Vulnerability Scanning Policy

Marketware, Inc. is proactive about information security & understands that vulnerabilities need to be monitored on an ongoing basis. Marketware, Inc. utilizes Nessus Scanner from AlienVault to consistently scan, identify, & address vulnerabilities on our systems. We also utilize OSSEC on all systems, including logs, for file integrity checking & intrusion detection.

Applicable Standards from the HITRUST Common Security Framework

- 10.m - Control of Technical Vulnerabilities

Applicable Standards from the HIPAA Security Rule

- 164.308(a)(8) – Evaluation

Vulnerability Scanning Policy

- Nessus management is performed by the Marketware, Inc. Security Officer with assistance from the VP of Engineering.
- Nessus is used to monitor all internal IP addresses (servers, VMs, etc.) on Marketware, Inc. networks.
- Frequency of scanning is as follows:
- on a weekly basis;
- after every production deployment.
- Reviewing Nessus reports & findings, as well as any further investigation into discovered vulnerabilities, are the responsibility of the Marketware, Inc. Security Officer.
- In the case of new vulnerabilities, the following steps are taken:
- All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.
- Vulnerabilities that are repeatable manually are documented & reviewed by the Security Officer, VP of Engineering, & Privacy Officer to see if they are part of the current risk assessment performed by Marketware, Inc.
- Those that are a part of the current risk assessment are checked for mitigations.
- Those that are not part of the current risk assessment trigger a new risk assessment, & this process is outlined in detail in the Marketware, Inc. Risk Assessment Policy.
- All vulnerability scanning reports are retained for 6 years by Marketware, Inc.

- Penetration testing is performed regularly as part of the Marketware, Inc. vulnerability management policy.
- External penetration testing is performed bi-annually by a third party.
- Internal penetration testing is performed quarterly.
- Gaps & vulnerabilities identified during penetration testing are reviewed, with plans for correction &/or mitigation, by the Marketware, Inc. Security Officer.
- Penetration tests results are retained for 6 years by Marketware, Inc.