Professional Services for Workspace ONE Security Assessment

At a glance

Reduce cybersecurity risk by evaluating the technical security configurations of your VMware Workspace ONE infrastructure while also gaining insights into governance and operational processes around the Workspace ONE platform.

Key benefits

- Identify security gaps in current Workspace ONE environment and managed device configurations.
- Prioritized recommendations across technical, operational, and organizational categories to remediate gaps and achieve target state.
- Assistance in preparing for regulatory compliance audits.
- Additional security value to complement Workspace ONE Health Check.

Availability

Please contact your VMware Client Solutions Executive for more information about this Statement of Work (SOW) service.

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 analysis of your Workspace ONE platform architecture and device security configurations. The service utilizes a series of collaborative workshops to identifying gaps in SaaS and On-Prem deployments while also evaluating the security posture of iOS, Android, Windows and macOS device types leveraging NIST and CIS security frameworks and benchmarks. In addition, the service will evaluate your governance, process and operational capabilities providing a holistic analysis of your Workspace One platform.

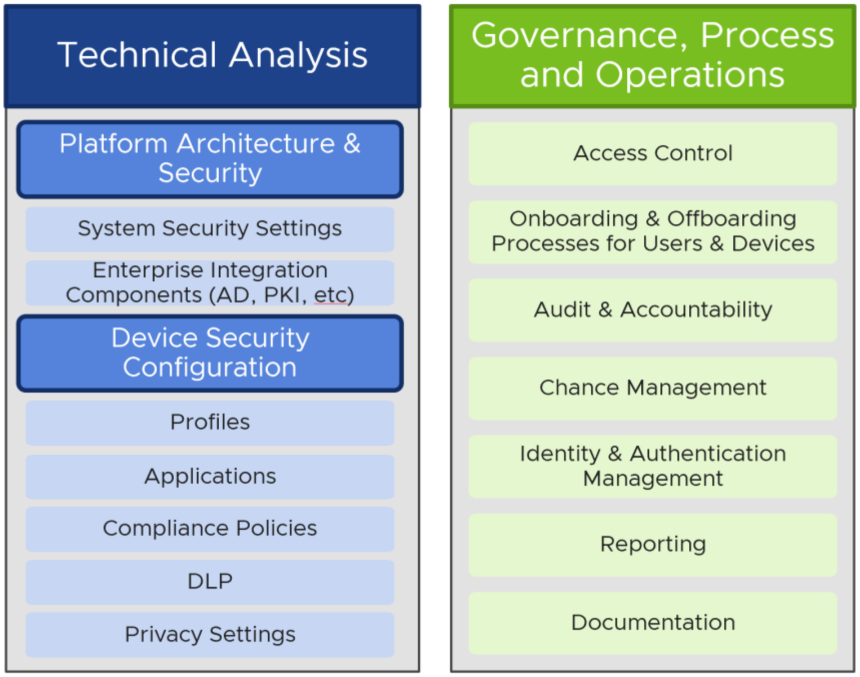
The service delivers a detailed findings report outlining assessment findings, actionable prioritized recommendations to achieve the target state, an assessment workbook and findings presentation highlighting key findings and recommendations for key stakeholders. With the VMware Security Posture Assessment service, our team will help you:

- Identify security configuration gaps in Workspace ONE architecture
- Improve operational processes supporting the Workspace ONE environment

- Improve Workspace ONE environment security posture with prioritized recommendations
- Leverage proven VMware security expertise and guidance

Methodology

This service provides recommendations categorized as Technical, Operational and Organizational. The service reviews around 230 technical configurations (depending on environment and use cases) as well as governance, process and operations capabilities providing holistic insight into the technical and operational capabilities of your Workspace ONE environment.



Technical Analysis

Platform Architecture & Security

System Security Settings

Enterprise Integration Components (AD, PKI, etc)

Device Security Configuration

Profiles

Applications

Compliance Policies

DLP

Privacy Settings

Governance, Process and Operations

Access Control

Onboarding & Offboarding Processes for Users & Devices

Audit & Accountability

Chance Management

Identity & Authentication Management

Reporting

Documentation

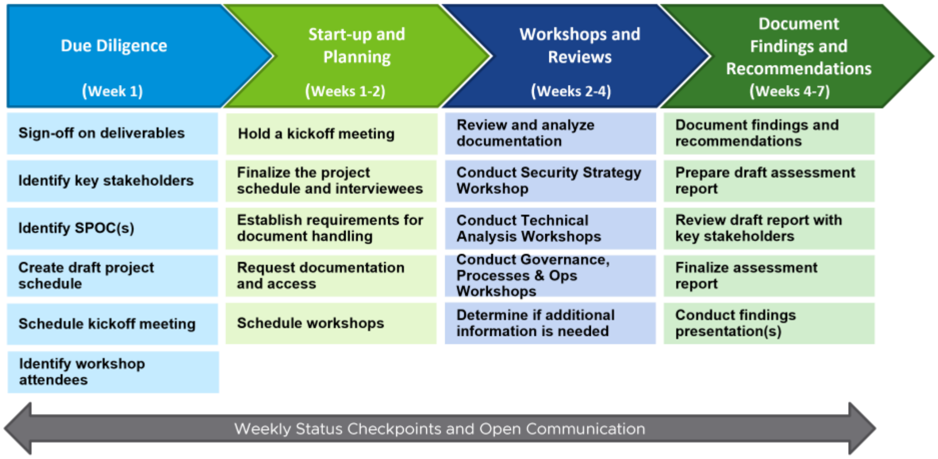
Service Engagement At-a-Glance

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, objectives and specific use cases with the assessment. Next the security consultant will work with Customers subject matter experts to review the current state environment. This is done via a series of workshops to review technical configurations and review governance, policy, and operational capabilities.

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 (Week 1)	Start-up and Planning (Weeks 1-2)	Workshops and Reviews (Weeks 2-4)	Document Findings and Recommendations (Weeks 4-7)
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 Technical Analysis Workshops	Review draft report with key stakeholders
Create draft project schedule	Request documentation and access	Conduct Governance, Processes & Ops Workshops	Finalize assessment report
Schedule kickoff meeting	Schedule workshops	Determine if additional information is needed	Conduct findings presentation(s)
Identify workshop attendees			

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

- Detailed report highlighting all findings and recommendations for in-scope products and evaluation criteria
- Findings and recommendations are aligned to the following categories:
  - Technical
  - Operational
  - Organizational

Supplemental Workbook

- Supplemental Excel Workbook documenting reviewed security controls mapped against CIS Benchmarks. This workbook supports the Findings report.

Findings Presentation

- Consolidated presentation of prioritized recommendations
- Provide the customer with an executive level overview of current state in relation to target state. The presentation will highlight key gaps and recommendations
- Provide prioritized roadmap to achieve target state

Learn more

Visit vmware.com/services.

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 Workspace ONE Security Assessment, you will achieve:

- Gain insights into the current security configurations of your VMware Workspace ONE infrastructure
- An understanding of any possible gaps in your Workspace ONE architecture and device security configurations and how to remedy those gaps
- A prioritized findings 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