GET STARTED

8 CRITICAL CAPABILITIES FOR DIGITAL WORKSPACE SECURITY

vmware®

Table of Contents

Many Threats, One Approach

Today's enterprises are perimeter-less. Your customers engage on the devices they prefer, and your employees work from everywhere. As business leaders increasingly demand greater information access to enhance service delivery and innovation, they are implicitly trusting you, their IT professionals, to watch for and prevent data theft.

Make sure your team is up for the challenge. When your IT staff can enforce security while empowering employees with apps they want and need to be more productive, the business wins. A defense-in-depth, digital workspace security approach is needed to not only protect your most sensitive assets, but also detect and remediate successful intrusions—when, not if, they occur.

VMware® Workspace ONE™ Trust Network provides a modern, comprehensive, and predictive approach to securing employees, applications, endpoints, and networks. Using a framework of trust and verification, IT teams can secure the components across their ecosystem that make up the evolving digital workspace. Eight protection, detection, and remediation capabilities form the core of what Workspace ONE Trust Network sets out to provide. These capabilities help deliver insights from collected data and can be used to make the right decisions about preventing, detecting, and stopping encroaching threats, and remediating when required.

Go ahead, secure your digital workspace.

> *"Businesses that empower employees with access to their preferred apps and devices see measurable gains on an individual level and an organizational level with a majority of all CIOs surveyed believing revenue can increase by more than 5 percent over three years when employees are empowered."*

– FORBES INSIGHTS
"THE IMPACT OF THE DIGITAL WORKFORCE: A NEW EQUILIBRIUM OF THE DIGITALLY TRANSFORMED ENTERPRISE"
OCTOBER 2017

Don't Bolt On, Build In Security

Mobility and digital workplace security investment is a top priority now because traditional and complex security technology silos no longer work. Your IT team knows that trying to chase down the root causes of multiple alert storms at once is nearly impossible. In the era of increasingly diverse work places and more dynamic cyber threats escalating to target new vulnerabilities beyond traditional perimeters, your enterprise needs security that adapts automatically.

Protect with Visibility and Control

Reputation is everything. When customers stop trusting a business, revenue decline can be quick to follow. Customers and investors expect businesses to protect their data and achieve compliance. It's only when they don't that trust erodes, and value suffers. With Workspace ONE Trust Network, your IT team can simultaneously provide consumer-simple access to users and gain enterprise-grade security through the digital workspace. Built-in configurable security and access controls coupled with visibility into all assets—from employees and applications to devices and networks—protect against internal and external threats.

Security is the top priority for mobility and digital workplace investment in 2018.[1]

[1] CCS INSIGHTS SURVEY, "IT BUYER SURVEY," SEPTEMBER 2017

Detect with Intelligence

The WannaCry cyberattack took advantage of a vulnerability in Microsoft Windows to target millions globally. Successes of that scale encourages copycats, so you need to remain vigilant against attacks growing annually in number and severity. Continuous, adaptive automated digital workspace monitoring and alerting capabilities with the Workspace ONE Trust Network approach give your IT staff a head start in threat discovery across endpoints and applications. IT stays in control by knowing who is accessing what information, from where, and how, across what networks, using abnormalities to identify active threats and make better decisions about what to do next.

Remediate with Automation

Intrusions are inevitable. It's what your enterprise does immediately following that matters most. An internal VMware study indicated that one-in-ten enterprise customers take a year or more to complete Windows patches that affect most or all of their endpoints. Manual remediation isn't agile enough for digital business to stop cyber criminals. Insights and automation with Workspace ONE Trust Network leverage pre-defined policies in the digital workspace to quickly automate response and recovery for best case results.

Keep Close to Trusted Security Partners

When you find solutions you like, and that work well, there's little appetite for ripping and replacing them with the unknown. VMware's approach recognizes this and also that with tremendous innovation happening in cybersecurity tools, your organization may also want flexibility in the future to protect a work edge that has become perimeter-less. Your business can confidently move forward with VMware because Workspace ONE Trust Network simplifies security using a framework that establishes trust between the components that secure the growing and evolving digital workspace to combats attacks.

