Enabling Zero Trust Security with VMware Workspace ONE

vmware®

Table of Contents

Executive Summary

You are probably thinking and talking about the topic of Zero Trust. Zero Trust is a modern security framework based on the concept of continuous verification of trust prior to allowing least-privilege access to enterprise applications and data.

As organizations seek a seamless user experience for the digital workspace, they must also pay special attention to securing the digital workspace. The security environment for the digital workspace no longer has perimeters; the main drivers for this world without perimeters are

- **Endpoint choice** – Mobile, desktop, bring your own (BYOD), organization-owned
- **Flexible workstyles** – Access to the organization's data from within and outside the internal network
- **Applications everywhere** – SaaS, web, native, and virtual

These drivers have contributed to exponentially increasing security vulnerabilities and expanding the attack surface. Zero Trust addresses these drivers by ensuring continuous verification of endpoint compliance, by allowing only conditional access to all applications, and by reducing the attack surface wherever possible.

Implementing a full Zero Trust model for the digital workspace includes continuously verifying trust and limiting access end to end—from the endpoint to applications in the data center or cloud. VMware lays out a journey to Zero Trust that consists of five pillars:

- Endpoint management and compliance
- Conditional access
- Application tunnel and proxy
- Risk analytics
- Automated remediation and orchestration

Not all five pillars of Zero Trust apply to every organization, but it is important for organizations to be true to the principles of Zero Trust as they define their own journey.

VMware Workspace ONE® has integrated all of the components required to enable the full journey to Zero Trust for the digital workspace. The five pillars of Zero Trust are intrinsic to the Workspace ONE platform. This includes the advanced features of risk analytics, automated remediation, and orchestration. In addition, Workspace ONE is extensible: You can integrate other security solutions from VMware Workspace ONE® Trust Network partners. With Workspace ONE, organizations have a platform that evolves with their needs and supports their long-term IT and Infosec strategies.

Introduction

If you are in information security (InfoSec) or IT, the topic of Zero Trust is probably one you are thinking and talking about frequently. No matter where you are in your journey to secure your users, applications, and endpoints, you can rely on VMware to satisfy the requirements of a Zero Trust architecture for the digital workspace.

The *Workspace ONE platform* has all of the components required to enable Zero Trust for the digital workspace. And Workspace ONE integrates well with other security solutions.

In this white paper, we explore what Zero Trust is and why Zero Trust is an important element of the modern digital workspace. Then we discuss how Workspace ONE enables Zero Trust for the digital workspace.

What Is Zero Trust?

Zero Trust is not a single product, but a modern security framework based on the notion of *never trust, always verify*. Zero Trust is a conditional access control model that requires *verification of trust* prior to allowing application access, and when that access is granted, it is with *least privilege*. The *principle of least privilege* means granting only the required access to applications for the user to complete their job, and no more. By never trusting, and always verifying, Zero Trust protects your data and applications not only at the start of a session, but also with continuous verification of users and endpoints throughout an application session.

What are the requirements of a Zero Trust architecture?

- **Continuous verification of endpoint compliance** – For access to be granted, endpoints must be continuously verified to be compliant with your organization's security policies.
- **Conditional access control to all applications** – For a user to gain access to applications, they must prove their identity.
- **Reduction of the attack surface** – To protect your organization's applications and data, each user must be granted only the least-privilege access to get their work done, and nothing more.

Traditional approaches to security compared to Zero Trust

Traditional approaches to security use a "castle and moat" model, with a castle representing the defined perimeter that needs protection, and the moat representing a barrier with limited points of access to the castle. This model typically uses firewalls, intrusion detection, and network access controls as the moat protecting the castle, and VPNs and firewall pinholes as the drawbridge that allows very limited access to the castle. However, this model is not sufficient anymore. Traditional approaches implicitly trust anyone inside the network, but then someone who is able to get inside the network and appear as an insider, by way of phishing, malware, or person-in-the-middle attacks, can have full access to the organization's data and applications.

In contrast, Zero Trust validates the posture of the endpoint, the identity of the user, and the security of the connection to the application prior to allowing access. These attributes are continually re-validated to ensure that the access is still acceptable. This is *never trust, always verify* in action.

