USING FIREEYE ENDPOINT FOR PCI AND HIPAA/HITECH COMPLIANCE

DirectDefense's analysis of FireEye Endpoint attests that the products help meet the HIPAA Security Rule and PCI DSS v3.2 requirements for malware protection, access control and for providing IPS/IDS protection. DirectDefense analyzed the FireEye Endpoint feature set and mapped those to HIPAA and PCI compliance requirements. The results showed that FireEye Endpoint applies to some key requirements which make it a valuable component of compliance for any entity.

During the course of the analysis of FireEye's Endpoint product DirectDefense mapped HIPAA and PCI requirements against the FireEye Endpoint product functionality. DirectDefense performed extensive testing in a lab environment. Testing was performed against malware found in the wild and DirectDefense's own home-written malware that tested for true "zero-day" detection of:

- Stealth Executable downloading
- DLL hooking
- Ransomware
- Memory scraping
- Kernel I/O hooking
- Registry monitoring
- Service listing
- Process listing
- VBscript code
- WMI querying
- Key Stroke Logging

This testing proved that FireEye Endpoint is not just a signature based detection product, but that it goes much deeper. Much of the test code was known to be zero-day since DirectDefense wrote it making signature analysis impossible because known signatures did not exist.

HIPAA BACKGROUND

HIPAA and its companion legislation, HITECH (which will be collectively referred to as "HIPAA" throughout), address the processing, storage and transfer of Protected Health Information (PHI) in all forms, including electronic PHI or "ePHI."

HIPAA regulations define requirements that a covered entity must implement, with the goal of eliminating the exposure of PHI to parties that are not directly involved with patient care and who do not have "a need to know" regarding an individual's PHI.

The general categories of HIPAA regulatory compliance are as follows:

§164.306 Security Standards – General Rules	General requirements for all covered entities and business associates.
§164.308 Administrative Safeguards	IT security, risk assessments, access to systems, disaster recovery, vulnerabilities and **Protection from malicious software.** **THIS IS THE CATEGORY THAT APPLIES TO FIREEYE ENDPOINT ("308")**
§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.

HOW FIREEYE ENDPOINT HELPS FACILITATE HIPAA COMPLIANCE

To comply with the regulations implementing the HIPAA Security Rule, organizations should use secure, widely accepted security techniques on all systems that will be used to process, store, and transfer PHI. Effectively implementing security for all processing, transmission and storage locations containing PHI is critical for HIPPA compliance.

There are two regulations implementing the HIPAA Security Rule for which FireEye Endpoint allows covered entities to achieve compliance:

- **§164.308(a)(5)(ii)(B)) Protection from Malicious Software (Addressable).**

  Procedures for guarding against, detecting, and reporting malicious software.

  Malicious software addresses all malware: phishing executables, viruses, worms, keystroke loggers, Trojan horses, rootkits and most of all the exfiltration of data.

  FireEye Endpoint is regarded as among the best regarding **Protection from Malicious Software.** Implementation specification requires healthcare entities to protect against malware by detecting it, stopping it from compromising PHI, and reporting its presence.

  DirectDefense performed extensive testing to confirm that FireEye Endpoint is an excellent choice for securing systems from malware attacks.

  NOTE: The term "addressable" means that the safeguard should be implemented, or another equivalent safeguard should be implemented. The authors of the standard wanted to ensure that they did not dictate technology and left the door open for other technologies; however today all health organizations are implementing anti-virus and other technologies to help protect against malware. In summary HIPAA requires a covered entity to implement measures designed to ensure that ePHI is secured with due diligence and due care effectively with secured systems that are not highly vulnerable to malware.

- **§164.308(a)(5)(ii)(C))** Log-in monitoring (Addressable).

  Procedures for monitoring log-in attempts and reporting discrepancies.

  Log-In Monitoring requires covered entities to implement procedures for monitoring log-in attempts and to look for anomalies in access patterns. Log-in Monitoring with FireEye Endpoint is done based on the FireEye "roles and rights" setting for users and generates logging alerts when users who have not been granted access to sensitive PHI data attempt to access FireEye secured systems.

  DirectDefense confirmed that by using FireEye Endpoint an entity can identify unauthorized access, intrusion and prevent HIPAA policy violations, thereby meeting **HIPAA 164.308(a)(5)(ii)(C))** compliance requirements.

PCI DSS BACKGROUND

The PCI web site states, *"We serve those who work with and are associated with payment cards. This includes: merchants of all sizes, financial institutions, point-of-sale vendors, and hardware and software developers who create and operate the global infrastructure for processing payments."* In effect, if a business takes credit cards they are "in scope" for PCI compliance. That means that just about every business must address PCI because almost all businesses are a "PCI merchant" to some extent since they take some form of payment via major credit card brands.

