WHITE PAPER – MAY 2021

PC MATIC FOR HIPAA AND HITECH

APPLICABILITY TO ASSIST CUSTOMERS IN HIPAA AND HITECH DEPLOYMENTS

COALFIRE OPINION SERIES

TONY COSTANZO

FINAL DRAFT V0.4

PC Matic

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

COALFIRE OPINION

Coalfire Systems, Inc. (Coalfire) reviewed the PC Matic platform for its efficacy in providing its covered entity and business associate (CE&BA) customers the ability to achieve or maintain compliance in their successful deployments using the PC Matic platform. The CE&BAs are identified as those entities that are defined under the Health Information Portability and Accountability Act (HIPAA) and enforced by the provision of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009. The purpose of this opinion white paper is to identify how the PC Matic platform's security capabilities, functions, and features align with the standards adopted by the Secretary of Health and Human Services (HHS) under the HIPAA of 1996 (HIPAA, Public Law 104-191) for protecting privacy and security of certain health information.

The HIPAA Security Rule specifically focuses on the safeguarding of electronic protected health information (ePHI) through the implementation of administrative, physical, and technical safeguards. CE&BA 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 (PHI), and ensure compliance by its workforce. In parallel to the Security Rule, the HHS mandated *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule) establishes a set of national standards for protection of certain health information while promoting the necessary flow of health information to facilitate high quality health care.

Practical implementation of a HIPAA compliance program typically requires the CE&BA have a solid Risk Analysis and Risk Management framework with controls-based compliance guidelines, such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 or the International Organization for Standardization (ISO) ISO 27001. HIPAA Security Rule mandates define technical outcomes which the controls-based guidelines may be used to achieve. HIPAA itself does not deliver the level of technical and organizational controls required to have a comprehensive program of compliance.

The PC Matic platform, as reviewed by Coalfire, **can be effective** in providing support for the outlined objectives and requirements of the HIPAA Security Rule in support of a HIPAA compliance program. Through proper implementation and integration into the organization's greater technical infrastructure and information security management systems, PC Matic may be useable in a HIPAA-controlled environment. The organization wishing to use PC Matic should consider the guidance provided by the National Institute of Standards and Technology, U.S. Department of Commerce (NIST) Special Publication (SP) 800-167 Guide to Application Whitelisting, when designing their implementation.

Coalfire Product Applicability Guides (PAGs) vary in their depth and focus based upon the product under evaluation. In this instance, the PC Matic platform was scored against a HIPAA controls matrix for four technical safeguards. For simple products that target a single function, a PAG can make statements about their use in a compliance program. For more complex products or platforms like the PC Matic platform that have diverse capabilities and require significant configuration before use, Coalfire recommends narrowing down the diversity by proposing a use case or scenario to measure its applicability to HIPAA (i.e., Privacy and Security Rules).

This PAG may be useful for CE&BAs desiring to utilize application whitelisting technologies within the HIPAA Security Rule compliance program framework, as it discusses the relevant PC Matic platform security capabilities applicable to supporting or addressing risks associated with application whitelisting and the specifics of HIPAA Security Rule requirements. This white paper focuses on the technical security features (i.e., safeguards) and capabilities of the PC Matic platform as they align with these requirements.

Use of the Terms *Review* and *Control*

Coalfire uses the term *review* as a notional method of conducting a use-case scenario in a hosted test environment on the Falcon Platform.

In this PAG, Coalfire will use the term *control* to denote the application of an approach to a HIPAA safeguard. Because it is customary that the CE&BA will use another controls framework (such as, NIST SP800-53 or ISO 27001) to create their actual program of security to satisfy the HIPAA Security Rule, Coalfire makes use of the term "control."

INTRODUCING THE HIPAA SECURITY RULE

The HIPAA Security Rule specifically focuses on the safeguarding of electronic Protected Health Information (ePHI) by implementing administrative, physical, and technical safeguards. Organizations that must comply with this rule face frequent challenges to safeguard ePHI from a myriad of internal and external risks. As it is a requirement of the Security Rule, compliance is mandatory for organizations defined by HIPAA as a CE&BA. The Security Rule is based on the fundamental concepts of flexibility, scalability, and technology neutrality. Therefore, no specific requirements for the types of technology to implement are identified. The Security Rule allows a covered entity to use any security measures (as best determined by the CE&BA) that allow it to reasonably and appropriately implement the standards and implementation specifications (HHS, 2007). As a subset of information, under 45 CFR § 164.306 Security standards: General rules, these organizations are required to:

- Ensure the confidentiality, integrity, and availability of all ePHI the CE&BA creates, receives, maintains, or transmits.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against anticipated unauthorized uses or disclosures of PHI not permitted by the Privacy Rule.
- Ensure compliance with its workforce.

Additionally, in § 164.306(b), the Flexibility of Approach provides key guidance for focusing compliance decisions, including factors a covered entity must consider when selecting security measures such as technology solutions. The requirements of the HIPAA Security Rule are organized according to safeguards, standards, and implementation specifications; the major sections include:

- Security Standards: General Rules
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures and 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 is 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 concerning 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 an addressable implementation specification or an alternative. If the organization chooses an alternative control or determines that a reasonable and appropriate alternative is not available, it must fully document its decision and reasoning.

The Relationship Between the Security Rule and the Privacy Rule

HIPAA required the Secretary of HHS to develop regulations protecting certain health information's privacy and security. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. Within HHS, the Office for Civil Rights (OCR) enforces these rules with voluntary compliance activities and civil money penalties (HHS, 2021). The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards to protect certain health information. The Security Standards for the Protection of Electronic Protected Health Information (known as the “Security Rule”) establishes a national set of security standards to protect certain health information held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that covered entities must put in place to secure individuals’ ePHI. This white paper's scope is to discuss how the PC Matic platform applies to the 4 HIPAA technical controls.

The Relationship Between HIPAA and HITECH

The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009 to help promote the adoption and use of health information technology. The HITECH Act was drafted and integrated into the HIPAA framework to extend protections and address the privacy and security concerns associated with the ePHI. HITECH introduces several new security standards and upgrades the existing standards in HIPAA to protect healthcare stakeholders.

