COALFIRE

WHITE PAPER

Broadcom Inc. VMware vDefend Product Applicability Guide for HIPAA

Applicability for use with the HIPAA Security Rule

COALFIRE OPINION SERIES – Version 1.6

CALEB PFANSTIEL, MBA, CCSK, SECURITY+ | CONSULTANT
GRC HEALTHCARE & PRODUCT GUIDANCE

877-224-8077 | info@coalfire.com | Coalfire.com

Table of contents

Executive summary

Broadcom Inc. (“Broadcom”) has engaged Coalfire Systems, Inc. (“Coalfire”) to conduct an independent technical review of its VMware vDefend (“vDefend”) solution for its efficacy in assisting organizations that use (or are considering using) vDefend to protect access to electronic protected health information (ePHI) and to support the technical and administrative requirements of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

This Product Applicability Guide (PAG) examines an entity’s adoption of the vDefend solution in alignment with the Administrative and Technical Safeguards of the HIPAA Security Rule. This PAG outlines Coalfire’s methodology for assessment and the approach used for this review, summarizes findings from Coalfire’s review of the product’s capabilities, provides context for the use of these capabilities, and states an opinion as to how the vDefend solution’s security capabilities, functions, and features can assist organizations with supporting HIPAA Security Rule Administrative and Technical Safeguards.

Coalfire PAGs provide a specific Coalfire opinion of a product’s applicability to standards, frameworks, and mandates through the “eyes of the assessor” and should not be construed as a specific endorsement. PAGs are provided as an element of Coalfire’s product guidance services and are authored solely to inform users currently leveraging vDefend as well as prospective customers who are interested in using the solution.

Coalfire opinion

Coalfire reviewed the vDefend solution and determined that it can support Administrative and Technical Safeguards of the HIPAA Security Rule when it is properly employed by customers in covered environments. Such support can be achieved by leveraging vDefend’s built-in micro-segmentation, advanced threat prevention, network traffic analysis, role-based policy enforcement, asset tagging, and threat detection and response functions, along with additional services discussed throughout this white paper. These functions can support numerous HIPAA Security Rule Administrative and Technical Safeguards by minimizing access privileges, optimizing network micro-segmentation, and enabling detection and prevention of suspicious network activity. vDefend focuses on network security, on establishing secure perimeters around integrated/connected networks, and on automating the response to potentially adverse traffic.

Coalfire’s opinion depends on underlying assumptions, such as the alignment of customer configuration to HIPAA objectives, customer capabilities for supplemental and complementary controls, and the alignment of HIPAA objectives across integrations with existing security tools such as endpoint detection and response (EDR) solutions, security information and event management (SIEM) systems, identity and access management (IAM) solutions, data loss prevention (DLP) tools, and third-party vulnerability management solutions. Within its domain, the vDefend solution can offer a viable foundation for supporting HIPAA Security Rule Technical and Administrative Safeguards.

Purpose

The primary purpose of this PAG is to render Coalfire’s opinion and to provide supporting observations, based on its review, of the vDefend solution’s suitability to assist Broadcom customers in meeting HIPAA Security Rule objectives. Coalfire used the following process in the development of this PAG:

- Perform a product walkthrough with subject matter experts.
- Collect artifacts and perform product review.
- Identify any dependencies used for review.
- Reveal additional technical details of the solution.

- Make relevant statements about the features of the vDefend solution that can support HIPAA Security Rule objectives.
- State Coalfire's opinion of the vDefend solution's capacity to be used for adherence to HIPAA Security Rule objectives.

Although the opinion itself may be helpful, this PAG also contains a representative overview of many aspects of the HIPAA Security Rule, which readers may also find of use. Coalfire also focused on the technical and administrative controls supporting HIPAA Security Rule objectives through interviews with subject matter experts and review of data sheets, written supporting materials, and other technical artifacts provided as part of vDefend solution documentation. Coalfire did not review organizational processes, procedures, or other non-technical artifacts.

Introducing the HIPAA Security Rule

Covered entities and business associates (CE&BAs) covered under HIPAA face a constant challenge in securing ePHI from a variety of internal and external threats. The HIPAA Security Rule is a federal regulation that mandates healthcare organizations to implement safeguards to protect ePHI.

Relationship between the HIPAA Security Rule and the HIPAA Privacy Rule

HIPAA mandates HHS to develop regulations for protecting health information privacy and security. These regulations are known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Office for Civil Rights (OCR) within HHS enforces these rules through compliance activities and potential civil money penalties (HHS, 2023).

- HIPAA Privacy Rule: Establishes national standards to protect individuals' health information.
- HIPAA Security Rule: Establishes national security standards for protecting ePHI.

The HIPAA Security Rule complements the HIPAA Privacy Rule by outlining the technical and non-technical safeguards that covered entities need to implement to secure ePHI.

About the HIPAA Security Rule

The HIPAA Security Rule is designed to be flexible and scalable, allowing CE&BAs to tailor their security measures to their organization's specific size, complexity, and risk environment. As stated in the introduction of the United States Department of Health and Human Services (HHS) Summary of the HIPAA Security Rule, the rule prioritizes technology neutrality. This means that the rule doesn't dictate specific technologies for implementation. Instead, CE&BAs can choose any security measures they believe are reasonable and appropriate to meet the required standards and implementation specifications of the HIPAA Security Rule.

The HIPAA Security Rule establishes core requirements for CE&BAs to ensure the confidentiality, integrity, and availability of ePHI. These requirements, as outlined in 45 CFR § 164.306 Security standards: General rules, are:

- Confidentiality, integrity, and availability: CE&BAs must ensure all ePHI they create, receive, maintain, or transmit is protected against unauthorized access, modification, or loss.
- Risk management: CE&BAs must identify and protect against anticipated threats or hazards to the security of ePHI.
- Authorization: CE&BAs must implement safeguards to prevent unauthorized disclosures of ePHI not permitted by HIPAA.

- Workforce compliance: CE&BAs must ensure their workforce is trained and compliant with HIPAA regulations.

45 CFR § 164.306(b): Flexibility of approach, provides guidance for selecting security measures. The HIPAA Security Rule categorizes its requirements into the following distinct categories:

- Security Standards: General Rules (§ 164.306)
- Administrative Safeguards (§ 164.308)
- Physical Safeguards (§ 164.310)
- Technical Safeguards (§ 164.312)
- Organizational Requirements (§ 164.314)
- Policies and Procedures and Documentation Requirements (§ 164.316)

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, however, that neither of these classifications should be interpreted as optional. An explanation of each is provided below:

- Required: Implementation specification identified as required must be fully implemented by the organization. Furthermore, all requirements identified as standards within the Security Rule are considered required.
- Addressable: Organizations have more flexibility with implementation specifications identified as addressable. They can choose to:
  - Implement the addressable implementation specification as defined.
  - Implement an alternative security measure that achieves the same outcome.
- Not implement the specification or an alternative but must document the decision and justification.

This concept of addressable implementation specifications allows covered entities flexibility in achieving compliance if the overall objectives of the rule are met. However, if an entity fails to properly assess flexibility and implement the appropriate HIPAA Security Rule safeguards, noncompliance can lead to severe consequences, including regulatory fines and legal action. Organizations must continuously assess and document their compliance strategies to mitigate financial, legal, and compliance risks.

Potential changes in the HIPAA Security Rule

HHS proposed updates to the HIPAA Security Rule on December 27th, 2024, to address evolving cybersecurity threats, enhance risk management requirements, and increase the accountability of CE&BAs. These proposed changes were closed for public comment on March 7th, 2025. Among many important proposed changes, the following are key to consider with this PAG:

- Where previously there was a distinction between "addressable" and "required" rules, this proposal looks to make all aspects of the Security Rule required. The elimination of "addressable" implementation specifications would remove implementation flexibility and would require all CE&BAs to uniformly implement the specified security measures. This means that organizations that previously justified alternative solutions or deferred certain security measures under the "addressable" category would now need to allocate additional resources to meet the stricter requirements.

