WHITE PAPER

Broadcom Inc. VMware vDefend Product Applicability Guide

Applicability to Assist Customers in Compliance with NIST CSF 2.0

COALFIRE OPINION SERIES, April 2026

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 VMware Cloud Foundation (VCF) to evaluate its effectiveness in assisting organizations that use (or are considering using) vDefend to strengthen their cybersecurity posture in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. This evaluation also considers the relationships between NIST CSF 2.0, the NIST Risk Management Framework (RMF), and the supporting control requirements defined in NIST Special Publication (SP) 800-53.

This Product Applicability Guide (PAG) examines how an organization’s implementation of the vDefend solution aligns with the NIST CSF 2.0 Core Functions: Govern, Identify, Protect, Detect, Respond, and Recover. This PAG outlines Coalfire’s methodology and assessment approach, summarizes key findings from Coalfire’s review of vDefend’s capabilities, provides context for applying these capabilities within an organization’s cybersecurity program, and presents Coalfire’s opinion on how vDefend’s security features can support adherence to NIST CSF 2.0 outcomes for VCF environments.

Coalfire PAGs present Coalfire’s professional perspective regarding a product’s applicability to established standards, frameworks, and mandates through the “eyes of the assessor” and should not be interpreted as a product endorsement. These PAGs are a component of Coalfire’s product advisory services and are designed to inform existing vDefend customers as well as prospective users evaluating the solution.

The vDefend solution for VCF provides protection for 32 Subcategories in the Identity, Protect, Detect, and Respond Functions of CSF 2.0. The majority of the requirements are fully met or strongly met, with some supplemental customer responsibilities while using vDefend needing to be fulfilled to fully meet the intent of the Subcategory requirements.

Introduction to NIST CSF 2.0

NIST CSF 2.0 is a risk-based framework designed to help organizations understand, manage, and improve their cybersecurity posture. NIST CSF 2.0 organizes key cybersecurity objectives into clear, outcome-focused areas that support stronger governance, better visibility into organizational risks, improved protection of systems and data, timely detection of threats, and effective response and recovery from cybersecurity incidents. The framework enables organizations to evaluate where they stand today, identify gaps, and prioritize actions that strengthen their overall resilience.

NIST CSF 2.0 defines six central Functions: Govern, Identify, Protect, Detect, Respond, and Recover, which together offer a comprehensive view of the practices and outcomes associated with managing cybersecurity risk. These Functions are further detailed into more specific outcomes that organizations can use to assess their cybersecurity activities and guide internal planning and decision making. Rather than prescribing specific technologies or configurations, the CSF emphasizes flexibility, allowing organizations to tailor the framework to their mission, risk profile, and operating environment. CSF outcomes apply across modern technology environments, including on-premises systems, cloud infrastructure, operational technology, mobile devices, and emerging technologies.

NIST CSF 2.0 is closely aligned with other NIST risk and control frameworks. Organizations using the NIST RMF can apply the CSF at a strategic level to define desired cybersecurity outcomes, while RMF provides specific processes for selecting, implementing, assessing, and monitoring controls. In addition, NIST 800-53 offers detailed control requirements that directly support many CSF outcomes. This alignment allows organizations to use the CSF to set direction and communicate priorities, while relying on RMF and NIST 800-53 to meet operational and technical control expectations. An additional mapping to NIST RMF and NIST 800-53 controls is included in Appendix A for reference.

Because the CSF focuses on cybersecurity results rather than certifying specific technologies, products are not "validated" against the CSF. However, independent technical analyses, such as Coalfire's PAGs, can help organizations understand how a product's capabilities can support CSF outcomes and where customer responsibilities remain.

This Coalfire PAG outlines how vDefend can support an organization's alignment with NIST CSF 2.0, including how its capabilities relate to RMF processes and NIST SP 800-53 control requirements. The intent is to provide practical, assessor-based insights to help current and prospective users incorporate vDefend effectively into their cybersecurity and risk management programs.

The Role of vDefend

vDefend represents a comprehensive approach to securing VCF private cloud environments. Designed with a focus on micro-segmentation, advanced threat prevention, and actionable security intelligence, vDefend helps organizations strengthen their security posture while supporting compliance with frameworks such as CSF 2.0.

The vDefend Solution

vDefend is purpose-built for VCF private cloud environments across all workloads (virtual machine [VM], Kubernetes, artificial intelligence [AI], and bare metal servers). It delivers key capabilities for critical CSF 2.0 compliance activities through integrations with security and monitoring workflows. vDefend's emphasis on visibility, automation, and actionable intelligence helps detect and respond to perimeter and lateral threats effectively. It provides organizations with tools to protect sensitive workloads, manage compliance challenges, and streamline security operations. Built with scalability and adaptability in mind, vDefend addresses current and emerging threats while facilitating compliance with federal frameworks such as CSF 2.0.

vDefend overlays actionable insights and automation on top of technical controls to enhance operational efficiency. For organizations managing complex environments, vDefend facilitates the detection, analysis, and remediation of threats while reducing the noise of false positives. This enables security teams to prioritize resources effectively, for faster response times and more efficient operations.

vDefend Firewall

VMware vDefend is offered as a single solution that includes Distributed Firewall, Gateway Firewall, Intrusion Detection and Prevention Service (IDS/IPS), Malware Prevention Service (MPS), Network Detection and Response (NDR) and NDR Sensor, Network Traffic Analysis (NTA), and deep traffic visibility. This simplifies operational complexity and offers a closed-loop security system for private cloud environments that ensures visibility, prevention, detection, and mitigation.

