WHITE PAPER

VMWARE CARBON BLACK CLOUD AND WORKSPACE ONE

HIPAA SECURITY RULE COMPLIANCE

LYLE MILLER | CISA, CISSP, QSA, PA-QSA
TERILYN FLOYD-CARNEY | CISA, CISSP, HCISSP, HITRUST CERTIFIED CSF PRACTITIONER

COALFIRE

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

VMware, Inc. ("VMware") engaged Coalfire Systems, Inc. ("Coalfire"), a provider of industry-specific cyber risk management and compliance services, to conduct an independent technical assessment of their VMware Carbon Black Cloud and Workspace ONE platforms against the requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Coalfire conducted assessment activities including technical testing, architectural review, and compliance validation.

In this paper, Coalfire will describe the results of its assessment of the VMware Carbon Black Cloud and Workspace ONE platforms to determine whether they can assist healthcare providers with satisfying the technical aspects of multiple requirements of the HIPAA Security Rule. An explanation of the testing activities performed during Coalfire's review is also included below.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

HIPAA is legislation enacted in the USA in 1996 that provides data privacy and security provisions for safeguarding medical information. The HIPAA Security Rule provides requirements on the safeguarding of electronic Protected Health Information (ePHI), which sets the standards for patient data security.

HIPAA SECURITY RULE

The HIPAA Security Rule specifically focuses on the protection of ePHI through the implementation of administrative, physical, and technical safeguards. Compliance is required of all organizations defined by HIPAA as a covered entity, business associate, or subcontractor. Organizations such as these are required to perform the following activities:

- 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 uses or disclosures of such information that are not permitted by the HIPAA Privacy Rule.
- 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

AUDIENCE

This assessment white paper has two target audiences:

1. **Covered Entities (CEs) and Business Associates (BAs):** This audience may be evaluating the VMware Carbon Black Cloud and Workspace ONE platforms for use within their organization to support HIPAA compliance initiatives.

2. **Administrators and Other Compliance Professionals:** This audience may be evaluating VMware Carbon Black Cloud and Workspace ONE platforms for use within their organization for HIPAA, Payment Card Industry (PCI), or other regulations.

METHODOLOGY

Coalfire completed a multi-faceted technical assessment during the course of this project using security industry and audit best practices. Coalfire conducted technical lab testing in VMware's hosted test environment from October 24, 2020, to November 11, 2020.

At a high level, testing consisted of the following tasks:

- Technical review of the architecture of the full solution and its components.
- Implementation of the VMware Carbon Black Cloud and Workspace ONE platforms agent software in the Coalfire lab environment.
- Introduction of malware binaries on local systems with antivirus (AV) agent software installed.
- Confirmation of the VMware Carbon Black Cloud 's ability to block and remove known malware samples.
- Validation of the Workspace ONE system to ensure HIPAA compliance and security best practices for multiple implementation specifications of the HIPAA regulation.

SUMMARY FINDINGS

The following findings are relevant highlights from this assessment:

- The VMware Carbon Black Cloud and Workspace ONE platforms, as reviewed by Coalfire, **can be effective** in providing support for the requirements of the HIPAA Security Rule listed in Appendix B in support of a HIPAA compliance program. Through proper implementation and integration into an organization's greater technical infrastructure and information security management systems, the VMware Carbon Black Cloud and Workspace ONE platforms may be useful in a HIPAA-controlled environment. An organization that wishes to use these platforms should consider the guidance provided by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-190 when designing its implementation.
- Coalfire's opinion is based on observations and analysis of the provided documentation, interviews with VMware 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 and configuration hardening as supported by the system components. This solution should be implemented in alignment with the customer organization's mission, values, business objectives, and general approach to security and security planning with respect to the overall organizational security and compliance program.
- Customers should consult with VMware for guidance to properly implement the VMware Carbon Black Cloud and Workspace ONE platforms. These platforms can provide coverage for the following safeguards of the HIPAA Security Rule, based on the sample testing and evidence gathered during the assessment:
  - **Administrative Safeguards:** Protection from Malicious Software – 164.308(a)(5)(ii)(B), Password Management – 164.308(a)(5)(ii)(D), Response and Reporting – 164.308(a)(6)(ii)
  - **Physical Safeguards:** Workstation Use – 164.310 (b), Workstation Security – 164.310(c)