VMware helps you lower complexity and operational costs associated with securing the digital workspace. Workspace ONE Trust Network takes advantage of APIs built on the proven Workspace ONE platform to enable a rich ecosystem of security solutions to communicate with the platform, and ultimately provide the aggregated view your IT administrators want and need to simplify security and management in areas including, but not limited to, OS security flaws visibility, device health assessment, device recovery, governing access and control, policy setting, virus scanning, patching, disaster recovery, and compliance monitoring.

By connecting security solution silos, your organization can leverage existing investments to exponentially improve continuous monitoring and risk analysis for faster response times, gaining a predictive security strategy based on trends and patterns that can scale with deployment. Workspace ONE Trust Network is an ideal foundation for moving your digital business forward quickly while mitigating risks, protecting your brand, reducing costs, improving agility, and providing a consumer-like experience on all devices wherever work gets done.

8 Must-Have Capabilities

The more integrated and comprehensive the features, the better you and your IT team can secure your end-user environment. Workspace ONE Trust Network includes eight key capabilities to secure endpoints, applications, employees, and networks, bridging security technology silos into one platform:

1. Single and Open Platform Approach
2. Data Loss Prevention (DLP) Policies
3. Contextual Policies
4. Protecting Applications
5. Access Management
6. Encryption
7. Micro-Segmentation
8. Analytics

1. Single and Open Platform Approach

Consider for a moment the amount of time your IT team spends simply managing existing devices and apps across your organization. When will you have time to introduce new devices and apps that help business teams innovate? If you don't, lines of business will continue to add apps they want, when they want, and the shadow IT challenge will continue to grow.

A single and open platform enables your IT team to strengthen security, simplify compliance enforcement, and reduce risk. You can combine access, device, and application management functionality on a single, open platform with analytics and intelligence to uniquely bridge existing complex and costly security silos. One platform with intelligence services ensures workspace data aggregation, correlation, and recommendations to deliver integrated insights and automation.

Workspace ONE Trust Network provides an aggregated view of employees, apps, endpoints, and networks. The platform is built on a framework of API communication that helps establish trust between the components in your ecosystem. As a result, your enterprise gains an interconnected, least-privileged system that empowers employees by having security follow them.

2. Data Loss Prevention Policies

Let's face it. Protecting data everywhere is hard with business happening everywhere—on PCs in cafes, on tablets at home, and on smartphones at airports and in shopping malls. Data loss prevention (DLP) policies help your enterprise protect data no matter where it resides, inside or outside of the data center.

With Workspace ONE Trust Network, your IT team can remotely lock or wipe a device if it's lost or stolen, locate a missing device, and obtain real-time device information such as operating system (OS) version, last update, location, and more. Utilizing virtual desktop infrastructure (VDI) to centralize desktops and apps, you can also reduce data loss from misplaced or stolen devices.

Across all endpoints, you should be able to enforce and manage security policies per application with native OS-provided DLP controls and prevent data loss across content with email attachment controls, cut/copy/paste restrictions, dynamic watermarking, and more. With Workspace ONE Trust Network, you can. You can also control and restrict a user's ability to remove content from corporate using a software development kit (SDK).

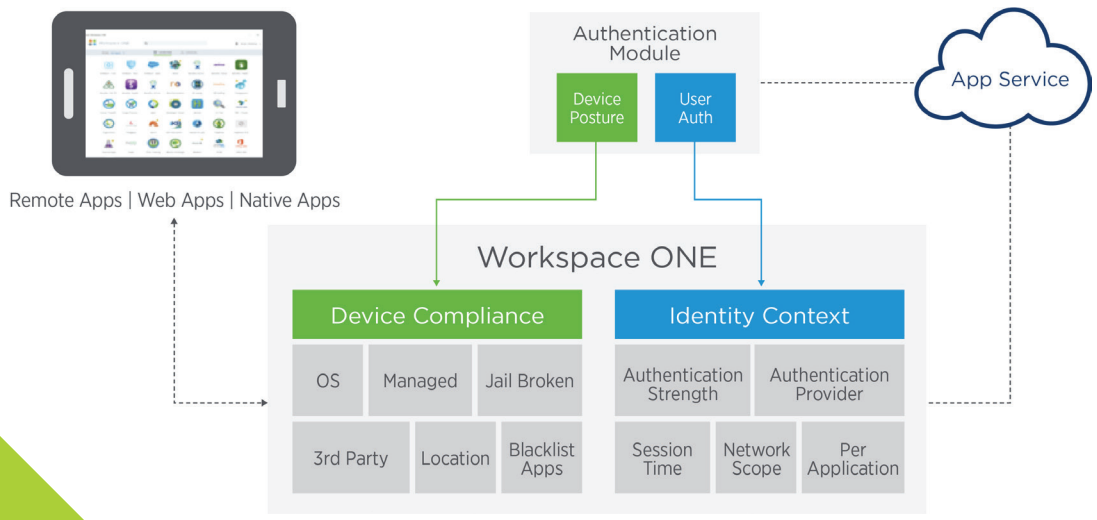
A decision engine in Workspace ONE, the digital workspace platform central to Workspace ONE Trust Network, can automate compliance for advanced DLP. These advanced security policies include setting protections against rooted or jailbroken devices, whitelisting and blacklisting apps, open-in app restrictions, geofencing, network configuration and blocking export and screenshots, as well as the backup or saving of company information to external SD cards or remote cloud backup solutions.