vDefend Distributed Firewall is a software-defined, hypervisor-embedded distributed firewall solution that addresses security gaps, improves segmentation posture, and ensures regulatory compliance. Distributed Firewall delivers a prescriptive, multi-stage segmentation deployment workflow to progressively secure east-west traffic in the VCF private cloud. Context-driven security policies offer access control for applications and protect against lateral movement of threats. Comprehensive application visibility of virtualized infrastructure and policy recommendations ensure that the appropriate security policy is applied to the right set of workloads.

vDefend Gateway Firewall is an enterprise-class next-generation internal firewall that enforces zone-based controls within a private cloud. It includes advanced features such as user identification, layer-7 application identification, and fully qualified domain name (FQDN)-based filtering. Together, these solutions offer a layered approach to network protection, addressing both internal and external threat vectors.

Both vDefend Firewall components integrate with security operations workflows, providing visibility and actionable intelligence for both proactive and reactive security measures.

Security Intelligence for vDefend

vDefend includes Security Intelligence and offers users flexibility at various stages of their security journey. Security Intelligence complements the vDefend Firewall and vDefend Advanced Threat Prevention (ATP) features by providing a tailored solution for automating security workflows. It provides visibility into network traffic patterns, allowing teams to identify anomalies and optimize segmentation strategies. With integration into security information and event management (SIEM) platforms and other security and incident response tools, Security Intelligence for vDefend supports threat hunting and long-term trend analysis, key components of an effective security program. Its integration with other vDefend components allows for continuous monitoring and automated policy recommendations, facilitating ongoing compliance with CSF 2.0. Security Intelligence can reduce manual effort and help maintain compliance in dynamic environments by automating policy recommendations and facilitating continuous monitoring.

vDefend ATP

vDefend ATP capabilities are integrated into the vDefend Firewall, providing threat detection and response without adding operational complexity.. Integration of these capabilities is designed to enhance an organization's incident response and forensic analysis capabilities.

IDS/IPS

IDS/IPS functionality supports multiple CSF 2.0 Functions by detecting, alerting on, and mitigating suspicious activities and threats in real time. This feature protects in-scope systems by preventing unauthorized access and lateral movement. The ability to enrich IDS/IPS alerts and events with broader network traffic analysis through NTA and NDR provides deeper context and faster threat validation.

NTA/NDR

NTA and NDR further enhance visibility by leveraging machine learning and behavioral analysis to detect anomalous patterns and potential threats across the network.

MPS

MPS extends vDefend’s value by providing deep malware analysis, examining files and URLs for malicious behavior in a controlled environment. This solution enhances vDefend’s threat prevention capabilities by identifying sophisticated attacks that might evade traditional defenses. This capability aids forensic investigations by offering granular insights into malware behavior, enabling teams to block advanced threats more effectively.

vDefend’s focus on micro-segmentation, advanced threat prevention, and security intelligence positions it as a strategic solution for organizations seeking to strengthen their security posture. By addressing both perimeter and internal threats, vDefend supports the broader CSF 2.0 compliance initiative while providing a foundation for more advanced security frameworks.

Scope and Approach

Coalfire began by examining the NIST CSF 2.0 Functions, Categories, and Subcategories, then identifying them as either organizational (non-technical) or technical. A Subcategory was determined to be either organizational or technical based on a review of the Category and Subcategory descriptions.

Organizational requirements include documented policies, procedures, and standards that were not considered directly applicable to the technical solution. Examples of non-technical requirements include maintaining facility visitor logs, verifying an individual’s identity before granting physical or logical access, performing periodic physical asset inventories, and other elements that vDefend could not satisfy.

Evaluation of CSF 2.0 and Scoring System

Coalfire used the CSF Core outlined in Appendix A of the NIST CSF 2.0 as the starting point for identifying relevant technical requirements. Once identified, technical Subcategories of the Functions were assessed to determine applicability to vDefend. If the achievement of the Subcategory was more likely to be met using an external and non-adjacent mechanism, the Subcategory was determined to be not applicable to vDefend and excluded.

Where the Subcategory was determined to be applicable, Coalfire assessed the capability of vDefend to address the requirement listed in the Subcategory using the NIST-provided Implementation Examples as a reference. In keeping with the desire to present the information compactly, Coalfire used Harvey Balls (https://en.wikipedia.org/wiki/Harvey_Balls) to assign each applicable Subcategory a coverage score if the solution had at least a partial capacity to support the requirement described in the Subcategory.

The table below is a key for the scores given to each requirement in the scoring tables below:

Symbol	Description	Definition
●	Full coverage	Fully supports or directly addresses the requirement. Minimal effort required of customers to provide full coverage.
◕	Strong coverage	Supports most aspects of the requirement but not entirely. Customers may have some responsibility to implement a business process or configuration to provide full coverage.
◑	Partial coverage	Supports some aspects of the requirement but not entirely. Customers have responsibility to implement a business process or configuration to provide full coverage.

Table 1: vDefend CSF Scoring System

vDefend Applicability to NIST CSF 2.0

vDefend applicability is determined by comparing the CSF Core to vDefend capabilities that aid organizations in meeting the CSF 2.0 cybersecurity requirements under the Govern, Identify, Protect, Detect, Respond, and Recover Functions. The following sections describe the level of coverage provided by vDefend in a VCF environment using the scoring system described in the Scope and Approach section.

