Implement App and Private Cloud Security

VCF Professional Services

At a glance

Strengthen the security posture of your VCF environment against sophisticated, frontier AI-driven threats faster with assistance from services experts.

Key benefits

- Accelerate time-to-protection with validated security controls and virtual patching.
- Reduce security risk by preventing lateral threat movement.
- Minimize operational challenges with technology experts.
- Achieve efficient operational self-sufficiency through knowledge transfers.

Defending private clouds against AI-driven threats requires a multi-layered defense. Perimeter security alone fails against lateral (east-west) attacks that exploit vulnerabilities and move across workloads. Deploying hypervisor-level microsegmentation, web application protection, network detection, and real-time virtual patching is complex. It demands specialized expertise and proven strategies to secure critical assets without slowing business agility. VMware Pro Cloud Services™ fast-tracks your path to app and private cloud security.

Service overview

VCF Professional Services implements a robust security architecture using VMware vDefend™ and VMware Avi™ Load Balancer to protect applications and infrastructure from advanced cyber threats including ransomware. Leveraging field-tested reference architectures and best practices, our team delivers a standardized, predictable, and low-risk implementation.

Implement vDefend Security Services Platform

Services experts design, deploy, and integrate the VMware vDefend Security Services Platform within the VMware Cloud Foundation® (VCF) environment protecting the Management and the Workload Domains. This prescriptive approach delivers Security Intelligence, Network Detection and Response (NDR), Malware Prevention, Network Traffic Analysis (NTA)", and security metrics for your VCF solution. Our team provides key project deliverables, including a tailored solution design, an installation and configuration workbook, and a security segmentation report summarizing your security posture.

Implement VMware Avi Load Balancer

Our experts design, deploy, and configure Avi Load Balancer Web Application Firewall (Avi WAF) solution to protect your mission-critical web applications and APIs against emerging cyber threats. The team implements a unified security stack with multi-layer inspection pipeline, real-time analytics and visibility further enhancing the security posture.

Learn more

Visit vmware.com/services

Implement Virtual Patching

We configure virtual patching capabilities across the VCF stack to shield vulnerable workloads and mitigate exploit traffic in real time. The team implements vDefend Intrusion Detection and Prevention System (IDPS) profiles for continuous inline threat prevention and configures Avi WAF for protecting web applications, APIs, and Container Ingress Services. This integrated approach establishes automated, defense-in-depth, layer-specific protection for critical application workloads prior to permanent patch deployment.

Secure the VCF Management Domain

Services experts establish hypervisor-level security enforcement across the VCF management domain using VMware vDefend™ Distributed Firewall. The team configures tailored rules for infrastructure-level protection and implements micro-perimeters around critical VMware Cloud Foundation® Operations fleet management services. To support ongoing administration, the engagement includes a solution design document detailing the firewall architecture and security rule framework.

Secure Shared Infrastructure Services and Environments

Our experts deliver microsegmentation across core infrastructure and environment boundaries using VMware vDefend™ Distributed Firewall. The team conducts a technical strategy session to establish a standardized security tagging taxonomy and dynamic Security Group criteria. Experts then design and implement DFW policies to protect shared infrastructure services (such as AD, DNS, and DHCP) while enforcing strict isolation between various environments such as production, QA, and development. Architecture models, tagging standards, and policy rules are captured in a solution design document.

Secure Applications

Services experts configure vDefend microsegmentation policies to enforce zero-trust security controls at the individual application level. By implementing granular, workload-to-workload firewall rules, the team isolates application tiers and restricts East-West traffic. This targeted policy configuration prevents lateral threat movement and minimizes the attack surface across your application portfolio.

Benefits

Partnering with VCF Professional Services accelerates your time-to-value while de-risking complex cloud security deployments. Our experts bring proven methodologies, field-tested reference architectures, and deep domain expertise directly to your team. By combining hands-on implementation with tailored knowledge transfer, we build an active zero-trust defense across your private cloud and applications—giving your organization the speed, confidence, and operational self-sufficiency needed to stay ahead of evolving threats.

vmware® by Broadcom