VMware vDefend

Comprehensive Zero Trust Lateral Security for VCF

vDefend benefits

- **Comprehensive Lateral Security:** Complete protection against lateral threats with a high-performance, scalable, distributed architecture that secures all VCF workloads directly at the hypervisor level, thereby eliminating security blind spots.
- **Accelerated Zero Trust:** A structured, multi-phase segmentation workflow enhances the security posture of east-west traffic in the VCF private cloud, accelerating the journey towards Zero Trust.
- **Actionable Security Intelligence:** A comprehensive view of workload activities, combined with AI-driven security policy recommendations and actionable insights, drastically simplifies security operations and policy enforcement.
- **Dynamic Policy Orchestration:** A dynamic, smart policy orchestration allows pre-creation of policies before workloads are deployed, and ensures workloads maintain policies throughout their lifecycle
- **Multi-Layered Threat Prevention:** A hypervisor-native IDS/IPS, behavior-based Network Traffic Analysis (NTA), and Malware Prevention Services (MPS) provide a multi-layered defense against zero-day, encrypted, and in-memory attacks, significantly enhancing the overall security posture of the private cloud.
- **AI-driven Threat Response:** A multi-context Network Detection and Response(NDR) engine correlates detection signals into unified intrusion campaigns, simplifying SOC analysis and enabling rapid, efficient threat mitigation through GenAI-assisted investigation.

Overview

Traditional private cloud security relies on perimeter defense—a boundary modern attacks easily breach. Once an attacker is inside, they move laterally to locate high-value assets for ransom or to exfiltrate data. As attackers increasingly leverage AI to accelerate autonomous attacks, adopting an 'assumed breach' mindset is essential. This necessitates implementing Zero Trust lateral security within the private cloud, extending protection beyond the perimeter to every workload and restricting lateral propagation of attacks.

VMware vDefend is a comprehensive Zero Trust lateral security solution for all VMware Cloud Foundation (VCF) private cloud workloads (VM, Kubernetes, Agentic AI workloads) and bare metal servers. This hypervisor-native, software-defined solution defends against lateral cyber threats by providing deep visibility into both network and application activity, eliminating security blind spots. It enforces a multi-layered defense and mitigation strategy against ransomware and advanced persistent threats.

VMware vDefend is offered as a single solution that includes a distributed and 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 by reducing tool sprawl associated with legacy point security solutions and offers a closed-loop security system for private cloud environments that ensures visibility, prevention, detection, and mitigation.