The PCI Data Security Standard (PCI DSS), which is a lengthy, detailed, prescriptive standard, is not a law. However, compliance with the PCI DSS is required by banks that issue major credit cards, and by the major card brands themselves. These credit card brands want to ensure that their issuers and merchants are secure so as to minimize the costs and consequences of data breaches. Therefore they require merchants and issuers to perform PCI DSS assessments based on their business priorities and the quantity of transactions the merchant makes.

The thoroughness of a merchant's assessment or whether one is even required depends largely upon the number of card transactions performed by the business entity each year and what the merchant's bank requires. Ultimately the bank decides what the merchant must do, but the card brands define PCI Levels which define the detail level of required assessments. In practice, any business submitting more than about 20,000 transactions per year is almost certainly required to show PCI compliance. Anything above 6 million transactions per year requires a PCI QSA assessor to be on site and perform a full PCI DSS assessment of the entity.

HOW FIREEYE ENDPOINT SECURITY FACILITATES PCI DSS COMPLIANCE

FireEye Endpoint addresses PCI DSS v3.2 in the following ways:

PCI DSS Requirement 5 - Anti-virus

Protect all systems against malware and regularly update anti-virus software or programs.

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

FireEye Endpoint is updated continually by the FireEye Labs Team that monitors every single attack found in real-world conditions. Updates are pushed to FireEye Endpoints every 30 minutes over HTTPS secured connections, or alternately can be updated manually on systems in "dark networks" not connected to the Internet.

5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

HX with Malware Protection covers malicious software including viruses, Trojans, worms, spyware, adware, and rootkits. FireEye Endpoint Security includes 4 unique engines that will detect, prevent, and clean up threats. The 1st engine is an indicator engine which leverages Indicators of Compromise and historical event recording to detect malicious actitivity, malicious tool use, and malware based on behavior. The 2nd engine is Exploit Guard which uses behavioral roles to identify and block memory exploits, application exploits, and malicious use of applications on highly targeted applications like browsers and office files. The 3rd engine is malware protection which detects, blocks, and removes malware include ransomware, adware, spyware, trojans, worms and other known malicious software. The 4th engine is a Malware Guard which leverages machine learning to static identify and block known threats variants of malware. FireEye posts threat rating in public third party testing sites include AV-Comparatives, Virus Bulletin and ICSALabs.

5.1.2 For systems considered to not be 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

FireEye is continually analyzing vulnerabilities for: Windows, Linux and Mac OSX systems. DirectDefense noted that this is over and above the usual PCI compliance levels they have seen.

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

- *Are kept current*

  FireEye Endpoint is continually updated. Agent software is kept current with the latest patterns, and the behavior analysis and exploit prevention engines continually learn new behavior.

- *Perform periodic scans*

  FireEye Endpoint can be configured to perform scans based on the configuration made by the IT Security staff that can be further divided into scan groups with differing granularity. (Master Boot Records, full scans, active memory….)

- *Generate audit logs which are retained per PCI DSS Requirement 10.7*

  FireEye Endpoint has a centralized logging console. It also generates syslog events for SEIM integration.

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

FireEye can be configured to not allow any end user interaction.

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

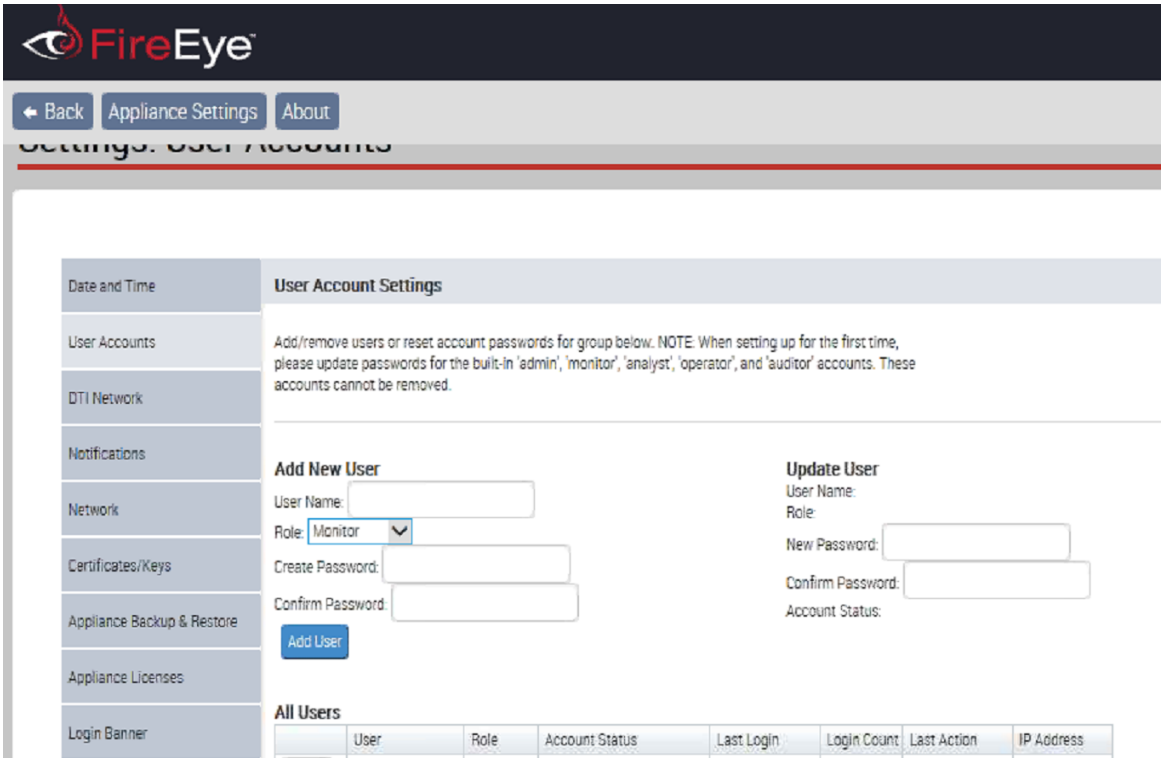
FireEye Endpoint can be documented in an organization's policies and procedures.

