American Data Cloud – Malware Prevention and Mitigation

Introduction

The most common security threat facing healthcare organizations in recent years is Ransomware. Ransomware is a form of malware that gets into a network and encrypts or "locks" your files so you can no longer open or access them.
The attacker then demands a payment for a program that can be used to decrypt or "unlock" your files. The following document will outline the most common intrusion point for these kinds of attacks, as well as what American Data Cloud and our hosting partner do to protect your ECS system from such attacks.

Types of Ransomware Attacks

The two most common types of Ransomware attacks are:

Indiscriminate Attacks

- These attacks are most common and generally proliferate by the attacker sending mass emails with malicious attachments or links.
- Once a user clicks on the malicious attachment or link, the Ransomware virus gets into the network and begins encrypting your files- usually starting with network file shares.

Targeted Attacks

- These attacks are less common, but are on the rise in recent years.
- The attackers explicitly target larger organizations that will be under substantial pressure to pay their requested sum of money.
- Rather than the indiscriminate attack through email attachments, they can intrude the network through any means the attacker chooses.
- They often lie dormant while seeking out and eliminating means for early detection or system restoration.

American Data Cloud – Prevention, Detection and Mitigation of Ransomware

With ransomware there are few major considerations when preventing and detecting ransomware attacks.

Email

- As mentioned previously, the majority of attacks come from untargeted email blasts that have malicious attachments or links.
- American Data Cloud does not host any email servers for our clients, so the risk of a user opening a malicious attachment or link on our servers does not exist.
- We only deploy the ECS client to our hosted customers, so they cannot run other applications like web browsers on our servers.

Endpoint Protection

- Our hosting provider uses centrally managed endpoint protection on the servers
- Multi-layer ransomware safeguards
- Protection against malware, spyware, and adware

Data Backups

Strong backup procedures are the most important way to prevent data loss in the event of a ransomware attack. With backups properly stored and air-gapped to offline locations, you can ensure that your backup set is safe from the source of an attack.

- Nightly full encrypted backups
- 120-day data retention
- Individual file or full server restores
- Off-Site Replication
- Ability to restore systems to alternate data facilities, including AWS or Azure
- Application-aware image-based backups
- air-gapped off-site to secondary facilities including Eagan, MN and Kansas City, KS

Standalone Servers

American Data Cloud servers are spun up on a per-client basis and are not part of a large Software as a Service (SaaS) configuration. This means that each client is siloed from the others, which theoretically will prevent the actions of another American Data Cloud customer from impacting your ECS system

Additional Security Information

Our hosting partner has a lengthy list of additional security considerations, including but not limited to:

- Gateway Security/Intrusion Prevention
- Physical Data Center Security
- SIEM and Log Correlation
- Pre-planned Incident Responses

For additional information on these features, please contact American Data Technical Support for the full breakdown.