- Additional Administrative, Physical, Technical, and Organizational Requirements could heighten the threshold required for compliance. Notably, the following should be considered by a CE&BA supporting HIPAA compliance with software-defined distributed firewalls:
  - Network maps and inventories: There is a proposed requirement to require CE&BAs to maintain network maps and inventories that must be updated at least every 12 months (unless there is an operational or environmental change)
    - These network maps must show all egress and ingress movement of data from the network.
    - Business associates may come into scope with the data flow diagrams, such as offshore support for claims processing.
  - Risk analysis: Annual risk analyses would be required, identifying all reasonable threats and potential vulnerabilities to the confidentiality, integrity, and availability of ePHI.
  - Healthcare clearinghouses: Should be logically separated from the enterprise.
  - Compliance audits: Regulated entities would be required to conduct compliance with the Security Rule annually, either internally or with a third party.
  - Session control: Automated session terminations would be required to be configured.
  - Multi-factor authentication: Would be required with limited exceptions.
- Encryption: Would be required to meet widely accepted encryption standards for ePHI at rest and in-transit, with limited exceptions.
  - Network ports: Unnecessary network ports would be required to be disabled.
  - Antimalware: Deployment of antimalware would be required.
  - Configuration management: The establishment and maintenance of the minimum baseline for each technology asset and relevant electronic formation system would be required.
  - Real-time auditing: Continuous auditing with the configuration of alerts for unauthorized activity would be required.

While these proposed changes have yet to be implemented as part of the HIPAA Security Rule, they are all best practices that organizations should strive toward to enhance their security and privacy program. For more information on how vDefend would apply to the proposed changes, refer to the Aligning product capabilities with the proposed HIPAA Security Rule changes section below.

Institute compliance with the HIPAA Security Rule

Shifting to a framework-based approach

The focus of HIPAA compliance has evolved from a static, location-based approach to one that requires a scalable and adaptable security framework capable of addressing dynamic risks across complex healthcare environments. Rather than relying solely on identity and context-based security, organizations must implement a comprehensive, framework-driven strategy that integrates technical, administrative, and physical safeguards to ensure long-term compliance.

A framework-based approach provides a structured methodology for scaling security programs to meet evolving regulatory and operational demands. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 framework, for example, is recognized as a leading framework for security and privacy controls, and offers a

comprehensive, flexible, and modular set of guidelines that can be customized to support HIPAA compliance while also mitigating broader cybersecurity threats.

NIST SP 800-53 Rev. 5 introduces a prescriptive, threat-informed approach that aligns with HIPAA's emphasis on safeguarding ePHI while also providing a framework for ongoing risk management, automation, and integration with emerging security technologies. The control families within the framework serve as a scalable foundation for organizations to build a robust HIPAA compliance program that is both resilient and adaptable to future regulatory changes.

By adopting a multi-layered security framework, organizations can facilitate a HIPAA-compliant environment that scales with their infrastructure while meeting regulatory requirements and strengthening cybersecurity resilience. At its core, Governance, Risk, and Compliance (GRC) provides a structured, programmatic approach that extends beyond technology alone. A GRC-driven security program helps ensure that security controls are not only implemented but continuously assessed, refined, and aligned with regulatory mandates. This approach treats security as an ongoing, adaptive process rather than a one-time implementation, integrating risk management, policy enforcement, and operational oversight into a unified compliance strategy. By making security measures repeatable, auditable, and effective against emerging threats, this proactive strategy can support long-term HIPAA compliance and enhance overall cybersecurity posture.

Challenges with HIPAA implementation

HIPAA compliance and distributed firewalls

Distributed firewalls provide a critical security layer for healthcare organizations seeking to meet the HIPAA Security Rule's requirements for access control, audit logging, and data integrity. By enabling micro-segmentation and granular policy enforcement, distributed firewalls help restrict access to ePHI based on identity, application, and network context. This segmentation is designed to prevent unauthorized lateral movement within networks and ensure that only approved entities can access sensitive data, supporting compliance with HIPAA's Technical Safeguards.

Comprehensive visibility and logging capabilities within distributed firewalls can further enhance an organization's ability to meet HIPAA Administrative Safeguards by facilitating continuous network traffic monitoring, event correlation, and audit trail maintenance. These features can enable proactive risk identification and governance, helping to maintain consistent enforcement and documentation of security policies.

By combining micro-segmentation and policy-driven security enforcement with the additional advanced threat prevention feature, distributed firewalls help enable healthcare organizations to establish a scalable, resilient security posture. This integrated approach helps security and compliance efforts remain adaptable to new risks and regulatory changes, reinforcing a proactive and sustainable cybersecurity framework.

By incorporating a layered security strategy aligned with GRC principles, underpinning the implementation of distributed firewall technology, organizations can establish proactive threat management processes, enforce security policies systematically, and support an ongoing compliance initiative.

Challenges to HIPAA compliance with east-west traffic

To achieve and maintain HIPAA compliance, organizations handling ePHI must ensure that robust network security measures are in place. Traditional, perimeter-based security approaches are increasingly inadequate due to the growing sophistication of adversarial tactics, techniques, and procedures (TTPs). A key challenge in modern healthcare networks is securing the lateral movement of data within an organization's internal network due to the level of trust in internal communications coming from users, applications, and devices operating within the same network or organization.

Unlike north-south traffic, which traverses the network perimeter and is typically well-monitored, east-west traffic refers to communication between systems within the internal network, such as between applications, servers, databases, or endpoints. This internal traffic can lack the same level of scrutiny, making it a prime target for attackers seeking to move laterally after breaching an initial access point. The lack of visibility and control into east-west traffic increases the risk of data exfiltration, unauthorized access to ePHI, and the spread of malware (including ransomware) within healthcare environments.

Furthermore, enforcing zero-trust principles such that every user, device, and workload is continuously authenticated, authorized, and monitored poses significant challenges in east-west traffic security. Many legacy systems and on-premises healthcare applications are not designed to accommodate zero trust, requiring significant architectural changes to implement proper segmentation, least-privilege access controls, and real-time threat detection.

Another critical challenge is the ability to monitor east-west traffic for anomalies that may indicate a security breach. Traditional Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) often focus on external threats, leaving organizations vulnerable to undetected lateral movement by threat actors. Effective anomaly detection and prevention requires an understanding of what east-west traffic is considered “normal” or “baseline,” but this can be costly and complex with certain implementations that require additional hardware in addition to software configurations. Without comprehensive visibility into east-west traffic patterns, security teams may struggle to detect and respond to potential breaches in a timely manner.

A multi-layered architecture with defense in depth security strategy helps to ensure continued, efficient operations while also securing systems and data from unauthorized access, change, or deletion. Strategies that would support this include micro segmentation for enhanced zero trust, advanced behavioral analytics for improved threat identification, continuous monitoring for accelerated response to activity, and integration of AI-driven threat detection to mitigate the risks associated with unauthorized lateral movement. These measures can significantly strengthen internal security and help healthcare organizations protect sensitive ePHI, reduce regulatory risks, and enhance HIPAA compliance.

The Broadcom approach

With a strong focus on enterprise-grade cybersecurity, Broadcom recognizes that the evolving healthcare landscape requires robust security measures that go beyond traditional perimeter defenses. As cyber threats continue to increase in sophistication, Broadcom is committed to delivering security solutions that support compliance, enhance operational efficiency, protect east-west private cloud traffic, and provide intelligent threat detection across complex network environments. By integrating security directly into the private cloud infrastructure, Broadcom aims to simplify security management for healthcare organizations, address the unique challenges of securing ePHI, and help users meet HIPAA regulations.

As part of this initiative, Broadcom delivers security solutions that align with the principles of zero trust. This means implementing technologies that verify every user, device, and workload before granting access to reduce the risk of unauthorized lateral movement within private cloud environments. By embedding security into the hypervisor layer, Broadcom helps to ensure that security policies are consistently enforced across distributed environments without introducing unnecessary complexity or performance overhead.

Broadcom’s alignment with HIPAA compliance is a strategic initiative aimed at helping healthcare organizations navigate the stringent requirements of the HIPAA Security Rule while maintaining a strong security posture. Broadcom has developed solutions that address challenges faced by organizations for providing sufficient visibility and control over east-west traffic. These solutions provide micro-segmentation, advanced threat analytics, and automated policy enforcement to help healthcare providers and their business associates meet regulatory mandates without disrupting their operations.

This strategy extends into Broadcom's private cloud security initiatives, which focus on integrating machine learning, behavioral analytics, and real-time threat detection into its security offerings. Broadcom's goal is to provide organizations with a proactive security tool that supports compliance requirements and helps to strengthen resilience against evolving cyber threats.

As part of this initiative, Broadcom has developed VMware vDefend, a solution designed to address the security challenges associated with east-west traffic in private cloud environments. By leveraging advanced micro-segmentation, network traffic analysis, network detection and response, and AI-driven security intelligence, vDefend can enable organizations to enforce zero-trust principles, detect anomalies, and prevent unauthorized access to sensitive data.

vDefend solution

Broadcom's VMware vDefend solution is purpose-built to secure east-west traffic within the private cloud, helping to contain and mitigate threats before they can move laterally across the environment. vDefend leverages machine learning, advanced behavioral analytics, and deep network visibility to help organizations to automate threat detection, plan for and enforce micro-segmentation, and maintain continuous compliance with evolving regulatory frameworks such as HIPAA.