The relationship between HITECH and HIPAA is in how HITECH strengthened the enforcement of the existing HIPAA security standards. This consists of three notable impacts to enforcement of the existing HIPAA security standards which includes:

- The scope of compliance was expanded to include the Breach Notification Rule to HIPPA
- The sharing of responsibilities was extended from not only CE’s but now also includes BE’s
- The penalties for noncompliance were increased and a new tiered fee system was introduced

SUGGESTIONS FOR THE USE OF THIS PAG

This white paper and the supporting controls workbook are intended to be used by various CE&BA and other interested parties involved in the sales, construction, operation, or infrastructure assessment based on the PC Matic platform. It guides PC Matic customers in understanding the controls built into the core infrastructure space, as well as the general availability of control options that the customer may implement.

PC Matic's customers may include hospitals and provider organizations; healthcare solution service providers; Software as a Service (SaaS) providers, designated entities, others who share responsibility with a covered entity.

ADDITIONAL USEFUL PUBLICATIONS

The National Institute of Standards and Technology (NIST) has also published Special Publication (SP) 800-167, Application Whitelisting Guide. The purpose of this document is to explain the security concerns associated with security technologies and make practical recommendations for addressing those concerns when planning for, implementing, and maintaining application whitelisting platforms. While NIST SP 800-167 is not specific to HIPAA, it can be useful guidance as it pertains to addressing the risk associated with application whitelisting.

Other publications that are useful in understanding the NIST and HIPAA Security Rule are the following:

- NIST SP 800-66 Rev. 1., An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.
  - This publication maps NIST SP 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations requirements to HIPAA Security Rule safeguards and requirements and ties the HIPAA Security Rule to a framework for managing risk.

OBJECTIVES OF THIS WHITE PAPER

The primary objective for this white paper is to render an opinion on the PC Matic platform's suitability to assist customers in meeting the requirements of HIPAA using a particular reference architecture, which is presented in detail here. It is the intent of the authors to use the following process to illustrate the findings and satisfy these objectives:

- Choose a likely and relevant use case for the PC Matic platform
- Show the specific configuration used for a test scenario
- Reveal additional technical details of the applications used to host and secure the infrastructure
- Collect artifacts, perform sampling, and document findings on a per-control basis
- Make relevant statements about each control family and the particulars of the PC Matic platform implementation that may support meeting objectives of controls
- Confirm Coalfire's opinion

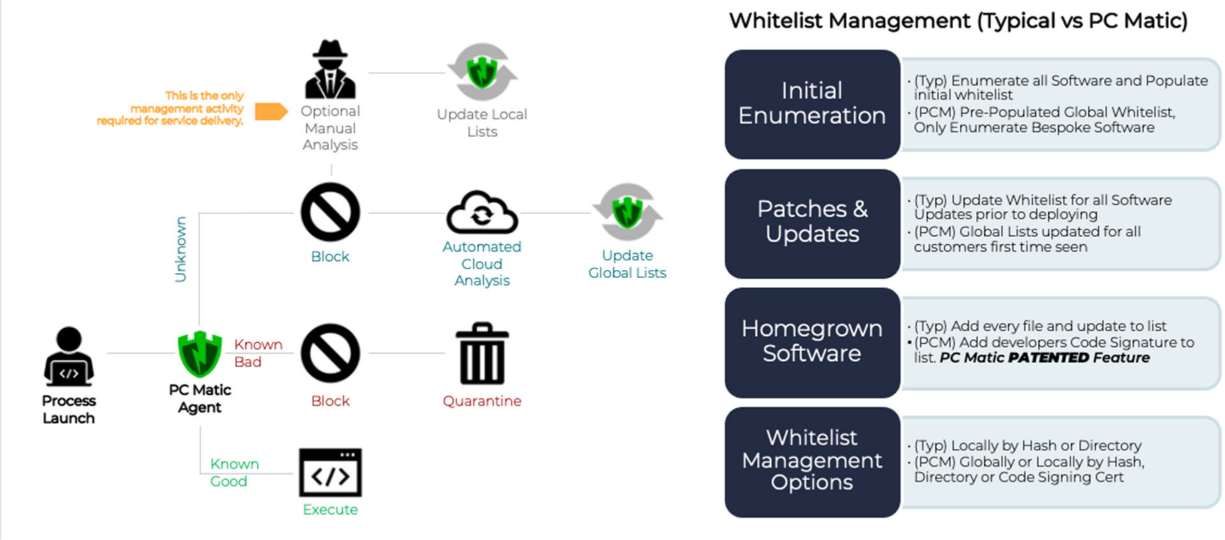
Although the opinion itself may be helpful, this paper also contains a representative overview of many aspects of the HIPAA process and practices. It is a secondary objective of this white paper to inform a newcomer to HIPAA of a technical approach to using application whitelisting to protect endpoint systems.

Since the review of the PC Matic platform was not being conducted on an actual CE&BA, Coalfire focused on the technical controls for HIPAA. Coalfire did not review organizational processes, training, procedures, written supporting materials, or other non-technical controls listed in the HIPAA Security Rule. The responsibility of HIPAA processes, such as organizational, procedural, and training controls, which pertain to the actuality of implementation by a CE&BA, falls on the customer.

This paper contains a representative overview of many aspects of HIPAA Security Rule processes and practices in the following section.

PC MATIC PLATFORM

The PC Matic platform is a comprehensive enterprise-grade cyber security endpoint solution that utilizes globally automated whitelisting technology, fileless malware detection, and remote desktop protocol (RDP) port protection from brute force attacks. The PC Matic platform helps healthcare organizations looking to protect their environments and meet HIPAA requirements by augmenting the existing endpoint security stack. The PC Matic platform achieves this by securing endpoints against threats through automating the whitelisting and blacklisting process with the use of its globally supported and managed whitelist technology. Below in figure 1 is PC Matic's whitelist management process compared to traditional whitelist management methods.



Whitelist Management (Typical vs PC Matic)

Initial Enumeration	· (Typ) Enumerate all Software and Populate initial whitelist · (PCM) Pre-Populated Global Whitelist, Only Enumerate Bespoke Software
Patches & Updates	· (Typ) Update Whitelist for all Software Updates prior to deploying · (PCM) Global Lists updated for all customers first time seen
Homegrown Software	· (Typ) Add every file and update to list • (PCM) Add developers Code Signature to list. ***PC Matic PATENTED Feature***
Whitelist Management Options	· (Typ) Locally by Hash or Directory · (PCM) Globally or Locally by Hash, Directory or Code Signing Cert

Figure 1: PC Matic Whitelist Management

The PC Matic platform provides proactive detection through the use of application whitelisting. Traditional whitelisting solutions require organizations to manually create whitelists for known good applications in the environment, which can create difficulties for security analysts to manage and keep up to date with the changing application and development needs of most healthcare and enterprise environments.