PCI DSS Requirement 7.2 - Access Control

Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

FireEye Endpoint monitors user activity and alerts on improper usage.

The product also has twelve (12) RBAC access roles for users of the console:



Requirement 10: - Logging

Track and monitor all access to network resources and cardholder data

FireEye Endpoint tracks activity performed within its managed systems and logs them to the central console. The agents which are running on the endpoints continuously monitor and record key user actions and system activity and can correlate events with past events to create alerts.

FireEye's Endpoint product ensures that system events are logged:

- Audit trails are enabled and active for system components.
- Access to system components is linked to individual users.

The FireEye Endpoint log entries include the PCI required fields:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event

888 720 4633
sales@directdefense.com
directdefense.com

PCI DSS Requirement 10.3.6 - *Identity or name of affected data, system component, or resource*.

Host name/ip address/user account/date and time of the event are logged in FireEye HX.

PCI DSS Requirement 11.4 – Intrusion Detection **5.2.c** Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that:

- The anti-virus software and definitions are current.
- Periodic scans are performed.

Use intrusion-detection systems and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises.

Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

.

FireEye Endpoint is an industry leader in endpoint detection and response. The FireEye Endpoint HX product in which IDS and IPS is managed and consolidated can be hosted in one of three systems:

- Hardware running a Bastion Linux OS
- Virtual Machine in the client's environment
- Cloud hosted by FireEye in strongly protected Amazon Web Services data centers

In addition to monitoring, automated actions are taken immediately to thwart attacks. All of this is provided in a console with a dashboard of status indicators, a logging system and a view into system inventories.

DIRECTDEFENSE TESTING OF FIREEYE ENDPOINT SECURITY

To properly gauge the accuracy of the FireEye Endpoint solution, DirectDefense tested the capabilities of the product on multiple endpoints. Tests were run on servers and workstations to ensure that FireEye Endpoint features apply to HIPAA and PCI compliance requirements.

Testing was performed using a test system with 139 endpoints. Approximately 300 samples of malware from the wild were tested (memory exploits, trojans, ransomware, adware, macro viruses, etc), and malware code written by DirectDefense to simulate true zero-day attacks were also tested (these are samples never seen in the wild…. not available in any malware database). Test cases were run for varying roles and rights, with differing levels of access (owner vs other users), different types of files and intrusions.

The FireEye Endpoint Agent works by combining several sources of intelligence along with several detection engines to find known attacks and unknown attackers. Intelligence downloaded to the endpoint included executables from Mandiant incident response investigators, FireEye Labs research, FireEye NX network protection devices, and in some cases indicators provided by customers. Engines that process this Intel include the Real-time Indicator Detection Engine, the Malware Protection Engine, Exploit Guard, and Event Monitor (event monitoring that records user and system behavior includes registry filesystem, network, and browser activity). For post-breach discovery, FireEye Endpoint leverages the capability to rapidly search for attacker artifacts with the Enterprise Search and Data Acquisition capabilities which are input into the Triage Summary and Audit Viewer.

CONCLUSIONS

In conclusion DirectDefense attests that FireEye Endpoint Security helps achieve compliance for HIPAA and PCI DSS V32 for protection of PHI and ePHI within the Electronic Healthcare Records (EHR) environment and systems within PCI scope affecting payment processes.

DirectDefense did extensive testing of FireEye Endpoint Security that was more comprehensive than industry standard testing done today. DirectDefense applied a wider variety of tests and more difficult tests to FireEye Endpoint Security than is normally done by reviewers. In doing so DirectDefense is very confident that FireEye Endpoint Security exceeds the compliance requirements outlined above as defined in HIPAA and the PCI DSS. FireEye Endpoint adds an extra layer of security and due diligence that stops many data breaches from occurring. Even with full access to a system, such as in the case of an internal employee seeking to access information without authorization, the strong protection and access controls in the FireEye Endpoint Security product offers powerful protection against unauthorized access to and compromise of sensitive ePHI and payment data.