The vDefend solution provides security functionality designed to protect network traffic, network segments, and data within private clouds. It integrates multiple security technologies to enforce zero-trust principles, helping to detect, analyze, and mitigate threats in real time. VMware vDefend Firewall ("vDefend Firewall"), the core solution of the vDefend solution, provides gateway or distributed firewalling and network/micro segmentation. VMware vDefend Advanced Threat Prevention ("vDefend Advanced Threat Prevention") is an optional additional solution to vDefend Firewall that incorporates IDS/IPS and Network Traffic Analysis (NTA), as well as multi-context Network Detection and Response (NDR), which correlates alerts and maps adversary tactics to the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. Additionally, the vDefend Advanced Threat Prevention's VM-aware Malware Prevention Service (MPS) leverages machine learning and sandboxing to detect evasive malware, while Security Intelligence for vDefend provides visibility, analytics, and policy enforcement to strengthen security operations. Finally, the Intelligent Assist for vDefend chatbot provides interpretability for TTPs and other adversarial data to contribute to understanding and responding to security events. Together, these components work in parallel to help enhance an organization's security posture, reduce their attack surface, and help organizations meet compliance and regulatory requirements within the private cloud.

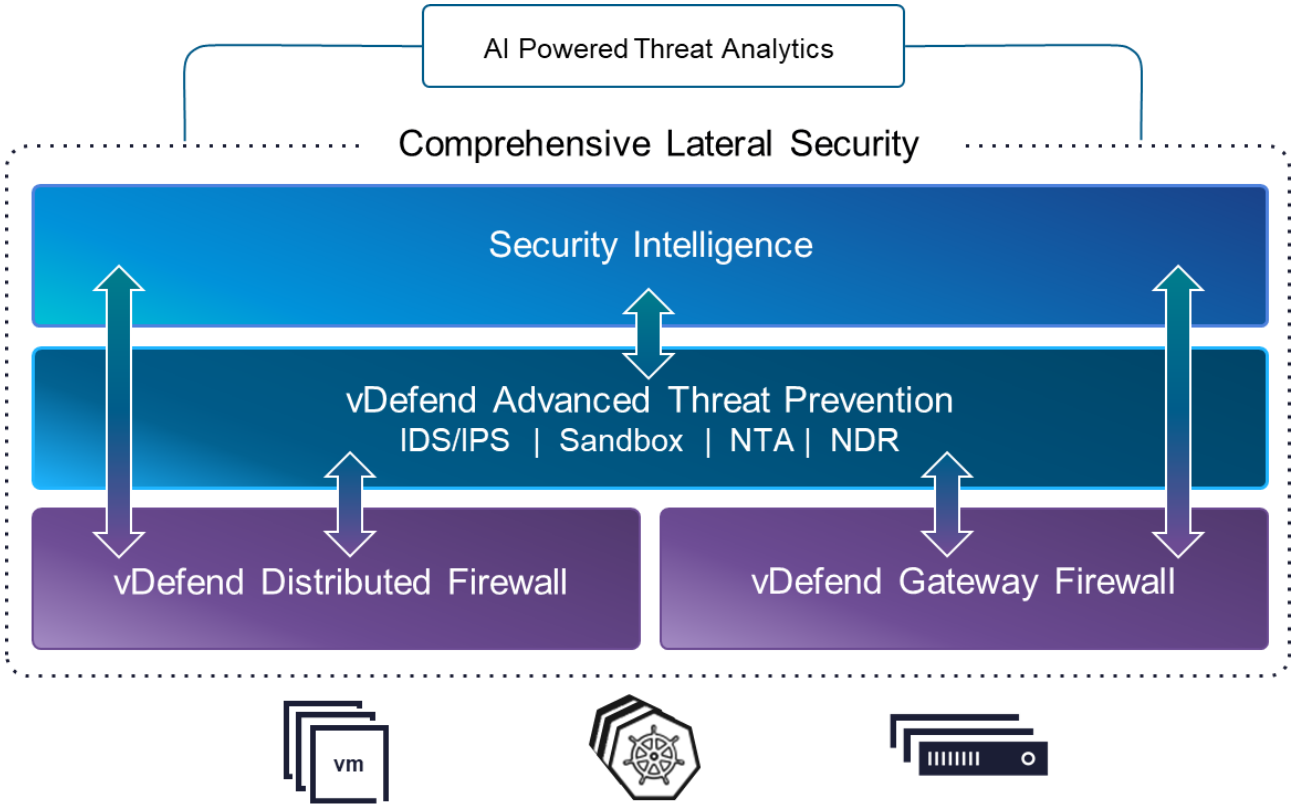

Figure 1: vDefend security components

It should be noted that while vDefend Advanced Threat Prevention is an add on to the vDefend Firewall offering, Coalfire assessed the product's applicability assuming both are implemented within a CE&BA's private cloud. Should a CE&BA only leverage vDefend Distributed Firewall, many of the recommended features and configurations Coalfire reviewed will not be available and the product's applicability for use for HIPAA compliance would be reduced.

vDefend offers a unified, intelligent security solution that integrates into private cloud environments and helps organizations to strengthen their security posture while minimizing operational complexity. By embedding security directly into the VMware Cloud Foundation (VCF) infrastructure, vDefend can support healthcare organizations and other regulated industries to meet compliance mandates, reduce the risk of data breaches, and maintain high-performance network operations.

vDefend Firewall

vDefend Firewall is designed to deliver distributed, software-defined security to enforce zero trust in private cloud environments, providing lateral protection against modern threats. Designed for Layer 2 through Layer 7 coverage, vDefend Firewall is deployed directly into the hypervisor, enabling firewalling across workloads running on virtualized workloads. This architecture provides deep visibility into network traffic, user behavior, and workload context, allowing organizations to identify and mitigate threats in real time. vDefend isolates critical services and applications, minimizing the attack surface and effectively preventing lateral movement.

vDefend Firewall incorporates security controls to enhance workload protection and enforce granular security policies. It dynamically applies least privileged access through user and application identity-based controls, permitting only authorized entities to interact with associated resources. Intelligent micro-segmentation simplifies policy management with automated flow visualization and AI-driven recommendations, helping reduce misconfigurations and improving

security posture. URL filtering and Transport Layer Security (TLS) decryption help block malicious or non-compliant web traffic while inspecting encrypted data for hidden threats. Additionally, advanced threat visibility provides real-time insights into network traffic patterns, application flows, and anomalous behavior, enabling proactive threat detection and response.

Organizations can tailor vDefend Firewall's capabilities to their security architecture with the following deployment models:

- Distributed Firewall: A lightweight, hypervisor-native security solution designed to enforce micro-segmentation across workloads and to provide scalable, east-west traffic protection without the need for additional hardware.
- Gateway Firewall: A next generation, software-defined internal firewall that enforces zone-based policies within the private cloud. With its multi-tenancy capability, it enables secure hosting of multiple tenants within an enterprise or service provider environment, while its security zones ensure security policy enforcement. Advanced features include user identification and application Layer-7 identification, and FQDN filtering. Not a replacement for traditional perimeter firewalls, but rather a complementary layer that reinforces perimeter defense.
- Identity Firewall (IDFW): Allows administrators to enforce user-based distributed firewall rules by linking firewall policies to user identities. This supports dynamic access control in environments, applications, networks, and workloads.

This firewalling technology provides organizations with the ability to logically separate and control access to workloads depending on use case, context, data type, geography, and other categorizations. CE&BAs can leverage this functionality to separate applications and databases supporting ePHI, control the flow of ePHI within the environment, or protect legacy medical systems.

