WHITE PAPER – **MARCH 2018**

A COMPREHENSIVE APPROACH TO SECURITY ACROSS THE DIGITAL WORKSPACE

vmware®

Table of Contents

Companies that empower their employees with the applications they want and need, and make them readily accessible—anytime, anywhere, on any device—can benefit from measurable decision making, productivity, and efficiency gains at the individual and organizational level.[1]

Introduction

Newly quantified business benefits—showing employees with digital workspaces are more productive and their companies outperform traditional workspaces—have increased enterprise interest in how to achieve similar gains while securely delivering applications to any device. Businesses want the advantages cited in the *Impact of the Digital Workforce* study by Forbes Insights, but none should have to compromise security to achieve them, even as the traditional work perimeter disappears.

Dissolving Work Perimeter Exposes Organizations

IT teams everywhere continue to fight security threats growing in number and severity. For many, malware intrusions have already resulted in costly interruptions to operations. For example, the WannaCry cyberattack took advantage of a vulnerability in Microsoft Windows to target millions, simultaneously holding computers across 150 countries hostage in exchange for ransomware fees. In the U.S., the number of data breach incidents tracked in 2017 hit a new record high.[2]

Today's expanding organizational and work perimeters provide even greater opportunities for cyber criminals. Modern zero-day threats and Man-in-the-Middle (MITM) attacks are good examples, the former named for the age of the exploit, which takes place before or on the first (or "zeroth") day of a developer's awareness of the bug; and the latter a form of eavesdropping where the attacker actively listens in by intercepting a public key message exchange and retransmits the messaging while replacing the requested key with his own, in effect, taking over, monitoring, and modifying communication between two users without their knowledge.[3] Advanced phishing techniques using social engineering and programming expertise, bots, and ransomware threats also more frequently expose organizations, even those working hard to stay one step ahead.

Combating Threats and Protecting Enterprise Data

A better approach to securing the evolving digital workspace by protecting, detecting, and remediating threats through an intelligence-driven platform is needed. With it, organizations can more effectively safeguard sensitive data as their digital workspace strategies expand and evolve at the same time as dynamic cyber threats escalate and adapt to target new vulnerabilities beyond traditional perimeters.

This paper describes a new, comprehensive and predictive approach to security in the modern perimeter-less world. It highlights the importance of securing the evolving digital workspace and the need for enterprises to embrace a framework of trust between the components in their ecosystem. It also introduces the eight core protection, detection, and remediation capabilities required to ensure IT organizations can take insights from collected data and use them to make the right decisions about preventing threats and stopping attacks from spreading.

[1] Forbes Insights. "The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT," October 2017.

[2] Identity Theft Resource Center. "2017 Annual Data Breach Year-End Review."

[3] Technopedia. "Zero-Day Threat," 2018.

"Security is the top priority for mobility and digital workplace investment in 2018."

– CCS INSIGHTS

Security is the Largest Barrier to a Modern Digital Workspace Strategy

Work now happens everywhere. Employees are accessing information and applications at the office, from home, in cafes, and even at 10,000 feet, on many personal and corporate endpoints, across a variety of networks. IT teams, recognizing employees' needs for greater choice in when, where, and on what device they work, are busy trying to accommodate employee preferences while still protecting valuable enterprise data.

Yet existing security solutions are inadequate. IT teams are still attempting to meet rapidly changing end-user needs with complex, often cobbled together, legacy security technologies; some of which are being deployed to secure things they are not meant to secure. As a result of IT teams acquiring many different solutions over time, many technologies don't communicate well with one another, offering a wide variety of potential avenues for attacks. While employee satisfaction is vital to their organization's success, IT leaders report that security is the top priority for mobility and digital workplace investment in 2018.[4]

Nearly half (47 percent) of IT buyers in a recent survey conducted by CCS Insights said network security was their biggest investment priority for the digital workplace over the next 12 months, followed by device security at 42 percent, and application security at 27 percent. These investments may better safeguard data and applications as workloads move; however, having silos of security solutions only increases complexity and still leaves room for error. For example, stopping an intrusion with network firewalling from potentially penetrating one system, then realizing the intrusion is infecting east-west traffic across a variety of systems because it went undetected for months can harm enterprises. With an approach that connects silos of security solutions based on a framework of trust, IT doesn't have to require the prioritization of protecting, detecting, and remediating threats—because it continuously does all three.