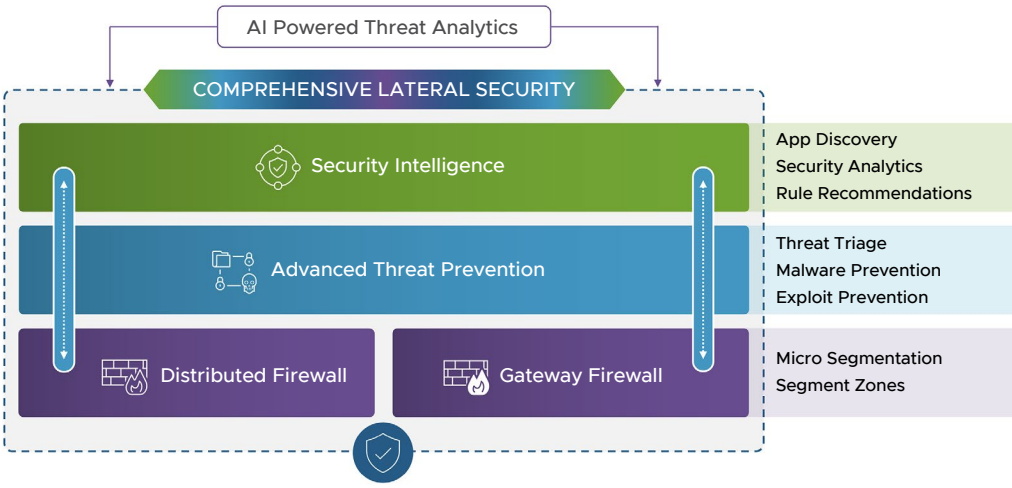

Figure 1: vDefend – Comprehensive security stack

vmware by Broadcom

Key use cases

- **Deep Visibility:** Gain comprehensive insights into all flows, from Layer 4 to Layer 7, across all VCF workloads through a hypervisor-native, software-defined solution that provides deep context on network, user, process, and application activities.
- **Zero Trust Lateral Security:** Implement a prescriptive, multi-stage macro- and microsegmentation solution using a distributed firewall to protect all workloads from lateral threats within the private VCF cloud.
- **Ransomware Prevention:** Protect critical workloads using vDefend's multi-layered defense (MPS, IDS/IPS, and NTA) to prevent advanced fileless and zero-day threats. Detect and stop ransomware activity and lateral spread across the VCF environment.
- **Consistent Policies:** Enforce consistent L7 security policies across all workloads, including VM, Kubernetes, and Baremetal.
- **Virtual Patching:** Proactively protect vulnerable workloads using distributed IDS/IPS, providing security teams time to plan and deploy patches.
- **Compliance:** Simplify audits and bring environments into compliance (PCI, HIPAA, etc.) by deploying a software-defined solution.
- **AI-powered Threat Investigation:** Empower SOC teams to visualize attack chains and conduct rapid triage, with campaigns mapped to MITRE ATT&CK techniques, by leveraging multi-context NDR and a GenAI-powered conversational interface.

Key capabilities

	vDefend Capabilities
Distributed Firewall	• Implements a hypervisor-native, distributed firewall architecture to secure workloads against lateral threats, eliminating traffic hairpinning and performance bottlenecks. • Supports granular Layer 2–7 access control with context-driven, identity- and application-aware policies, including URL filtering. • Enables prescriptive, multi-stage macro and microsegmentation deployment workflow. • Supports "Security as Code" with an API-driven, object-based model that automates deployment, configuration, and operationalization • Enables "Dynamic policy orchestration" to ensure that workloads maintain their policies throughout their lifecycle.
Advanced Threat Prevention • IDS/IPS • MPS • NTA/NDR	• Implements a distributed, hypervisor-native IDS/IPS to inspect east-west and north-south traffic directly within the VCF environment. • Provides comprehensive signature-based threat detection and prevention, including support for custom signatures to swiftly address industry-specific threats and emerging vulnerabilities. • Provides Behavior-based Network Traffic Analysis (NTA) with AI/ML baselining, identifies high-fidelity anomalies across protocols, hosts, and applications. • Implements multi-layered Malware Prevention Service (MPS) with hypervisor-based Guest Introspection to provide deep, agentless visibility into files, processes, and memory. • Enables detection of encrypted and in-memory attacks to stop evasive malware and strengthen overall security posture. • Provides multi-context Network Detection and Response (NDR) by aggregating and correlating signals from IDS/IPS, NTA, and MPS to detect malicious activity. *ATP continues next page*

vDefend features

Micro-segmentation

Macro-segmentation

L2-L7 firewalling

User identity-based access control

Application identity-based access control

L2 and L3 VPNs

Intelligent flow visualization and policy recommendations

DFW 1-2-3-4 automated workflow with recommendations

Firewall rule analysis and optimization

URL filtering

TLS decryption

Intrusion Detection/Prevention Service (IDPS)

Malware Prevention Service

Network Traffic Analysis (NTA)

Network sandbox

Network Detection and Response (NDR)

Gen AI-powered Intelligent Assist

Further reading

For more information on VMware vDefend solutions for private cloud, please visit:

www.vmware.com/products/security/vdefend-distributed-firewall

www.vmware.com/products/security/vdefend-advanced-threat-prevention

Key capabilities, continued

	vDefend Capabilities
Advanced Threat Prevention • IDS/IPS • MPS • NTA/NDR	• Accelerates threat investigation and response with high-fidelity, correlated insights, reducing alert noise and simplifying security operations. • Integrates seamlessly with SIEM platforms to deliver enriched alerts and correlated campaigns. • Extends detection to non-virtualized environments with lightweight NDR sensors delivering out-of-band monitoring and deep visibility without impacting performance. • Enables Gen AI-powered Intelligent Assist for rapid triage and mitigation, allowing efficient investigation and response.
Zone-based Security with Gateway Firewall	• Implements zone-based firewalling to create secure security zones within private cloud environments and enforce granular segmentation policies • Enables secure multi-tenancy with isolated security zones to protect tenants within enterprise and service provider environments • Enables unified security management for both lateral security and zone-based security for all workloads within VCF • Extends microsegmentation to non-virtualized workloads, such as bare metal servers
Security Intelligence	• Provides a comprehensive view of all workload activity by correlating and analyzing multiple layers of context, including Network (IPs, App IDs), Security (DFW/IDS/IPS rules), Business/DC (Tags, Groups), and Application (Users, Processes). • Offers recommendations for security policies by automatically detecting unprotected flows, workloads, and applications. • Acts as the core engine for security operations, converting raw data into actionable insights to enhance security policy monitoring and enforcement.

Item No: vmw-vdefend-ds-042026

vmware® by Broadcom