COALFIRE LABS

TRAPS ADVANCED ENDPOINT PROTECTION SECURITY SOLUTION FOR HIPAA COMPLIANCE WHITEPAPER

September, 2016

Prepared For:

Palo Alto Networks

Prepared by:

Coalfire Systems

North America I Latin America I Europe

877.224.8077 | info@coalfire.com | coalfire.com

TABLE OF CONTENTS

Executive Summary **3**
Audience 4
Methodology 4
HIPAA Security and Breach Notification Rules 4
Summary Findings 5
Application Architecture and Security **6**
Exploit & Malware Prevention **6**
Technical Assessment **8**
Conclusion: **10**

EXECUTIVE SUMMARY

Palo Alto Networks, Inc. (Palo Alto) engaged Coalfire Systems Inc. (Coalfire), to conduct an independent technical assessment of their Traps Advanced Endpoint Protection application as it pertains to HIPAA Security Rule as well as the requirements of the Breach Notification Rule as formalized by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and the Omnibus Rule of 2013.

The purpose of this white paper is to provide an overview of Coalfire's assessment of the Traps architecture and to confirm to what extent Traps helps satisfy the technical requirements (i.e. Technical Safeguards) of the HIPAA Security Rule. The scope for validation was derived through collaboration with Palo Alto Networks development team and Coalfire assessors. The review and testing was performed based on the use cases generated for validation of HIPAA requirements that are addressed when Traps solution is utilized.

The assessment performed included the following components:

- Review overall design and architecture of Traps solution.
- Technical Testing and related evidence collection for the use cases provided:
  - Re-performance testing of the solution
  - Observation of the solution including installation, configuration and functional capabilities
- Interviews with Subject Matter Experts (SMEs).
- Review and feedback of supporting documentation.

It's Coalfire's determination that an organization who was using a traditional AV to remain HIPAA compliance can confidently replace that solution with Traps and remain compliant. The Traps Advanced Endpoint Protection solution meets the requirements of HIPAA rule 164.308(a)(5)(ii)(B) and can be used in PHI environments allowing a customer to satisfy and exceed HIPAA HITECH compliance requirements for protection from malicious software.

There are no known inhibitors identified with the Traps solution which would prevent an organization from implementing it in an environment containing electronic Protected Health Information (ePHI). Additionally, there are features within Traps which facilitate meeting certain requirements of the HIPAA Security Rule. Every organization has unique business, technical and security governance requirements, as a result this paper does not provide detailed recommendations for how to configure Traps application to meet the applicable portions for HIPAA compliance.

AUDIENCE

This assessment white paper has two target audiences:

- Administrators and Other Compliance Professionals: This audience may be evaluating Traps for use within their organization for compliance requirements.
- Healthcare Organizations: This audience is evaluating Traps for deployment in their ePHI environment and what benefits could be achieved from using this solution.

METHODOLOGY

Coalfire has implemented industry best practices in our assessment and testing methodologies. Coalfire completed a multi-faceted technical assessment process during the course of this project using common scenarios and best practices. Coalfire conducted technical lab testing remotely on 8/1/2016.

The Coalfire methodology for performing HIPAA assessments is based on established and repeatable assessment frameworks compiled from the National Institute of Standards and Technology (NIST) and the OCR Audit Protocols. Specifically, NIST 800-66 serves as the de facto standard for directing organizations on the typical activities that should be considered when pursuing HIPAA compliance as part of an overarching information security program. Additionally, Coalfire gives consideration to NIST 800-53 to provide a greater level of review where outside risk remains from NIST 800-66 and the OCR Audit Protocols. NIST 800-53 provides security and privacy controls for federal information systems and organizations. NIST special publications have been supported and referenced by the OCR as viable interpretations and guidance for achieving HIPAA compliance.

The outcome of this testing provides verification that customers implementing Traps will be able to meet specific HIPAA requirements (known as Standards and Implementation Specifications) in their real world ePHI environments. A broad spectrum of network, system and application scenarios was used in our validation testing. Test results and lab configurations are summarized in the technical section of the white paper.