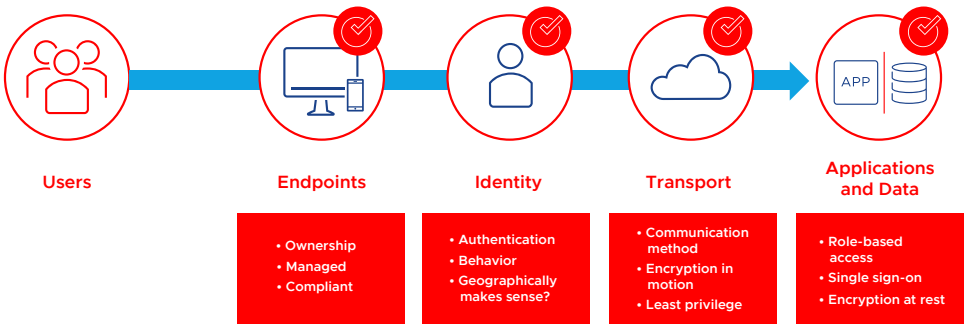

Figure 1. Zero Trust Checkpoints for User Access to Applications and Data in a Digital Workspace

In Figure 1, with Zero Trust architecture, users access applications and data from a digital workspace as follows:

- **Users** – A user requests access to applications and data.
- **Endpoints** – A unified endpoint management system looks at the endpoint (desktop, mobile, or IoT) and determines if that endpoint is compliant. Also, the ownership and management scope of the endpoint must be considered. If the endpoint is trusted, then user identity is checked.
- **Identity** – Each user must pass a required level of authentication, sometimes with multi-factor methods, to verify their identity and role. Also, the context of the user must make sense relative to their normal behavior.
- **Transport (network)** – The communication method must be valid, and encryption must be in place. To reduce the attack surface further, each application can have a single secure tunnel into the data center.
- **Applications and data** – Access to applications and data must be role-based and include policies for data loss prevention. (Data loss prevention includes restrictions that prevent a user from copying data to other applications.) With Zero Trust, the applications and data are checked not only once, but also continuously. Also, the application server must be protected from remote access via the public Internet.

Why Is Zero Trust Important?

In today's world of the digital workspace, the traditional "castle and moat" model of blanket security for data and applications no longer works. We need a new approach to security that adapts to the modern workspace and provides security for any application on any endpoint.

Changes to the attack surface

Factors contributing to the enlarged scope of vulnerability are

- **Flexible workstyles** – Users no longer work only on premises or within the organization's network. They also work remotely and are mobile. Users work from the office, from coffee shops, from home, and on transit. As a result, access to the organization's data and applications is required from outside the organization's traditional perimeter.
- **Endpoint choice** – Users request access to the organization's applications and data from many types of endpoints—mobile and desktop—and from endpoints belonging to the organization or personally owned.
- **Applications everywhere** – Applications can be in the cloud or on premises (in your data center, behind the firewall). Many organizations have a mixture of cloud and on-premises applications.

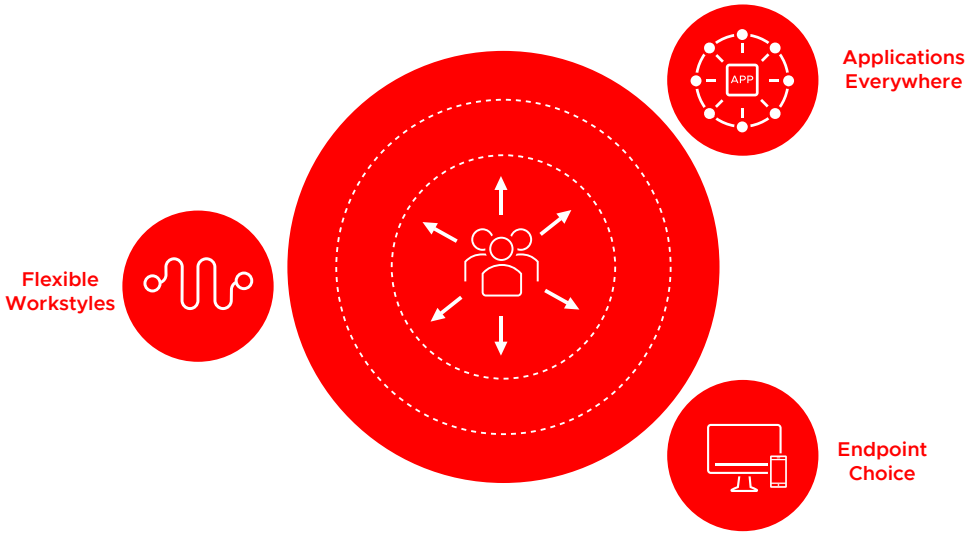

Figure 2. Today's Attack Surface Has Increased

In today's modern digital workspace, applications reside everywhere, and users access those applications from many kinds of endpoints in various locations. As a result of these trends, the potential security attack surface has increased exponentially and is constantly changing. Security threats have become more pervasive and complex and have adapted to this new era.

