> Solution Brief

DATATRUST SOLUTIONS

Ransomware Security using Secure Archive Manager

Rethinking your approach to defend against Ransomware…

Ransomware continues to threaten the data of organizations big and small. It can encrypt files and hold the decryption key until the ransom is delivered by the user being attacked. This type of malware is now responsible for payments in the billions of dollars in extortion each year.

What is Ransomware?

Ransomware is a type of malware that prevents or limits its victims from accessing their personal data and forces them to pay ransom to get it back.

Most ransomware attack by encrypting files and force its victims to use online currencies like Bitcoin to pay the ransom. Keep in mind there's no guarantee you'll get your files back if you pay, it will just encourage more ransomware attacks. Even worse, there have been instances where the ransom gets paid, and the attacker still damages or even destroys the files anyway.

"34 percent of businesses hit with malware took a week or more to recover full access to their data." - Kaspersky

How dangerous can a Ransomware attack be?

On August 16th, 2019, 22 Texas municipalities became victims of ransomware attacks that halted business and financial operations for several cities. Here are some important facts about this attack:

- Months after the attack it was still being mitigated, with the attackers still demanding several million dollars to unlock the encrypted files.
- Borger, Texas was not able access birth and death certificates or accept any utility payments, affecting over 13,000 residents.
- Keene, Texas was completely locked out of their city payment systems, and the attack circumvented the security defenses installed by their outsourced IT company.
- By striking multiple cities at once, it's one the largest coordinated ransomware attack in recent memory.

These Texas towns have not been the only state and local government agencies targeted by ransomware attackers. Within 2019 alone, ransomware intrusions have struck agencies within Florida, New York, Georgia, and Maryland.

> *The United States is the country with the highest attack rate of ransomware, accounting for 53% of global ransomware attacks. 36% of local agencies have paid the ransom but only 17% got their data back in its original state. - Kaspersky*

How does Secure Archive Manager (SAM) defend Ransomware?

Ransomware and other malware have made data security top of mind in all storage decisions independent of the storage type or storage location. SAM has excellent features to protect the data it manages locally, on the network or in the cloud.

The first aspect of data security is protecting access to data. The first line of defense is an integrated firewall with many traditional firewall features. The firewall verifies that the traffic is of the expected type. If a Doman user attempts to encrypt files, they get automatically blackballed and locked out until after administrative review.

The second line of defense is that SAM uses Virtual File Systems, not physical file systems. This means attacks targeted at file systems are ineffective since there are no OS file systems to attack. SAM intercepts file system tasks from the OS file system stack. SAM routes the requests to a database that represents the VFS.

Encryption is the third line of defense. Via Policy data archived to SAM can be encrypted at rest and in transit to the cloud or other network storage. SAM utilizes AES 256-bit encryption to encrypt every file in an Archive with encryption turned on. Note keys are pre-generated as to not impact performance.

Obfuscation is the fourth line of defense. Files can be converted into objects referenced by GUIDs, thus removing any reference to the source file name path. The Container feature combine lots of files into a single proprietary file or object that must be opened and navigated before a file can be recalled. Also encrypted files can be put into Containers. Each of these options removes any reference to the original file’s name and path, thus making it impossible to tie any front-end file/path structure to anything in back-end storage.

Versioning is the fifth line of defense. With SAM Versioning you maintain multiple versions of files. Which allows you to recover to a date you are certain files are not corrupted. The SAM database is critical to provide users and applications access to data protected and managed by SAM. The brains of SAM are in a database and configuration files and it is imperative that these items be backed up. SAM provides integrated backup functionality or third-party applications can be utilized.

The second aspect of data security is protecting the content itself. With SAM both the access/permissions to data and the data can be independently protected with a variety of strategies depending upon the deployment model and storage options. SAM supports local clusters and a global name space across geographic locations, in addition to backup options. Thereby protecting the metadata needed to access content archived to SAM and the end storage locations and pathways needed to retrieve the content. Protecting the data can be done by mirroring drives in a VM. The data protections options are many and a discussion with SAM engineers would help match your organizations unique needs to the appropriate SAM options.

The third aspect of data security is verifying the integrity of the content. SAM uses content based cryptographic hashes (e.g. MD5, SHA-1, SHA-256) to verify the integrity of every file. SAM offers both read and write verification options. SAM also conducts a periodic audit of the stored content to check for bit rot. If a file is found to not match the original hash value then a copy from another storage location is retrieved and saved, after which the VFS is updated.

The fourth aspect of data security is making the data tamper proof. This is accomplished by two processes. First, SAM creates audit logs for all User and Administrator access and actions. The integrity of the Audit logs is maintained by using content-based hashes. The contents of the logs can be protected by encrypting them with a separate certificate than used for data. The logs can also be written to a location other than SAM. The second process is locking down the capability of the Root User. SAM does not allow the Root User to delete files or modify Audit logs.

Please keep in mind that SAM is purposely built to manage historical, fixed content data. When analyzing most storage environments today, up to 90% the data is a target for archive. A strategy using SAM would focus the backup application on the smaller capacity active data. SAM improves storage efficiency, along with better data security, due to managing (outlined above) the historical, fixed content data outside the usual backup process. With modern backup applications, whether on-premise or cloud-based, your backup sets will be focused on the smaller active data, allowing for a series of recovery points throughout the day. This strategy will improve any response to issues like ransomware attacks, allowing you to roll-back your data to a recovery point before the corruption occurred.

Summary

SAM is a virtual file system solution that provides better security, data protection and scalability over traditional data management software. SAM is designed to help your organization manage data over its lifecycle, independent of any storage protocol or hardware. We are storage agnostic and leave the task of managing the hardware to the makers of the hardware. SAM protects your digital assets from corruption inherent in technology itself, and from malicious attempts like ransomware. This is accomplished through multiple layers of feature sets that all work together to provide the best in data integrity.

DataTrust Solutions, Inc.
720.502.1030
info@datatrustsolutions.com