HIPAA SECURITY AND BREACH NOTIFICATION RULES

The HIPAA Security Rule specifically focuses on the safeguarding of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is mandated to all organizations defined by HIPAA as a Covered Entity and Business Associate. These organizations are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI that it creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against reasonably anticipated unauthorized uses or disclosures of protected health information; and
- Ensure compliance by its workforce.

The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications. The major sections include:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

- Organizational Requirements
- Policies and Procedures
- Documentation Requirements

While the administrative, physical, and technical requirements identified under HIPAA are mandatory, their implementation may differ based on the type of requirement. Under the HIPAA Security Rule, Standards and Implementation Specifications are classified as either “Required” or “Addressable”. It’s important to note that neither of these classifications should be interpreted as “optional”. An explanation of each is provided below:

- **Required** – Implementation specifications identified as “required” must be fully implemented by the covered organization. Furthermore, all HIPAA Security Rule requirements identified as “Standards” are classified as “required”.
- **Addressable** – The concept of an “addressable” implementation specification was developed to provide covered organizations flexibility with respect to how the requirement could be satisfied. To meet the requirements of an addressable specification, a covered organization must: (a) implement the addressable implementation specification as defined; (b) implement one or more alternative security measures to accomplish the same purpose; or (c) not implement either an addressable implementation specification or an alternative. Where the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, the organization must fully document their decision and reasoning.

The HIPAA Breach Notification Rule, 45 CFR §164.404 - 414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. The major sections of the rule include:

- Notification in the Case of Breach
- Notification to the Media
- Notification to the Secretary
- Notification by a Business Associate
- Law Enforcement Delay

SUMMARY FINDINGS

When properly implemented, Traps provides the following benefits:

- Traps architecture and implementation requirements can be deployed in an ePHI environment.
- Traps provides protection against both unknown and known malware and exploit-based attacks.
- Traps can provide ability to detect and prevent malware, minimizing the impact of data breach when implemented appropriately.
- When properly configured, Traps can provide audit trail of all detected malware and keep records for required timeframe.
- When properly deployed and configured, Traps solution can satisfy 164.308(a)(5)(Ii)(B) HIPAA rule by directly meeting the requirement.

APPLICATION ARCHITECTURE AND SECURITY

The Traps solution, which comprises a central Endpoint Security Manager (an ESM Server, ESM Console, and database) and the Traps agent protection software installed on each endpoint, takes an effective approach to prevent malicious attacks. Rather than try to keep up with the ever-growing list of known exploit-based attacks, Traps sets up a series of roadblocks that prevent the attacks at their initial entry points—that point where legitimate executable files are about to unknowingly allow malicious access to the system.

Traps targets software vulnerabilities in processes that open non-executable files using exploit prevention techniques. Traps also uses malware prevention techniques to prevent malicious executable files from running. Using this two-fold approach, the Traps solution can prevent all types of attacks, whether they are known or unknown threats.

Traps enterprise solution consist of multiple components:

- Component one – Traps agent
- Component two – Endpoint Security Manager (an ESM Server, ESM Console, and database)
- Component three – The WildFire service is a natively integrated cloud-based malware analysis service.

EXPLOIT & MALWARE PREVENTION

When a user opens a non-executable file, such as a PDF or Word document, and the process that opened the file is protected, the Traps agent seamlessly injects code into the software. This occurs at the earliest possible stage before any files belonging to the process are loaded into memory. The Traps agent then activates one or more Exploit Protection Modules (EPMs) inside the protected process. The EPM targets a specific exploitation technique and is designed to prevent attacks on program vulnerabilities based on memory corruption or logic flaws.

Examples of attacks that the EPMs can prevent include dynamic-link library (DLL) hijacking (replacing a legitimate DLL with a malicious one of the same name), hijacking program control flow, and inserting malicious code as an exception handler.

In addition to automatically protecting processes from such attacks, Traps reports any prevention events to the Endpoint Security Manager, and performs additional actions according to the settings of the security policy rules. Common actions that Traps performs include collecting forensic data and notifying the user about the event.