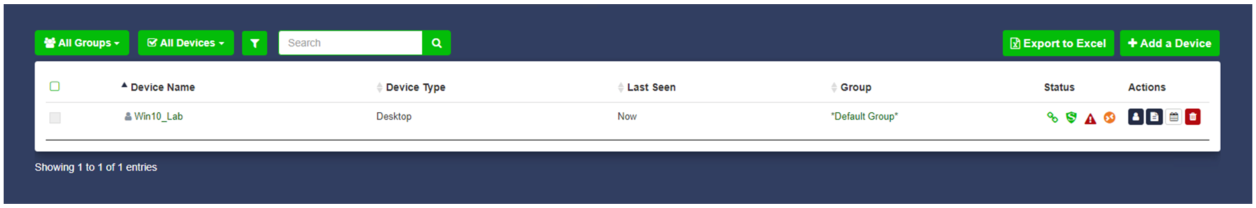
The PC Matic platform helps mitigate this by utilizing a globally automated whitelist solution managed by a team of professional malware researchers that analyze the applications detected in the organizations and categorizes them by level of threat.

PC MATIC CORE SERVICES

The PC Matic platform contains the following features that assist healthcare and enterprise organizations with managing the security of their endpoint environments. The core services are accessible from the PC Matic platform console, which provides the user with a centralized source for an organization's endpoints. The PC Matic platform provides flexibility to organizations of any size to manage their environment with pre-configured, out of the box security for less hands-on organizations, while also providing advanced capabilities for more in-depth configurations and control for organizations that require it.

Devices

The Devices tab allows the viewing of the endpoints that have the PC Matic platform shield installed. From the device tab shown in figure 2, the status and health of the endpoints can be viewed, and action can be taken to manage the endpoints.



□	Device Name	Device Type	Last Seen	Group	Status	Actions
□	Win10_Lab	Desktop	Now	*Default Group*		

Showing 1 to 1 of 1 entries

Figure 2: Devices Tab View

The endpoints can be placed in groups to allow for granular policy control according to best practices for the organization's environment, as seen in Figure 3.

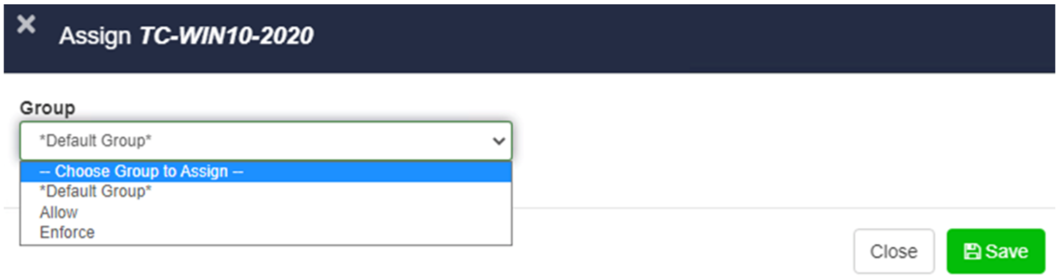
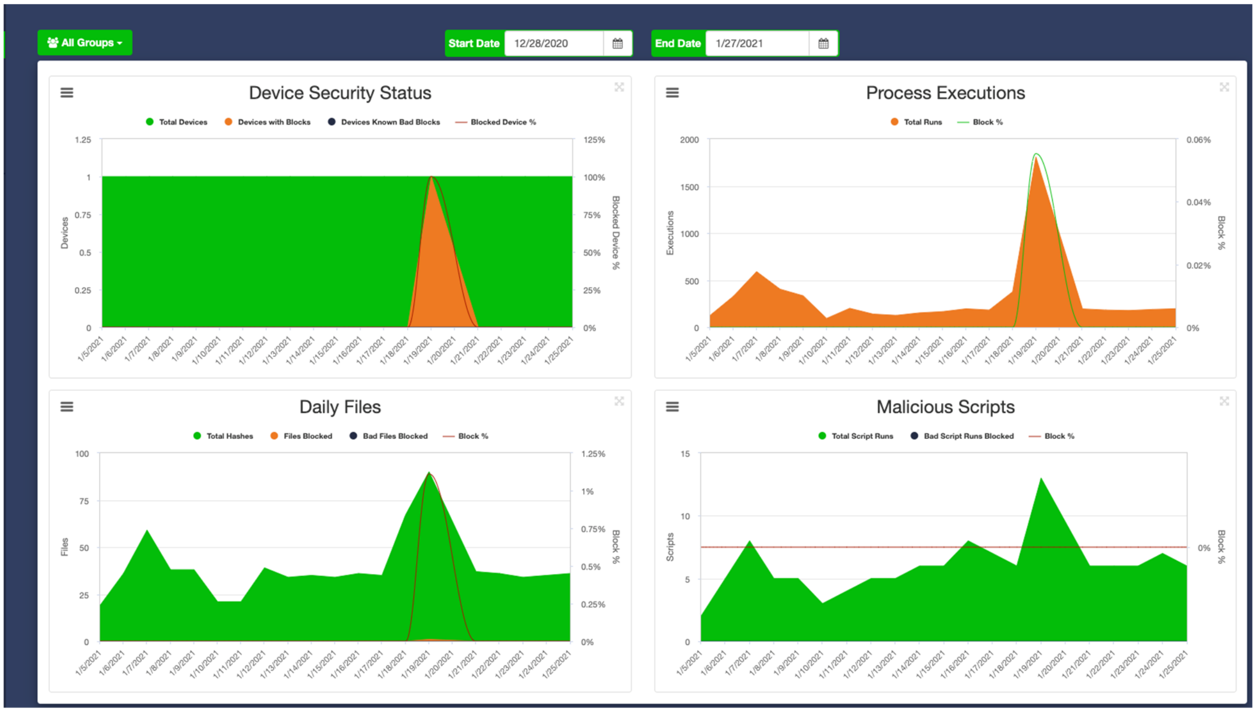


Figure 3: Example of Groups

These groups can be managed from the console. Placing endpoints into groups allows organizations to manage the settings, policies, and patch management of the endpoint agents by grouping them based on the level of control or restrictiveness required.

Dashboard

The dashboard shown below in figure 4 provides a high-level view into endpoint events and health. The view can be changed to show all device groups or the individual groups, with the ability to adjust the date range to view current or historical events. The dashboard can be beneficial to organizations that need to monitor specific endpoint groups or for the overall organization.