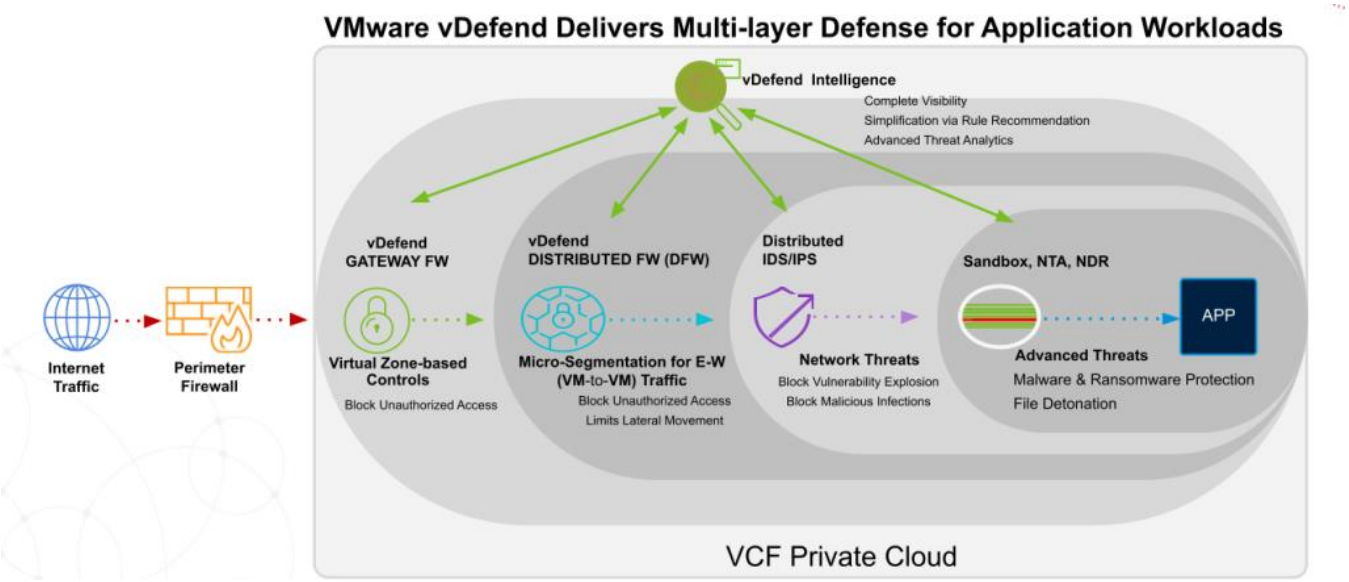

Figure 2: vDefend Defense in Depth

In addition to the above firewall capabilities, the VMware Avi Load Balancer solution's Web Application Firewall (WAF) enhances security by protecting web applications from OWASP Top 10 attacks and other common vulnerabilities. It performs traffic filtering based on signatures, application learning, and anomaly detection capabilities to support HIPAA safeguards aimed at securing and monitoring workloads.

vDefend Advanced Threat Prevention

vDefend Advanced Threat Prevention is offered as an addition to the vDefend Firewall and comprises multiple detection and prevention technologies, including IDS/IPS, multi-context VM-aware MPS, and NTA. NDR aggregation, correlation, and context engines pull from these detection technologies to provide comprehensive visibility and help improve response to alerts and events. By combining these elements, vDefend Advanced Threat Protection creates a cohesive and layered defense mechanism designed to enhance detection accuracy, reduce the rate of false positives, and enable faster, more effective remediation, as well as to minimize the need for manual interventions.

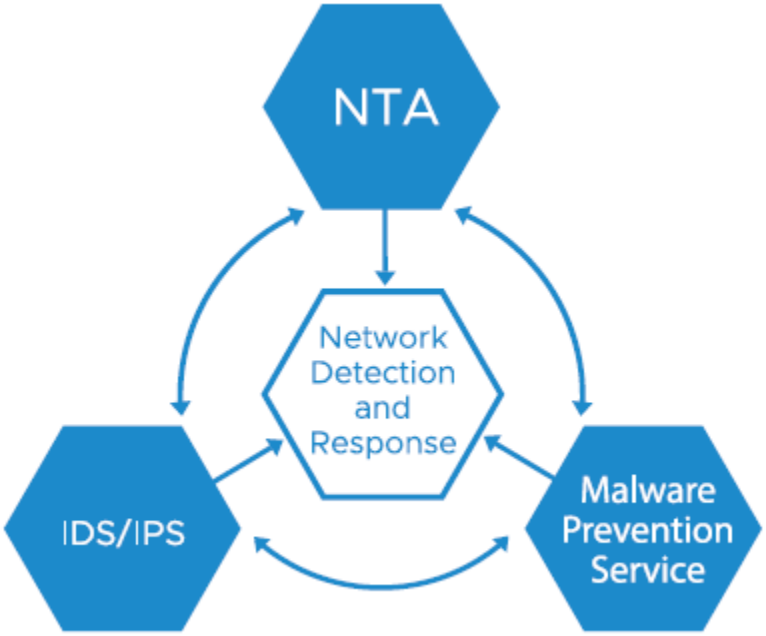

Figure 3: vDefend Advanced Threat Prevention

The subsections below provide more information on the specific roles and unique capabilities of each subcomponent of vDefend Advanced Threat Prevention.

Distributed Intrusion Detection/Prevention System

The Distributed Intrusion Detection and Prevention System is a core component of the vDefend Advanced Threat Prevention suite designed to monitor and protect all traffic entering or exiting the network perimeter. This system uses sophisticated pattern recognition algorithms to detect and block known threats, helping ensure that malicious actors cannot compromise critical systems, sensitive data, or the broader network. The IDS/IPS scans traffic flows for signatures and behavioral patterns of known attack vectors, generating real-time alerts that feed into the NDR tool. This functionality can enable healthcare organizations to detect sensitive data being transferred in abnormal patterns and to prevent these transfers from occurring, helping reduce the potential for a security incident or breach. Additionally, all detected incidents are logged in detail, providing a data source for post-incident analysis, forensic investigations, and long-term threat intelligence development.

VM-aware Malware Prevention Service

VM-aware MPS is designed to deliver advanced malware analysis and prevention by leveraging machine learning algorithms, static and dynamic analysis techniques, and in-depth memory analysis to detect and neutralize sophisticated and previously unknown threats, including zero-day vulnerabilities.

In addition, VM-aware MPS's Guest Introspection capability operates at the hypervisor level and monitors and analyzes activities with additional context and accuracy through deep visibility into file systems, active processes, and registry activities across all virtual hosts. Guest Introspection can also facilitate the inspection and uncovering of hidden threats within encrypted data streams.

VM-aware MPS also uses Broadcom's sandboxing technology to help identify Indicators of Compromise (IoCs). This sandbox provides researchers with detailed IoCs that can assist with the thorough investigation of malware and its behavior. Key attributes analyzed within the sandbox include:

- Malware information: The malware's name and category, evasive actions, mutex activity, contents of malware memory, applicable screenshots, and files and registry keys accessed by the malware.
- System IoCs: Process dumps, files and registry keys written by the malware, malware filename, command line details, and hash information.
- Network IoCs: Internet Protocol (IP) addresses and domains contacted by the malware, Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) port activity, Domain Name System (DNS) requests, and network packet capture data.

This comprehensive IoC data can assist security teams in conducting in-depth analyses of malware, helping them to understand and mitigate emerging threats.

Something that CE&BAs operating in HIPAA-regulated environments must consider when implementing vDefend Advanced Threat Prevention is how VM-aware MPS in its current state handles file analysis. If malware is not identified through hash-based or static analysis functions, a quarantined file may be sent to VMware's cloud-based sandbox for deeper inspection. This process provides critical threat intelligence but could also introduce the risk of sensitive data leaving the regulated environment. To mitigate this, organizations can configure VM-aware MPS to disable sandboxing for specific file types, such as those containing ePHI, or implement policies to properly flag and control the handling of sensitive data before it is processed. Alternatively, the cloud sandbox feature can be disabled altogether. While fully disabling this function or just for certain file types ensures that sensitive data remains within the environment, it reduces the overall effectiveness of VM-aware MPS's advanced threat prevention capabilities by limiting the depth of malware analysis. For example, true zero-days would typically require sandboxing to identify. However, local analysis is still active while the sandbox is disabled and can help to identify and prevent some file-based attacks.

Network Traffic Analysis

NTA technology monitors network traffic and traffic flow records. NTA employs machine learning (ML) algorithms and advanced statistical models to establish a baseline of typical network activity, allowing for the identification of deviations from normal behavior. These deviations, which may involve unusual protocol usage, unexpected traffic patterns, or host-specific anomalies, are flagged for further examination.

As not all anomalies indicate malicious activity, NTA incorporates additional analytical layers to combine advanced ML models with rule-based detection techniques. This dual approach helps to contextualize anomalies and assess their potential to represent actual threats, helping to minimize false positives.

Healthcare entities can leverage these capabilities to proactively identify and mitigate potential security threats before they escalate into breaches. If an anomaly is detected in east-west traffic patterns within a hospital's internal network, security teams can quickly determine whether the deviation is due to a misconfigured device, an unauthorized data transfer, or a potential cyberattack. Additionally, integrating these insights with automated policy enforcement enables real-time response mechanisms, such as blocking malicious traffic, isolating compromised devices, or triggering alerts for further investigation.

