TECHNOLOGY WHITE PAPER

AI Ransomware Protection in Afi SaaS Backup

Introduction

The 2019 study from Symantec shows that enterprise ransomware attacks continue to grow. Infected email attachments remain an important attack vector and ransomware infections are becoming more targeted – focusing on larger organizations and governments.

In ransomware attacks, hackers encrypt victim's data, making it unreadable. Victim is then instructed to pay a ransom to the hackers in exchange for decrypting the data. The malware may also erase the data permanently after a few days of delay.

Ransomware is increasingly affecting new cloud data sources, including G Suite, Office 365 and other SaaS applications. These can be high-value targets for attackers, and the security processes and tools aren't in place to defend them.

The Role of Backup in Ransomware Protection

Given the rapidly evolving threat of ransomware, it’s likely that even organizations with strong security technology and policies will be affected. Reliable backup and recovery has quickly become a crucial line of defense against ransomware. It allows companies to roll back in time and recover files or databases to just prior to the infection with ransomware.

Gartner recommends using backup as a defense for desktops, laptops, and file shares that are particularly vulnerable to ransomware. The same approach is a must for cloud applications, especially as attackers have begun to target them.

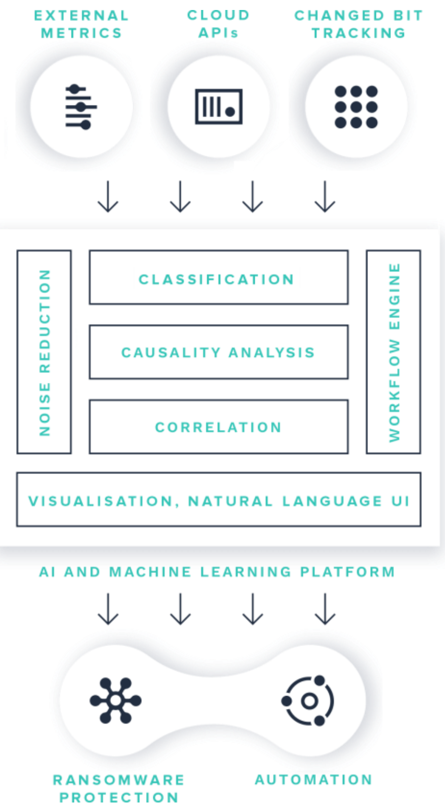
Backup and recovery is a critical part of the security infrastructure. A good SaaS backup and recovery solution makes it possible to go back to a specific point in time and restore part or all of the database from that point.

Even if ransomware was dormant on the system, point-in-time recovery makes it easier to identify, quarantine, and recover from infections without losing data.

How Afi Protects Cloud from Ransomware

GENERAL PRINCIPLE

Afi has an AI-based security engine detects harmful changes to the data, performs high-frequency backups in critical moments & labels key recovery points to assist recovery:



01 Afi monitors all changes to cloud data in Shared Drives, Drives, OneDrive and SharePoint using changed bit tracking technology (CBT).

02 AI-based security engine detects suspicious changes to the data, including mass-deletion and mass-encryption operations. This enables to identify ransomware attacks at their beginning.

03 Afi triggers preemptive backups of unaffected accounts and shared storage locations in order to capture the most recent versions of the data.

04 Simultaneously Afi sends email notifications to the administrators informing of the attack.

05 AI-based classification engine marks the last unaffected versions in backed up data. The enables admin to use point in time restore to quickly recover the most recent clean versions without manual comparison & browsing.

SCOPE OF AFI RANSOMWARE PROTECTION

Afi ransomware protection helps to eliminate or limit data loss due to ransomware by lowering the recovery point objective (RPO) to minutes and seconds instead of days and hours in standard cloud backup solutions.

The protection engine does not depend on the type of encryption performed by ransomware and is effective against data erasure (due to insider or other non-ransomware attacks).

The following types of attacks were detected by Afi in 2019'1H:

- SamSam
- Dharma/Crysis
- Ryuk
- Insider Attacks (rouge admins)

In all incidents company administrators were notified via email, and all protected G Suite and/or Office 365 data were restored.

Conclusion

Afi SaaS backup provides a key security layer in ransomware protection. As there are often too many exposed points for enterprises to completely secure, Afi enables to minimize or wipe out completely consequences of ransomware attacks when they happen.

Afi SaaS backup acts as a last line of defense against ransomware when it penetrates other security countermeasures, enabling organizations to recover the most recent unaffected versions of the data using ransomware detection, preemptive backups and fast point-in-time restore with AI-labelled recovery points.

To find out more about how to protect your cloud applications against ransomware, visit us at www.afi.ai.