All Groups

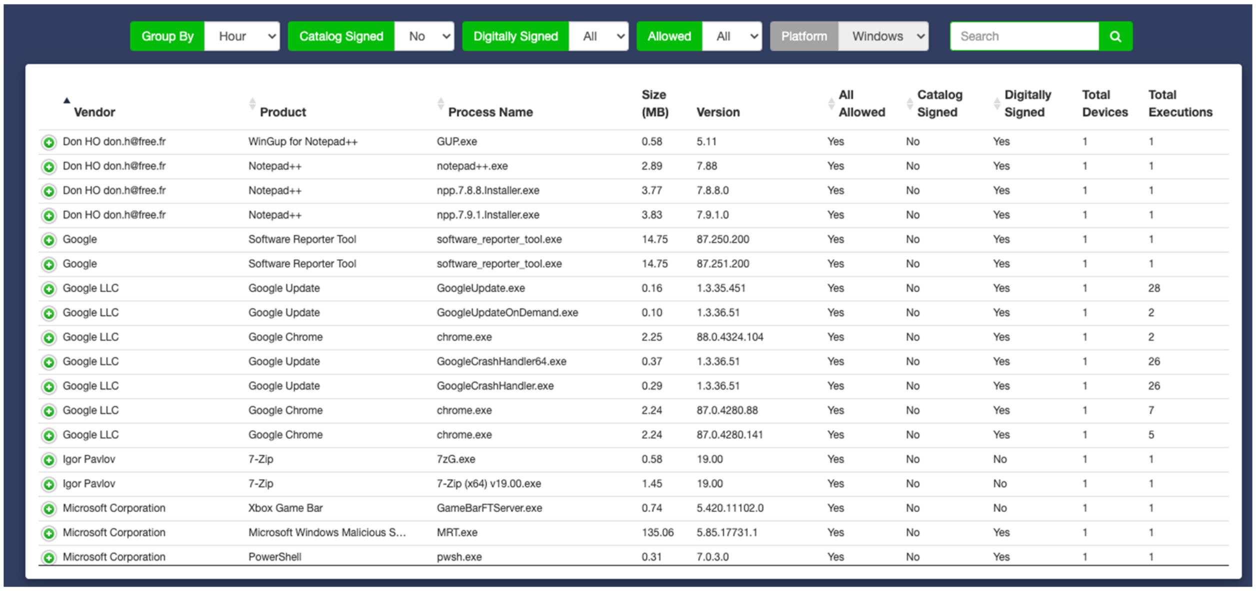
Start Date: 12/28/2020

End Date: 1/27/2021

Figure 4: PC Matic Platform Dashboard

Process Activity

The process activity dashboard seen below in figure 5 provided by the PC Matic platform allows a security analyst to see all processes that have been executed in the environment. Understanding what processes are running on an endpoint and how they are being consumed is a key component to threat hunting. Identifying which processes were successful and which ones were unsuccessful gives a view of what is occurring at the endpoint and if there are abnormalities that could represent a vulnerability.

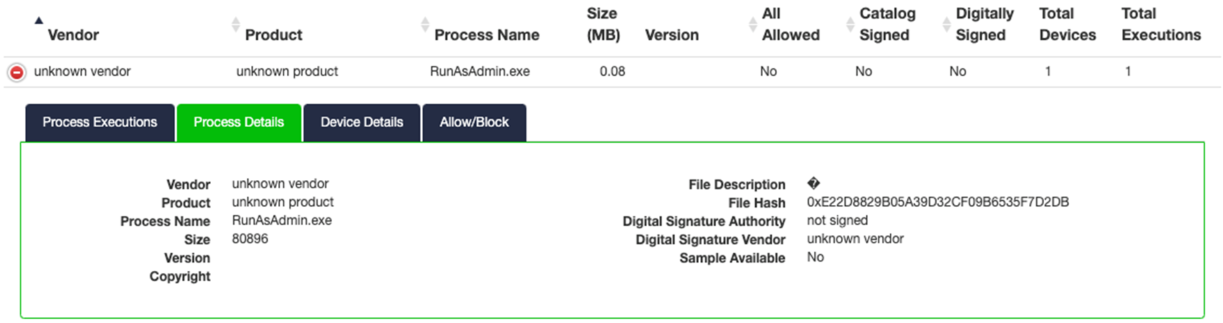


Group By: Hour | Catalog Signed: No | Digitally Signed: All | Allowed: All | Platform: Windows | Search

Vendor	Product	Process Name	Size (MB)	Version	All Allowed	Catalog Signed	Digitally Signed	Total Devices	Total Executions
Don HO don.h@free.fr	WinGup for Notepad++	GUP.exe	0.58	5.11	Yes	No	Yes	1	1
Don HO don.h@free.fr	Notepad++	notepad++.exe	2.89	7.88	Yes	No	Yes	1	1
Don HO don.h@free.fr	Notepad++	npp.7.8.8.Installer.exe	3.77	7.8.8.0	Yes	No	Yes	1	1
Don HO don.h@free.fr	Notepad++	npp.7.9.1.Installer.exe	3.83	7.9.1.0	Yes	No	Yes	1	1
Google	Software Reporter Tool	software_reporter_tool.exe	14.75	87.250.200	Yes	No	Yes	1	1
Google	Software Reporter Tool	software_reporter_tool.exe	14.75	87.251.200	Yes	No	Yes	1	1
Google LLC	Google Update	GoogleUpdate.exe	0.16	1.3.35.451	Yes	No	Yes	1	28
Google LLC	Google Update	GoogleUpdateOnDemand.exe	0.10	1.3.36.51	Yes	No	Yes	1	2
Google LLC	Google Chrome	chrome.exe	2.25	88.0.4324.104	Yes	No	Yes	1	2
Google LLC	Google Update	GoogleCrashHandler64.exe	0.37	1.3.36.51	Yes	No	Yes	1	26
Google LLC	Google Update	GoogleCrashHandler.exe	0.29	1.3.36.51	Yes	No	Yes	1	26
Google LLC	Google Chrome	chrome.exe	2.24	87.0.4280.88	Yes	No	Yes	1	7
Google LLC	Google Chrome	chrome.exe	2.24	87.0.4280.141	Yes	No	Yes	1	5
Igor Pavlov	7-Zip	7zG.exe	0.58	19.00	Yes	No	No	1	1
Igor Pavlov	7-Zip	7-Zip (x64) v19.00.exe	1.45	19.00	Yes	No	No	1	1
Microsoft Corporation	Xbox Game Bar	GameBarFTServer.exe	0.74	5.420.11102.0	Yes	No	No	1	1
Microsoft Corporation	Microsoft Windows Malicious S...	MRT.exe	135.06	5.85.17731.1	Yes	No	Yes	1	1
Microsoft Corporation	PowerShell	pwsh.exe	0.31	7.0.3.0	Yes	No	Yes	1	1

Figure 5: Process Activity Dashboard

The process activity dashboard will show the process details shown in figure 6 including the vendor's name, product, file hash, and other information that is vital to understanding what threats could be present on the endpoint.



