Professional Services for VMware vSphere® Security Hardening

Reduce risk for your environment

At a glance

Reduce the risk footprint of your critical VMware infrastructure by ensuring that your VMware vSphere® environment is configured in a secure manner.

Key benefits

- Ensure VMware vSphere is configured in a secure and hardened manner
- Reduce the risk profile of your VMware vSphere environment
- Prepare for and ensure alignment to regulatory compliance requirements

Availability

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

In the rapidly evolving landscape of today's technology, it can be difficult to determine whether your organization is utilizing your VMware architecture suite to its fullest potential while implementing cybersecurity measures that safeguard your investments against cyber threats.

Cyber threats and ransomware attacks can present significant business challenges for organizations including downtime, data loss, reputational damage, financial loss, and compliance challenges.

Security hardening plays a critical role in protecting against cyber threats and ransomware attacks and involves implementing security measures to reduce the attack surface and make it more difficult for attackers to gain unauthorized access to the system. Strengthening and developing your VMware configurations to optimize your ability to detect and respond to cyber threats can help your organization maintain uninterrupted operations and minimize your exposure to security risks.

Service overview

VMware's Professional Services security experts will reduce the risk profile of your VMware vSphere environment by ensuring that it is hardened based on industry and VMware best practices. This service leverages a series of security design workshops to understand your specific security requirements and discuss recommended security configurations and environment design considerations.

Service scope

This service evaluates and implements hardened configuration for three VMware vSphere components: VMware vCenter®, ESXi hosts, and virtual machine management.

Design Components

To get to a hardened state, VMWare Professional Services will review 156 design decisions across four focus areas through a series of integrated design workshops:

- System design: 14 security considerations
- VMware vCenter server: 55 configurations
- ESXi hosts: 61 configurations
- Virtual maching management: 26 configurations

Note: System design security considerations will not be implemented as part of this service. VMware Professional Services will only provide recommendations for system design considerations for the environment.

Execution

This service leverages a four-step process to harden your VMware vSphere environment.

1. **Determine Framework Alignment**
    - All hardening configurations are mapped to the following frameworks:
        a. NIST 800-53
        b. PCI DSS 3.2.1
        c. ISO 27001:2013
        d. NIST 800-171 / Cybersecurity Maturity Model Certification (CMMC)
    - VMware Professional Services will review the frameworks with you and determine the framework that you want to serve as the foundation for your alignment. The framework is typically aligned to internal security practices and regulatory/industry requirements.
2. **Review Configurations Recommendations and Make Design Decisions**
    - Each security configuration for each of the four design components outline above will be reviewed during a series of design workshops. The output of the design workshops is the future state hardened configuration of the environment.

Learn more

Visit vmware.com/services.

3. **Implement Configurations**
    - Based on the design workshops, the future state configurations are implemented into the environment leveraging a phased rollout approach. This is done to reduce the potential for error and environment downtime.
4. **Perform POST Implementation Verification**
    - After the configurations have been implemented, VMware Professional Services will perform post operability checks on the environment to ensure it is in a functioning state and verify that the new hardened current state configurations match the design.

Benefits

VMware Professional Services has the experience, best practices, and proven methodologies to ensure that your VMware vSphere environment is resilient and secure. Our broad expertise and deep knowledge of VMware technology can help reduce risk and complexity. Our holistic approach helps you minimize business disruption and realize predictable outcomes that maximize productivity during periods of technology change. Our services can enable you to:

- Gain insights into strategies and best practices to protect your VMware vSphere environment from threats.
- Improve the security posture of your VMware vSphere environment.
- Prepare your environment to meet compliance and regulatory requirements.
- Improve the performance of your VMware vSphere environment by reducing the risk of system downtime and data loss.