  - **Technical Safeguards:** Access Control – 164.312(a)(1), Unique User Identification – 164.312(a)(2)(i), Automatic Logoff – 64.312(a)(2)(iii), Encryption and Decryption – 164.312(a)(2)(iv), Audit Controls – 164.312(b), Person or Entity authentication – 164.312(d), Transmission Security – 164.312(e)(1), Encryption – 164.312(e)(2)(ii)

- The VMware Carbon Black Cloud detected and effectively prevented the execution of known malware samples as required by the 164.308(a)(5)(ii)(B) requirement, Protection from Malicious Software.
- The VMware Carbon Black Cloud client effectively mitigated malware with the following solutions:
  - Blocked and quarantined (i.e., prevented the execution or installation of) malware files
  - Blacklisted malware
  - Deleted malware
  - Terminated malicious processes
- The VMware Carbon Black Cloud and Workspace ONE platforms adequately generated logs of events such that malicious activity, security incidents, and their outcomes could be documented to help meet the requirements of 164.308(a)(6)(ii), Response and Reporting.
- The VMware Carbon Black Cloud and Workspace ONE clients can be prevented from being disabled by unauthorized users.
- The VMware Carbon Black Cloud and Workspace ONE platforms provide features for Windows and MAC operating systems (OSs) to perform folder scanning, periodic full system scans, whitelisting scripts that could be executed to prevent execution of any unknown scripts, and whitelisting and blacklisting files.

ASSESSOR COMMENTS

The assessment scope focused on validating the use of VMware Carbon Black Cloud and Workspace ONE platforms in a HIPAA environment, including its impact on the HIPAA Security Rule's Administrative and Technical Safeguards. The VMware Carbon Black Cloud and Workspace ONE platforms, when properly implemented following guidance from VMware, can be utilized to meet the technical portions of multiple HIPAA requirements detailed in the testing tables below. However, as most computing environments and configurations vary drastically, it is important to note that use of this product does not guarantee security and even the most robust AV solutions can fail when improperly implemented or maintained. A defense-in-depth strategy that provides multiple layers of protection should be followed as a best practice. Customers should consult with VMware for policy and configuration questions and best practices.

It should also not be construed that the use of the VMware Carbon Black Cloud or Workspace ONE platforms guarantees full HIPAA compliance. Security and business risk mitigation should be any company's goal and focus for selecting security controls.

The VMware Carbon Black Cloud and Workspace ONE platforms can benefit an organization by potentially reducing the cost of a HIPAA compliance assessment by eliminating the exposure of ePHI to point-of-sale (POS) applications through the controls described in the testing tables below, providing an increased value proposition to their clients.

APPLICATION ARCHITECTURE AND SECURITY

VMWARE CARBON BLACK CLOUD PLATFORM

The following product descriptions are taken from Carbon Black documentation.[1]

The VMware Carbon Black Cloud platforms consolidate multiple endpoint security capabilities using one agent and console, to help organizations operate faster and more effectively. As part of VMware's intrinsic security approach, VMware Carbon Black Cloud spans the system hardening and threat prevention workflow to accelerate responses and defend against a variety of threats. VMware utilizes the following key components to implement its security solution:

- Endpoint Standard is a next-generation AV and behavioral endpoint detection and response (EDR) solution that analyzes attacker behavior patterns over time to detect and stop never-seen-before attacks, whether they are malware, file-less or living-off-the-land attacks.
- Managed Detection offers managed alert monitoring and triage. Customers gain 24-hour visibility from VMware's security operations center of expert analysts, who provide validation, context into root cause, and automated monthly executive reporting.
- Audit and Remediation offers real time device assessment and remediation that helps track and harden security posture through audit reporting of the current system state for all protected devices.
- Enterprise EDR features threat hunting and containment capabilities which proactively hunt for abnormal activity using threat intelligence and customizable detections.
- Cloud Workload delivers advanced protection purpose-built for securing modern workloads to reduce the attack surface and strengthen security posture.