Vendor	Product	Process Name	Size (MB)	Version	All Allowed	Catalog Signed	Digitally Signed	Total Devices	Total Executions
unknown vendor	unknown product	RunAsAdmin.exe	0.08		No	No	No	1	1

Vendor	unknown vendor	File Description	�
Product	unknown product	File Hash	0xE22D8829B05A39D32CF09B6535F7D2DB
Process Name	RunAsAdmin.exe	Digital Signature Authority	not signed
Size	80896	Digital Signature Vendor	unknown vendor
Version		Sample Available	No
Copyright			

Figure 6: Detailed Process Activity

The process activity dashboard will also disclose why a process was allowed or why it may have been blocked. This allows a security analyst to gain real-time visibility into endpoints, detect threats, and take the proper action. Understanding all processes that are normal on an endpoint can be a difficult task without the proper tools, which could lead to threats being missed because the processes can change due to updates and other changes to the endpoint. A security analyst may have to spend time to detect if a process is truly malicious or a false positive.

Lifelines

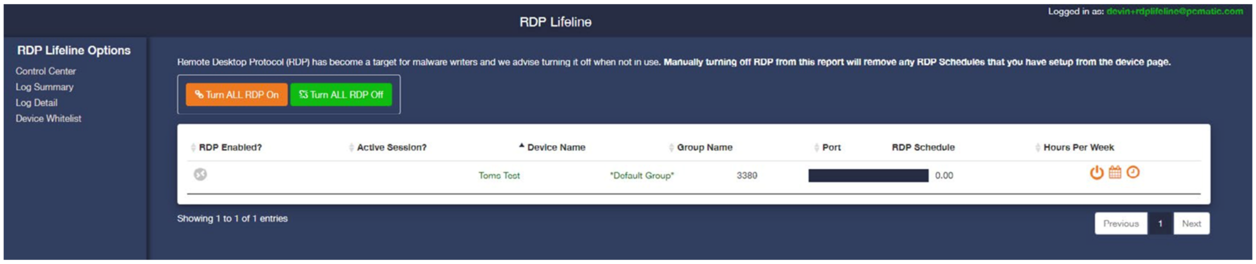
The PC Matic platform offers healthcare organizations Lifeline service options that make managing the solution more accessible to organizations, especially in situations where facilities may not have onsite IT support staff to maintain day to day operations and may not possess the depth of experience in cyber security to keep on top of emerging threats. These Lifelines include services such as RDP Lifelines and Ransomware Lifelines.

Ransomware Lifelines

Ransomware Lifelines provides an out of the box solution that is designed for organizations with the need for enterprise-level protections but may not have available security analysts or support staff to manage the day-to-day operations and configuration of the endpoint security tools. Ransomware Lifelines provides a pre-configured and automated whitelist solution that is managed by a team of professional malware researchers that can automatically analyze and categorize blocked or unknown applications.

RDP Lifelines

RDP Lifelines gives organizations additional tools to protect against the risk of malicious attacks that can be executed through exploiting the RDP ports. Security teams can leverage the capabilities in RDP Lifeline to manage the availability of the RDP sessions by scheduling available times or by enabling or disabling the access per device as needed (as seen in Figure 7). All remote session activity is captured in a comprehensive audit log that enables visibility for security teams.



Remote Desktop Protocol (RDP) has become a target for malware writers and we advise turning it off when not in use. **Manually turning off RDP from this report will remove any RDP Schedules that you have setup from the device page.**

RDP Enabled?	Active Session?	Device Name	Group Name	Port	RDP Schedule	Hours Per Week
⊗		Toms Test	*Default Group*	3380	▬ 0.00	⏻ 📅 ⏲

Showing 1 to 1 of 1 entries

Figure 7: RDP Lifeline Controls

Vulnerabilities

Managing application vulnerabilities in the healthcare endpoint environment is a key requirement to effectively develop a vulnerability management approach. Once the software discovery requirement is satisfied, vulnerability tools can be used to detect vulnerabilities that are present, and the steps required to remediate. This allows an organization to gain an understanding of the threat landscape that may be present at any time. However, these solutions require extensive staff and can be time consuming to perform correctly. The PC Matic platform provides extensive reporting and complete endpoint visibility, giving the organization a comprehensive view of the health of the endpoint and the processes and software that are running on the endpoint. This can reduce the manual effort that is often required to conduct software discovery and mapping.

THREAT MANAGEMENT

For healthcare organizations, meeting the requirements for HIPAA requires selecting the best antivirus solution for the endpoint systems that protects both the operation of the business and the patient data that may be accessible from the endpoints. The PC Matic platform augments the healthcare organizations existing endpoint zero-trust security strategy by filling in potential gaps in the organization’s overall security.

The PC Matic platform approaches application whitelisting by analyzing several attributes of the application or files to determine whether it is a known good or a known bad. These attributes are populated and checked against PC Matic’s custom Global Allowlist. The PC Matic platform provides flexibility when it comes to selecting the best application whitelisting approach for an organization’s environment. There are three main approaches to implementing application whitelisting that are configurable within the PC Matic platform:

- File & Folder Path Attributes - While this is not the most secure approach for application whitelisting, it offers a more convenient way for organizations to implement this solution quickly in the environment by selecting the file name, file size, or an entire directory the files reside in to be set as known good. This is typically a recommended solution for developers or application testers to have a designated directory from which they can execute applications that may normally be flagged. Using this approach, however, could create a potential exploitable safe area for malicious code to be executed from.
- Digital Signature Attributes - This method offers more security by using the digital signatures of applications to verify the authenticity of the application publisher and detect if it has been modified, which could lead to potential malicious behavior.
- Cryptographic Hash Attributes - Using the cryptographic hash values of an application to identify the unique hash identifier MD5, SHA-1, or SHA-256 value of the file is the most secure method implementing application whitelisting. This method, when combined with digital signatures, provides a secure and manageable solution to using application whitelisting in any environment.

