Professional Services for VMware Zero Trust for Readiness Assessment

Transform and protect your environment across every control point.

AT A GLANCE

Assesses your people, processes and VMware technologies based on NIST standards to improve your Zero Trust Architecture.

KEY BENEFITS

- Identify security gaps in your current environment
- Implement recommended changes without disrupting daily business operations
- Transform your environment to meet industry standards and security practices
- Gain access control to all applications and protect sensitive data
- Build trust one control point at a time
- Reduce attack surface
- Create a security system for the Apps everywhere world
- Build a future-proof framework prepared for new workstyles and devices

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 firms to embrace and prioritize solutions to combat the changing cybersecurity landscape.

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

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

Service overview

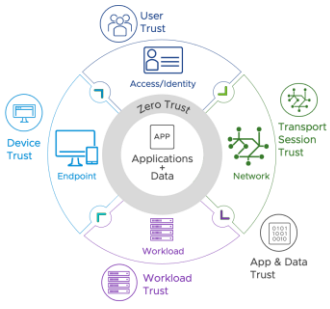
VMware's Zero Trust Readiness Assessment helps you build a threat detection, prevention, and response system to protect access/identity, endpoints, workloads, and networks using a Zero Trust Architecture.

As part of the assessment, a VMware expert evaluates your existing operation, processes, and VMware technologies; delivering prioritized recommendations to ensure a 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 the current security state, competencies and capabilities.

Assessment Evaluation Areas

We will evaluate the four control points and associated five trust pillars against the NIST 800-53v4 standard.



Strategy, Risk, and Compliance
Evaluate the security strategy around technical controls/process

Security Architecture and Deployment
Evaluate the design, configuration and implementation of technical controls and/or processes of VMware products

Policy Governance
Evaluate the maturity if the policies, standards and procedures around technical control and/or processes

Security Operations
Evaluate the operational (people/process) capabilities around technical control/processes

LEARN MORE

Visit *vmware.com/services*.

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 Assessment Report: A detailed assessment report that describes existing gaps and misalignments, VMware best-practice counsel and high-level scoring for individually assessed sections.
- 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 experts deliver an outcome-focused assessment into any perceived, potential, and existing gaps in your current environment and provide insight into best practices for implementing and operating a 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 move toward a Zero Trust Architecture.

- 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

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com