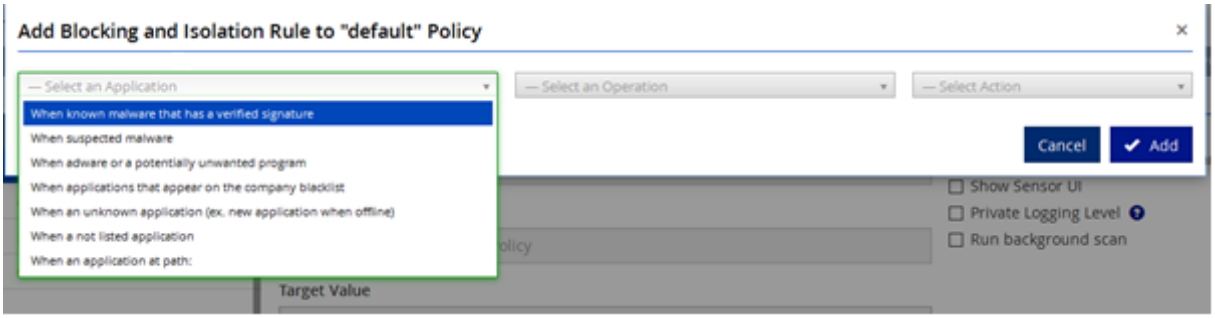

Figure 1: Example Policy Protection Settings from Centralized Management Interface

VMWARE WORKSPACE ONE

The following product descriptions are taken from Workspace One documentation.[2]

VMware Workspace ONE is an intelligence-driven digital workspace platform that can deliver an engaging employee experience. VMware Workspace ONE delivers and manages any application on any device. Workspace ONE integrates access control, application management, and multi-platform endpoint management into a single platform available as a cloud service or on-premises deployment. At the time of publication, Workspace ONE delivers the following:

[1] https://www.carbonblack.com/products/vmware-carbon-black-cloud-endpoint/
[2] https://www.vmware.com/products/workspace-one.html

- Engaging Employee Experiences from Onboarding to Offboarding – Enables enterprises to maximize employee engagement and productivity by empowering employees with a personalized experience and day one access to any application on any device.
- Unified Endpoint Management – Consolidate management silos across mobile devices, desktops (including Windows 10 and MacOS), rugged devices, and "things." Reduce costs and improve security with real-time, over-the-air modern management across all use cases (including bring-your-own [BYO] devices).
- Intelligence Across the Digital Workspace – Aggregated and correlated data across an organization's entire digital workspace to drive insights, analytics, and powerful automation of common information technology (IT) tasks that improve user experience and strengthen security.
- Virtual Desktops and Apps – Workspace ONE provides VDI and published apps with integrated VMware Horizon and VMware Horizon Cloud, which provides simplicity, flexibility, speed, and scale. A common control plane across the "multi-cloud" enables an architecture and cost model that meets organizational requirements.
- Secure and Simple Application Access – Secure, password-free single sign-on (SSO) to software-as-a-service (SaaS), mobile, Windows, virtual, and web apps on any phone, tablet, or laptop using a single app catalog.
- Simplify Zero Trust Security – Combines intrinsic security across devices, users, and apps to simplify the enablement of zero trust access-controls. Workspace ONE has the ability to integrate with complementary security solutions through VMware's Technology Alliance Partner (TAP) Program, such as a mobile/malware threat detection. These solutions, paired with existing threat data for mobile platforms within Workspace ONE Intelligence, can be managed, deployed and enabled through Workspace ONE, providing additional EDR capabilities for meeting a Zero Trust Architecture.

TECHNICAL SECURITY ASSESSMENT

ASSESSMENT METHODS

The assessment used the following methods to assess the potential HIPAA coverage of the solution:

- Analysis of the architecture and configuration of the solution in accordance with vendor guidelines.
- Deployment of client software to a Windows test machine, Android test machine, and iOS test machine, along with enablement of strict policies to enforce the detection and prevention of known malware.
- Examination of agent configurations to confirm that protection cannot be turned off by non-administrators.
- Execution of known malware samples (e.g., ransomware, backdoors, droppers, PUAs, spyware, viruses, worms) deliberately propagated to test machines and mobile devices.
- Review of back-end components for the verification of detection, execution prevention, and removal of all test samples.
- Evaluation of back-end components for verification that agents are deployed, communicating, up to date, performing periodic scans, and protecting against real-time threats.
- Validate technical controls against the HIPAA Security Rule for password management, workstation use and security, access control, unique user identification, automatic logoff or timeout,

encryption and decryption storage and transmission, audit controls, and the ability to enable security incident procedures for response and reporting.