Network Detection and Response

NDR is designed to enhance threat detection and response capabilities through aggregation, correlation, and contextual analysis. By integrating multiple security signals and advanced analytics, NDR can enable healthcare organizations to proactively identify, investigate, and mitigate threats that could compromise ePHI.

NDR also supports mechanisms for organizations to securely update threat intelligence in standalone operations without external network access. This ensures that all detection, correlation, and response activities are executed entirely within a closed/private network, leveraging both internally and externally sourced threat intelligence. This approach uses local storage and processing, ensuring real-time analysis and threat response while mitigating the risks associated with external connectivity, which CE&BAs may find valuable for high-security, regulatory-sensitive, and isolated networks.

The aggregation engine collects and consolidates signals from a range of detection technologies, including IDS/IPS, NTA, and behavioral analytics. This holistic data collection can allow for a more accurate classification of network activities as malicious or benign, helping to improve detection accuracy and minimize false positives. By synthesizing data from multiple sources, CE&BAs can gain insight into network anomalies that may indicate unauthorized access attempts, lateral movement, or data exfiltration attempts targeting ePHI.

Rather than treating each alert as an isolated event, the NDR correlation engine groups related security alerts into a unified narrative, referred to as an “intrusion campaign.” This approach provides security teams with a broad view of attack patterns and can help them to identify coordinated cyber threats such as ransomware propagation or persistent threat actor activity.

The context engine also integrates external intelligence sources, asset inventories, and third-party security tools to help provide security analysts with the necessary context to differentiate between routine network activity and potential threats to ePHI. For example, if an unusual outbound connection is detected from a medical device, the context engine can correlate this event with known threat intelligence, vulnerability data, and past incidents to assess the level of risk and determine an appropriate response. Additionally, NDR integrates with the MITRE ATT&CK framework, mapping adversary behavior to known tactics and techniques, allowing security teams to proactively hunt for threats within their environment, identifying indicators of compromise associated with ePHI breaches, and refine security policies to prevent future incidents.

By leveraging NDR capabilities, healthcare organizations can enhance their ability to detect, analyze, and respond to security threats in real time. The ability to correlate network anomalies with advanced threat intelligence supports a proactive security posture, ensuring continuous monitoring and compliance with the HIPAA Security Rule. This approach can strengthen defenses against cyberattacks while safeguarding the integrity, confidentiality, and availability of ePHI across healthcare environments.

Security Intelligence for vDefend

Security Intelligence for vDefend is a distributed visibility and policy recommendation engine designed to assist with network segmentation, anomaly detection, and workload classification. Security Intelligence for vDefend leverages real-time analytics and machine learning to help enable security teams to visualize traffic flows, identify security posture gaps, and apply zero-trust micro-segmentation policies based on workload behaviors and data sensitivity. These capabilities can help maintain continuous compliance with HIPAA by enforcing access controls and preventing unauthorized lateral movement.

CE&BAs can use Security Intelligence for vDefend to group assets and workloads based on data sensitivity by leveraging contextual insights from real-time traffic monitoring and behavioral analytics. By aggregating metadata from all workloads in the VCF private cloud, application, Security Intelligence for vDefend creates a comprehensive inventory of workloads, categorizing them based on security policies, user interactions, and application dependencies. For example, workloads

handling ePHI can be dynamically grouped and segmented separately from general IT workloads, helping to ensure strict access controls and monitoring policies.

Security Intelligence for vDefend also supports real-time network activity visualization, automatic policy recommendations, and security validation to help segment sensitive workloads. The Security Intelligence for vDefend engine continuously cross-references network activity against established baselines and security threat models, detecting deviations that may indicate unauthorized access or policy misconfigurations. This proactive approach can help healthcare organizations prevent misconfigurations, troubleshoot policy conflicts, and enforce security controls.

By dynamically classifying workloads and applying policy-driven segmentation, Security Intelligence for vDefend can enable healthcare organizations to minimize their attack surface, enhance regulatory compliance, and safeguard ePHI from cyber threats.

Intelligent Assist for vDefend

Intelligent Assist for vDefend is designed to enhance threat explainability and remediation through Large Language Model (LLM), AI-powered contextual insights, helping security teams understand detection events in plain language. This capability can provide rapid analysis and understanding of the threat as well as clear documentation, which are all necessary for security incidents involving ePHI in HIPAA-regulated environments.

By automatically correlating threat events and identifying IoCs, Intelligent Assist for vDefend can help reduce investigative complexity to assist healthcare organizations in assessing potential breaches and in minimizing false positives. Its ability to provide comprehensive impact assessments can assist security and compliance teams in making informed decisions, help streamline incident response and audit readiness, and aid in maintaining the standards of the HIPAA Security Rule.

It should be noted that Intelligence Assist for vDefend is not trained on, nor does it interact with ePHI. Rather, it leverages network analytics, traffic flows, threat intelligence, and vulnerability information to provide additional understanding for explainability and remediation to the security team. It would therefore be the responsibility of the security and compliance team to understand the nature of the data on the relevant systems impacted by a threat to meet HIPAA and other compliance requirements.

Sensitive data considerations

When CE&BAs are using, or are considering using, the services of the vDefend solution, it is crucial to consider the access and egress of data, specifically PHI. Coalfire noted two instances of potential incidental egress or exposure of PHI to VMware, and both are optional and can be disabled or are disabled by default. Previously, it was noted that the MPS has a cloud-based sandbox for deeper file inspection. This can be disabled entirely or for specific workload types, such as those that contains ePHI. Additionally, VMware support leverages host support bundles to help customers diagnose and resolve problems specific to deployment. As such, VMware support may request these support bundles that contain data and metadata about a deployment to perform diagnostic activities. It is therefore the customer's responsibility to ensure that all data deemed sensitive, such as log messages, core dumps, and environmental information, are removed from the host before collecting the host support bundle.

Coalfire also reviewed the ability that CE&BAs have to optionally elect to share telemetry data with VMware to address performance issues and concluded that there were no areas of concern relating to incidental exposure of sensitive data.

Applicability to the HIPAA Security Rule

This section describes Coalfire's compliance findings and the corresponding customer requirements and responsibilities for the vDefend solution as it was reviewed in Coalfire's analysis.

The narratives that follow detail the HIPAA Security Rule Administrative Safeguards and Technical Safeguards that the vDefend solution has applicability to address or support. Coalfire considers as "applicable" solution features that are either customer configurable or that have a native and default capability to address or support the safeguard. For this section, Broadcom customers are referred to as a CE&BAs. The findings assume that the vDefend solution is used in conjunction with workloads that contain ePHI. Therefore, the vDefend solution is considered in scope for applications within a HIPAA-compliant security program.

It is crucial to understand that HIPAA Security Rule compliance requires a coordinated effort to secure ePHI applications and then to augment the healthcare data platforms with technology that maintains secure access to those applications. vDefend falls into the non-ePHI application category and may only be used to secure workloads. vDefend can only provide enablement and support for HIPAA Security Rule compliance, as its primary function supports other elements of a compliance program.

Successful implementation of any technology relies on the supporting control environment and the applied use of the technology in accordance with defined policies, processes, standards, and procedures. Complementary customer controls are the responsibilities and dependencies that customers should address to ensure the efficacy of the vDefend solution in supporting HIPAA Administrative Safeguards and Technical Safeguards. Typically, this includes an in-depth approach that leverages other, specialized technologies and security controls.

Capabilities supporting the HIPAA Security Rule

The vDefend suite integrates a variety of components that, collectively, support HIPAA Security Rule Administrative Safeguards and Technical Safeguards. These components can help ensure comprehensive administration and protection of ePHI through use of a security management process, workforce security, information access management, security incident procedures, contingency plan, access control, audit controls, data integrity, transmission security, and user authentication mechanisms.

Below is a summary of how solution components support the specific Security Rule Administrative Safeguards and Technical Safeguards mandated by HIPAA.