Each organization has the heightened challenge of maintaining not only security of the network, but also security of applications, data, endpoints, and users, all of which can be everywhere. Every resource must be considered vulnerable and must be constantly verified.

Typically, organizations secure their environment by tacking on a variety of security solutions to their existing "moat" that protects the "castle." Each security solution is effective, but often not integrated with the other solutions. The IT and InfoSec environments have exploded in complexity, and the number of security alerts has become overwhelming. Most organizations receive more than 10,000 security alerts per day, and that number can reach 1,000,000 for some organizations[1]. Security personnel experience alert fatigue, cannot respond to all of the security threats, and may even ignore alerts. This puts the organization's security at risk, even with all of these security solutions.

Journey to Zero Trust

To meet the challenges of the changed security environment, Zero Trust architecture requires the following solutions:

- **Endpoint choice** – Zero Trust requires continuous verification of endpoint compliance
- **Applications everywhere** – Zero Trust requires conditional access control to all applications
- **Flexible workstyles** – Zero Trust requires a reduction in the attack surface

VMware believes that the full journey to Zero Trust, which implements these solutions, has five pillars:

- Endpoint management and compliance
- Conditional access
- Application tunnel and proxy
- Risk analytics
- Automated remediation and orchestration

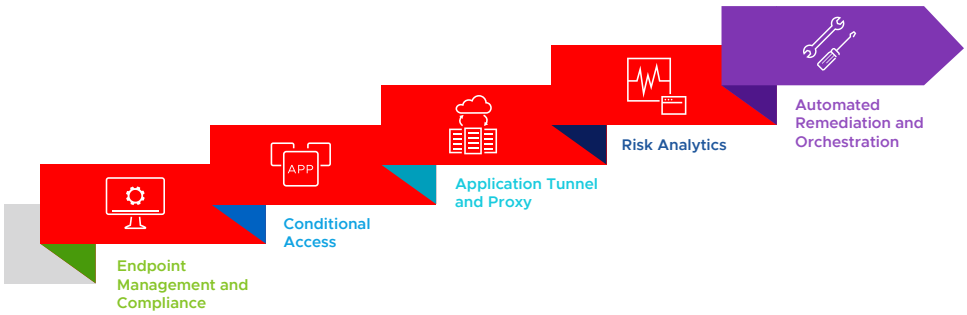

Figure 3. The Journey to Zero Trust

Your own journey to Zero Trust can be a non-linear journey that is customized to your organization. And Workspace ONE can enable any model of Zero Trust that you adopt.

1 Imperva. "Survey: 27 Percent of IT professionals receive more than 1 million security alerts daily." Tami Casey, May 2018.

VMware Workspace ONE Zero Trust Architecture

When you look at your current security architecture for the digital workspace, is it a unified system, or a fragmented one? Workspace ONE simplifies and unifies your IT and InfoSec needs and satisfies the requirements of Zero Trust architecture for the digital workspace.

Workspace ONE has integrated all of the components required to enable the full journey to Zero Trust for the digital workspace. The five pillars of Zero Trust are intrinsic to the Workspace ONE platform.

How does Workspace ONE satisfy Zero Trust?

Workspace ONE is a digital workspace solution that integrates user access control, endpoint management, and application management into a single platform with a seamless single-sign-on user experience.

Workspace ONE empowers IT and InfoSec to provide users with Zero Trust access to any application on any endpoint. It combines conditional access, unified endpoint management, and machine-learning-based risk analytics. Workspace ONE continuously verifies user contexts and endpoint compliance prior to granting least-privilege access to cloud-based, on-premises, and virtual applications.

All of the components of Zero Trust are enabled with the Workspace ONE digital workspace platform. If you are using VMware Workspace ONE now, you probably have implemented some of the components of this unified Zero Trust architecture, such as conditional access or endpoint management. Over time, you can add more of the integrated components.

Unique security features of Workspace ONE

Workspace ONE has unique and robust functionalities that make Zero Trust architecture for the digital workspace a reality.

