DataKeep™

SECURITY BULLETIN

The most effective Ransomware Recovery solution!

Ransomware (via Wikipedia) "***Ransomware*** *is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.*"

"Ransomware attacks are typically carried out using a Trojan that is disguised as a legitimate file that the user is tricked into downloading or opening when it arrives as an email attachment. However, one high-profile example, the "WannaCry worm", traveled automatically between computers without user interaction."

According to the US Department of Homeland Security (DHS) - the only effective way to mitigate a Ransomware attack is with an effective backup/restore capability or Disaster Recovery plan enabled.

There are 2 aspects to this definition of a Ransomware attack:

1. Encrypting or wiping (wiperware) your data to restrict your access until a ransom is paid
2. Threatening to expose your data if it the ransom is not paid …. which implies that they were successful in exfiltrating (copying via hack) your data to another location

Further - if someone gets a Trojan or malicious software into your network, past your firewall, anything within your network - including backup storage - would most likely be affected.

So – what to do? How can each of these threats be mitigated?

Let's start with the exfiltration (hack) of your data. You need a strong data-centric solution that couples encryption with access controls, logging, auditing, will render the data useless to the hacker.

The second step, back to the point made by DHS – is the need for a strong backup/restore solution - that houses a copy of your data OUTSIDE your network.

DataKeep can help in both cases – Ransomware Recovery

DataKeep is an integrated data-centric solution suite that provides all the tools one needs to significantly reduce risk associated with digital data - as well as keep costs under control with a single integrated solution. Ransomware mitigation and recovery is right in DataKeep's wheelhouse.

First: Protect your data with the DataKeep Agents: File with Policy, Volume, and Volume with Policy. With the ability to include Role Based Access Controls (RBAC), Privileged Access Management (PAM), process controls, and logging for auditability - these agents provide the basis for data-centric protection - regardless of location on-premise, remote, or in a cloud environment.

Second: Each of these agents includes a native backup/restore capability that provides security from the active server environment through, to, and including in your backup storage environment. Options include either a full or incremental backup (just what has changed since the last backup) - it is efficient and can be setup as a recurring job at intervals chosen by the customer to optimize backup coverage while minimizing operational impacts.

Third: Where is the best place to store your backup? Best Practices indicate that the backup storage should be located outside the operational network used for day to day business to avoid the risk of Ransomware contamination. Such a location could be on-premise, but on a different network; a remote data-center, or in a cloud environment. This last alternative, a cloud, is a particularly attractive solution given its remoteness and separate firewall - and DataKeep's Object Store Agent provides the best alternative by securing your backup prior to storage and giving you the flexibility to use any S3 compatible object storage environment. If using a cloud, DataKeep's OSA also can shard the data with resiliency. For example - sharding the data into 3 shares that can each be stored in a different cloud - but only needing any 2 of them to restore the data. This has the advantage of avoiding cloud vendor lock-in, while providing low-cost backup storage.

In summary

You can finally leverage the low-cost of object storage in the cloud with the trust needed to assure data privacy and resiliency with DataKeep and its Object Store Agent. Low cost backup/restore, and leading ransomware recovery capabilities are at hand.

SecurityFirst™ delivers data-centric solutions that address the high-profile cyber threats facing organizations today, such as data breaches, ransomware and cloud security. We emphasize protection of the data itself to serve as your last line of defense. Data is always protected no matter where it resides and recoverable in the event of an unexpected failure or malicious attack. As organizations and governments mandate stricter requirements for data privacy, SecurityFirst helps protect data from compromise and exposure.

DataKeep™, by SecurityFirst, secures critical data at its core to deliver unrivaled protection, control and resiliency. Customer-defined access policies, strong encryption and event logging combine with native secure backup/restore capabilities to address your data privacy, compliance and recovery needs. Organizations can utilize the backup and restore capabilities with object storage for secure cloud backup and archiving to improve resiliency and enable prompt recovery of archived data in the event of a ransomware attack.

SecurityFirst™
Data-Centric Cyber Solutions

For a product demonstration or more information call
1-888-884-7152
securityfirstcorp.com

80-20679-000 Rev. A0