Applicable HIPAA Security Rule Administrative Safeguards (§ 164.308)

Applicable HIPAA Security Rule Administrative Safeguards (§ 164.308)	
Safeguard	**Capabilities**
Security Management Process (§ 164.308(a)(1)) **(i) Standard: Security management process**. Implement policies and procedures to prevent, detect, contain, and correct security violations. **(ii) Implementation specifications**:	**Security Intelligence for vDefend** • Risk analysis: When vDefend is configured such that a CE&BA has identified and flagged workloads supporting ePHI, Security Intelligence for vDefend and vDefend dashboards can support a healthcare entity's risk analysis by providing insights about network traffic security to workloads, as well as bringing awareness to

Applicable HIPAA Security Rule Administrative Safeguards (§ 164.308)	
(A) *Risk analysis (Required)*. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate. **(B)** *Risk management (Required).* Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). **(C)** *Sanction policy (Required)*. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate. **(D)** *Information system activity review (Required).* Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	vulnerable configurations, such as insecure ports and layer 7 protocols, along with unsegmented applications. Full compliance with the HIPAA risk analysis implementation specification (§164.308(a)(1)(ii)(A)) necessitates that CE&BAs conduct thorough assessments of the systems supporting the data, beyond just the network traffic. **vDefend Advanced Threat Prevention** • Risk reduction: In addition to the vDefend Firewall, which enables CE&BAs to reduce lateral movement risk through micro-segmentation and unapproved communication blocking, vDefend Advanced Threat Prevention can support the reduction of lateral movement-based risks within restricted systems and workloads and can be configured to monitor for and block exploitation attempts, malicious tool use, vulnerabilities, and threat-driven activity. Best practice for full HIPAA compliance includes a risk management function that identifies, tracks, and mitigates risks and vulnerabilities, beyond network-driven threats. **Network Traffic Analysis** • Sanction policy and activity review: NTA leverages AI-driven analytics to identify deviations from normal access patterns, unauthorized privilege escalations, or unusual authentication attempts and provide security teams with automated alerts. This can help them quickly investigate and mitigate risks before they escalate. It can also be used to support information system activity review by providing an accessible and data-driven audit activity log. **Intelligent Assist for vDefend** • Risk analysis, management, and reduction: Intelligent Assist for vDefend provides insights to healthcare security teams to understand threats and vulnerabilities posed against the workloads within the environment, along with suggested steps for how to mitigate or reduce the risk of the identified issues. This can help CE&BAs to respond to and remediate risks in a manner commensurate with the criticality of the identified risk. **Network Detection and Response** • Information system activity review: NDR's holistic data collection enables the collection of system and user activity from across the environment. This enables CE&BAs to accurately review network and user activity for malicious or anomalous activity.
Workforce Security (§ 164.308(a)(3)) **(i)** **Standard: Workforce security**. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	**vDefend Distributed Firewall** • Supervision, clearance, and termination: Role-based access control automation through the distributed firewall automates the enforcement of access control policies by dynamically assigning user privileges based on predefined roles and system/application tagging. This means that only authorized personnel can access specific systems or ePHI, supporting the principle of least privilege. The Identity Firewall (IDFW) component

Applicable HIPAA Security Rule Administrative Safeguards (§ 164.308)	
(ii) Implementation specifications: **(A)** *Authorization and/or supervision (Addressable).* Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed. **(B)** *Workforce clearance procedure (Addressable)*. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate. **(C)** *Termination procedures (Addressable).* Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	of the solution can be integrated into identity management sources to specific application and network access. The configurability of the product and IDFW component allows for granularity in access, such that a user's access can be driven by authorization, clearance, and employee status, including termination. Full compliance with the HIPAA Workforce Security Standard requires CE&BAs to maintain procedures to authorize, ensure the appropriateness of, and terminate access to ePHI.
Information Access Management (§ 164.308(a)(4)) (i) **Standard: Information access management**. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part. (ii) **Implementation specifications**: **(A)** *Isolating health care clearinghouse functions (Required)*. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization. **(B)** *Access authorization (Addressable).* Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism. **(C)** *Access establishment and modification (Addressable)*. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	**vDefend Distributed Firewall** • Isolating health care clearinghouse functions: The distributed firewall rulesets and tagging functionality can enable clearinghouses to isolate and restrict access to only users with an assigned group or to workloads only assigned to a specific group. Compliance with this standard, however, assumes that the CE&BA has established groups and has assigned appropriate tags to workloads supporting clearinghouse functions. • Access modification: The distributed firewall automatically enforces the rulesets that are established for user groups and system tags to ensure that users within a group change automatically as a group's membership changes. Full HIPAA compliance with the Access authorization (§164.308(a)(4)(ii)(B)) and Access establishment and modification (§164.308(a)(4)(ii)(C)) implementation specifications require that the CE&BA implements a process for administering access and for changing access appropriately, including policies, documentation, and review.
Security Incident Procedures (§ 164.308(a)(6)) (i) **Standard: Security incident procedures**. Implement policies and procedures to address security incidents. (ii) **Implementation specification**: *Response and reporting (Required)*. 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.	**vDefend Advanced Threat Prevention** • Incident response and reporting: Advanced Threat Prevention enables healthcare organizations to have visibility to traffic leaving from workloads with sensitive data in abnormal patterns along with the ability to prevent these transfers from occurring, which can reduce the potential for a security incident or breach. Intrusion campaign logging from NDR and Malware and NTA can provide additional support for documenting the security incident and its outcome. The integration between ATP and security tools such as SIEM and SOAR enable CE&BAs to have a more comprehensive view and ability to respond to incidents. Full HIPAA compliance requires further implementation of response and reporting processes for managing the entire life cycle of an incident.

Table 1: Applicable HIPAA Security Rule Administrative Safeguards - §164.308

Applicable HIPAA Security Rule Technical Safeguards (§ 164.312)

Applicable HIPAA Security Rule Technical Safeguards (§ 164.312)	
Safeguard	**Capabilities**
Access Control (§ 164.312(a)) **(1) Standard: 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]. **(2) Implementation specifications**: **i.** *Unique user identification (Required)*. Assign a unique name and/or number for identifying and tracking user identity. **ii.** *Emergency access procedure (Required)*. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency. **iii.** *Automatic logoff (Addressable)*. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. **iv.** *Encryption and decryption (Addressable)*. Implement a mechanism to encrypt and decrypt electronic protected health information.	**vDefend Distributed Firewall** • Unique user identification: Systems, environments, or machines that store, process, or interact with ePHI can be dynamically classified using automated tagging mechanisms, allowing granular access control policies to be applied. These tags can enforce context-aware access restrictions, helping ensure that only authorized users and machine-to-machine communications can interact with sensitive workloads. Additionally, Security Intelligence for vDefend and the Distributed Firewall can integrate with identity providers to align access policies with role-based access control frameworks, further strengthening access governance. • Emergency access: Policy automation and intelligent flow visualization allows administrators to either use pre-configured or customer-defined environment-specific policies for emergency access to critical systems while maintaining auditability. Real-time visibility into traffic flows is also provided, helping with rapid identification of anomalous access attempts during emergency situations. • Automatic logoff: Provides session timeout and access restrictions to help enforce session timeouts and restrict access to unapproved or high-risk URLs, reducing the risk of unauthorized access to ePHI through inactive sessions. Additionally, firewall rules can be configured to only allow access during specific times of day. This function limits exposure to external threats by controlling which web-based applications and resources users can access. **Security Intelligence for vDefend** • Encryption and decryption: Workloads tagged as storing, processing, or interacting with ePHI are continuously monitored within the Security Intelligence for vDefend dashboard to help ensure that all approved ingress and egress flows enforce encryption protocols and use approved cryptographic standards. Security Intelligence for vDefend also provides policy validation tools to help CE&BAs confirm compliance with encryption requirements, helping with proper key management practices and encryption strength. For full implementation of encryption and decryption, organizations must complement vDefend's monitoring capabilities with appropriate key life cycle management to prevent unauthorized decryption or exposure of sensitive data.
Audit Controls (§ 164.312(b))	**vDefend Suite**

Applicable HIPAA Security Rule Technical Safeguards (§ 164.312)	
Standard: 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.	• Audit log aggregation: The vDefend suite collects and aggregates system logs across environments that can be integrated into a SIEM system to provide a comprehensive view of user actions, system activities, and access to ePHI. This enables audit trails that support compliance with regulatory requirements and helps identify suspicious activities that may indicate unauthorized access or data breaches. Real-time log monitoring and alerts can be configured to continuously monitor logs for predefined events, such as unauthorized access attempts or changes to sensitive data, and triggers alerts for immediate investigation. This can enhance incident response by providing timely and actionable data for security teams. • Audit intrusion campaigns: The vDefend suite collects and fully correlates system logs, intrusion campaigns, and individual threat detection events that can be ingested into a SIEM, which helps Security Operations Center operators to triage and respond to threats. Threat event logging can also help organizations to meet compliance requirements for mapping threats to assets. Full packet captures (PCAPS) for associated IDS detection events are also available to assist in threat investigation. **vDefend Distributed Firewall:** • Audit logs for traffic: Intelligent flow visualization and logging for the Distributed Firewall provides real-time and historical visibility into network traffic, enabling security teams to monitor and track access to systems containing ePHI. All permitted and denied traffic flows are logged, which can support forensic investigations and compliance audits. • Audit logs for users: User-identity-based access control with event logging captures user authentication and access events, ensuring accountability by maintaining detailed records of who accessed ePHI, when, and from where. This can support integration with SIEM solutions for centralized log analysis and compliance reporting.
Integrity (§ 164.312(c)) **(1) Standard: Integrity**. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. **(2) Implementation specification**: *Mechanism to authenticate electronic protected health information (Addressable)*. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	**vDefend Distributed Firewall:** • Integrity of data access: vDefend enforces strict security policies at the hypervisor and workload levels, helping ensure that only authorized applications and users can access or modify ePHI. Unauthorized traffic attempting to interact with ePHI systems is blocked, helping prevent data tampering and unauthorized alterations. • Integrity of application-aware data integrity protection: By verifying application identities, vDefend can ensure that only approved applications can modify or transmit ePHI. This helps prevent unauthorized software or malicious code from altering sensitive health records. **vDefend Gateway Firewall:** • Integrity of data in transit: vDefend uses TLS decryption and deep packet inspection to analyze encrypted traffic