3. Contextual Policies

Making organizational changes? Filing financial forms? Sending customer communications? Managers and other senior staff in your organization know which employees should be able to see what information, where and when. Now your enterprise can enforce those policies through software.

Enterprises must be able to establish conditional access—by role, department, clearance level, etc.—so only authorized users can get to certain information and resources. Workspace ONE Trust Network includes contextual policies to set and enforce end-user conditional access to help ensure only authorized users have access to your organization's sensitive information and resources when they need it.

By combining policy enforcement with access and device management using Workspace ONE Trust Network, your IT team can restrict user permissions to data, applications, or devices. The same technologies can also be used to apply conditional access to mobile apps and ensure that only compliant applications can access internal systems.



4. Protecting Applications

Hackers are continually adapting malware to gain penetration into IT environments. Stop them earlier with protections that adapt. By enforcing DLP policies at the application level, enterprises take another giant step toward more granular access policies that better safeguard data. Digital workspaces should include DLP policies (see #2) that deliver the same functionality at the application and endpoint level.

For both bring-your-own (BYO) and corporate devices, application management capabilities in Workspace ONE Trust Network facilitate provisioning and control access, in effect, wrapping applications in policies defined by identity. Similarly, cloud data loss protection, as well as governing access and activities in sanctioned and unsanctioned cloud services, better secures data and protects against threats.

Workspace ONE Trust Network provides the ultimate flexibility in security with support for full-device VPN, per-app VPN, and SDK-based proxy gateway communication across all major operating systems.

Workspace ONE offers productivity apps (e.g., email, document management, etc.) with DLP and Rights Management Services (RMS) functionality, including:

- Information Rights Management (IRM) secured email
- S/MIME with PKI
- Email classification
- Sensitive or personally identifiable information (PII) policies
- Attachment encryption
- Access policies for printing, viewing and roaming,
- Document expiration
- Watermarking

With support for full-device VPN, per-app VPN, and SDK-based proxy gateway communication across all major operating systems, including iOS, Android, macOS, and Windows 10, Workspace ONE Trust Network provides IT with the flexibility to choose the right solution to secure application connectivity.

5. Access Management

A single platform can eliminate access management burdens to support line-of-business requests. Enterprises can strengthen data protection by verifying user identity using multiple factors. To eliminate the increasingly complex task of having to set individual policies for a constantly growing number of applications, devices, and cloud services, enterprises should be able to use the end user's identity to establish security parameters while making it easy to access apps.

One-touch, single sign-on (SSO) through Workspace ONE allows users to access desktop, mobile, and cloud applications —avoiding the time and hassle of multiple log ins. Through SSO, the identity of a user can be verified for many apps at once, in effect, providing a single key for a single digital workspace door to open access to a variety of web, mobile, SaaS, and legacy applications on the end point of choice from an application catalog.

Through multi-factor authentication (MFA), the identity of users and system components can be verified in Workspace ONE Trust Network using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function.

6. Encryption

With clear text data traversing the network, anyone can read data passing across your organization. Encrypting data provides greater protection against the information theft. That means your organization can worry less about someone stealing sensitive information from prototypes, designs, and sensitive documents.

For critical business processes, best practices include encrypting all data, while stored or transmitted. In the event of a data breach, stealing critical files should only result in obtaining unreadable data. Utilizing an advanced encryption standard such as AES-256bit encryption for data-in-transit and data-at-rest is critical.