Coalfire compared the vDefend solution capabilities to the 106 Subcategories available in NIST CSF 2.0 and determined about one third of the CSF 2.0 requirements are at least partially covered when using vDefend to secure a VCF environment. The capability to monitor, inspect, and protect the east/west traffic within a VCF environment enables vDefend to provide cybersecurity protection of the Identify, Protect, Detect, and Respond Functions of the CSF 2.0. The CSF Functions and Subcategories are broad, high-level requirements that are not specific to security solutions or capabilities. The intention is to provide an open framework for evaluating an organization's cybersecurity. Since many requirements are related to organizational and business processes, they cannot be fully addressed by a security solution alone.

The summary of Functions vDefend provides coverage for are provided in the vDefend NIST CSF 2.0 Function Coverage table below. The Subcategory, Implementation, and Score are included in the following sections under the header for each respective Function.

Function	Full Coverage	Strong Coverage	Partial Coverage
Identify	6	4	1

Function	Full Coverage	Strong Coverage	Partial Coverage
Protect	2	2	1
Detect	6	3	0
Respond	2	3	2

Table 2: vDefend NIST CSF 2.0 Function Coverage

Categories and Subcategories not at least partially met by vDefend will be omitted from the scoring tables in the following Govern, Identify, Protect, Detect, Respond, and Recover section. Only requirements where vDefend provides a score with at least partial coverage are included below.

Govern

The Govern Function of NIST CSF 2.0 establishes organizational-level expectations for cybersecurity strategy, risk management, roles and responsibilities, policies, oversight, and governance processes. These requirements focus on enterprise governance activities such as establishing risk management frameworks, defining accountability structures, setting cybersecurity strategy, and managing legal, regulatory, and oversight obligations, which are outside the scope of vDefend's technical functionality.

While vDefend provides security capabilities that contribute to a stronger security posture, it does not perform governance tasks, create or manage policies, assign organizational responsibility, or operate as part of executive-level cybersecurity oversight. Accordingly, vDefend cannot directly fulfill any of the governance-level controls within the Govern Function. Its support is indirect, limited to supplying technical insight that organizations may incorporate into broader governance processes.

Identify

The Identify Function of NIST CSF 2.0 establishes the foundational understanding an organization needs to manage cybersecurity risk effectively. It focuses on developing visibility into organizational assets, including workloads, data flows, software, systems, and supplier dependencies, and understanding the threats, vulnerabilities, and business context associated with them. By building this baseline, organizations can determine what is most critical to their mission, assess inherent risks, and prioritize protection and detection efforts accordingly. Within this Function, vDefend contributes by providing deep visibility into virtualized environments, mapping east/west traffic flows, identifying workload dependencies, and surfacing behavioral anomalies. Although vDefend does not replace formal enterprise risk management or asset governance programs, its Security Intelligence capabilities provide risk visibility and risk scoring based on workloads, traffic flows, and policy posture. These analytics and segmentation insights help organizations better understand their operational environment, identify relative risk exposure, and enhance the accuracy and depth of risk assessments within the NIST CSF Identify Function.

Category	Subcategory	Implementation	Score
Asset Management (ID.AM)	ID.AM-01: Inventories of hardware managed by the organization are maintained	vDefend inventories supported physical servers within the VCF private cloud. The Security Services Platform can provide the bare metal server inventory to NSX Manager when the Bare Metal Security feature is activated. This provides visibility extending beyond virtualized workloads to	●

Category	Subcategory	Implementation	Score
		include physical hosts and their associated traffic flows.	
Asset Management (ID.AM)	ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	vDefend's Security Intelligence aggregates metadata from workloads, creating a comprehensive inventory of workloads deployed in private cloud environments.	●
Asset Management (ID.AM)	ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	vDefend provides real-time visibility into traffic flows, enabling organizations to map internal communication patterns and dependencies within the private cloud environment.	●
Asset Management (ID.AM)	ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	vDefend provides workload classification based on behavior and data sensitivity, which can inform asset prioritization. Customers using vDefend are responsible for using the information provided by vDefend to assign the appropriate business criticality.	◕
Asset Management (ID.AM)	ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	vDefend supports segmentation by identifying and classifying workloads based on observed data sensitivity and traffic behavior. Customers must use Security Intelligence to review and modify the workload as needed to ensure the workloads are accurately and appropriately classified for their environment.	◕
Risk Assessment (ID.RA)	ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	vDefend supports threat identification through anomaly detection, posture analysis, and risk-based insights derived from observed traffic, behaviors, and security gaps. Detection and correlation of vulnerabilities is performed, though scanning is not proactive or as deep as a pure vulnerability scanning solution would perform.	◕
Risk Assessment (ID.RA)	ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	Cyber threat intelligence is integrated into vDefend, and ATP receives threat intelligence feeds from vDefend Threat Intelligence Service (vTIS). vTIS is continuously updated with known threats, IDS signatures, URL/IP reputations, and NDR threat metadata.	●
Risk Assessment (ID.RA)	ID.RA-03: Internal and external threats to the organization are identified and recorded	Threat monitoring by ATP provides information on potential attacks, likelihood, and impact. Customers are responsible for leveraging the information and analysis	◑

