VMWARE WORKSPACE ONE TRUST NETWORK

Security for the Evolving Digital Workspace

AT A GLANCE

VMware Workspace ONETM Trust Network™ gives organizations a comprehensive and modern enterprise security approach to secure their employees, apps, endpoints and networks. With capabilities to protect, detect and remediate modern-day threats, Workspace ONE Trust Network augments the inherent security capabilities of the intelligence-driven Workspace ONE platform with a rich ecosystem of integrated partner solutions to deliver continuous risk monitoring and rapid mitigation response across the digital workspace.

KEY BENEFITS

Workspace ONE Trust Network simplifies security and management with a framework of trust and verification. With Workspace ONE Trust Network, IT can:

- Remove security solution silos with an action-based framework that provides an aggregated view and reduce complexity across the digital workspace
- Uniquely combine access, device and app security and management with insights and automation to mitigate risk across an end-user computing ecosystem
- Leverage an open and trusted partner ecosystem and continue to use existing investments, helping reducing costs

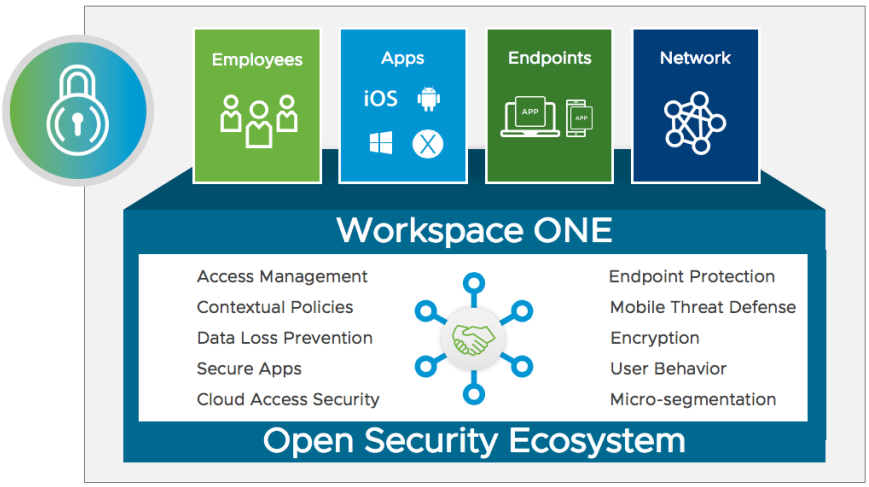

Figure 1: VMware Workspace ONE Trust Network™

Security – The Largest Barrier to a Modern Digital Workspace Strategy

A digital workspace can increase employee productivity by 5X[1], enabling employees with simple and secure access to apps and data from the device of their choice. As organizations continue to move towards digital transformation, the digital workspace ecosystem of employees, apps, endpoints and networks continues to grow and evolve beyond the traditional perimeter with common trends such as adoption of BYOD and the consumerization of IT. And as the traditional perimeter dissolves, advanced cyber threats such as zero-day attacks, Man-in-the-Middle (MiTM) attacks, phishing, bots and ransomware start to emerge.

Security is the top priority for mobility and digital workplace investment[2], yet existing security tools provide IT with only limited visibility, focusing only on silos of security that provide legacy functionality. This results in a band-aid approach that impacts organizations with high-costs due to complexity and requirement of manual tasks to secure a digital workspace. Consequently, security has become the largest barrier to a modern digital workspace strategy.

1 Source: https://www.vmware.com/radius/impact-digital-workforce/
2 Source: https://www.idg.com/tools-for-marketers/cio-tech-poll-tech-priorities-2019/

Comprehensive and Predictive Security in the Perimeter-less Organization

A new set of requirements to satisfy security needs without compromising user experience must be met:

1. To get an aggregated view, organizations need to use a framework to establish trust between the components securing their ecosystem.
2. And to continuously mitigate risk, organizations must be able to take insights from their environment to make predictive and automated decisions towards securing their digital workspace.

Workspace ONE Trust Network gives organizations a comprehensive and modern enterprise security approach to secure their employees, apps, endpoints and networks. Workspace ONE Trust Network provides a set of capabilities to protect, detect and remediate threats across the evolving digital workspace, based on a framework of trust and verification. When trust is established across a digital workspace, the result is an interconnected, least-privilege system that empowers employees by having security follow them. To manage risks related to modern-day cyber threats, Workspace ONE Trust Network combines insights from the intelligence-driven Workspace ONE platform with trusted security partner solutions to deliver predictive and automated security in the digital workspace.

