Zero Trust Security with Workspace ONE

Q. What is Zero Trust?

A. Zero Trust is a conditional access control model that requires continuous verification of trust prior to allowing least privilege access to applications and data. Strategy behind Zero Trust boils down to moving away from traditional methods of security in which all resources inside the network perimeter are considered trustworthy and instead adopting a "never trust, always verify" approach. As compared to traditional methods of security, with Zero Trust there are dynamic decision points that verify trust and influence access levels to enterprise applications and data.

Q. Is Zero Trust an idea, feature or a product?

A. Zero Trust is a security model with a set of guidelines aimed at providing end-to-end security to enterprises even as IT embraces new technologies such as mobility and cloud. It relies on the concept of continuous verification of device compliance and user identity prior to granting access to enterprise applications and data with minimum required privilege.

Q. Why is Zero Trust needed?

A. Traditional methods of security were developed in a perimeter-bound world and assume implicit trust for anybody inside an organization's network. This is akin to the "castle and moat" approach where the focus is almost always on building the "moat" via technologies such as VPN and Network Access Controls. However, today the network perimeter as we know it has dissolved with the advent of technologies such as mobility and cloud. We need a new approach to security – one that relies on continuous verification of compliance and can protect applications and data irrespective of where it is being accessed from and on which device. Zero Trust does exactly that.

Q. Why is Zero Trust relevant now?

A. Zero Trust was coined by John Kindervag of Forrester in 2010 as an approach to security that relies on the concept of "never trust, always verify". This places emphasis on the concept of trust and how it's the malicious actors infiltrating through seemingly trusted devices that are actually compromised (i.e. by phishing attacks, malware etc.) that benefit. As organizations embrace the digital workspace, concepts such device choice (mobile, desktop, IoT), flexible workstyles (within and outside network) and application heterogeneity (SaaS, Web, Native, Virtual) become a reality and co-exist. In such a dynamic environment in which users access any app from any device, we need a security approach that is also dynamic and verifies trust continuously prior to allows access to sensitive information. Security breaches are on the rise and most of the recent ones were caused by companies having an outdated security policy. Zero Trust approach is more relevant now than ever.

Q. What the main tenets of Zero Trust?

A. While there are multiple Zero Trust Access Models defined by different companies and organizations (BeyondCorp by Google, Zero Trust eXtended by Forrester, CARTA by Gartner etc.), VMware's Zero Trust Architecture prescribes five main tenets:

- Device Management and Compliance - ensures the compliance state of the device
- Conditional Access - serves to confirm the identity of the user with features around step-up authentication among others
- App Tunnel and Proxy - secures the path to the Datacenter, and Virtual desktops and deploys technologies to reduce the attack surface
- Risk Analytics - elevates security with increased visibility and behavior analytics
- Remediation and Orchestration - enhances security and experience with auto remediation and orchestration

Q. Do customers have to follow all the tenets to have a Zero Trust IT environment?

A. Following all the tenets of the Zero Trust Journey would give enterprises end-to-end secure access control in an evolving IT environment that includes providing access to applications in the cloud or on-premises. However, for most organizations, Zero Trust will be a multi-year journey while companies re-think and invest in technologies that give them a full Zero Trust environment. Additionally, every organization will have its own journey depending on what applications they want to protect and how they embrace digital transformation.

vmware®

Q. My customers already have other security solutions. How will Zero Trust affect those investments?

A. VMware's Zero Trust approach for the Digital Workspace is vendor neutral. This approach lays out the main tenets based on what gives the best security to the Enterprise while staying aligned to Zero Trust principles of "Never Trust, Always Verify". Workspace ONE offers end-to-end Zero Trust Security that is cross platform, flexible and supports all applications. As part of being flexible and extensible, Workspace ONE also easily integrates with other 3rd party solutions for threat ingestion or orchestration giving customers the ability to leverage their existing investments while still achieving their Zero Trust goals.

Q. Can customers purchase Zero Trust as a product?

A. No. Customers will have to determine their requirements and map them to the appropriate Workspace ONE SKU. More information about Workspace ONE SKUs can be obtained here.

Q. How does VMware's acquisition of Carbon Black influence VMware's Zero Trust positioning?

A. As an industry leader in endpoint and workload security, Carbon Black brings great value to VMware's Zero Trust security offering. With the new Workspace Security Bundle, Workspace ONE Advanced customers can take advantage of the Workspace ONE Intelligence and existing Trust Network integrations to ingest real-time data on threat detected from Carbon's Black Next-Gen Antivirus (NGAV) and Endpoint Detection and Response (EDR) product – CB Defense, to calculate risk scores and assess compliance state. This helps in continuous verification of trust and augments VMware's Zero Trust offering for the Digital Workspace.

Q. Where can I find out more about Zero Trust?

A. Anybody interested in learning more about VMware's position on Zero Trust as it applies to the digital workspace can get more information by visiting the Security website for the Digital Workspace here. You can also get in-depth technical information on our tech zone site here

Q. Will professional services be able to help in executing a Zero Trust plan for customers?

A. Yes. Professional services offering that help you enable various services to embark on the Zero Trust journey is available today. Please contact your account executive for more details on how to get started

Q. How can customers start their Zero Trust journey?

A. Customers can visit TechZone for detailed technical documentation and use-case based implementation guides to get you started. Contact your account executive to understand more about the different Workspace ONE solutions that can help you in your journey A. VMware Solution Exchange at https://marketplace.vmware.com/vsx/ will provide more information on partners' solutions.

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