The default endpoint security policy protects the most vulnerable and most commonly used applications, but users can also add other third-party and proprietary applications to the list of protected processes.

Malicious executable files, known as malware, are often disguised as or embedded in non-malicious files. These files can attempt to gain control, gather sensitive information, or disrupt the normal operations of the system.

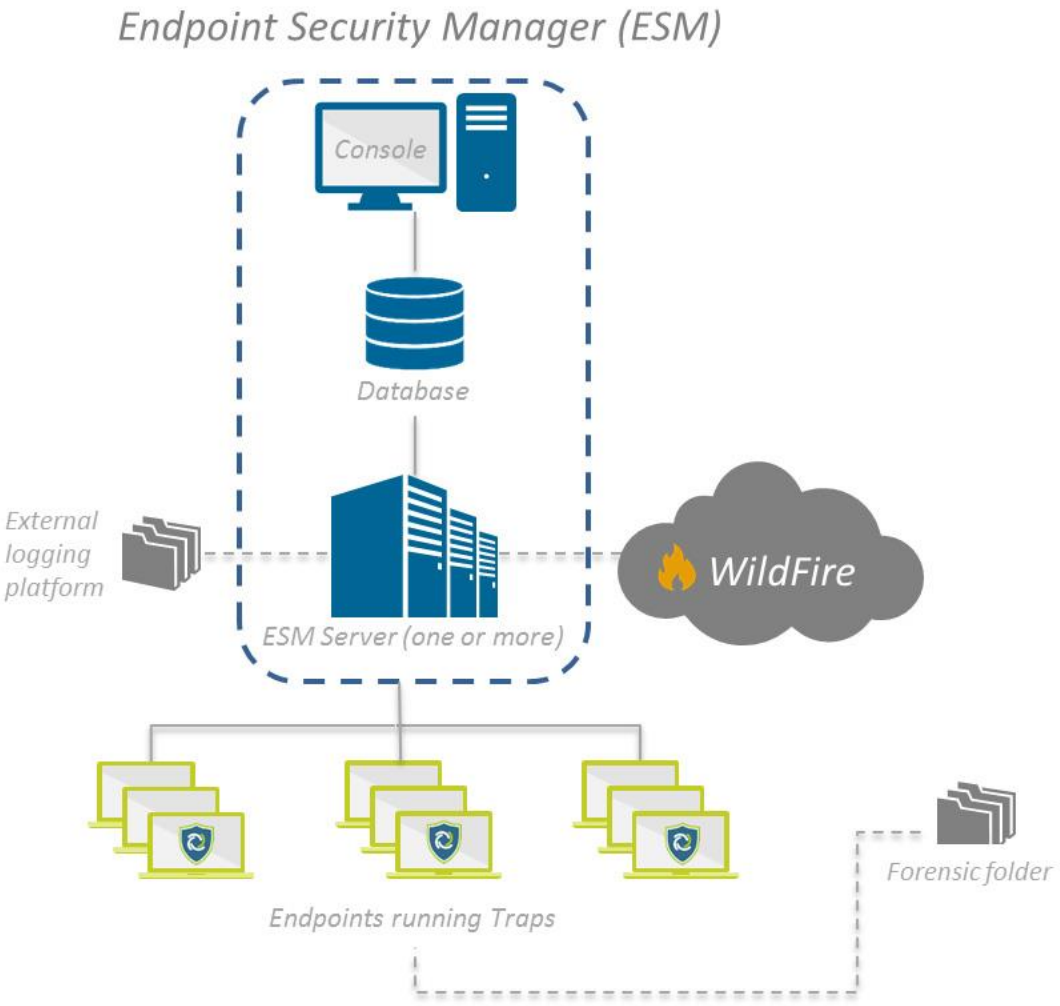
1. Local Analysis via Machine Learning: This method delivers an instantaneous verdict for any unknown executable before it is allowed to run. Traps examines hundreds of the file's characteristics, without reliance on signatures, scanning or behavioral analysis.
2. WildFire Inspection and Analysis: Leverages the power of Palo Alto Networks WildFire (tm) cloud-based malware analysis environment to detect unknown malware and automatically reprogram Traps to prevent known malware.