ASSESSMENT ENVIRONMENT

The VMware Carbon Black Cloud and Workspace ONE platforms were hosted in the cloud for testing purposes, and client software was installed on the following systems:

- Windows 2016 Server deployed in a physical environment, including default Windows applications with other AV solutions running.
- Android Nexus 6 device (Android version 6.0).
- iPhone 7 Model A1778 iOS mobile device (iOS version 10.3.2).
- Windows 8, 8.1 and 10
- macOS X: 10.12, 10.13, 10.14, 10.15
- Linux RedHat (RHEL) and CentOS 6/7

NETWORK TRAFFIC ASSESSMENT

A Wireshark Ethernet port sniffer was used to monitor the following traffic for components within Workspace ONE:

- **Traffic from Local Windows Machine and Workspace ONE Appliance Machine (Figure 2):** No sensitive data was transmitted over the network from the Windows machine to the appliance server and any log data or alert information was encrypted via Transport Layer Security (TLS) 1.2.

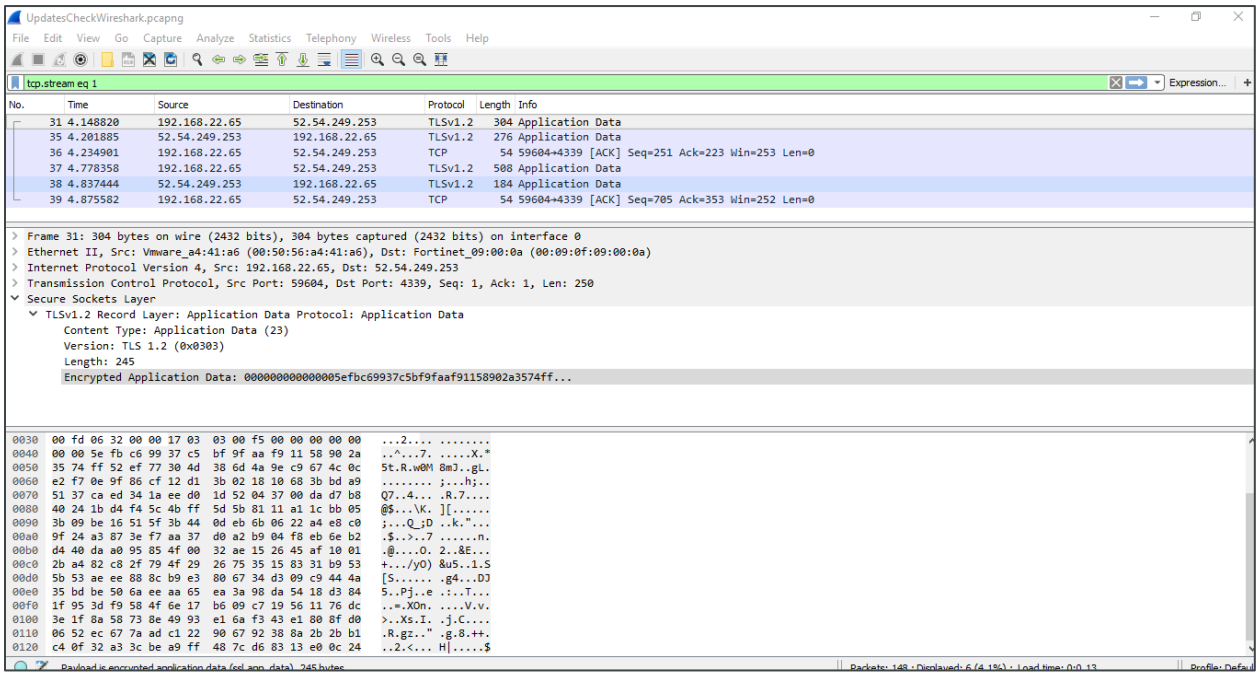

Figure 2: Communication Between a Windows Machine and a VMware Carbon Black Cloud Appliance Machine Hosted in the Cloud

- **Traffic from Mobile Device and Workspace ONE Appliance Machine (Figure 3):** No sensitive data was transmitted over the network from mobile devices to the appliance server and any log data or alert information is encrypted over TLS 1.2.