One of the most common challenges for organizations implementing application whitelisting is managing false positives. False positives in traditional application whitelisting solutions occur when an application is blocked even though it was believed to be a known good application. This requires IT support staff to manage a list of allowed applications and maintain it as new or updated applications are introduced into the environment.

The PC Matic platform helps organizations manage application whitelists by providing a centralized platform and addressing the three main approaches of a mature whitelisting program, as described above.

SCOPE AND APPROACH FOR REVIEW

The understanding of the PC Matic platform and its combined capabilities was gained through a product specification and documentation provided by PC Matic and generally made available from PC Matic's public-facing website. Coalfire has further conducted interviews and engaged in live product demonstrations with PC Matic personnel and subject matter experts. The Coalfire Opinion Series PAGs benefit from the careful selection of possible and impactful use cases, highlighting critical areas within a product to evaluate potential HIPAA compliance.

Coalfire's review of the PC Matic platform began with a general alignment of the technology's applicability against the high-level HIPAA requirements and objectives. This was further narrowed down to specific requirements that the PC Matic platform's capabilities and features could support. An analysis of the reviewed technology capability to address applicable requirements was then conducted. This analysis primarily focused on what an assessor might review when following HIPAA testing guidance during a HIPAA technical safeguards assessment.

The review of requirements was comprehensive and included identifying gaps for which the technology may not be sufficient to address. This does not include addressable requirements through other means, including, but not limited to, organizational procedures or the provision of additional third-party technologies.

SCOPE OF TECHNOLOGY AND SECURITY STANDARD TO REVIEW

The review's primary focus included the features and functionality of the PC Matic platform, along with the supporting underlying features and functionality as deployed in CE&BA architecture.

For this review, Coalfire included requirements from the HIPAA of 1996 and the Health Insurance Reform: Security Standards; Final Rule publication dated February 20, 2003, from the Department of Health and Human Services (HHS) Office of the Secretary available from https://www.hhs.gov. For a broader understanding of the requirements and their applicability to technical solution implementation, Coalfire also reviewed supporting documentation provided by NIST and HHS, including assessment guidance, the HIPAA Security Risk Assessment Tool, Security Rule Guidance Material, and Frequently Asked Questions. Applied understanding of the HIPAA Security Rule requirements and guidance was supplemented by documentation and guidance on relevant subjects, including NIST SP 800-167.

PC Matic Suggested Use Case

Coalfire selected a generalized use case for the evaluation of the PC Matic platform.

This use case is defined as either a CE&BA, operating at one or multiple on-premises user locations, providing services as a healthcare provider, health plan entity, healthcare clearinghouse, or a supporting business associate.

Data services to the entity are delivered from any combination of co-located data centers, external hosting, or cloud hosting facilities that deliver line-of-business applications, and externally hosted Software as a

Service (SaaS) providers, who provide services under a business associate agreement (BAA). ePHI is contained within firewall-controlled boundaries at the on-premises user location and at all hosting sites. Cloud-based PC Matic control services are delivered over an Internet connect to the entity endpoints, and centrally managed for enrollment, updates, and alerting.

The PC Matic platform whitelisting and blacklisting baselines are configured to specifically allow all required line-of-business applications used to manage ePHI and for other business operations on the endpoints. Endpoints have the PC Matic platform installed, licensed, activated, and pervasively connected to the PC Matic cloud service. A zero-trust model, which specifically whitelists approved applications and denies all unlisted applications.

COALFIRE EVALUATION METHODOLOGY

Coalfire initially examined the HIPAA Security Rule requirements and identified them as either procedural (e.g., organizational) or technical (e.g., implementation). Qualification of a procedural or technical requirement was based on a review of the requirement narrative, testing procedures, and guidance.

Non-technical procedural requirements including the definition and documentation of policies, procedures, and standards were not considered directly applicable to the technical solution. Likewise, non-technical requirements, including operational procedures that describe manual processes, were not assessed against the technology’s capability. Examples of these types of non-technical requirements generally included maintaining facility visitor logs, verifying an individual’s identity before granting physical or logical access, the performance of periodic physical asset inventories, or generation of network topology or flow diagrams.

Technical requirements were assessed to determine the solution or solution components' applicability to address all requirements that are part of the standard. The achievement of the requirement objectives was more likely to be met using a technology external to the PC Matic platform or was not an inherent feature or capability of the PC Matic platform. The assessed technology was determined to be not applicable or capable of addressing the safeguard or requirement. An example of HIPAA requirements that Coalfire determined that the PC Matic Platform was not able to inherently address are the Administrative Safeguards, Physical Safeguards, Organizational Safeguards, and Policies and Procedures and Documentation Requirements. These safeguards and requirements are the customer’s responsibility. These areas would more likely be addressed by adding a third-party, or partner solution, which can be applied to or integrated with the platform. All HIPAA Security Rule standards are considered pertinent and applicable to any system that stores, processes, or transmits ePHI.

Coalfire further assessed the capability or the degree to which the solution could address the HIPAA Security Rule standard Security Rule standard. Coalfire designated a qualitative category of capability for applicable requirements, including whether the solution was determined to support the requirement, partially support the requirement fully, or unable to support the requirement. In cases where the requirement was determined to be applicable but unsupported, additional thought for using third-party solutions should be considered.

EVALUATION OF HIPAA CONTROLS SCORING SYSTEM

Where the requirement was qualified as applicable, Coalfire further assessed the capability of the solution to address the requirement. For applicable requirements and in keeping with the desire to present the information compactly, Coalfire designated a qualitative category of capability, including whether the solution had a fractional capacity to support a percentage of the controls.

This key, using Harvey Balls (https://en.wikipedia.org/wiki/Harvey_Balls), describes the meaning of the Score column for each requirement in the scoring tables below:

SYMBOL	DESCRIPTION	DEFINITION
U	Solid	>75% Supported
T	Three-fourths	>50% - 75%
W	Half	>25% - 50%
R	One-quarter	>0% - 25%
Q	Empty	Impedes Support
	Blank	Not Applicable (N/A)
n̲	n-bar	Notional Control

Table 1: Key for Score and Other Symbols

Summary of Overall PC Matic Platform HIPAA Scoring

Coalfire's scoring system, shown below in the PC Matic Platform column, summarizes Coalfire's findings for the PC Matic platform's HIPAA control applicability to the four HIPAA technical safeguards. The PC Matic platform fully supports each technical safeguard within its platform. Table 2 below shows the PC Matic platform's overall scoring.