Category	Subcategory	Implementation	Score
		provided to confirm and record the internal and external threats to the organization.	
Risk Assessment (ID.RA)	ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	vDefend identifies application dependencies through traffic flow analytics. ATP monitors events and provides information including the Common Vulnerability Scoring System (CVSS) score, attack type, target information, and an impact score. The information to identify and record potential threats exploiting vulnerabilities is made available by vDefend and can be used by organizations to determine validate potential threats.	●
Risk Assessment (ID.RA)	ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	vDefend detects anomalous behavior and security posture gaps through monitoring of IDS/IPS events. ATP provides the CVSS score, severity rating, impact score, target, and additional details on threats from traffic flow analysis that can be used to inform risk response prioritization.	●
Improvement (ID.IM)	ID.IM-01: Improvements are identified from evaluations	NDR and NTA support continuous monitoring of the private cloud network traffic to identify threats, patterns, and anomalies or suspicious behavior. vDefend contributes to continuous improvement to network cybersecurity; however, customers are responsible for ensuring cybersecurity improvements are identified across all CSF Functions.	◕

Table 3: vDefend Applicability to NIST CSF 2.0 – Identify (ID) Function

Protect

The Protect Function of NIST CSF 2.0 focuses on implementing safeguards that reduce the likelihood and impact of cybersecurity events. It encompasses capabilities that secure identities, control access, harden platforms, protect data, and ensure the resilience of technology infrastructure. These activities form the technical foundation that restricts threat opportunities and strengthens an organization's overall security posture. Within this Function, vDefend directly supports many outcomes through identity-focused micro-segmentation, distributed firewall enforcement, advanced threat prevention, and secure traffic handling. By tightly controlling east/west communication, enforcing least-privilege access between workloads, and integrating threat detection into segmentation policies, vDefend enables organizations to reduce attack surfaces and maintain a more consistent security baseline across their virtualized environments.

Category	Subcategory	Implementation	Score
Identity Management, Authentication, and	PR.AA-03: Users, services, and hardware are authenticated	vDefend provides the capability to integrate with directory services and federation through Security Assertion Markup Language (SAML).	◑

Category	Subcategory	Implementation	Score
Access Control (PR.AA)		Customers are responsible for setting up the authentication and authorization services in a manner that meets their security needs.	
Identity Management, Authentication, and Access Control (PR.AA)	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	vDefend can support account management rules in the private cloud with Identity Firewall (IDFW), which allows creating firewall policies and rules based on Active Directory user for access management. The vDefend solution itself enables the use of role-based access controls for managing vDefend, with a combination of Roles and Permissions used to separate and enforce access. Customers are responsible for writing the policy defining the roles and appropriate access, which will then be enforced by vDefend. Customer security administrators must ensure that the thin agent is installed and running in each guest VM to effectively use this capability.	
Platform Security (PR.PS)	PR.PS-01: Configuration management practices are established and applied	vDefend supports secure configurations and hardening through distributed firewalling and malware prevention capabilities (MPS) within cloud infrastructure. vDefend Security Intelligence provides firewall rule suggestions to aid customers in identifying more secure configurations. vDefend provides the capability to publish and revert firewall rules. Customers are responsible for deciding on and applying the appropriate configurations needed to protect their workloads.	
Platform Security (PR.PS)	PR.PS-04: Log records are generated and made available for continuous monitoring	Logging is generated and made available in vDefend, including firewall logs and NSX appliance logs. Required logs are available and can be captured for continuous monitoring when configured by the customer using guidance outlined in the VMware vDefend technical documentation.	
Technology Infrastructure Resilience (PR.IR)	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	vDefend protects networks using Distributed Firewall, Gateway Firewall, NDR, and NTA to block unauthorized traffic and conduct continuous network analysis to detect anomalies and suspicious behavior in the private network. Continuous analysis is performed to understand network traffic patterns and detect threats.	

Table 4: vDefend Applicability to NIST CSF 2.0 – Protect (PR) Function

Detect

The Detect Function of NIST CSF 2.0 ensures that organizations can quickly identify potential cybersecurity events through continuous monitoring, behavioral analytics, anomaly detection, and event correlation. Effective detection enables timely investigation, containment, and response, forming the bridge between protection and incident handling. vDefend provides strong support for this Function by offering real-time visibility into workload traffic flows, integrating behavioral analytics and machine learning to detect anomalies, and incorporating IDS/IPS capabilities to identify known and emerging threats. Its security intelligence and event correlation features help organizations surface suspicious activity earlier, understand lateral movement attempts, and generate actionable signals for incident responders. Although vDefend does not define detection roles or organizational responsibilities, it provides the analytics necessary to strengthen an organization's threat detection capabilities.

Category	Subcategory	Implementation	Score
Continuous Monitoring (DE.CM)	DE.CM-01: Networks and network services are monitored to find potentially adverse events	vDefend provides continuous real-time traffic analytics, visibility into east/west flows, and threat detection.	●
Continuous Monitoring (DE.CM)	DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	Micro-segmentation and behavioral analytics detect lateral movement attempts or unauthorized workload interactions. Customers can also configure IDFW to detect logins using Guest Introspection (GI) or Event Log Scraping (ELS). This provides greater ability to monitor and manage user activity with some caveats. To make this work, customer security administrators must ensure that the thin agent is installed and running in each guest VM and that authenticated users do not have the privilege to remove or stop the agent.	◕
Continuous Monitoring (DE.CM)	DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	vDefend provides logging and monitoring of activity within VCF for adverse events, including vulnerability information, threat impact scores, and metadata to support identification and classification.	●
Adverse Event Analysis (DE.AE)	DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	vDefend records details to facilitate analysis and remediation when a vulnerability or intrusion event is detected. Information captured includes: • Threat classification: Specific malware names or Common Vulnerabilities and Exposures (CVE) IDs. • Intrusion details: Severity ratings (CVE and CVSS scores). • Attack context: Attack target, product affected, time detected,	●