As a relay between device platforms and enterprise systems, IT can use tunnels or per-app VPNs as a part of Workspace ONE Trust Network to authenticate and encrypt traffic from individual applications on compliant devices to the back-end system they are trying to reach using unique certificates.

7. Micro-segmentation

Once an intruder is in your IT environment, it can be difficult to know how much information has been compromised, and what additional targets they are pursuing. Your organization can more aggressively combat threats, reduce risk, and increase its security posture with micro-segmentation across your networks.

Micro-segmentation provides a combination of capabilities including:

- Reducing the attack surface within the data center perimeter through distributed stateful firewalling and ALGs (Application Level Gateway) on a per-workload granularity
- Enabling the use of security groups for object-based policy application for VMs, including virtual desktops and virtual application hosts, creating granular application level controls
- Logical Network overlay-based isolation and segmentation that can span across racks or data centers regardless of the underlying network hardware, enabling centrally managed multi-data center security policy

As part of Workspace ONE Trust Network, VMware helps you divide whole IT environments into smaller parts to make them more manageable to protect or to contain damage if one part is compromised.

Segregation of east-west traffic, or micro-segmentation, from application to specific workloads in the data center substantially reduces the attack vector of malware/viruses that aim to do significant harm to the business.

8. Analytics

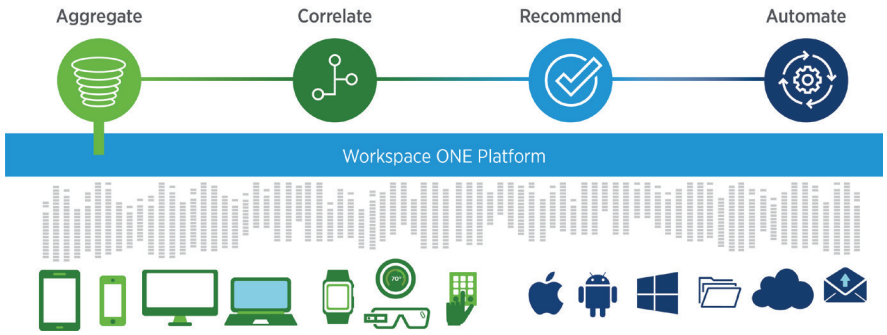
Continuous improvement is a goal of every IT organization. Workspace ONE Trust Network can help your enterprise improve its security posture by leveraging actionable insights from app deployment and usage.

Workspace ONE Trust Network combines the core of Workspace ONE's digital workspace functionality—access, device and app management—with analytics, powered by Workspace ONE Intelligence, to uniquely bridge existing security solution silos.

Aggregated application deployment, usage, device security, and end-user experience details help you better understand the performance and security of your digital workspace environments. The built-in intelligence service with automated actions accelerates planning, enhances security, and improves end user experiences. It also delivers ongoing security risk monitoring and rapid mitigation responses in today's perimeter-less world.

Together with a decision engine, Workspace ONE Intelligence helps you correlate information to detect threats and automate remediation based on access policies. By augmenting Workspace ONE Trust Network capabilities with the Workspace ONE Intelligence service, you gain ongoing security risk monitoring and rapid mitigation responses in today's perimeter-less world.

The 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, your IT team 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 applications and services at the group or individual level.