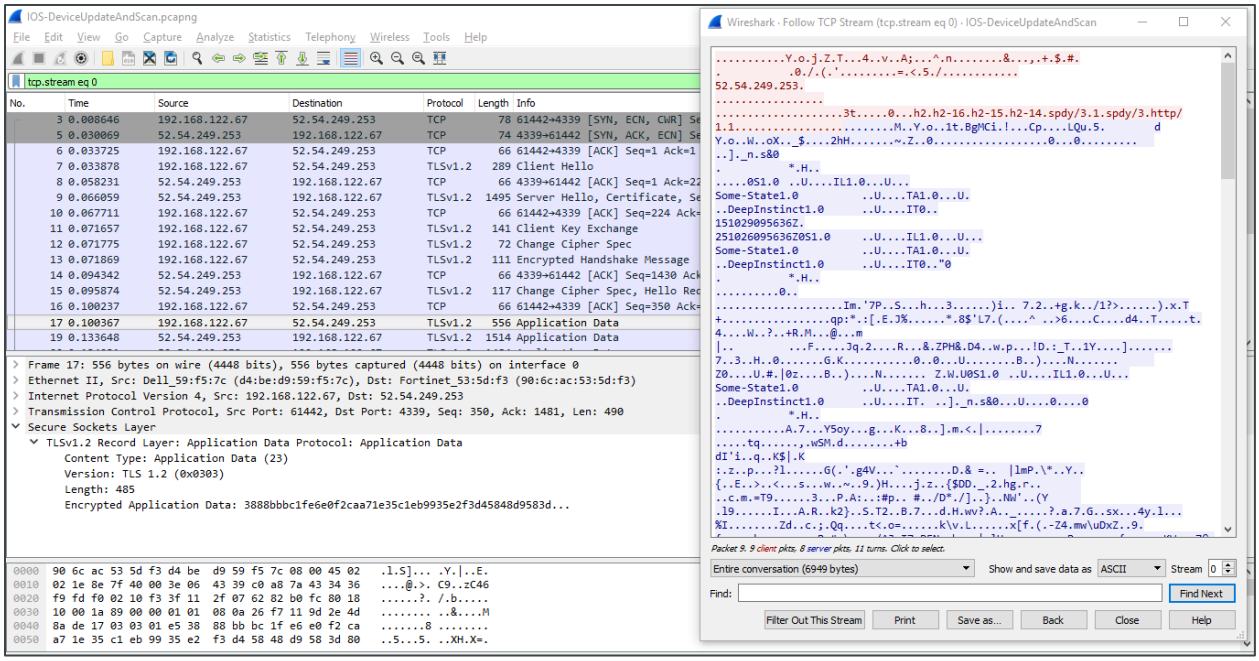

Figure 3: Communication between mobile device and Workspace ONE Appliance Machine Hosted in the Cloud

APPENDIX A: EXECUTED TEST PLAN FOR PROTECTION FROM MALICIOUS SOFTWARE

Testing for malicious software was done with the VMware Carbon Black Cloud Endpoint.

BEST PRACTICES	COALFIRE TEST VALIDATION PLAN	VMWARE CARBON BLACK CLOUD RESULTS
Deploy AV software on all systems commonly affected by malicious software, especially personal computers and servers.	For a sample of system components, including all OS types commonly affected by malicious software, verify that AV software is deployed if applicable AV technology exists.	Coalfire produced a report or log record that indicated that the VMware Carbon Black Cloud agent was installed, active, and gathered events to detect and prevent threats from endpoints that were in scope.
Ensure that AV programs are capable of detecting, removing, and protecting against all known types of malicious software.	Review vendor documentation and examine AV configurations to verify that AV programs: • Detect all known types of malicious software. • Remove all known types of malicious software. • Protect against all known types of malicious software. Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.	**Detect known types of malicious software:** Viruses obtained from a known malware repository were observed to be successfully removed by the system. **Remove all known types of malicious software:** Testing of the solution demonstrated that VMware Carbon Black Cloud deleted files that were detected as malware or triggered a batch that deleted or moved files that were detected as malware. **Protect against all known types of malicious software:** Testing of the solution demonstrated how the solution detected, then banned or blocked known malware that was part of the known malware list from a virus repository or the VMware Carbon Black Cloud policy.
For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats to confirm whether such systems continue to not require AV software.	Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software to confirm whether such systems continue to not require AV software.	Testing of the solution demonstrated how the VMware Carbon Black Cloud agent was deployed on any given system (i.e., OS coverage and implementation features). It also illustrated how any given system was assessed even if it was not part of the in-scope systems.