HIPAA INDEX	POLICY AREA	STANDARD	PC MATIC PLATFORM
164.312(a)(1)	Access Control	Access Control	T
164.312 (a)(2)(i)	Access Control	Unique User Identification	T
164.312 (a)(2)(iii)	Access Control	Automatic Logoff	W
164.312 (b)	Audit Controls	Audit Controls	W

Table 2: HIPAA Overall PC Matic Platform Scoring

The table above is an aggregate score of the PC Matic platform based on a composite of the scores shown below. Any customer responsibilities for the platform's elements are called out in their respective detailed section. In this overall scoring representation, Coalfire has included only the requirements that were applicable to the PC Matic platform.

Summary of Customer Responsibilities for HIPAA Standards

The summary below shows HIPAA compliance framework responsibilities that CE&BAs should include in their environment.

- Create a risk management plan to evaluate potential risks to ePHI and business continuity, and to respond with actions to support HIPAA security and privacy rules
- Design and deploy technical infrastructure, hardware, and software to ultimately support the HIPAA policy by compliance with the cybersecurity framework's controls.
- Ensure the confidentiality, integrity, and availability of all ePHI the CE&BA creates, receives, maintains, or transmits.

- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required.
- Ensure compliance by its workforce with appropriate training, separation of duties, and authorization to access all entity systems, including those containing ePHI.
- Use security measures dictated by the cybersecurity framework to implement the technical controls, policies, and procedures reasonably and appropriately.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

PC MATIC PLATFORM APPLICABILITY TO HIPAA

This section reveals Coalfire's compliance findings and the corresponding customer requirements and responsibilities for the PC Matic platform elements as it was reviewed in Coalfire's analysis of the suggested use case.

The narratives that follow detail HIPAA Security Rule technical safeguards that PC Matic has applicability to address or support. This applicability applies either as a customer configurable item within the PC Matic platform or as a native and default capability to address or support the safeguard. The PC Matic customer is also referred to as the CE&BA. The findings are specific to the PC Matic platform and are not inclusive of security control implementation necessary for the underlying layers of the comprehensive environment, including hardware, additional software, or additional underlying platforms and components.

PC MATIC APPLICABILITY DETAIL

The section details the PC Matic platform's inherent capabilities for alignment to address or support HIPAA Security Rule technical safeguard requirements.

Access Control

164.312(a)(1) Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4) [Information Access Management].

General Guidance

The CE&BA should inventory and understand the technical access control capabilities available to customers and systems for the PC Matic platform. The CE&BA should also inventory and understand the administration, user, and system access methods and requirements for PC Matic. The CE&BA should then analyze the operations to identify all customers' access needs and systems both to and from the PC Matic platform and the endpoints. This will be the framework for assigning and providing specific and organizationally defined access to the PC Matic platform.

The CE&BA should understand how role-based access controls (RBACs) are defined, assigned, and enforced within the PC Matic platform.

The CE&BA should ensure that all system users are assigned a unique identifier. Any default, generic, or group identifiers and associated credentials for customers that cannot be tied back to a specific user identity should be disabled or archived. All activities recorded by PC Matic customers should be logged with enough storage space to support log retention standards. Audit logs should be sent to a third-party log aggregation solution or security information and event management (SIEM) solution.

CE&BA's should be properly trained, including platform-specific security awareness training aligned to the role and function they perform. The CE&BA should establish formal policies, processes, and procedures to guide access control for the organization, including access controls relative to the PC Matic platform.

As a part of access control procedures, the CE&BA should identify responsible parties for managing, implementing, and maintaining the access control procedures. Procedures will also be necessary for performing the regular review of granted access as part of ongoing operations. Procedures should include steps for the assignment or updating of access, including initial access, increased access, and access to additional systems and applications. The CE&BA will also want to establish procedures for the termination of access that accounts for all previously granted access assigned to the terminated user.

User and System Access

The PC Matic platform's RBACs enable granular control on which users can perform what actions on entities such as endpoints and applications. These capabilities provide the technical controls required to manage access rights across the platform. Using the RBACs allows customers to define different roles in their organization and assign permissions according to job role.

The PC Matic platform provides support for the unique user identification access control measures by providing an authentication feature that requires an agent to be installed on the host endpoint the user is accessing the console from.

Automatic logoff controls are managed through the PC Matic platform. The login page automatically logs out sessions that are idle for 15 minutes. The customer cannot change this from the console, but the duration can be modified by request during the onboarding of the PC Matic platform.

HIPAA INDEX REQUIREMENT	CORE PLATFORM
Access Control 164.312 (a)(1)	T
Access Control 164.312 (a)(2)(i)	T
Access Control 164.312 (a)(2)(iii)	W

Table 3: PC Matic Access Control Scoring

Customer Responsibilities for HIPAA Access Control

It is recommended that administrator or privileged access be limited through defined control points such as a designated host or endpoint. This approach limits direct access for privileged access to the PC Matic platform console. At this point, additional access controls can be enabled and enforced, such as idle session termination.

A CE&BA can comply with this standard through a combination of access control methods and technical controls, a variety of which are available within most information systems. The HIPAA Security Rule does not identify a specific type of access control method or technology to implement.

The implementation specifications that apply to the PC Matic platform and are associated with the Access Control standard include the following:

1. Unique User Identification (Required)
   - A CE&BA must determine the best user identification strategy based on job function and operations.
2. Automatic Logoff (Addressable)

- The CE&BA should ensure that a session after a predetermined time of inactivity is disconnected.

Audit Controls

164.312(b) Audit Controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

Guidance

Typically, the CE&BA's endpoints directly access ePHI and should determine the activities that will be tracked and audited, to including activities specific to the functioning of the PC Matic platform and activities associated with the management and operation of the PC Matic platform itself. The discovered and defined activities the CE&BA selects for audit may likely include those that represent the greatest risk to the confidentiality, integrity, and availability of ePHI. The organization can identify the parts of the system, applications, or processes that can potentially introduce vulnerabilities to the data for tampering, inappropriate uses, or disclosures. It will be important for the CE&BA to understand the context of actions that can be performed with the PC Matic platform. The CE&BA should define what data should be captured to represent best an audit trail that can support the recreation or retracing of actions or steps carried out as part of the incident investigation.