3. Trusted Publisher Execution Restrictions: allows organizations to identify executable files that are among the “unknown good” because they are published and digitally signed by trusted publishers-entities that Palo Alto Networks recognizes as reputable software publishers.
4. Policy-Based Execution Restrictions-Organizations can easily define policies to restrict specific execution scenarios, thereby reducing the attack surface of any environment. For example, Traps can prevent the execution of files from the Outlook “temp” directory or prevent the execution of a particular file type directly from a USB drive.
5. Admin Override Policies- Define policies, based on the hash of an executable file, to control what is allowed to run in any environment and what is not. This fine-grained whitelisting (or blacklisting) capability controls the execution of any file, based on user-defined conditions that tie into any object that can be defined with Microsoft Active Directory.

APPLICATION ARCHITECTURE

The Traps solution consists of the Endpoint Security Manager (ESM) and the Traps agent protection software. The Traps agent is installed on each endpoint in the organization.

The following diagram displays the Traps components and their relationships to each other and to other security components.



TECHNICAL ASSESSMENT

Coalfire performed testing using remote Palo Alto Networks environment running Windows 2012 Server with Endpoint Security Manager (ESM) as well as Windows 7 with the Traps agent.

The scope of the assessment was defined with the following tasks:

- Understand product functionality, architecture, implementation and operation
- Review installation guidance and supporting documentation
- Test Traps product for required controls in the lab environment
- Review and verify Traps administrator's guide for any hardening best practices
- Review Traps configurations and capabilities
- Verification of solution for security and compliance with HIPAA Security Rules

VALIDATION FINDINGS FOR TRAPS APPLICATION

HIPAA Rule	How Traps Supports HIPAA Security Rule Requirements	Test Procedure
Security Awareness and Training – 164.308(a)(5)(i) **Implement a security awareness and training program for all members of its workforce (including management).**		
Protection from Malicious Software – A 164.308(a)(5)(ii)(B) Procedures for guarding against, detecting, and reporting malicious software.	**Traps** software is capable of detecting, removing and protecting against all known types of malicious software. • Traps can stop cyber threats that evade antivirus and other traditional defenses using zero-day and targeted attacks. • Traps provides signature-less detection and prevention of advanced threats • Traps provides recorded history of all endpoint and server activity to rapidly respond to alerts and incidents	Deployed Traps agent and attempted to run various software including malicious software on the system with Traps endpoint agent. Traps was able to block the attempt and provided alert notification in the ESM administrator backend.

CONCLUSION:

After reviewing the Traps environment with respect to the HIPAA Security Rule, Coalfire determined through review of business impact and technical assessment that the Traps solution meets certain HIPAA requirements. The ability to achieve overall compliance with any regulation or standard will be dependent upon the specific design and implementation of the Traps products in the context in which it is implemented.

It's Coalfire's determination that an organization who was using a traditional AV to remain HIPAA HITECH compliant can confidently replace that solution with Traps and remain compliant.

The Traps application demonstrated a high level of performance compared to industry standard AV solutions available. Innovative malware detection and exploit prevention mechanisms provided by the Traps application allows for excellent performance in the real world scenarios.

The Traps Advanced Endpoint Protection solution meets the requirements of HIPAA rule 164.308(a)(5)(ii)(B) and can be used in PHI environments allowing a customer to satisfy HIPAA compliance requirements for protection from malicious software.

ABOUT COALFIRE

Coalfire is the global technology leader in cyber risk management and compliance services for private enterprises and government organizations. Our professionals are renowned for their technical expertise and unbiased assessments and recommendations. Coalfire's approach builds on successful, long-term relationships with clients to achieve multiple cyber risk management and compliance objectives, tied to a long-term strategy to prevent security breaches and data theft.