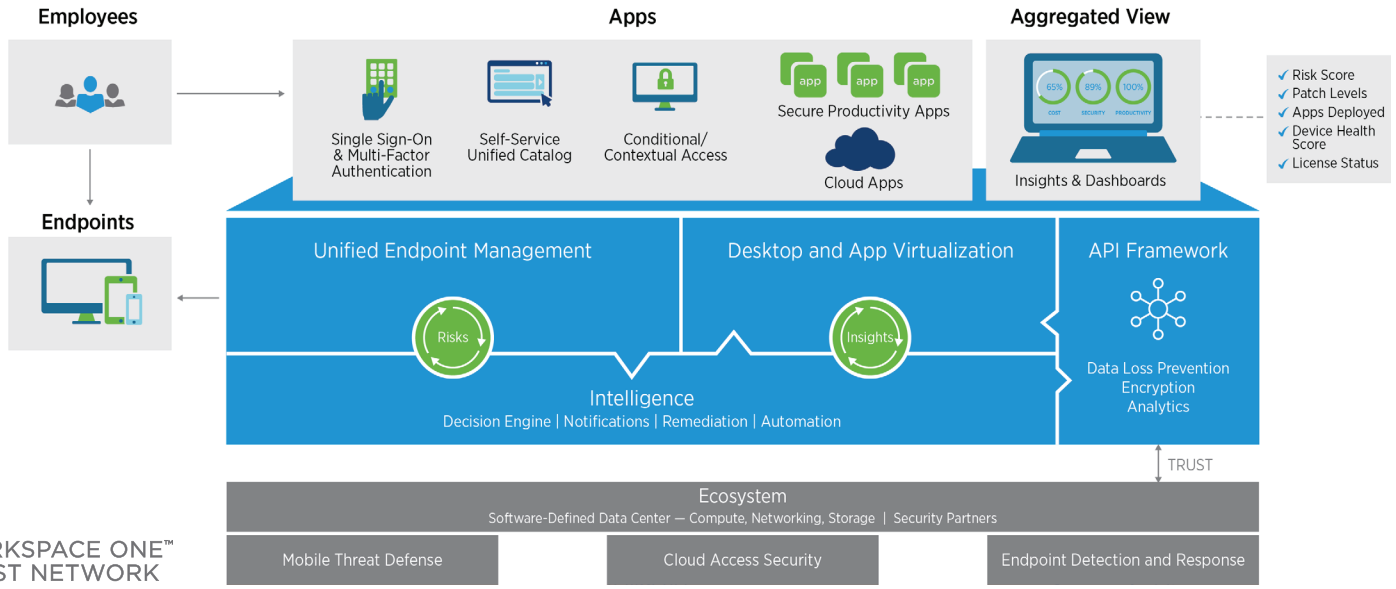


Workspace ONE Trust Network

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 Workspace ONE, the intelligence-driven digital workspace platform, with trusted security partner solutions to deliver predictive and automated security in the digital workspace.

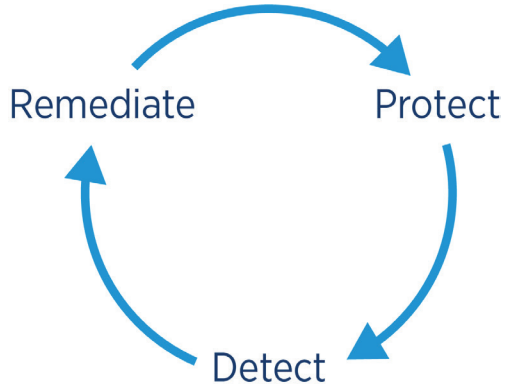
Workspace ONE Trust Network is a comprehensive and modern enterprise security approach for enterprises to secure employees, applications, endpoints and networks. It includes capabilities to protect, detect and remediate threats across the evolving digital workspace, based on a framework of trust and verification.

VMware Workspace ONE Trust Network



Protect, Detect, and Remediate Threats to Your Business

VMware's approach helps your IT operations and security teams manage cybersecurity-risk by simplifying the mapping of security functions, for example using a framework such as the NIST Cybersecurity Framework, to solution capabilities available with the Workspace ONE Trust Network approach:



- **Protect** – Security capabilities begin by protecting the digital workspace, which includes using machine learning to recognize malware; leveraging micro-segmentation of networks to protect against advanced persistent threats (APTs); and preventing data exfiltration from corporate cloud-based apps.
- **Detect** – When threats enter the digital workspace, VMware security capabilities detect them using continuous and adaptive monitoring across mobile and desktop endpoints and apps.
- **Remediate** – This approach then automates remediation using a powerful decision engine. For example, if a Trojan horse or Man-in-the-Middle (MITM) attack is detected based on behavioral anomalies, the Workspace ONE Trust Network capabilities help initiate an automated policy to block access to corporate data.

vmware WORKSPACE ONE™ TRUST NETWORK

Learn More

When your IT team leverages the Workspace ONE Trust Network model, it can more confidently empower employees to be more productive and efficient, benefiting both workers and your businesses. Get security concerns out of the way of productivity and efficiency by using Workspace ONE Trust Network to ensure comprehensive security is in place to safeguard sensitive data as your digital workspace strategy expands and evolves beyond traditional work perimeters. Secure your digital workspace with a framework of trust today.

Learn more at http://www.vmware.com/products/workspace-one/security

vmware® | vmware WORKSPACE ONE™ TRUST NETWORK

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