Enterprises' can more effectively combat ever-evolving cyber threats targeting systems and data with a modern approach to digital workspace security, one in which security follows the employee's digital workspace. This model should establish trust between the components securing the end-user computing ecosystem—employees, applications, endpoints, and networks—and only allow authorized access based on verification. Comprehensive and integrated, a framework of trust can help ensure data is protected, and through insights and automated intelligence, used for on-going detection and remediation to minimize risk.

[4] CCS Insights Survey, "IT Buyer Survey," September 2017.

NEW SECURITY REQUIREMENTS

- To safeguard the organization, introduce the eight core protection, detection, and remediation capabilities.
- For an aggregated view, use a framework to establish trust between the components securing the ecosystem.
- To continuously mitigate risk, take insights from the environment to make predictive and automated decisions toward securing the digital workspace.

Three Steps to Comprehensive Security in the Evolving Digital Workspace

IT organizations need a comprehensive enterprise security approach to secure their end-user environments. This model encompasses security across endpoints, applications, employees, and networks by bridging together security technology silos. To achieve the best results, IT must consider these steps to strategically secure their evolving digital workspace.

Step 1: Protect, Detect, and Remediate Threats

Cyber threats have evolved. What may have started as mischievous hacking activities, for example, students impressing friends with their IT prowess by entering and immediately exiting unauthorized systems, is now almost always a hacker or hackers with malicious intent. Protecting against cybercrime requires a comprehensive response that both enforces good while chasing bad, in order to:

Protect

Enterprises—particularly regulated ones such as financial services and healthcare—go to great lengths to meet compliance requirements around the back-end storage of highly sensitive and valuable data. Yet a client manager today can access sensitive data on a mobile device during a customer meeting and then accidently leave a tablet in a taxi where sensitive data can potentially be stolen. This lost and compromised customer information would almost certainly result in negative brand and financial impacts.

Providing seamless consumer-simple access for employees to data and apps should not come at great risk to companies. That's why enterprise security capabilities start by protecting their employee's digital workspace. IT should be able to prevent malware from entering environments by educating workers not to click suspicious links and by deploying policies to prevent data loss. Further identifying vulnerabilities and protecting environments against inside and outside threats comes when organizations gain complete visibility into all of their assets from employees and applications to devices and networks. Only when they can fully implement a variety of protections—including issuing policies, such as access controls, sensitive data classification, and device usage restrictions, as well as regularly patch applications—can they gain peace of mind and set the stage for advancing to detection. After all, protection initiatives without equally effective detection methods prevent IT from knowing if they are even addressing the most critical issues.

Detect

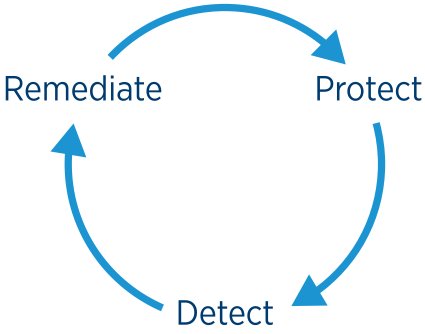
Dissolving perimeters, insider threats, and increasingly inventive cyber criminals have devolved the security conversation from "if" to "when" an attack will occur. That makes it necessary for enterprises to look beyond protecting assets to detecting when intrusions happen—from credentials being compromised to unpatched vulnerabilities being exploited. IT teams must be able to identify and neutralize an active threat before it has a chance to do more significant damage to the organization. Detection must also be implemented in a manner that doesn't lead to alert fatigue.

When threats enter the digital workspace, prepared enterprises can detect them using continuous and adaptive monitoring, enabling their IT operations and security teams to find threats on mobile and desktop endpoints and applications. With automated, continuous monitoring and alerting of who is accessing what information, from where, and how, across what networks, IT stays in control. Then, using last-known good state, logging, and intelligence in the form of analytics, IT has the tools in place to recognize what is different and use that insight to make better decisions about what to do next.

Remediate

Digital business moves fast, making traditional security solutions that require manual remediation for most tasks obsolete. Enterprises today require rapid response when they are dealing with malicious intrusions and unexpected outages. Waiting for a response can lead to even greater breach penetration. An internal VMware study indicated that one-in-ten enterprise customers takes a year or more to complete Windows patches that affect most or all of their endpoints. This gives cybersecurity criminals time to invent exploitation methods.

IT teams must be able to leverage insights from their environment to confidently pre-define policies, based on root causes, to quickly automate response and recovery for best results. Through automation, IT may choose to quarantine, suspend, or block access to an application or cloud service. After threats are detected, the most prepared enterprises have an effective solution to automate remediation through an engine that can detect behavioral anomalies and initiate an automated policy to block access to sensitive data.