The CE&BA should define policies, processes, procedures, and standards for audit controls that include who is responsible for the overall audit process and results, how often audits will take place, how often audit results will be analyzed, where the audit information will reside, and what actions will be taken for audit findings that reveal employee violations. Additional elements of audit controls that are important for consideration include defining processes and mechanisms for reporting, notification, incident response, and review. Finally, the CE&BA will be responsible for ongoing assessment of the effectiveness of their audit process to detect and report on security incidents with a plan to revise as necessary to continuously improve the audit program's effectiveness.

PC Matic Support for Audit Controls

The PC Matic platform can generate audit logs that can track the access and actions taken by users and services within the platform. The PC Matic platform can support the audit requirements by generating auditable events and logs that contain information to establish what type of event occurred, when the event occurred, where the event occurred and the identity of the service, or individual associated with the event.

The PC Matic platform generates audit records and events of actions taken by customers or system components against endpoints and web console activity. The CE&BA should be responsible for determining the system's capabilities for auditing events that the organization defines as important or necessary for identifying security incidents.

HIPAA INDEX REQUIREMENT	CORE PLATFORM
Audit Controls 164.312 (b)	W

Table 4: PC Matic Audit Controls Scoring

Customer Responsibilities for HIPAA Audit Controls

The Audit Controls standard requires a CE&BA to implement hardware, software, or procedural mechanisms that record and examine activity in systems that contain or access ePHI. The HIPAA Security Rule does not specify the type of data gathered by the audit controls or how often the audit reports should be reviewed. A CE&BA should consider its risk and organizational factors, such as the current technical infrastructure, hardware, and software security capabilities, to determine the appropriate audit controls for systems that contain or use ePHI.

The PC Matic platform provides the CE&BA the ability to create an S3 bucket to store audit logs. However, it is the CE&BA's responsibility to ensure the audit logs are properly stored based on organizational policies and regulations.

COALFIRE CONCLUSION

Coalfire reviewed the PC Matic platform for its efficacy in assisting covered entities and business associates in successful deployments resulting in a compliant HIPAA Security Rule program and has the following opinion of the potential product use in the compliance program.

The PC Matic platform, as reviewed by Coalfire, **can be effective** in providing support for the outlined objectives and requirements of the HIPAA Security Rule in support of a HIPAA compliance program. With proper implementation and integration into the organization's greater technical infrastructure and information security management systems. The PC Matic platform may be useable in a HIPAA controlled environment. The organization wishing to use PC Matic should also consider the guidance provided by NIST SP 800-167 when designing their implementation.

Coalfire's opinion is based on observations and analysis of the provided documentation, interviews with PC Matic personnel, and hands-on engagement with a lab environment. The provided conclusions are based upon several underlying presumptions and caveats, including adherence to vendor best practices the and hardening of configuration supported by the system components. This solution should be implemented in alignment with the organization's mission, values, business objectives, general approach to security and security planning, and concerning the overall organizational security and compliance program.

A COMMENT REGARDING REGULATORY COMPLIANCE

Coalfire disclaims generic suitability of any product to cause a customer using that product to achieve regulatory compliance. ***Customers attain HIPAA compliance through a Governance, Risk, and Compliance (GRC) program, not via the use of a specific product. This is true for covered entities, business associates, service providers, and customers targeting compliance with other regulations.***

LEGAL DISCLAIMER

Coalfire expressly disclaims all liability concerning actions taken or not taken based on the contents of this whitepaper and the supporting controls workbook, and the opinions contained therein. The opinions and findings within this evaluation are solely those of Coalfire and do not represent any other parties' assessment findings or opinions. This document's contents are subject to change at any time based on revisions to the applicable regulations and standards (e.g., Health Information Portability and Accountability Act [HIPAA], PCI DSS, et al.) Consequently, any forward-looking statements are not predictions and are subject to change without notice. While Coalfire has endeavored to ensure that the information contained in this document has been obtained from reliable sources, there may be regulatory, compliance, or other reasons that prevent Coalfire from doing so.

Consequently, Coalfire is not responsible for any errors or omissions, or the results obtained from the use of this information. Coalfire reserves the right to revise any or all of this document to reflect an accurate representation of the content relative to the current technology landscape. To maintain this document's contextual accuracy, all references to this document must explicitly reference the document's entirety, including the title and publication date. Neither party will publish a press release referring to the other party or excerpting highlights from the document without the other party's prior written approval. For questions regarding any legal or compliance matters referenced herein, you should consult legal counsel, your security advisor, or the relevant standard authority.

REFERENCE MATERIALS

We recommend that you review this helpful reference material:

1. PC Matic Pro technical and marketing information may be located at: https://www.pcmatic.com/pro/
2. Introductory details of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) may be found on the US Department of Health and Human Services (HHS) website at: https://www.hhs.gov/hipaa/index.html
3. Additional information on the 2009 HITECH Act is located at: https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html
4. National Institute of Standards and Technology (NIST) SP 800-167 Guide to Application Whitelisting is available in a final 2015 revision at this link: https://csrc.nist.gov/publications/detail/sp/800-167/final
5. NIST SP 800-53 rev. 5, Security and Privacy Controls for Information Systems and Organizations is available in the most recent 2020 revision at this link: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
6. Coalfire corporate information is available at https://www.coalfire.com/About

ABOUT THE AUTHOR AND CONTRIBUTORS

Tony Costanzo | Author | Senior Consultant, Product Guidance, Coalfire

As Senior Consultant, Tony is an author and thought leader on information security topics for Coalfire with a specialization in enterprise security.

Chris Krueger | Contributor | Principal II, Product Guidance, Coalfire

As Principal, Chris contributes as an engineer, author, and thought leader on regulatory compliance, information security, and product design topics for Coalfire’s customers in “new and emerging” cybersecurity arenas.

Byron Estrada | Contributor | Senior Consultant, Product Guidance, Coalfire

As Senior Consultant, Byron holds a BSc and a MSc in Cybersecurity and is an author and thought leader on information security topics for Coalfire’s clientele, with a focus on enterprise architecture, cybersecurity, and regulatory compliance frameworks.

Brandon Sessions | Contributor | Chief Revenue Officer, PC Matic

As a Chief Revenue Officer, Mr. Sessions coordinates corporate strategy across operations and sells to ensure continuity of service delivery for all customers.

Andy Paul | Contributor | Director of Service Delivery, PC Matic

As Director of Service Delivery, Mr. Paul leads the operations and compliance efforts for PC Matic, including support for all enterprise customers with a focus on efficiency and customer success.

Published June 2021.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for over 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.