

Professional Services for VMware Zero Trust Readiness Assessment

Protect your environment across every control point

At a glance

This service assesses your people, processes, and VMware technology 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

Today's world requires a new approach to verify trust and grant user access to the hundreds – even thousands – of applications in your organization. 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. 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

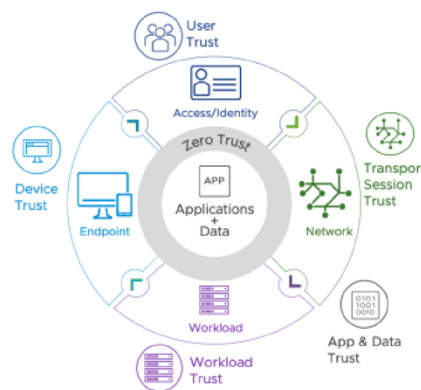
VMware's Zero Trust Readiness Assessment helps you build a threat detection, prevention, and response system to protect access/identity, endpoints, workloads, and networks using a Zero Trust Architecture.

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.

Assess 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

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.



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-practices 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.
-

Learn more

Visit vmware.com/services.

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-premises 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: devices, users, transport sessions, applications, and data