Category	Subcategory	Implementation	Score
		traffic type, source and destination IP addresses, protocol, and the rule/profile associated with the signature. • NTA: Details from IDS events and NTA for vDefend events. • Malicious file analysis: Information about malicious files extracted from network traffic, including hash-based detection, local analysis, and cloud analysis results.	
Adverse Event Analysis (DE.AE)	DE.AE-03: Information is correlated from multiple sources	The NDR correlation engine performs advanced analysis, contextual enrichment, and threat correlation by processing events from various sources, such as malicious file transfers, suspicious flow events, and IDS-based detections. vDefend can also be integrated with SIEM tools to support additional correlation and analysis of security events.	●
Adverse Event Analysis (DE.AE)	DE.AE-04: The estimated impact and scope of adverse events are understood	vDefend provides analysis and supporting information to establish the impact and scope of adverse events to the VCF environment. Leveraging threat intelligence integrated into vDefend and ATP, information is provided to estimate the impact and scope, including: • Threat classification • Intrusion details • Attack context • NTA details from IDS events • NTA for vDefend events • Malicious file analysis	●
Adverse Event Analysis (DE.AE)	DE.AE-06: Information on adverse events is provided to authorized staff and tools	Information on vulnerabilities, threats, anomalies, and suspicious behavior are identified in vDefend, and capabilities exist for utilizing alarms, dashboards, and reporting. Security Intelligence can correlate events and organize related events into a timeline to support further investigation by network security teams. Customers are responsible for establishing the process and configuration of vDefend to ensure authorized staff are notified.	◕
Adverse Event Analysis (DE.AE)	DE.AE-07: Cyber threat intelligence and other	Cyber threat intelligence is integrated into vDefend, and ATP receives threat	●

Category	Subcategory	Implementation	Score
	contextual information are integrated into the analysis	intelligence feeds from vTIS. vTIS is continuously updated with known threats, IDS signatures, URL/IP reputations, and NDR threat metadata. This information is used in traffic flow analysis performed by ATP.	
Adverse Event Analysis (DE.AE)	DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	ATP monitors events and provides information, including the CVSS score, attack type, target information, and an impact score. Network traffic is analyzed by vDefend, and threats are assigned impact scores based on the severity and the confidence in the accuracy of the detection. This contextual analysis provided by vDefend provides criticality and meaningful information related to adverse events detected in the VCF environment. Customers must make the final determination on organization-specific risk scoring and known false positives when declaring an incident.	◕

Table 5: vDefend Applicability to NIST CSF 2.0 – Detect (DE) Function

Respond

The Respond Function of NIST CSF 2.0 focuses on the actions organizations take once a cybersecurity incident is detected, including containment, analysis, mitigation, communication, and coordination activities. These actions reduce the impact of an incident and prevent further compromise. vDefend plays a meaningful role within this Function by enabling rapid technical containment through micro-segmentation, isolating compromised workloads, and blocking malicious traffic patterns. Its threat analytics, segmentation logs, IDS/IPS alerts, and behavioral event data support detailed incident analysis and help responders understand the nature and scope of an intrusion. While vDefend does not execute organizational response processes, define escalation paths, or manage stakeholder communications, its detection and enforcement capabilities equip response teams with the technical insight needed to assess, contain, and remediate incidents more effectively.

Category	Subcategory	Implementation	Score
Incident Management (RS.MA)	RS.MA-02: Incident reports are triaged and validated	NDR collects events and provides events that require further analysis to ATP for correlation and visualization. Correlation of events from IDS/IPS, MPS, and NTA are aligned with Campaigns, which provide a comprehensive view of the threat and are aligned to the MITRE ATT&CK framework. Customers must review the correlated events to triage and validate whether incident response activities should occur.	◕

Category	Subcategory	Implementation	Score
Incident Management (RS.MA)	RS.MA-03: Incidents are categorized and prioritized	NDR categorizes and prioritizes incidents detected based on a severity rating. Customers are responsible for reviewing and confirming the category and priority of incidents based on the analysis provided from NDR, along with applying judgement on how and if the incident impacts their organization.	◕
Incident Analysis (RS.AN)	RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	vDefend provides network flow data, segmentation logs, and analytics. vDefend performs the initial analysis of potential and confirmed suspicious activity and provides an impact score factoring in the threat, likelihood, and impact of a vulnerability being exploited. This provides the data needed to facilitate an analysis. Customers are responsible for validating the information and confirming the root cause of an incident.	◕
Incident Analysis (RS.AN)	RS.AN-08: An incident's magnitude is estimated and validated	vDefend ATP provides an impact score for incidents identified, which is a combined value that includes the severity of the threat (risk score) and strength of the detection being correct (confidence score).	●
Communications (RS.CO)	RS.CO-02: Internal and external stakeholders are notified of incidents	vDefend produces analyses and summarizes risk and impact of confirmed or potential incidents. vDefend has alarm and alerting capabilities. Customers must manage stakeholder communication by assuring processes are developed and vDefend is configured to support notification of incidents to the appropriate internal and external stakeholders.	◑
Incident Mitigation (RS.MI)	RS.MI-01: Incidents are contained	vDefend's micro-segmentation and policy enforcement can block malicious lateral movement and isolate workloads during an incident. vDefend IDS/IPS capabilities can detect and contain unauthorized access.	●

Category	Subcategory	Implementation	Score
Incident Mitigation (RS.MI)	RS.MI-02: Incidents are eradicated	IDS/IPS supports blocking and containing traffic based on signature and behavioral threat detection. Security Intelligence recommendations and segmentation tuning support customers in adjusting policies based on incident patterns. Customers are responsible for tuning the ATP thresholds, limits, and rate filters related to alerting to find the balance between sufficient alerting on potential incidents and being flooded with false positives.	◑