BEST PRACTICES	COALFIRE TEST VALIDATION PLAN	VMWARE CARBON BLACK CLOUD RESULTS
Ensure that all AV mechanisms are maintained as follows: • Virus definitions are kept current. • Critical system file scans are performed during system boot and every 12 or 24 hours. • Periodic reviews or scans can be set up to be required of installed software and the data content of systems to identify and, where possible, remove any unauthorized software. • Audit logs are generated and retained.	Examine policies and procedures to verify that AV software and definitions are required to be kept up to date. Examine AV configurations, including the master installation of the software, to verify that AV mechanisms are: • Configured to perform automatic updates. • Configured to perform periodic scans. Examine a sample of system components, including all OS types commonly affected by malicious software, to verify that: • The AV software and definitions are current. • Periodic scans are performed.	Testing of the solution demonstrated that the VMware Carbon Black Cloud met requirements through the following activities: • Data retrieved malware information from threat and virus informational feeds. • Policies and threat intelligence data were updated, set to dynamically source current information, or could be updated. • The system periodically scanned in-scope systems for malware. • Virus definition policies were sourced from current repositories. • The system periodically scanned in-scope systems that were members of the policy.
Malicious code and spam protection mechanisms should be centrally managed, and AV mechanisms should be actively running. AV mechanisms should not be able to be disabled or altered by users, unless specifically authorized by management case-by-case for a limited time period. Note that AV solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management case-by-case. If AV protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period of time during which AV protection is not active.	Examine AV configurations, including the master installation of the software and a sample of system components, to verify that the AV software is actively running. Examine AV configurations, including the master installation of the software and a sample of system components, interview responsible personnel, and observe processes to verify that the AV software cannot be disabled or altered by users unless specifically authorized by management case-by-case for a limited time period.	Testing of the solution demonstrated via log reports or live console view that the VMware Carbon Black Cloud met the following requirements: • The agent was running, and the policy was enforcing the proper configuration per the specifications for in-scope assets. • The agent had tamper protection and the proper administrative parameters in place. • The agent could be configured by a user with proper administrative access and a policy was in place that dictated when authorized changes could be made.

APPENDIX B: HIPAA REQUIREMENTS COMPLIANCE MATRIX

Some features described in the tables below extend beyond the requirements of the HIPAA Security Rule. They are noted for audience review purposes.

COMPLIANCE LEVEL	DESCRIPTION
✓	Compliance directly supported via use of the VMware Carbon Black Cloud and Workspace ONE platforms.
✓	Requires action by organization for full compliance.

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
HIPAA Security Rule **Administrative Safeguards – §164.308**		
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.*	✓	Coalfire examined the VMware Carbon Black Cloud and found that the system provides the following features: • Direct deployment of agents on Windows systems, and macOS devices. • Direct monitoring capability for the agent deployed systems through the VMware Carbon Black Cloud management console. • VMware Carbon Black Cloud includes the following capabilities: – Analysis of billions of system events to understand what is normal in an environment. – Prevention of attackers from abusing legitimate tools. – Automation of investigation workflows to respond efficiently. • Administrators can configure the policies on Windows systems and mobile devices to detect and prevent malware. • Periodic scans can be performed either monthly, weekly, or daily while the client's software detects threats in real time. • Action policies for malicious files can be set to be delete the file or quarantine the file. Action policies must be configured by administrators to be compliant with all HIPAA requirements.
Password Management **§ 164.308(a)(5)(ii)(D)** *Procedures for creating, changing, and safeguarding passwords.*	✓	Coalfire examined password settings that enable the enforcement of the following recommended HIPAA minimum password requirements at both the management console and Workspace ONE client levels: • **Minimum password length:** 8 characters

