Overview

Security Assessment Services

Understand your security posture

Get a clear view of your risk profile to maximize your technology’s value

A security assessment can help organizations gain knowledge about their security posture and possible vulnerabilities in their technology ecosystem. It can also help organizations better understand security gaps to maximize technology investments with customized recommendations and best practices.

VMware security assessments follow industry-leading frameworks to help organizations of any size reduce risk while maintaining industry standards and meeting compliance regulations.

Assessments available to fit your environment

- Professional Services for Security Posture Assessment
- Professional Services for VMware Zero Trust Readiness Assessment
- Professional Services for VMware Cloud Foundation Compliance Readiness Assessment
- Professional Services for Cybersecurity Maturity Model Certification (CMMC) Readiness Assessment

Thinking About a Security Assessment?

VMware has the right fit for you!

Discover Your Goals
Our assessments were designed with you in mind – starting with your goals to help you achieve them.

Customizable for your industry
- Healthcare
- Government
- Finance
- And many others
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

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 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

In-Scope Products
This service can be used to evaluate the technical configurations for the following VMware products:

- vCenter Server
- ESXi Hosts
- Virtual Machines

*Note: 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.
Deliverables

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

<table>
<thead>
<tr>
<th>Detailed Findings Report</th>
<th>Scan Result Workbook</th>
<th>Findings Presentation</th>
</tr>
</thead>
</table>
| • Detailed report highlighting all findings and recommendations for in-scope products and evaluation criteria  
  • Aligned to technical best practices | • Supplemental Excel Workbook documenting all product findings individually. Aids in remediation of settings identified in the Findings Report | • 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 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
- 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
Professional Services for VMware Zero Trust for Readiness Assessment

Transform and protect your environment across every control point.

**Business challenge**

Today’s world requires a new approach to verify trust and grant user access to the hundreds – even thousands – of applications in your organization. However, traditional security models are proving inefficient in defending against burgeoning, sophisticated attacks. As a result, the pressure is on for firms to embrace and prioritize solutions to combat the changing cybersecurity landscape.

Security leaders are looking at emerging Zero Trust models to control access to applications, reduce surface attacks and establish continuous verification. However, before launching Zero Trust Architecture, an organization must assess its current state and understand what’s required to realize desired outcomes.

VMware has a portfolio to help our customers begin their Zero Trust journey and build a framework for success.

**Service overview**

VMware’s Zero Trust Readiness Assessment helps you build a threat detection, prevention, and response system to protect access identity, endpoints workloads, networks and cloud infrastructures using Zero Trust Architecture.

As part of the assessment, a VMware consultant evaluates your existing operation, processes and VMware technologies and delivers a prioritized presentation of recommendations to ensure successful Zero Trust implementation.

We perform the readiness assessment across hundreds of capabilities around the five pillars of Zero Trust to create an integrated picture of current state security competencies and capabilities.

**Assessment Evaluation Areas**

Evaluate four control points and associated five trust pillars against the NIST 800-53v4 standard.
Service Engagement at-a-Glance

The engagement includes a readiness assessment that identifies gaps and requirements to support, integrate and manage your Zero Trust environment.

Service Deliverables

The assessment includes an executive presentation of the engagement overview, workshop findings and prioritized guidance presented with the following deliverables:

- Readiness for Zero Trust Architecture Recommendations Presentation: A consolidated presentation of prioritized recommendations with an overview of the current state, existing gaps and next steps.

Benefits

Begin your Zero Trust journey with knowledge and expertise.

Experienced VMware consultants deliver an outcome-focused assessment into any perceived, potential and existing gaps in your current environment and our best practice guidance you need before implementing Zero Trust Architecture.

Build a future-proof framework while supporting business continuity and operations.

Security transformation involves evaluating, modifying and improving a complex matrix of operational capabilities, policy standards and architectural design and deployment. VMware’s methodology helps you evolve to achieve everything you expect from Zero Trust:

- Enhanced visibility into apps on-prem and on multiple clouds
- Securely support remote workforce using Zero Trust principles
- Reduced security risks and exposure to data breaches in critical Zero Trust areas:
  1. Devices
  2. Users
  3. Transport Sessions
  4. Applications
  5. Data

LEARN MORE
Visit vmware.com/services.
Professional Services for VMware Cloud Foundation Compliance Readiness Assessment

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 assessment of your VMware Cloud Foundation (VCF) infrastructure to VMware and industry security best practices. The service evaluates over 200 individual VCF configurations across five (5) VMware products: ESXi, vCenter Server, NSX-T Data Center, vSAN and SDDC Manager. 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 VCF Compliance Assessment service, our team will help you:

- Assist in meeting industry and regulatory security requirements by mapping each individual configuration to the following security industry and regulatory frameworks:
  - NIST 800-53
  - PCI DSS
  - ISO 27001:2013

At a glance
Reduce cybersecurity risk and ensure your environment is in alignment with regulatory compliance standards by evaluating the technical security configurations of your VMware Cloud Foundation infrastructure for VMware and industry security best practices.