Protecting, Detecting and Remediating

It's not a matter of if an organization will encounter a cyber-attack, but when. With these expectations in place, IT ops and security teams can manage cybersecurity-risk by simplifying the mapping of security functions, for example using a framework such as the NIST Cybersecurity Framework, to capabilities provided by Workspace ONE Trust Network:

- Security capabilities begin by protecting a digital workspace, which include preventing malware using machine learning, preventing data exfiltration from corporate cloud-based apps and micro-segmenting networks against advanced persistent threats (APTs).
- When threats enter the digital workspace, they can be detected using continuous and adaptive monitoring, enabling IT ops and security teams to detect threats on mobile and desktop endpoints and apps.
- After threats are detected, Workspace ONE Trust Network can automate remediation, leveraging a powerful decision engine. When an attack is detected based on behavioral anomalies, an automated policy to block access to corporate data can be initiated.

Unifying Access, Device and App Security, and Management with Analytics

Workspace ONE Trust Network combines the inherent security capabilities of the intelligence-driven Workspace ONE platform, which include access, device and app security and management with analytics, to uniquely bridge silos of management security solutions create. The Workspace ONE Intelligence service powers analytics on the Workspace ONE platform and provides workspace data aggregation, correlation and recommendations to deliver integrated insights and automation. By integrating Workspace ONE Trust Network capabilities with the Intelligence service, organizations can deliver ongoing security risk monitoring and rapid mitigation responses in today's perimeter-less world.

A decision engine helps correlate information such as out-of-network corporate devices with user behavior to detect threats and automate remediation through access policies. Integrated insights into threats data and granular device compliance status offer an easy way to identify and mitigate security issues in real-time improving security hygiene for the digital workspace. With the decision engine, IT can create rules to automate and optimize common tasks, such as remediating vulnerable Windows 10 endpoints with a critical patch and setting conditional access controls to apps and services at the group or individual level.

LEARN MORE

Find of more about Workspace ONE Trust Network by visiting: www.vmware.com/products/workspace-one/security

Try a Hands-on-Lab for free: htpps://www.vmware.com/go/workspace-hol

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

CALL

877-4-VMWARE (outside North America, +1-650-427-5000)

VISIT

http://www.vmware.com/products, or search online for an authorized reseller

Leveraging Rich Ecosystem of Trusted Partner Solutions

To enable comprehensive security across the digital workspace, trust must be established between the components that secure a growing and evolving digital workspace. 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 administrators want to simplify security and management. By connecting security solution silos, customers 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, that can scale with deployment.

Key Features

Organizations can take advantage of these critical security capabilities that Workspace ONE Trust Network provides to protect, detect and remediate against the evolving landscape of cyber threats.

CAPABILITY	DESCRIPTION
A Foundational Digital Workspace Platform that Connects Security Solutions	Simplify security and management with a framework of trust that leverages APIs to allow an open security ecosystem to communicate with Workspace ONE.
Access Management that Simplifies your Business	Empower IT to deliver application provisioning, a self-service catalog, multi-factor authentication and single sign-on (SSO) for all apps.
User Experience and Security Optimized with Contextual Policies	Control authentication with conditional access policies based on device compliance state, user authentication strength, data sensitivity, user location and more.
Data Loss Prevention (DLP) Policies Help Prevent Data Leakage	Enable device-level encryption, data encryption and hardware security policies. Configure policies including app blacklists, device pairing, Wi-Fi security and TLS enforcement. Monitor for malware threats, malicious apps, in-memory attacks or jailbroken devices and automatically remediate with a remote lock, device wipe, blocking access or customizable device quarantine controls.
Securing Applications Without Sacrificing User Experience	Utilize security controls in VMware secure productivity apps – VMware BoxerTM, BrowserTM and Content LockerTM. Detect threats and automate remediation for all other apps and cloud services.
Encryption for Data at-Rest and Data In-Transit	Authenticate and encrypt traffic from apps on devices into the data center with VMware Tunnel. Secure app data at-rest and in-transit with AES 256-bit encryption.
Micro-segmentation Automates Security Across Networks	Minimize the attack surface in the data center by using micro-segmentation capabilities with VMware NSX®, automating security across the network.
Integrated Insights and Automation Drive Predictive Security	Identify and mitigate security issues in real-time with integrated insights into threat data and granular device compliance status provided by Workspace ONE Intelligence.

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