Table 6: vDefend Applicability to NIST CSF 2.0 – Respond (RS) Function

Recover

The Recover Function of NIST CSF 2.0 focuses on restoring systems, services, and operational capability following a cybersecurity incident. This includes disaster recovery planning, restoration activities, recovery communications, and continuous improvement based on lessons learned. These activities require enterprise-level processes, backup and restoration mechanisms, continuity planning, and organizational execution that fall beyond the operational design of vDefend. Although vDefend can support incident response through detection, segmentation, and security event visibility, it does not provide data backup capabilities, system restoration functions, or business continuity tooling necessary to meet the Recover Function's requirements. As such, vDefend cannot directly satisfy any of the technical or procedural expectations defined within the Recover Function and is considered not applicable, aside from indirectly enabling more secure environments in which recovery processes occur.

VMware Live Recovery, a separate service that enables ransomware and disaster recovery for VCF environments, provides options for cyber recovery and site recovery to support customers' recovery needs.

Customer Responsibilities for Use of vDefend

To minimize the impact on compliance initiatives and maintain the security posture of the in-scope environment, customers must address specific responsibilities and considerations when integrating vDefend into their CSF 2.0 program. The following guidance highlights key areas of focus.

Shared Responsibility Model

Customers must recognize that VMware vDefend operates within a shared responsibility framework. While vDefend provides technical capabilities (e.g., firewalls, IDS/IPS, segmentation), customers retain ultimate responsibility for implementing, configuring, and monitoring controls to meet CSF 2.0 requirements.

Configuration and Management

Customers must define and maintain firewall rules, segmentation policies, and access controls to align with their CSF 2.0 scope. This includes isolating sensitive workloads and implementing least privilege principles. Customers must ensure only required services, protocols, and ports are enabled, and insecure ones are restricted or mitigated. Firewall and segmentation configurations must be reviewed to confirm they remain effective.

Logging and Monitoring

Customers are responsible for integrating vDefend-generated logs with a centralized logging solution (e.g., VMware Log Insight, SIEM tools) to meet logging and retention requirements. Customers must ensure that logs

are retained in accordance with organizational and contractual requirements. Access to logs and configuration settings must be limited to personnel with a job-related need, ensuring compliance with logging access controls.

Vulnerability and Risk Management

While vDefend's ATP can detect vulnerabilities, customers must correlate identified risks with CVSS scores and prioritize remediation efforts. vDefend does not manage system patching; customers must ensure all system components are patched according to organizational and regulatory timelines applicable to the customer environment. Customers must perform targeted risk analyses for configurations and identified vulnerabilities to justify their frequency of review and remediation actions.

Incident Response

Customers are responsible for configuring and responding to IDS/IPS alerts provided by vDefend. This includes incorporating these alerts into an incident response plan to address potential security events. Customers must maintain records of incidents, actions taken, and resolution to support ongoing compliance and audits.

Policy and Procedure Alignment

Customers must update security policies, diagrams, and procedures to reflect the integration of vDefend into the environment, ensuring alignment with CSF 2.0 documentation requirements. They must train relevant staff on using and managing vDefend in the context of CSF 2.0 requirements.

Scope Validation

Customers must perform a review of the sensitive workloads and segmentation boundaries post-implementation of vDefend to ensure that its integration does not inadvertently alter scope or introduce new risks. They must ensure segmentation controls that are implemented using vDefend are validated through annual penetration testing.

Conclusion and Coalfire Opinion

vDefend is a network security and threat prevention solution for VCF designed to enhance workload protection, enforce micro-segmentation, and mitigate risks through capabilities such as distributed firewalling, IDS/IPS, behavioral analytics, and secure traffic inspection. Coalfire reviewed vDefend for its applicability in assisting organizations in aligning to NIST CSF 2.0 and provides the following opinion regarding its use within a cybersecurity and risk management program:

Coalfire concludes that vDefend is effective in supporting many of the technical and operational cybersecurity outcomes described in the Identify, Protect, Detect, and Respond Functions of NIST CSF 2.0. vDefend's capabilities for visibility into workload communications, identity-focused micro-segmentation, intrusion detection and prevention, anomaly detection, and east-west traffic control position it as a strong enabling technology for organizations implementing CSF-aligned safeguards and detection mechanisms. These capabilities directly support several CSF outcomes and indirectly strengthen foundational activities such as asset understanding and threat analysis.

This opinion applies broadly to organizations operating modern virtualized environments and is based on vDefend's demonstrated capabilities and the expected shared responsibility model. While vDefend provides technical controls that secure and monitor in-scope workloads, customers remain responsible for governance-level processes, policy creation, risk management activities, recovery planning, and other organizational controls required for full CSF alignment. vDefend should therefore be implemented as a component of a broader cybersecurity architecture, not as a standalone compliance tool.

vDefend must be deployed and operated in alignment with an organization's mission, policies, procedures, and governance, risk, and compliance (GRC) objectives. As with any security technology, effectiveness depends on correct configuration, ongoing policy tuning, and integration with supporting operational processes. This opinion presumes the existence of a mature cybersecurity program, including:

- Selection and adoption of an appropriate risk management framework (e.g., NIST RMF, NIST SP 80053, NIST SP 800171, ISO/IEC 27002, Center for Internet Security [CIS] Controls, or NIST CSF Profiles)
- Development of cybersecurity and risk-management policies and procedures that align with CSF expectations
- Use of VMware and Broadcom best practices for deploying and maintaining vDefend and related platform components
- Implementation of organizational controls for roles, responsibilities, monitoring, incident response, change management, and operational security
- Physical and environmental controls for facilities, equipment, and access management
- Establishment of trained cybersecurity personnel and security operations resources to monitor, analyze, and act upon vDefend analytics
- Dedicated information technology (IT) and cybersecurity staff to support the enterprise security program and maintain workload and infrastructure operations

In Coalfire's opinion, when implemented alongside the above organizational controls, vDefend is a highly effective technology for enabling and strengthening the technical cybersecurity outcomes of NIST CSF 2.0. Organizations that incorporate vDefend into a layered, risk-based security approach will be better positioned to protect workloads, detect threats, contain incidents, and enhance overall cyber resilience in accordance with CSF 2.0 expectations.

Additional Information and Resources

Broadcom Resources

- Secure your Private Cloud with VMware vDefend
  https://www.vmware.com/docs/vmware-secure-private-cloud-with-vmware-vdefend
- VMware vDefend Distributed Firewall
  https://www.vmware.com/products/security/vdefend-distributed-firewall
- VMware vDefend Gateway Firewall
  https://www.vmware.com/products/security/vdefend-gateway-firewall
- VMware vDefend Advanced Threat Prevention
  https://www.vmware.com/products/security/vdefend-advanced-threat-prevention
- VMware vDefend Firewall
  https://www.vmware.com/docs/vmw-vdefend-firewall-1

NIST CSF 2.0 References

- The authoritative source for NIST Cybersecurity Framework (CSF) 2.0 is maintained by NIST and can be accessed here:
  https://www.nist.gov/cyberframework

- The full NIST CSF 2.0 publication, including the Core, Quick Start Guides, Profiles, Tiers, and supporting materials, is available here:

  https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
- NIST SP 800-37 Revision 2, which outlines the RMF process referenced throughout this PAG, can be found here:

  https://csrc.nist.gov/pubs/sp/800/37/r2/final
- NIST SP 800-53, Revision 5, which provides the security and privacy controls aligned with CSF outcomes, is available here:

  https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
- NIST CSF 2.0 Informative References, which includes mappings to NIST SP 800-53, RMF, ISO/IEC 27001/27002, CIS Controls, and other frameworks, can be found here:

  https://www.nist.gov/cyberframework/informative-references

Coalfire Resources

The Coalfire advisory services references and the Solutions Engineering offerings may be found at the following links:

- https://coalfire.com/services/advisory
- https://coalfire.com/services/security

Coalfire corporate information is available at the following link:

- https://www.coalfire.com/about

Appendix A: vDefend Control Mapping (NIST RMF and NIST SP 800-53)

The NIST CSF 2.0 is closely aligned with the NIST RMF and NIST SP 800-53 security and privacy controls. While CSF provides outcome-driven cybersecurity objectives, RMF provides the process for selecting, implementing, and assessing controls, and SP 800-53 provides the specific technical and administrative control requirements.

This section summarizes how the NIST CSF 2.0 Functions, Categories, and Subcategories, previously evaluated for vDefend applicability, map to the corresponding RMF tasks and SP 800-53 control families. While vDefend supports CSF outcomes that relate to these RMF and SP 800-53 controls, it does not independently satisfy the full scope of RMF process tasks or SP 800-53 control requirements.

Govern

The Govern Function of NIST CSF 2.0 addresses organizational-level cybersecurity governance, including strategy, risk management frameworks, roles and responsibilities, policy creation, oversight mechanisms, and regulatory alignment. These outcomes require executive decision making, policy development, organizational accountability structures, and enterprise-level governance processes that extend beyond the capabilities of a technical security product. While vDefend can generate insights such as workload behaviors, segmentation gaps, and security analytics that may inform an organization's governance efforts, it does not create policies, assign governance roles, define strategy, or participate in oversight processes. Because vDefend cannot directly satisfy or implement any Govern Function outcomes, no Govern mapping tables are included in this PAG.

Identify

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
ID.AM-01: Inventories of hardware managed by the organization are maintained	P-10	CM-08, PM-05
ID.AM-02: Inventories of software, services, and systems managed by the organization are maintained	P-10	AC-20, CM-08, PM-05, SA-05, SA-09
ID.AM-03: Representations of the organization's authorized network communication and internal and external network data flows are maintained	P-11, P-13, P-16	AC-04, CA-03, CA-09, PL-02, PL-08, PM-07
ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission	P-3, P-6, P-8, P-10, P-14	RA-03, RA-09, RA-02
ID.AM-07: Inventories of data and corresponding metadata for designated data types are maintained	P-12, P-13	CM-12, CM-13, SI-12
ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded	P-3, P-14, A-3, M-1, M-2	CA-02, CA-07, CA-08, RA-03, RA-05, SA-11(02), SA-15(07), SA-15(08), SI-04, SI-05