Key benefits
- Gain valuable insights into how security controls are implemented in your VCF components
- Reduce the risk of exposure to increasingly frequent and dangerous cyberthreats
- Prioritized roadmap and actionable recommendations to remediate gaps and achieve target state
- Ensure VCF components are in alignment with compliance requirements

Availability
Please contact your VMware Client Solutions Executive for more information about this Statement of Work (SOW) service.
Professional Services for Security Posture Assessment

- NIST 800-171/Cybersecurity Maturity Model Certification (CMMC).
- 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

In-Scope Products

This service can be used to evaluate the technical configurations for the following VCF Components:

- vCenter Server
- ESXi Hosts
- NSX
- vSAN
- SDDC Manager

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 Compliance Strategy Workshop which is designed to review and align the Customer’s compliance 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**

<table>
<thead>
<tr>
<th>Action</th>
<th>Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-off on deliverables</td>
<td>Start-up and Planning</td>
</tr>
<tr>
<td>Identify key stakeholders</td>
<td>Workshops and Reviews</td>
</tr>
<tr>
<td>Identify SPOC(s)</td>
<td>Document Findings and</td>
</tr>
<tr>
<td>Create draft project schedule</td>
<td></td>
</tr>
<tr>
<td>Schedule kickoff meeting</td>
<td></td>
</tr>
<tr>
<td>Identify workshop attendees</td>
<td></td>
</tr>
</tbody>
</table>

**Workshops and Reviews**

<table>
<thead>
<tr>
<th>Action</th>
<th>Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hold a kickoff meeting</td>
<td>Start-up and Planning</td>
</tr>
<tr>
<td>Finalize the project schedule and interviewee</td>
<td>Workshops and Reviews</td>
</tr>
<tr>
<td>Establish requirements for document handling</td>
<td>Document Findings and</td>
</tr>
<tr>
<td>Request documentation and access</td>
<td></td>
</tr>
<tr>
<td>Schedule workshops</td>
<td></td>
</tr>
<tr>
<td>Determine if additional information is needed</td>
<td></td>
</tr>
</tbody>
</table>

**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
- Aligned to technical best practices

**Scan Result Workbook**

- Supplemental Excel Workbook documenting all product findings individually. Aids in remediation of settings identified in 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](http://vmware.com/services).

**Benefits**
VMware consultants’ knowledge and expertise will help you make the most of your VCF architecture with cybersecurity best practices. When we help you with a VMware Cloud Foundation Compliance Assessment, you will achieve:

- Gain insights into the current security configurations of your VCF infrastructure
- An understanding of any possible gaps in your VCF components and how to remedy those gaps
- A prioritized roadmap and actionable recommendations to remediate gaps and achieve a target state
- Alignment of VCF security configurations to regulatory and industry frameworks

Learn more Visit [vmware.com/services](http://vmware.com/services).
Professional Services for Cybersecurity Maturity Model Certification (CMMC) Readiness Assessment

Business Challenge
Many organizations provide services and products that the Department of Defense (DoD) needs and wants. However, becoming a supplier for the DoD requires Cybersecurity Maturity Model Certification (CMMC) compliance. Identifying cybersecurity gaps to meet requirements will help your organization more efficiently remediate any risks and improve time to market.

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
When you work with VMware’s Professional Services for Cybersecurity Maturity Model Certification Assessment, our team will help you:

• Deeply analyze your current security protection level
• Demonstrate compliance with DoD standards and regulatory rules
• Comply with government security acts and industry-specific regulations
• Protect your brand reputation and enhance your credibility with your stakeholders and within your industry

At a glance
Gain the knowledge to confidently meet and execute the required CMMC framework for all Department of Defense (DoD) suppliers.

Key benefits
• Comply with CMMC regulations to work with the DoD
• Develop a security policy to keep pace with the onslaught of digital threats
• Comply with government security and industry-specific regulations

NOTE: VMware does not certify organizations nor are organizations allowed to certify themselves. Certification is achieved through a third party.
Assessment Evaluation Areas

We will evaluate the four control points and associated five trust pillars against the NIST 800-53 standard.

Service Engagement At-a-Glance

The engagement includes an assessment that identifies gaps and requirements to support, integrate, and manage your environment.

Deliverables

You will receive a detailed assessment report that describes existing gaps and misalignments, VMware best-practice counsel, and high-level scoring for individually assessed sections. You will also receive a consolidated presentation of prioritized recommendations with an overview of the current state, existing gaps, and next steps.
Learn more
Visit [vmware.com/services](http://vmware.com/services).

**Benefits**

VMware consultants’ knowledge and expertise will help you meet the requirements of CMMC to be able to do business with the DoD. When we help you with a CMMC Assessment, you will gain:

- The tools to become compliant with CMMC regulations in order to do business with the DoD
- The necessary skills and knowledge to implement a security policy that keeps pace with the onslaught of digital threats
- The ability to comply with government acts and industry-specific regulations
- The knowledge to achieve all required standards and regulatory compliance milestones pertinent in your industry