Applicable HIPAA Security Rule Technical Safeguards (§ 164.312)	
	for potential threats, helping prevent attackers from bypassing security controls to manipulate or exfiltrate ePHI. It is able to detect and block integrity threats such as data injection attacks, unauthorized modifications, and protocol misuse. **vDefend Firewall Flow Visualization:** • Integrity monitoring: vDefend provides real-time visibility into network traffic and system interactions, flagging anomalies that may indicate integrity violations. Unauthorized modifications to ePHI, unexpected data flows, or suspicious activity generate alerts and visual indicators, helping security teams to take immediate action.
Person or Entity Authentication (§ 164.312(d)) **Standard: Person or entity authentication**. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	**vDefend Distributed Firewall:** • Person authentication: Role-based access control policy enforcement helps ensure that only authenticated and authorized users can access systems containing ePHI based on system and user tagging. vDefend verifies user credentials and permissions before granting access, helping ensure users can only interact with data necessary for their role. • Entity authentication: Enforces strict machine and workload verification by requiring cryptographic certificates or tokens for system authentication. This can prevent unauthorized or unmanaged devices from communicating with ePHI systems, helping ensure that only trusted entities can access sensitive healthcare data. • Authentication anomaly detection: Continuous monitoring captures detailed authentication logs, tracking login attempts, access approvals, and failures. By identifying suspicious patterns, such as repeated failed logins, access attempts from unusual locations, or anomalous workload requests, vDefend Firewall helps detect potential brute-force attacks, compromised credentials, or attempted lateral movement.
Transmission Security (§ 164.312(e)) **(1) Standard: Transmission security**. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. **(2) Implementation specifications**: **i.** *Integrity controls (Addressable)*. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of. **ii.** *Encryption (Addressable)*. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	**vDefend Gateway Firewall** • Integrity and encryption: Data integrity assurance helps ensure data integrity during transmission by inspecting encrypted traffic for potential threats, unauthorized modifications, or injection attacks. It also can detect and block man-in-the-middle attacks and other threats that could alter ePHI in transit. **vDefend Distributed Firewall** • Encryption: Secure application-layer enforcement restricts which applications can transmit ePHI, helping ensure that only approved and authenticated services are sending sensitive data and that it is sent with encryption. Secure data transmission secures ePHI in transit by encrypting network communications using IPSec VPN tunnels, helping prevent unauthorized interception or access. The firewall supports site-to-site

Applicable HIPAA Security Rule Technical Safeguards (§ 164.312)	
	VPNs to help secure encrypted communication between data centers, remote users, and cloud environments. **vDefend Advanced Threat Prevention** • Integrity monitoring: The vDefend Advanced Threat Prevention function monitors network traffic in real time to detect anomalies, unauthorized modifications, and potential data tampering. This helps prevent alteration of ePHI in transit by identifying malicious activity such as injection attacks or unauthorized data manipulation. **Security Intelligence for vDefend** • Integrity monitoring: Security Intelligence for vDefend provides visibility into network traffic flows, allowing security teams to track data movement and enforce segmentation policies. Detection of misconfigurations and security gaps can reduce the risk of unauthorized data transmission by recommending appropriate security controls. Unencrypted flow identification provides real-time monitoring of unencrypted traffic, allowing administrators to flag and reconfigure flows to enforce encryption where necessary. Insecure port and protocol detection highlights potential vulnerabilities by identifying open, misconfigured, or unauthorized ports and protocols, helping security teams to apply mitigation strategies and strengthen transmission security.

Table 2: Applicable HIPAA Security Rule Technical Safeguards - §164.312

It is Coalfire's opinion that these components collectively establish a strong framework for securing ePHI, detecting security incidents, and maintaining compliance with the HIPAA Security Rule Administrative Safeguards and Technical Safeguards. By leveraging these capabilities, vDefend can support addressing the specific security and compliance needs of healthcare environments.

Complementary customer controls for compliance

Healthcare entities, including CE&BAs, cannot achieve comprehensive HIPAA compliance solely by implementing security technologies. While the HIPAA Security Rule establishes required safeguards for protecting ePHI, it does not provide prescriptive technical guidance. To bridge this gap, organizations should adopt a structured cybersecurity framework, such as NIST SP 800-53, to inform their approach and enhance compliance efforts. The following subsections outline key customer responsibilities when integrating vDefend into a HIPAA-regulated environment.

Shared responsibility model

vDefend operates within a shared responsibility framework, providing advanced security capabilities such as network micro-segmentation, IDS/IPS, and security intelligence. However, customers retain ultimate responsibility for properly configuring, managing, and monitoring these controls to ensure compliance with HIPAA requirements. Below are some examples of additional customer responsibilities to support a more complete HIPAA compliance program:

Administrative Safeguards (§ 164.308)

- **Security management process (§ 164.308(a)(1)):** While vDefend detects network vulnerability exploits, CE&BAs must perform regular vulnerability and risk assessments, correlate findings with CVSS scores, and prioritize remediation efforts to address potential threats to ePHI. CE&BAs should also establish a formal vulnerability management program that aligns with HIPAA requirements.
- **Information access management (§ 164.308(a)(4)):** vDefend helps enforce access controls, but CE&BAs must establish approval processes to ensure users can access workloads and segments based on their roles and responsibilities.
- **Security awareness training (§ 164.308(a)(5)):** CE&BAs must update security policies to reflect vDefend's integration and train personnel on its role in protecting ePHI. Training should cover threat awareness, incident response, and secure configuration practices.
- **Security incident procedures (§ 164.308(a)(6)):** Customers must incorporate vDefend alerts into their broader incident response plan to address potential security events. This includes establishing protocols for detecting, containing, mitigating, and documenting security incidents involving ePHI.
- **Contingency plan (§ 164.308(a)(7)):** CE&BAs must develop policies and procedures to ensure the availability, integrity, and security of ePHI during emergencies, including system failures, cyber incidents, and natural disasters. This includes data backup strategies, disaster recovery planning, and emergency mode operations to maintain critical business functions while mitigating risks to protected health information.

Technical Safeguards (§ 164.312)

- **Access control (§ 164.312(a)(1)):** Customers must configure role-based access control within the vDefend platform to enforce the principle of least privilege and ensure that only authorized personnel have access to ePHI. Role assignments should be reviewed regularly to prevent unauthorized access.
- **Audit controls (§ 164.312(b)):** Customers are responsible for integrating vDefend-generated logs with a centralized logging solution (e.g., SIEM tools) to meet audit trail requirements. While HIPAA does not mandate a specific retention period, organizations should retain logs based on their risk management strategy and compliance policies.
- **Integrity (§ 164.312(c)(1)):** Customers must configure vDefend's monitoring capabilities to detect and alert on unauthorized system modifications or anomalies in network traffic that could compromise ePHI integrity.
- **Person or entity authentication (§ 164.312(d)):** Customers must configure authentication settings within vDefend to require strong credentials and, where applicable, multi-factor authentication to verify user identities accessing ePHI.
- **Transmission security (§ 164.312(e)(1)):** While vDefend provides encryption support, customers must ensure that ePHI transmitted over networks is encrypted using industry-standard encryption protocols to protect data in transit.

By implementing these complementary controls, CE&BAs can maximize the effectiveness of vDefend in supporting the HIPAA Security Rule. A well-configured and actively managed vDefend deployment can enhance ePHI protection, strengthen security governance, and support compliance with evolving regulatory requirements.