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		– The solution dashboard can be configured to require passwords of any length from 4 to 8 characters. • **Password complexity:** Enabled – The solution dashboard can be configured to require passwords of any length from 4 to 8 characters. • **Password history:** Last 4 – The solution dashboard can be configured to prevent the reuse of 0 to 5 previous passwords. • **Password encryption:** Enforced by default – This solution allows for the configuration of recommended password and authentication settings. Customers must establish procedures for creating, changing, and safeguarding user passwords.
Security Incident Procedures – 164.308(a)(6)(i) *Implement policies and procedures to address security incidents.*		
Response and Reporting – R 164.308(a)(6)(ii) *Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.*	✓	This process or procedure requirement can only be partially met by the VMware Carbon Black Cloud and Workspace ONE platforms, as they do not cover all security incidents; these platforms only focus on malicious software incident and workstation-level controls. The documentation of security incidents and their outcomes remains the responsibility of the customer organization. Coalfire examined the VMware Carbon Black Cloud and Workspace ONE platforms' controls, which provide the following functionality: • Administrators can configure the policies on Windows systems and mobile devices to detect and prevent malware. Action policies for prevented files can be set to be deleted and quarantined. Action policies must be configured by administrators to be compliant with HIPAA regulations. • The VMware Carbon Black Cloud performs deep learning to classify the malware type and can provide guidance to customers to classify the risks related to malware type for the Windows system, Android, and iOS mobile system components. Information is gathered from various third-party companies, Darknet scans, and forums regarding malicious files or threats that could exist. • Logging and alerting features are provided through the management console for all malware-related threats and policy violations, as well as actions taken by users or administrators. The solution provides features to be integrated with security

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		information and event management (SIEM) products and Simple Mail Transfer Protocol (SMTP) servers for log forwarding to retain logs as required by the organization's retention policy. The policies and procedures can be developed by the customer organization and the alerting mechanisms of the VMware Carbon Black Cloud and Workspace ONE platforms can be used to address the security incidents that occur for endpoints and mobile devices. Additional security incidents must be documented and implemented by the organization, as this platform only provides notifications on actions taken on file events, file-less events, audit logs, and non-compliant issues. Customers are responsible for responding to security incidents identified by the VMware Carbon Black Cloud and Workspace ONE platforms. Responses should be previously defined in an incident response plan and periodically tested.
HIPAA Security Rule Physical Safeguards – §164.310		
Workstation use § 164.310 (b): *Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.*	✓	Coalfire examined the system geographic location functionality of the Workspace ONE client, which provides healthcare organizations with the ability to restrict access to applications that access ePHI when the workstation or laptop is not at a specified destination or network. Ultimately, the healthcare organization is responsible for enabling location services on enrolled devices. Customers are responsible for implementing policies and procedures regarding the use of workstations within their environment. Policies and procedures must include proper functions to be performed and the manner in which those functions are to be performed, physical attributes of the surroundings where the workstations are installed or placed, and the ePHI those workstations may access.
Workstation security § 164.310 (c): *Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.*	✓	Coalfire examined policy and profile functionality of the Workspace ONE client to determine that the control checked for the security requirements of a workstation connecting to the network. The required security functionality (e.g., AV, hard drive encryption), when missing, forced the workstation to be updated to comply before allowing connectivity to networks or applications that have access to ePHI. Coalfire examined system capability to wipe devices in the event of a lost or stolen device and determined that this functionality would benefit organizations when tracking a lost or stolen laptop or mobile device.

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		Customers are responsible for implementing physical safeguards for all workstations that can access ePHI and restricting access to those users that have been authorized for access to such data.
HIPAA Security Rule **Technical Safeguards – §164.312**		
Access Control **§ 164.312(a)(1):** *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).*	✓	Coalfire examined policy and profiles for user authentication functions within the Workspace ONE client. Similar to the security for workstations, these profiles can be set to restrict users from accessing application or networks that have access to ePHI based on a number of factors. Coalfire examined authentication processes, including attempting short passwords and passwords from a one-character set. The system enforces passwords of the length specified by the organization and the use of multiple character sets (i.e., alphabetical, numeric, special) as specified by the organization. Customers are responsible for maintaining and implementing technical policies and procedures for systems that maintain ePHI and allowing only persons or software programs that have been authorized to access this information.
Unique User Identification **§ 164.312(a)(2)(i):** *Assign a unique name and/or number for identifying and tracking user identity.*	✓	Coalfire examined user authentication functions within the Workspace ONE client and management platform, including creating duplicate user IDs, passwords, changing passwords, and reuse of recent passwords. The system enforced unique user identification by preventing the creation of identical user IDs and the management dashboard requires a unique user IDs. Coalfire examined authentication processes, including attempting short passwords and passwords from one-character sets. Coalfire observed the system did not allow passwords shorter than 5 characters, or passwords containing only numeric or alphabetic characters. Customers are responsible for requiring a unique username or number for the purpose of tracking user activity based on identity.
Automatic Logoff **§ 164.312(a)(2)(iii):** *Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.*	✓	Coalfire examined the Workspace ONE client and management platform for idle session timeout. In both cases, the systems automatically required user re-authentication after a predetermined idle period. The Workspace One client idle session timeout is configurable in policy or profile. Customers are responsible for maintaining and implementing electronic procedures to terminate a user's