Enterprises that choose a strategic framework that can establish trust between the components in their ecosystem and solutions securing those components will be in the best position to fully protect critical corporate assets and speed time to detection and remediation.

Step 2: Capabilities to Protect, Detect, and Remediate

These eight critical capabilities move enterprises toward modern and comprehensive digital workspace security:

Single and Open Platform Approach	A single and open platform enables IT to simplify compliance enforcement—for example, of devices and apps—and reduce risk. Enterprises should adopt a single, open platform combining access, device, and application management functionality with analytics and intelligence to uniquely bridge complex and costly existing security solution silos. One platform with intelligence services ensures workspace data aggregation, correlation, and recommendations to deliver integrated insights and automation. Enterprises using this approach should get an aggregated view of employees, apps, endpoints, and networks. This platform approach should be built on a framework of API communication that helps establish trust between the components in the enterprises' ecosystem. This is critical because establishing trust across a digital workspace results is an interconnected, least-privilege system that empowers employees by having security follow them.
Data Loss Prevention (DLP) Policies	DLP policies help organizations protect data no matter where it resides, inside or outside of the data center. IT teams should be able to 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 can help reduce data loss from misplaced or stolen devices. Across all endpoints, enterprises also 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. Control and restriction of a user's ability to remove content from corporate using a software development kit (SDK) is a requirement. A policy and compliance engine can help automate compliance for advanced DLP. 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
Contextual Policies	Using contextual policies to set and enforce end-user conditional access can help ensure only authorized users have access to sensitive information and resources. 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. By combining policy enforcement with access and device management, IT 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.

Protecting Applications	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 (outlined previously in capability two) that deliver the same functionality at the application level. For both bring-your-own (BYO) and corporate devices, mobile application management facilitates 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. With support for full-device VPN, per-app VPN, and SDK-based proxy gateway communication across all major OSs, including iOS, Android, macOS, and Windows 10, IT gains the flexibility to choose the right solution to secure application connectivity. In addition, productivity apps (e.g., email, document management, etc.) must provide 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
Access Management	Enterprises strengthen data protection by verifying user identify with multiple factors or all at once for many applications. 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. One-touch, single sign-on (SSO) 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 using multiple factors (not just simple passwords) and be commensurate with the risk of the requested access or function.
Encryption	Encryption assures organizations that sensitive data is protected by preventing non-intended recipients from seeing data as it is sent and received. 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 to authenticate and encrypt traffic from individual applications on compliant devices to the back-end system they are trying to reach using unique certificates.

Micro-segmentation	Organizations can more aggressively combat threats, reduce risk, and increase their security postures with micro-segmentation across their 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 Whole IT environments divided into smaller parts make them more manageable to protect or to contain damage if one part is compromised. Segregation of east-west traffic 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.
Analytics	Enterprises improve their security posture with actionable insights from app deployment and usage. Aggregated application deployment, usage, device security, and end-user experience details help IT better understand the performance and security of their digital workspace environments. A 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, an intelligence service helps correlate information to detect threats and automate remediation based on access policies.

Step 3: Trusted Partners Insert Security Everywhere

Security threats are increasing both in frequency and cost, as well as focus and sophistication, making a single platform with seamless and trusted security partner vendors an ideal approach to threat protection, detection, and remediation. Legacy, stand-alone security tools, designed to protect valuable information provide limited visibility for IT, and often, lead to the creation of solution silos across the environment. This results in an uncoordinated approach that negatively impacts organizations, raising costs due to complexity and the manual tasks associated with trying to secure a digital workspace.

Trust established between the components that secure a growing and evolving digital workspace helps ensure comprehensive security. The ideal approach is through a framework of trust that takes advantage of APIs built on a proven digital workspace platform. This is because APIs enable a rich ecosystem of security solutions to communicate with the platform, and ultimately provide the aggregated view administrators want and need to simplify security and management.