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
ID.RA-02: Cyber threat intelligence is received from information sharing forums and sources	P-3, P-14	SI-05, PM-15, PM-16
ID.RA-03: Internal and external threats to the organization are identified and recorded	P-3, P-14, A-3, M-1, M-2	PM-12, PM-16, RA-03, SI-05
ID.RA-04: Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded	P-3, P-14	PM-09, PM-11, RA-02, RA-03, RA-08, RA-09
ID.RA-05: Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization	P-3, P-14, R-2, R-3	PM-16, RA-02, RA-03, RA-07
ID.IM-01: Improvements are identified from evaluations	P-2. P-3, P-7, P-14, A-3, A-4, A-5, A-6, M-2	AC-01, AT-01, AU-01, CA-01, CM-01, CP-01, IA-01, IR-01, MA-01, MP-01, PE-01, PL-01, PM-01, PS-01, PT-01, RA-01, SA-01, SC-01, SI-01, SR-01, CA-02, CA-05, CA-07, CA-08, CP-02, IR-04, IR-08, PL-02, RA-03, RA-05, RA-07, SA-08, SA-11, SA-17(06), SI-02, SI-04, SR-05

Table 7: vDefend Control Mapping from NIST CSF 2.0 – Identify (ID) to NIST RMF and NIST SP 800-53

Protect

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
PR.AA-03: Users, services, and hardware are authenticated	N/A	AC-07, AC-12, IA-02, IA-03, IA-05, IA-07, IA-08, IA-09, IA-10, IA-11
PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	N/A	AC-01, AC-02, AC-03, AC-05, AC-06, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13
PR.PS-01: Configuration management practices are established and applied	N/A	CM-01, CM-02, CM-03, CM-04, CM-05, CM-06, CM-07, CM-08, CM-09, CM-10, CM-11
PR.PS-04: Log records are generated and made available for continuous monitoring	N/A	AU-02, AU-03, AU-06, AU-07, AU-11, AU-12, SA-15(13)
PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	P-2, P-15, P-16, P-17	AC-03, AC-04, SC-04, SC-05, SC-07

Table 8: vDefend Control Mapping from NIST CSF 2.0 – Protect (PR) to NIST RMF and NIST SP 800-53

Detect

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
DE.CM-01: Networks and network services are monitored to find potentially adverse events	N/A	AC-02, AU-12, CA-07, CM-03, SC-05, SC-07, SI-04
DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events	N/A	AC-02, AU-12, AU-13, CA-07, CM-10, CM-11
DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events	N/A	AC-04, AC-09, AU-12, CA-07, CM-03, CM-06, CM-10, CM-11, SC-34, SC-35, SI-04, SI-07
DE.AE-02: Potentially adverse events are analyzed to better understand associated activities	N/A	AU-06, CA-07, IR-04, SI-04
DE.AE-03: Information is correlated from multiple sources	N/A	AU-06, CA-07, PM-16, IR-04, IR-05, IR-08, SI-04
DE.AE-04: The estimated impact and scope of adverse events are understood	N/A	PM-09, PM-11, PM-18, PM-28, PM-30
DE.AE-06: Information on adverse events is provided to authorized staff and tools	N/A	IR-04, PM-15, PM-16, RA-04, RA-10
DE.AE-07: Cyber threat intelligence and other contextual information are integrated into the analysis	N/A	PM-16, RA-03, RA-10
DE.AE-08: Incidents are declared when adverse events meet the defined incident criteria	N/A	IR-04, IR-08

Table 9: vDefend Control Mapping from NIST CSF 2.0 – Detect (DE) to NIST RMF and NIST SP 800-53

Respond

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
RS.MA-02: Incident reports are triaged and validated	N/A	IR-04, IR-05, IR-06
RS.MA-03: Incidents are categorized and prioritized	N/A	IR-04, IR-05, IR-06
RS.AN-03: Analysis is performed to establish what has taken place during an incident and the root cause of the incident	M-3	AU-07, IR-04, SI-02(07)
RS.AN-08: An incident's magnitude is estimated and validated	M-3	IR-04, IR-08, RA-03, RA-07

CSF 2.0 Subcategory	RMF Tasks	SP 800-53 Controls
RS.CO-02: Internal and external stakeholders are notified of incidents	M-3	IR-04, IR-06, IR-07, SR-03, SR-08
RS.MI-01: Incidents are contained	M-3	IR-04
RS.MI-02: Incidents are eradicated	M-3	IR-05, SI-04

Table 10: vDefend Control Mapping from NIST CSF 2.0 – Respond (RS) to NIST RMF and NIST SP 800-53

Recover

The Recover Function of NIST CSF 2.0 focuses on restoring systems, services, and operations following a cybersecurity incident. It encompasses recovery planning, backup and restoration processes, service continuity, communication during recovery, and improvement of resilience practices after an event. These activities are organizational in nature and rely on business continuity planning, disaster recovery procedures, enterprise coordination, and operational execution, which are capabilities that vDefend does not provide. Although vDefend supports incident containment and provides security insights that may aid recovery teams, it does not offer backup, restoration, continuity, or recovery-orchestration capabilities. As such, vDefend cannot directly fulfill any Recover Function outcomes, and this PAG does not include mapping tables for the Recover Function.

Legal Disclaimer

About the Author

Keith Kidd, *Principal, Coalfire Public Sector Advisory*

Keith is a Principal with Coalfire's Public Sector Advisory practice with over 20 years of experience in information technology, security, compliance, and data analysis. He has supported commercial and public sector assessment and advisory engagements throughout his career, acting as an internal auditor, independent assessor, and trusted consulting advisor.

About Coalfire

Coalfire®, headquartered in Chicago, Illinois, is a global leader in cybersecurity services and solutions. The company offers cutting-edge security, advisory, and assessment services, as well as develops technology platforms that automate defenses against security threats for the world's leading enterprises, cloud providers, and SaaS companies. Coalfire is the foremost provider of FedRAMP assessments and penetration testing services in the United States. For more information, visit Coalfire.com.

WP_vDefend_CSF_2026