Aligning product capabilities with the proposed HIPAA Security Rule changes

As HHS moves to eliminate “addressable” implementation specifications and mandate stricter security measures across all covered entities and business associates, organizations must reassess their security posture to ensure full compliance. vDefend can help healthcare entities navigate these new requirements by integrating robust security capabilities that align with the proposed updates. Outlined below is how, based on Coalfire’s analysis, vDefend’s suite of capabilities can be leveraged to support compliance with potential new mandates:

- **Elimination of addressable specifications**: With the elimination of flexibility in HIPAA compliance, CE&BAs must adopt a comprehensive security approach that fully meets all prescribed safeguards. When properly implemented, vDefend provides a holistic, integrated security framework that enforces consistent security policies across network infrastructure, workloads, and cloud environments. Its automated policy enforcement engine can help ensure that security measures are applied uniformly, reducing the risk of gaps in compliance.
- **Network mapping and inventory management**: The proposed changes require organizations to maintain an up-to-date network map that details the movement of ePHI. The Security Intelligence for vDefend module offers real-time visibility into network traffic, automatically generating and updating network topology maps that document data flows within and outside of an organization’s environment. This capability can support compliance by ensuring that network maps remain current and accurate.
- **Session control and automated termination**: To meet the new requirement for automated session terminations, the vDefend session timer functionality enforces session-based access restrictions, which can ensure that inactive or unauthorized sessions are terminated automatically. By leveraging behavioral analytics and AI-driven monitoring, vDefend can identify abnormal session activity, trigger automated terminations, and alert security teams to potential risks.
- **Encryption for data in transit**: vDefend maintains visibility into what workloads enforce encryption between one another, helping organizations to plan, track, and monitor the movement of ePHI within its environment, along with enforcing security ruleset compliance.
- **Network port security and access control**: To address the requirement for disabling unnecessary network ports, the vDefend Advanced Threat Prevention module continuously scans network configurations and dynamically blocks unauthorized or unused ports. Additionally, vDefend enables role-based firewall policies, ensuring that only required ports remain open while blocking all others, helping reduce the attack surface and prevent unauthorized access.
- **Real-time auditing and continuous monitoring**: vDefend’s Multi-context NDR enables real-time auditing by continuously analyzing network traffic, user behaviors, and system events. Through automated alerting and forensic data collection, organizations can meet the proposed new HIPAA requirement for continuous monitoring and detect unauthorized activity as it occurs. The integration of MITRE ATT&CK mapping helps ensure that adversarial tactics are identified and mitigated before they result in a security breach.

As HIPAA compliance becomes more stringent, healthcare organizations and their business associates must adopt solutions that not only meet regulatory requirements but also enhance overall cybersecurity resilience. vDefend provides an integrated, automated, and intelligence-driven approach to security that can help organizations adapt to evolving regulatory landscapes without disrupting operations. By leveraging real-time monitoring, automated enforcement, advanced threat prevention, and adaptive security controls, vDefend can assist healthcare organizations with staying ahead of compliance requirements while helping to strengthen their defenses against modern cyber threats. With these

capabilities, organizations can navigate the proposed HIPAA Security Rule updates and help ensure compliance, security, and operational efficiency.

Conclusion

Coalfire has determined that the vDefend solution can be effective in supporting CE&BAs in meeting the requirements of the HIPAA Security Rule Administrative Safeguards and Technical Safeguards. Its strengths support micro-segmentation, role-based access control, security policy automation, and threat intelligence utilization, along with advanced threat prevention. The solution's comprehensive network security approach, which includes effective distributed firewalling technology and advanced threat prevention, demonstrates a robust capability for protecting ePHI and helping ensure secure data transmission.

Achieving optimal HIPAA compliance requires a comprehensive strategy that extends beyond the capabilities of any single solution. This white paper explored how vDefend supports the HIPAA Security Rule Administrative Safeguards and Technical Safeguards and highlighted the customer responsibilities that are crucial for successful implementation.

By understanding these alignments and responsibilities, healthcare organizations can leverage the vDefend solution's strengths while implementing additional security controls and processes to achieve a comprehensive HIPAA compliance posture. This layered approach, combining solution capabilities with a commitment to best practices and compliance requirements, provides organizations with the ability to ensure the confidentiality, integrity, and availability of ePHI, mitigate risks, and continuously improve their security posture.

Legal disclaimer

Additional information, resources, and references

This section contains a description of the links, standards, guidelines, and reports referenced for the materials used to identify and discuss the features, enhancements, and security capabilities of vDefend.

Broadcom resources

- Architecture and capabilities of the vDefend suite, focusing on its integration with Security Intelligence for vDefend for secure private cloud environments.
  - https://www.vmware.com/docs/vmware-secure-private-cloud-with-vmware-vdefend
- Features of the vDefend Distributed Firewall and Gateway Firewall, including micro-segmentation and automated policy enforcement for network security.
  - https://www.vmware.com/docs/vmw-vdefend-firewall-1
- Advanced threat detection capabilities, including IDS/IPS, malware prevention, and anomaly detection for traffic flows.
  - https://www.vmware.com/docs/vmware-advanced-threat-prevention-with-nsx-distributed-firewall
- Security Intelligence for vDefend's features for monitoring, visibility, and analytics that support segmentation, tagging, and compliance reporting.
  - https://www.vmware.com/docs/vmware-nsx-intelligence-solution-brief
- Insights into the network traffic analysis tools within Security Intelligence for vDefend, emphasizing application-aware traffic inspection and protocol decoders.
  - https://www.vmware.com/docs/vmware-nsx-network-traffic-analysis
- IDS/IPS features for detecting and mitigating threats at the network perimeter and internal boundaries.
  - https://www.vmware.com/docs/vmware-nsx-distributed-ids-ips-solution-overview
- Advanced sandboxing capabilities for analyzing and preventing malware and other threats.
  - https://www.vmware.com/docs/vmw-nsx-sandbox-solution
- Intelligent Assist large language model module for assessing security vulnerabilities and risks.
  - https://blogs.vmware.com/security/2024/11/intelligent-assist-for-vdefend.html
- Walkthroughs on configuring the platform based on business requirements.
  - https://www.youtube.com/@vmwarevdefend
- Knowledge-based article expounding on securing sensitive data when collecting support bundles.
  - https://knowledge.broadcom.com/external/article/327899

HIPAA resources

- U.S. Department of Health and Human Services (HHS) HIPAA Guidance. Provides comprehensive guidance on the HIPAA Privacy, Security, and Breach Notification Rules.
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

- HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework. Aligns the HIPAA Security Rule to the NIST Cybersecurity Framework to help healthcare organizations manage cybersecurity risks.
  - https://www.hhs.gov/hipaa/for-professionals/security/nist-security-hipaa-crosswalk/index.html
- NIST SP 800-66 Revision 1. Provides an implementation guide for the HIPAA Security Rule.
  - https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
- HHS OCR Cybersecurity Guidance. Offers resources and guidance on cybersecurity best practices for HIPAA covered entities.
  - https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/index.html
- HealthIT.gov HIPAA Security Risk Assessment Tool. An interactive tool to assist small to medium-sized healthcare practices in conducting security risk assessments as required by the HIPAA Security Rule.
  - https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment

Coalfire resources

- The Coalfire corporate healthcare and life sciences advisory offerings may be found at the following links:
  - https://www.coalfire.com/industries/healthcare-life-sciences
  - https://coalfire.com/the-coalfire-blog/service-lines/healthcare-grc
  - https://coalfire.com/services/advisory
- Coalfire corporate information is available at the following link:
  - https://www.coalfire.com/about

About the author

Caleb Pfanstiel | *Consultant, GRC Healthcare*

Caleb Pfanstiel has considerable experience in risk management, compliance, and securing complex healthcare operations. He is passionate about bridging the gap between technical challenges and business needs, helping organizations navigate the ever-evolving cybersecurity landscape. With a focus on healthcare and life sciences, Caleb combines a strong understanding of regulatory frameworks with practical strategies to protect sensitive data and critical systems. His work ensures organizations can innovate confidently while maintaining robust security postures.

About Coalfire

The world's leading technology infrastructure providers, SaaS companies, and enterprises – including the top 5 cloud service providers and 8 of the top 10 SaaS businesses – rely on Coalfire to strengthen their security posture and secure their digital transformations. As the largest firm dedicated to cybersecurity, Coalfire delivers a comprehensive suite of advisory and managed services, spanning cyber strategy and risk, cloud security, threat and vulnerability management, application security, privacy, and compliance management. A proven leader in cybersecurity for the past 20 years, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success. For more information, visit **Coalfire.com**.