliance up and running within an hour.

Easy restore - The appliance provides a simple-to-use software that enables data restoration as easy as pie. This simplicity saves time for IT administrators and enables them to stay focused on the core business operations.

Easy reporting - Reporting is necessary; however, manual backup reports consume hours to prepare in an enterprise environment. DR365™ makes it easy by making reporting automated and customizable.

Easy troubleshooting - DR365™ provides customizable widgets in its dashboards. This is important when something goes wrong, that's because these dashboards provide a clear picture of the protected environment. Using the web console, IT admins can see what's backed up, how often and how much data they have and how much space is left on the backup and DR appliance.

What should you do now

As you can see, having an easy and reliable backup and DR really means you can do more. It enables increased productivity and reduced risk of data loss, which is very important in today's business environment.

Instead of waiting for a ransomware attack, setup purpose-built backup and DR for your mission critical workloads beforehand. To acquire and setup our enterprise-level backup and DR solution give us a call or send us an email and let us offer you with a full-featured and custom-built backup and disaster recovery solution.

About StoneFly

StoneFly, Inc. (StoneFly) was founded as a venture-backed startup in April, 2006 to deliver on the vision of simple and affordable storage optimization and disaster recovery protection through IP Storage Area Network (IP SAN) solutions.Based in California, StoneFly is a subsidiary of Dynamic Network Factory, Inc. (DNF), a leading maker of high performance network attached storage (NAS), storage area networks (SAN), RAID and iSCSI systems.

In addition to IP Storage Solutions, StoneFly has developed a series of Unified Storage and Server (USS™) and Unified Scale-Out (USO™) NAS products, providing a one stop solution to datacenter sprawl. StoneFly is a member of the Storage Networking Industry Association (SNIA) and a founding member of the IP Storage Institute (IPSI).

Corporate Headquarters:

Address: 26250 Eden Landing Rd.
Hayward, CA 94545,
USA.

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

STONEFLY
www.stonefly.com
www.iscsi.com