IDS Policy

In order to preserve the integrity of data that Marketware, Inc. stores, processes, or transmits for Customers, Marketware, Inc. implements strong intrusion detection tools and policies to proactively track and retroactively investigate unauthorized access. Marketware, Inc. currently utilizes AlienVault's Security Monitoring Solution to track file system integrity, monitor log data, and detect rootkit access.

Applicable Standards from the HITRUST Common Security Framework

- 09.ab - Monitoring System Use
- 06.e - Prevention of Misuse of Information
- 10.h - Control of Operational Software

Applicable Standards from the HIPAA Security Rule

- 164.312(b) - Audit Controls

Intrusion Detection Policy

- ALIENVAULT is used to monitor and correlate log data from different systems on an ongoing basis. Reports generated by ALIENVAULT are reviewed by the Security Officer on a monthly basis.
- ALIENVAULT generates alerts to analyze and investigate suspicious activity or suspected violations.
- ALIENVAULT monitors file system integrity and sends real time alerts when suspicious changes are made to the file system.
- Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems (DOS attacks).
- Marketware, Inc. firewalls monitor all incoming traffic to detect potential denial of service attacks. Suspected attack sources are blocked automatically. Additionally, our hosting provider actively monitors its network to detect denial of services attacks.

- All new firewall rules and configuration changes are tested before being pushed into production. All firewall and router rules are reviewed every quarter.
- Marketware, Inc. utilizes redundant firewall on network perimeters.
- Static IP addresses are used for Marketware, Inc. servers.