Professional Services for Security Posture Assessment

At a glance

Reduce cybersecurity risk by evaluating the technical security configurations of your VMware infrastructure for VMware and industry security best practices.

Key benefits

• Gain valuable insights into how security controls are implemented in your datacenter

• Reduce the risk of exposure to increasingly frequent and dangerous cyberthreats

• Prioritized roadmap and actionable recommendations to remediate gaps and achieve target state

Business Challenge

In today's ever-changing environment, it can be challenging to know if your organization is fully leveraging your VMware architecture suite with cybersecurity best practices that protect your investments. Improving and evolving VMware configurations for the most effective vigilance and resilience against cyberthreats will help your operations maintain continuity and reduce risk footprint.

Understanding your current security posture and risk profile will help you set up security best practices that reduce your risk while maintaining required industry standards and meeting compliance regulations.

Service Overview

VMware's Professional Services security experts will perform a detailed technical security posture assessment of your VMware infrastructure by comparing your current product configuration(s) to VMware and industry security best practices. The service utilizes a combination of workshops and technical configuration reviews to analyze the current state environment to desired target state. The service delivers a detailed findings report outlining assessment findings, actionable recommendations to achieve the target state and a roadmap to help prioritize remediation activities. With the VMware Security Posture Assessment service, our team will help you:

- Identify configuration gaps to VMware and industry best practices

- Develop a clear roadmap with recommendations for advanced security controls

- Leverage proven VMware security expertise and guidance

- Protect your brand reputation and enhance your credibility with your stakeholders and within your industry

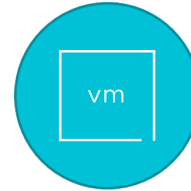**vm**ware®

In-Scope Products

This service can be used to evaluate the technical configurations for the following VMware products:

vCenter Server   ESXi Hosts   Virtual Machines

Additional products are continuously being added to this service. For assessment of VMware products not included on the list, please contact your VMware representative for more details.
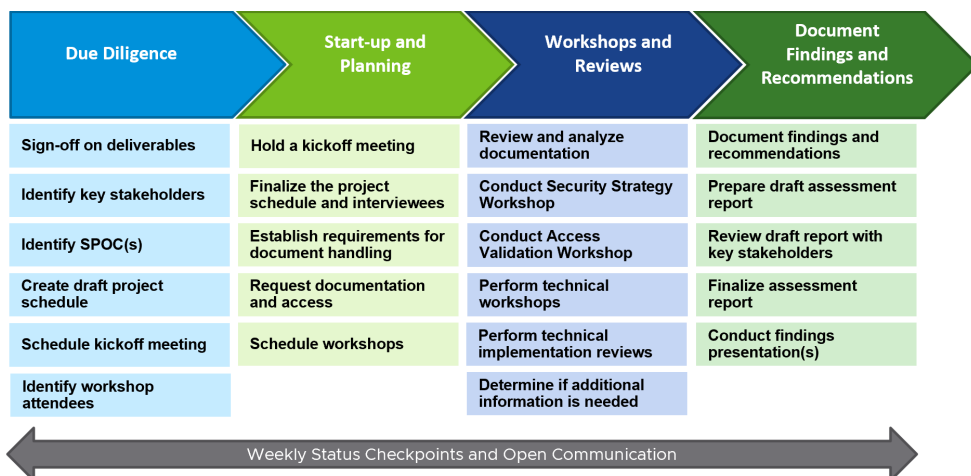
Service Engagement At-a-Glance

The service is delivered leveraging a four phased approach. During the Due Diligence phase VMware security consultants and Project Manager will work with the Customer to identify a Single Point of Contact (SPOC) to ensure efficient communication between the Customer and VMware during the engagement. During this phase VMware will work with the Customer SPOC to identify key stakeholders and schedule the kickoff meeting.

In phase 2, Start-up and Planning, VMware will hold the project kickoff meeting, finalize the project schedule, document handling and access requirements, as well as identify Customer interviewees, contacts, and schedule technical workshops.

The Workshops and Reviews phase begins with the security consultant conducting the Security Strategy Workshop which is designed to review and align the Customer's security goals and objectives with the assessment. Next the security consultant will conduct an Access Validation Workshop to ensure the consultant has all required access and permissions to perform technical reviews. Once these workshops are completed the security consultant will work with Customers subject matter experts to review the current state environment. This is done via a series of technical workshops and technical implementation reviews leveraging scripts and manual configuration reviews.

During the final phase, Document Findings and Recommendations, the security consultant will perform the gap analysis of the current state environment to the target state. A draft findings report will be provided to key Customer stakeholders for review and input. Once Customer feedback is received, the security consultant will conduct a findings presentation for Customer key stakeholders. The findings presentation will provide an overview of the engagement, technical findings, and prioritized recommendations/next steps.

Due Diligence	Start-up and Planning	Workshops and Reviews	Document Findings and Recommendations
Sign-off on deliverables	Hold a kickoff meeting	Review and analyze documentation	Document findings and recommendations
Identify key stakeholders	Finalize the project schedule and interviewees	Conduct Security Strategy Workshop	Prepare draft assessment report
Identify SPOC(s)	Establish requirements for document handling	Conduct Access Validation Workshop	Review draft report with key stakeholders
Create draft project schedule	Request documentation and access	Perform technical workshops	Finalize assessment report
Schedule kickoff meeting	Schedule workshops	Perform technical implementation reviews	Conduct findings presentation(s)
Identify workshop attendees		Determine if additional information is needed	

Weekly Status Checkpoints and Open Communication

Deliverables

At the conclusion of the security assessment, the Customer will be provided with the following deliverables:

- Detailed Findings Report: Highlights all findings and recommendations for in-scope products and evaluation criteria and is aligned to technical best practices

- Scan Result Workbook: Supplemental Excel Workbook documents all product findings and aids in remediation of settings identified in the Detailed Findings Report

- Findings Presentation: Consolidated presentation of prioritized recommendations that provides the customer with an executive-level overview of current state in relation to target state and highlights key gaps and recommendations as well as provides a prioritized roadmap to achieve target state

Benefits

VMware consultants' knowledge and expertise will help you make the most of your VMware architecture with cybersecurity best practices. When we help you with a VMware Security Posture Assessment, you will achieve:

- Gain insights into the current security configurations of your VMware infrastructure

- An understanding of any possible gaps in your cybersecurity and how to remedy those gaps

vmware®

Learn more

Visit vmware.com/services.

- A prioritized roadmap and actionable recommendations to remediate gaps and achieve a target state

- Alignment of VMware security configurations to your security strategy, industry, and VMware security best practices