Using Cylance for HIPAA HITECH

DirectDefense's analysis of CylancePROTECT on various Windows Desktops (XP/7/8) and Servers (2003/2008/2012) has determined CylancePROTECT meets all of the HIPAA Security Rule requirements for anti-virus/anti-malware solutions as defined in §164.308(a)(5)(ii)(B).

Background

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public law 104-91) called for the establishment of standards and requirements for transmitting certain health information inclusive of protective measures to ensure patient privacy. The Health Information Technology for Economic and Clinical Health (HITECH) Act, was signed into law on February 17, 2009, to promote the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information known as electronic health records (EHRs). The HIPAA HITECH security standards are known as the HIPAA Security Rule. Specifically, the HIPAA Security Rule §164.308(a)(5)(ii)(B) references the protection, detection and reporting of malicious software.

To comply with the HIPAA Security rule, organizations should run anti-virus programs on hosts that have operating systems known to be vulnerable to malware. Effectively implementing anti-virus/anti-malware programs (such as CylancePROTECT) for all hosts considered in scope for HIPPA HITECH compliance.

The specific HIPAA Security Rule regarding protection against malicious software states:

§164.308 – "*Administrative Safeguards"* **(a)5(ii)** – "*Implementation Specifications"* **(B)** - "*Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software."*

How CylancePROTECT Applies to the HIPAA HITECH

If an organization processes, stores, or transmits electronic protected health information (EPHI), it must comply with the HIPAA Security Rule. The HIPAA Security Rule is separated into six main sections written to define a minimum level of security protections that an organization must implement. The Security Rule sections contain standards and implementation specifications that all covered entities must comply with in order to meet the standard. The implementation specification provides a detailed description of the approach to be used to meet a standard and is defined as required (R) or addressable (A).

Addressable implementation specifications indicate covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment.

The table that follows lists the six sections that all covered entities must comply with to meet the HIPAA Security Rule:

§164.306 Security Standards – General Rules	General requirements for all covered entities and business associates.
§164.308 Administrative Safeguards	**Administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's and business associate's workforce in relation to the protection of that information.** **5(ii) – "*Implementation Specifications*" (B) - "*Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.*"**
§164.310 Physical Safeguards	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
§164.312 Technical Safeguards	The technical policy and procedures that protects electronic protected health information to control access, integrity and maintain audit controls.
§164.314 Organizational Requirements	Standards for business associate's contracts or other arrangements between covered entities and business associates.
§164.316 Policies, Procedures and Documentation Requirements	Requires implementation of reasonable and appropriate policies and procedures to comply with the standards and implementation specifications.

Note: §164.308 Administrative Safeguards is the key section containing the protection against malicious software subpart that DirectDefense asserts CylancePROTECT addresses. If completely deployed within the Windows portion of the HIPAA environment and being properly monitored, DirectDefense believes that an organization will be 100% compliant regarding HIPAA Security Rule §164.308(a)5(ii)(B).

Below is an analysis of CylancePROTECT as it applies to each sub-control of §164.308(a)5(ii)(B).

§164.308(a)**5(ii)(B)** - "*Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.*"

Protection

- CylancePROTECT can quarantine or block malware.
- DirectDefense tested CylancePROTECT and found it does more than just protect against all known types of malicious software, and CylancePROTECT has also been tested successfully with Microsoft's VB100 program.
- Anti-virus mechanisms are maintained as follows:
    1. CylancePROTECT is updated continually and has self-learning capabilities
    2. CylancePROTECT performs full disk scans, which can be scheduled in CylancePROTECT Venue console and CylancePROTECT performs a pre-execution quick scan of all modules in real-time (takes 10 – 100 ms).
    3. CylancePROTECT generates syslog entries which are the most common logging facility/interface available today.

Detecting

- Detect all known types of malicious software - DirectDefense found CylancePROTECT to be significantly superior in finding malicious software than any other anti-virus or anti-malware product we have encountered.

Reporting

- CylancePROTECT sends alerts of threats or abnormal executable behavior to the client as well as the management portal to be displayed at the dashboard level. Details for each flagged executable are available as well as the ability to override any potential false positives.

CylancePROTECT Solution Overview and Effectiveness Analysis

CylancePROTECT Management:

The CylancePROTECT solution provides the administrator with the ability to manage and control the policy settings from the https://my.cylance.com management portal. Assets can be assigned to specific zones and policies for controlling how malware is analyzed and how to respond to the identification of malware can be configured on a zone or individual asset basis.

CylancePROTECT Policy Control:

From the management portal, the device policy allows an administrator to control the analysis policy by the following three areas:

File Actions – This area provides controls on how CylancePROTECT monitors executables files and allows the administrator to send samples to the Cylance cloud for analysis as well as if they wish to automatically Quarantine files.

Memory Actions – This area provides control on how CylancePROTECT monitors and manages the memory actions performed by an application or executable and provides the admin with the ability to ignore, alert, block, or even terminate unwanted or malicious behaviors.

Protection Settings – This area provides control on how CylancePROTECT scans for files on the target system. An administrator can control how Protect looks for files to inspect. You may choose to only watch for new files or scan the whole disk on a periodic basis or both.

CylancePROTECT Notifications:

Alerts of threats or abnormal executable behavior are displayed to the local instance of the CylancePROTECT client as well as they are sent back to the management portal and displayed at the dashboard level. Details for each flagged executable are available as well as the ability to override any potential false positives.

CylancePROTECT Accuracy and Effectiveness:

Testing Results:

To properly gauge the accuracy of the CylancePROTECT solution, DirectDefense used a private sampling of malware that we maintain, in addition to our own custom exploit payloads that we leverage during the course of our penetration tests that have been designed to bypass most anti-virus solutions.

For this review, we configured the CylancePROTECT solution block and alert on malicious memory actions, automatically flag malicious or abnormal executables with the file actions, and scan all new files as well as periodically scan the whole disk of our sample system.

In each test case, the CylancePROTECT solution properly flagged and blocked of samples of un-obfuscated malware, polymorphic (constantly changing versions of code) malware, metamorphic (the decrypted code changes with each instance) malware and custom packed (compressed to obfuscate) malware code. Additionally, CylancePROTECT flagged our own custom exploit payloads and had 100% accuracy in detecting our samples of crypto locker.

Why was CylancePROTECT so successful?

Unlike traditional anti-virus and anti-malware solutions, CylancePROTECT does not rely solely on matching a known file signature. Protect tests not only the executable file, but also monitors the functions an executable may attempt to perform.

As an example, our custom payloads simulate your typical “0-day” exploit or attack in that no signature has ever been created for our custom executable so a conventional anti-virus has no frame of reference to trigger or flag the payload as a threat. However CylancePROTECT can not only send our file off for detailed analysis if needed, but can also monitor the actions of the file once it has been executed and monitor the behavior of our payload. In short, CylancePROTECT has true “0-day” anti-malware protection since it does not require the offending code to be well known.

Conclusions

In conclusion DirectDefense attests that CylancePROTECT is 100% compliant with HIPAA HITECH malicious software protection, detection and reporting requirements when it has been properly deployed within the environment. CylancePROTECT exceeds the HIPAA HITECH compliance requirements, and can also be very effective in protecting your organization’s overall IT desktop and server infrastructure from the day-to-day threats they face.