Continuous verification of trust

To continuously verify trust and allow access, Workspace ONE provides risk analytics and ongoing monitoring of users, endpoints, applications, and transport. The Workspace ONE platform

- Develops contextual risk assessments for endpoints, users, and networks
- Integrates third-party security products
- Provides insights, automated remediation, and orchestration

If the identity of the user, compliance of the endpoint, or deviations from baseline behavior change, then Workspace ONE triggers automated remediation. Instead of cutting off the user completely, Workspace ONE gives the user various options to remediate the situation, such as multi-factor authentication. The user is quarantined only temporarily while the problem is remediated, and then access is restored.

Reduction of the attack surface and least-privilege access

Continuous verification of endpoint compliance and conditional access to applications serve to reduce the attack surface. With these in place, we can ensure that trust is continuously verified and access is allowed only when the endpoint, user and connection are fully trusted.

Additionally, VMware provides a Unified Access Gateway, which acts as an enforcement point to control and secure access to applications and resources. Unified Access Gateway can deploy different edge services depending on the type of access requested. These edge services include per-application VPN, Content Gateway, Web Reverse Proxy (WRP), and VMware Horizon Edge Service. Per-application VPN limits access to only the specific

application on the endpoint that is requesting data, without exposing enterprise data to anything else on the endpoint. Virtual applications and desktops are more secure by definition. By supporting secure connections to the virtual infrastructure by means of the Horizon Edge Service, the capabilities of Unified Access Gateway can also extend to applications and data behind the firewall.

Open, flexible, extensible platform

Workspace ONE can enable a full Zero Trust architecture. In addition, the open, flexible, extensible platform allows you to integrate your current third-party security and IT service management (ITSM) investments. VMware has an extensive partner ecosystem for the Workspace ONE platform called the Workspace ONE Trust Network.

Components of the Workspace ONE Platform

The Workspace ONE platform includes the following components that enable Zero Trust:

- VMware Workspace ONE® Intelligent Hub
- VMware Workspace ONE® Access
- VMware Workspace ONE® Unified Endpoint Management
- VMware Unified Access Gateway
- VMware Workspace ONE® Intelligence
- VMware Workspace ONE Trust Network

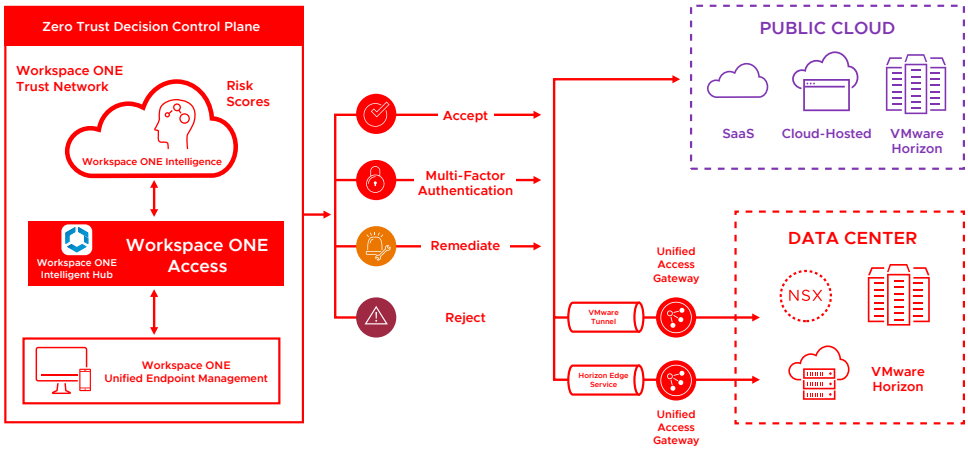

Figure 4. Workspace ONE Components for Zero Trust

Workspace ONE Intelligent Hub

Workspace ONE Intelligent Hub is the portal for users to access applications to accomplish their daily work. Each of the user's endpoints can have the portal agent installed, customized with the items the user has permission to access. The user signs in once with secure single sign-on (SSO) and may use whatever items are offered on their portal. And the applications can be integrated through SSO so that data flows from one application to another.

The user's selections from Workspace ONE Intelligent Hub trigger security checks by Workspace ONE Access and Workspace ONE Unified Endpoint Management.

Workspace ONE Access

Workspace ONE Access handles conditional access through a policy engine. After the user selects an application from Workspace ONE Intelligent Hub, Workspace ONE Access verifies the user's identity, rejects the request, accepts the request, requires multi-factor authentication, or requests remediation before it grants access.

