# VMware vDefend

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.

# VMware vDefend for VCF 9.0

### Course Code: ANS00007

## Course Description

This five day instructor led course has been built from the ground up to show the power and ease of securing the VMware private cloud with VMware firewall solutions. The course focuses on controlling lateral movement within the data center and is built with a simple to follow, prescriptive, step-by-step plan that attendees can use in their own work environments.

You will be exposed to all security focused solutions including **vDefend Firewall**, **vDefend ATP**, and the **Avi Web Application Firewall**. Through lectures, discussions and hands-on-labs, you will leave the course with knowledge to make an education decision around the capabilities of VMware security solutions.

## Delivery Method

Instructor-Led

## Duration

Five Days

## Course Objectives

Upon completion of this course, you will be able to:

- Make educated decision around the capabilities of VMware security solutions

## Hands-On

This course includes practical hands-on exercises that enable you to test your new skills and begin to use those skills in a working environment.

## Prerequisites

- None

Course Outline

**Module 1 Introduction to Private Cloud Security**

**Module 2: Understanding the VMware vDefend Architecture**

**Module 3: Managing the VMware vDefend Distributed Firewall**

**Module 4: Implementing Infrastructure Policies**

**Module 5: Implementing Zone Policies**

**Module 6: Implementing Emergency Policies**

**Module 7: Implementing Application Segmentation**

**Module 8: Deploying the Security Service Platform**

**Module 9: Security Journey**

**Module 10: Planning and Implementing Micro Segmentation with Security Intelligence**

**Module 11: Securing the VCF Management Domain**

**Module 12: Layer 7 Firewall**

**Module 13: Performing Security Assessments**

**Module 14: GFW**

**Module 15: Securing Container Workloads**

**Module 16: Implementing IDS/IPS**

**Module 17: Implementing Malware Detection and Prevention**

**Module 18: Implementing Network Traffic Analysis**

**Module 19: Implementing Network Detection and Response**

**Module 20: Using Intelligent Assist**

**Module 21: Integrating Security Automation and Orchestration**

**Module 22: Troubleshooting Security**

**Module 23: Implementing VMware vDefend for VMware Private AI Foundation**

**Module 24: Bare Metal Agents**