Using Cylance for PCI DSS Anti-virus

DirectDefense's analysis of CylancePROTECT on multiple Windows Desktops (XP/7/8) and Servers (2003/2008/2012) has determined CylancePROTECT meets all of the PCI DSS requirements for anti-virus/anti-malware solutions as defined in PCI DSS Requirement 5. Delivering stronger protection against unknown or new variants of malware, than any traditional antivirus that was tested.

Background

To comply with PCI DSS Requirement 5, PCI states that organizations must run anti-virus programs on hosts that have operating systems known to be vulnerable to malware. Effectively Requirement 5 denotes that organizations must implement anti-virus/anti-malware programs (such as CylancePROTECT) for all Windows hosts considered in scope for PCI.

PCI Requirement 5 Overview:

5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)

5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software

5.2 Ensure that all anti-virus mechanisms are maintained as follows:

- Are kept current
- Perform periodic scans
- Generate audit logs which are retained per PCI DSS Requirement 10.7

5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period

5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties

How CylancePROTECT Applies to the PCI Standard

If your organization processes, stores, or transmits payment cardholder information, it must comply with the Payment Card Industry Data Security Standard (PCI DSS). The twelve Requirement sections defined in this prescriptive standard are written to define a minimum level of security protections that your organization must implement. Each Requirement has multiple sub-items that organizations must be compliant with.

The twelve requirements are listed below:

Requirement 1	Install and maintain a firewall configuration to protect cardholder data
Requirement 2	Do not use vendor-supplied defaults for system passwords and other security parameters
Requirement 3	Protect stored cardholder data
Requirement 4	Encrypt transmission of cardholder data across open, public networks
Requirement 5	**Protect all systems against malware and regularly update anti-virus software or programs**
Requirement 6	Develop and maintain secure systems and applications
Requirement 7	Restrict access to cardholder data by business need to know
Requirement 8	Identify and authenticate access to system components

Requirement 9	Restrict physical access to cardholder data
Requirement 10	Track and monitor all access to network resources and cardholder data
Requirement 11	Regularly test security systems and processes
Requirement 12	Maintain a policy that addresses information security for all personnel

Note that Requirement 5 (anti-virus) is the key requirement that we assert that CylancePROTECT addresses. If completely deployed within the Windows portion of the PCI environment and its monitoring results are monitored, we, (in our official ruling as PCI QSAs) believe that an organization will be 100% compliant regarding PCI DSS Requirement 5.

Below is an analysis of CylancePROTECT as it applies to each sub-control of Requirement 5.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

- 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, by having no reliance on signatures, it is possible for CylancePROTECT to discover malware weeks before traditional A/V's have created signatures to detect.
- Remove all known types of malicious software - CylancePROTECT can quarantine malware in real time, before it executes on the host, as well as supporting full whitelisting and blacklisting capabilities, to respond to non-traditional attacks.
- Protect against all known types of malicious software – DirectDefense tested CylancePROTECT and found its efficacy to exceed traditional Tier 1 A/Vs on commoditized known malware, as well as being able to identify and block new variants in true APT style attacks, where traditional vendors had efficacy rates under 50%.
- Ensure that all anti-virus mechanisms are maintained as follows:
    1. Are kept current. – CylancePROTECT is updated continually and has self-learning capabilities, updates are pushed to the endpoint via HTTPS, or can be updated manually on air-gapped systems.
    2. Perform periodic scans. – CylancePROTECT has the capability to perform full disk scans (every 9 days), as well as offering on-execution scanning of all portable executables, with a delay in load time that did not exceed 100ms during testing.
    3. Generate audit logs which are retained per PCI DSS Requirement – CylancePROTECT has multiple audit log features, including a centralized console, as well as supporting full syslog traps, and full SEIM integration.

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 malicious code executes, anti-memory exploitation protection, and whitelist and blacklist functionality based on sha256 hashes.

CylancePROTECT Policy Control:

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

Analysis 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. This includes protection against the gamut of exploitation techniques, such as stack pivots and out of process communications.

Protection Settings – This area provides additional control on how CylancePROTECT searches and responds to malware on the endpoint, enabling the ability to perform ongoing scheduled scans for files on the target system, monitor for new files added to the system, while still providing the same pre-execution machine learning identification of malware, blocking it from executing and infecting the target system.

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 (or SEIM) and displayed at the dashboard level. Details for each flagged executable are available as well as the ability to override any potential false positives, an even blacklist potentially unwanted programs (PSexec, RATs, etc).

CylancePROTECT Accuracy and Effectiveness:

Testing Results:

To properly gauge the accuracy of the CylancePROTECT solution, DirectDefense used a sampling of malware that public sources (Virus Total) as well as malware we have collected from customer breaches, 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 ransomware, and all publically available samples of POS malware from recent high profile breaches.

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 evaluates not only the executable file, but deduces what 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. By using an ensemble of machine learning algorithms CylancePROTECT is able to determine an executable’s intent, and probability of malicious intent, without ever having to execute the file, and put any customer systems at risk.

Conclusions

In conclusion DirectDefense attests that CylancePROTECT is 100% compliant with PCI DSS when it has been properly deployed in a PCI environment. CylancePROTECT not only meets the PCI compliance requirements, but is also industry leading in protecting your organization's desktop and servers from the day-to-day threats they face.