Workspace ONE Unified Endpoint Management

The user's selection from the Workspace ONE Intelligent Hub triggers a check of endpoint compliance through Workspace ONE Unified Endpoint Management. Workspace ONE Unified Endpoint Management is a cross-platform solution for desktop, virtual, and mobile endpoints, with any operating system.

Unified Access Gateway

Unified Access Gateway is an extremely useful component within a Workspace ONE and VMware Horizon deployment because it enables secure remote access from an external network to a variety of internal resources.

Unified Access Gateway supports multiple use cases, including

- Per-application tunneling of native and web applications on mobile and desktop platforms to secure access to internal resources through the VMware Tunnel™ service. This unique feature helps to reduce the attack surface by enlisting VPN only on the application in use, instead of on the entire endpoint.
- Access from VMware Workspace ONE® Content to internal file shares or SharePoint repositories by running the Content Gateway service.
- Reverse proxying of web applications.
- Identity bridging for authentication to on-premises legacy applications that use Kerberos or header-based authentication.
- Secure external access to desktops and applications on VMware Horizon® Cloud Service on Microsoft Azure, and VMware Horizon® 7 on premises.

Workspace ONE Intelligence

Workspace ONE Intelligence is a cloud service that provides risk analytics, insights, and automated remediation and orchestration.

Workspace ONE Intelligence

- Continuously verifies risk through machine learning
- Detects user behavior anomalies in context, such as a rapid jump from one geographical area to another
- Creates user and endpoint risk scores
- Uses security algorithms that are dynamic, not static
- Reduces security-alert fatigue by gathering data from many sources and enforcing endpoint compliance in the cloud, in real time

If a user is at risk, or an endpoint is out of compliance, Workspace ONE Intelligence gives insights to IT and InfoSec and allows the setup of automation rules to remediate the problem so that the user can access the applications and data that they need, in real time. This approach is not just reactive, but proactive.

Workspace ONE Trust Network

Workspace ONE Trust Network provides a framework of trust by taking advantage of APIs built on the Workspace ONE platform. These APIs allow a rich ecosystem of security solutions to communicate with Workspace ONE and ultimately provide the aggregated view that administrators want for simplifying security and management. By connecting security solution silos, organizations can leverage their existing investments to exponentially improve continuous monitoring and risk analysis for faster response times. This results in a predictive security strategy, based on trends and patterns, which can scale with the deployment.

Integration with VMware NSX

You can further enhance security and segment the perimeter by adding VMware NSX® to the solution. NSX uses micro-segmentation to secure east-west traffic for applications and desktops in the data center and the cloud. NSX thus reduces the attack surface by micro-segmenting the entire architecture.

Summary: VMware Workspace ONE for Zero Trust Architecture

You can customize your journey to Zero Trust on the digital workspace; no one path is more correct than another. After you prioritize the use cases and components of the journey that are important to your organization, you can implement Workspace ONE to enable a unified Zero Trust architecture for the digital workspace. With Workspace ONE, you can begin by implementing Zero Trust for a few applications to assess the results, and then you can plan your next steps.

VMware Workspace ONE

- Satisfies the requirements of Zero Trust in one integrated digital workspace solution
- Is compatible with all types of endpoints and all types of applications
- Reduces the attack surface by enabling least-privilege access to applications after establishing trust
- Uses analytics and machine learning to give you insights into your organization's dynamic security environment
- Is open and extensible, and able to integrate with partner security solutions
- Unifies the management of the digital workspace for IT and InfoSec

VMware Workspace ONE satisfies the following essential requirements of Zero Trust:

- Continuous verification of endpoint compliance
- Conditional access control to all applications
- Reduction of the attack surface

In addition, Workspace ONE supplies the following add-ons to the basic requirements of Zero Trust:

- Continuous verification of trust
- •Analytics and automated remediation
- Risk scores
- Multi-factor authentication
- Application tunnel and proxy; micro-segmentation at the application level
- Virtualization of applications and desktops
- Networking and security virtualization software

Workspace ONE ensures that the goal of Zero Trust is met: never trust, always verify.

For more information, see the following additional resources.

Additional Resources

The following resources provide in-depth information about the enablement of Zero Trust architecture with Workspace ONE.

Security for the Digital Workspace

VMware Digital Workspace Tech Zone: Zero Trust

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: 5606-VMW-ENABLE-ZT-SECURITY-WS1-WP-20191030 10/19