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
		session if it has been idle for more than the specified period of time.
Encryption and Decryption § 164.312(a)(2)(iv): *Implement a mechanism to encrypt and decrypt electronic protected health information.*	✓	Coalfire examined VMware Carbon Black Cloud and Workspace ONE enrolled devices and the status of whole-disk encryption. The dashboard shows enrolled devices as compliant if whole-disk encryption is enabled. Devices without encryption enabled show as non-compliant. Administrators may escalate to ensure that encryption is enabled on devices. Customers are responsible for implementing a mechanism to protect ePHI with encryption and decryption.
Audit Controls – R 164.312(b) *Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.*	✓	Coalfire examined the VMware Carbon Black Cloud and Workspace ONE platforms and found the below statements to be true: • Both platforms can support this requirement by examining malicious activities on the information systems that could potentially contain ePHI; however, ePHI data cannot be distinguished by these platforms, and it remains the responsibility of the customer organization to deploy the client software on all endpoints for compliance. • The management and monitoring services shows the monitoring status (offline or online status mode) of all client-software-deployed devices through the management consoles. Offline and online status mode is also visible directly on client software deployed device or machines. • The management console provides the functionality to disable or remove the device based on the administrator role setting and permissions. Policy configurations determine if users can disable the client software running locally on the machines and mobile devices and define the appropriate administrator permissions. • Logging and alerting features are provided through the management console for all policy or profile violations, malware-related threats, as well as actions taken by users or administrators. The solution provides features to be integrated with SIEM products and SMTP servers for log forwarding to retain logs per the customer retention requirements. Customers are responsible for monitoring logs provided by the VMware Carbon Black Cloud and Workspace ONE platforms or implementing the logging of activities on systems containing ePHI.

HIPAA COMPLIANCE REQUIREMENT	COMPLIANCE SUPPORTED	ASSESSOR COMMENTS
Person or entity authentication § 164.312(d): *Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.*	✓	Coalfire examined policy and profiles for user authentication functions within the VMware Carbon Black Cloud Endpoint and Workspace ONE platforms, including security for workstations. These profiles can also be set to restrict users from accessing applications or networks that have access to ePHI based a number of factors. The system requires that users identify themselves by logging with a user ID and password to gain access to the system. Customers are responsible for implementing procedures to positively verify the identity users requesting access to ePHI.
Transmission security § 164.312(e)(1): *Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.*	✓	Coalfire examined data transmitted from the VMware Carbon Black Cloud Endpoint Platform and Workspace ONE client systems to the management cloud platform and found that all data was transmitted over the network protected with TLS 1.2. Customers are responsible for ensuring that ePHI transmitted over networks is protected with an industry standard method.
Encryption § 164.312(e)(2)(ii): *Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.*	✓	Coalfire examined policy and profile settings related to device encryption. The VMware Carbon Black Cloud Platform and Workspace ONE management dashboard shows enrolled devices as compliant if whole-disk encryption is enabled. Devices without encryption enabled show as non-compliant. Administrators may escalate to ensure that encryption is enabled on devices. Customers are responsible for enabling whole-disk encryption on protected devices.

ABOUT THE AUTHORS

Lyle Miller | Principal

Lyle Miller is an application security specialist for the Solution Validation team at Coalfire. Lyle has over 20 years of experience in information security, and over 9 years of experience working as a QSA and PA-QSA, helping clients secure their systems and software for use in PCI DSS environments. Lyle currently holds CISA, CISSP, QSA, PA-QSA, SSA, and SSLC-A certifications. As a PA-QSA, Lyle supports assessments for some of the largest payment software providers in the world, helping teams recognize the importance of secure code development and information security within their operational practices.

Terilyn Floyd-Carney | Senior Consultant

Terilyn Floyd-Carney is a Senior Consultant and application security specialist with Coalfire. Terilyn has several years of experience working as a PA-QSA and HITRUST Certified CSF Practitioner, helping clients develop systems and software for use in healthcare, pharmacy, and retail environments. Terilyn has also authored and spoken on multiple security topics, including application security, cybersecurity best practices, and compliance. She holds CISSP, CISA, HCISSP, HITRUST Certified CSF Practitioner, and QSA certifications.

Published January 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 nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.