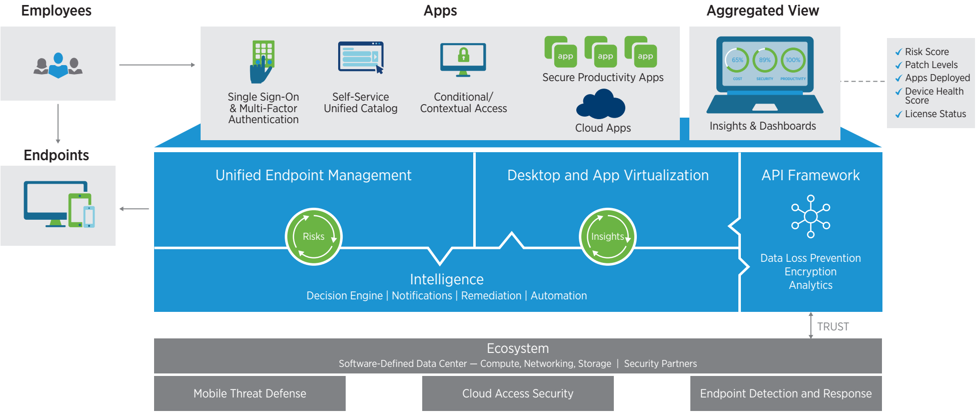
A robust digital workspace strategy will include an open ecosystem of trusted security solutions that specialize in thwarting attacks and mitigating risk in areas such as:

- OS security flaws visibility
- Device health assessment
- Device recovery
- Governing access and control
- Policy setting
- Virus scanning
- Patching
- Disaster recovery
- Compliance monitoring

How VMware Helps Transform Traditional Digital Workspace Security

Although there is tremendous innovation happening in cybersecurity tools, the sheer number and variety on the market has reinforced the message that IT leaders should wait for a best-practices approach to digital workspace security. Today, enterprises can confidently move forward with VMware helping to simplify security with a framework to combat attacks across the changing threat landscape.

VMware® Workspace ONE™ Trust Network™ gives organizations a comprehensive and modern enterprise security approach to secure employees, applications, 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 Workspace ONE, an intelligence-driven digital workspace platform, with trusted security partner solutions to deliver predictive and automated security in the digital workspace.



Protect, Detect, and Remediate

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:

- 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.
- When threats enter the digital workspace, VMware security capabilities detect them using continuous and adaptive monitoring across mobile and desktop endpoints and apps.
- This approach then automates remediation using a powerful decision engine. For example, if a Trojan horse or MITM attack is detected based on behavioral anomalies, an automated policy initiates to block access to corporate data.

Unify Access, Device, and App Management with Analytics

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. The Workspace ONE Intelligence service provides workspace data aggregation, correlation and recommendations to deliver integrated insights and automation. By augmenting Workspace ONE Trust Network capabilities with the Workspace ONE Intelligence service, VMware ensures enterprises 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 applications and services at the group or individual level.

Leverage an Ecosystem of Trusted Partner Solutions

Comprehensive security across the digital workspace requires trust to be established between the components that secure a growing and evolving digital workspace. VMware does this with Workspace ONE Trust Network, which provides a framework of trust by taking advantage of APIs built on the Workspace ONE platform. These APIs help ensure a rich ecosystem of security solutions can communicate with Workspace ONE and ultimately provide the aggregated view administrators want to simplify security and management.

By connecting security solution silos, VMware customers 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.

VMware customers 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.

The need for enterprises to adopt a new digital workspace security approach is imperative because the work edge has become perimeter-less. A framework that establishes trust between the components in their ecosystem accommodates new employees, new apps, new devices, and new networks. It serves as the foundation for moving forward as your digital enterprise seeks to move fast while mitigating risks, protecting your brand, reducing costs, improving agility, and providing a consumer-like experience on all devices at work.

Protect, Detect, and Remediate: 8 Must-Have Capabilities

vmware® WORKSPACE ONE™
TRUST NETWORK

CAPABILITY	WHY IT MATTERS
Single, Open Platform Approach	Simplify compliance enforcement and reduce risk by eliminating technology silos across platforms, apps, and user profiles.
Data Loss Prevention (DLP) Policies	Protect data no matter where it resides with device wipe, remote locking, and per app security policies.
Contextual Policies	Ensure only authorized users have access to sensitive information and resources with conditional access policy enforcement.
Protecting Applications	Safeguard information by controlling who can access which resources with DLP policies at the application level.
Access Management	Strengthen data protection by verifying user identity with multiple factors or all at once for many applications with single sign-on.
Encryption	Protect sensitive data by preventing non-intended recipients from seeing data as it is sent and received.
Micro-Segmentation	Reduce the attack surface of your organization by segregating workloads and traffic.
Analytics	Improve security posture and compliance with actionable insights, application analytics, and automation.

Learn More

Empowering employees with a digital workspace benefits both workers and businesses. Don't let IT security concerns get in the way of productivity and efficiency advantages. The Workspace ONE Trust Network approach helps provide capabilities your enterprise requires to ensure comprehensive security is in place to safeguard sensitive data as your digital workspace strategy expands and evolves with dynamic cyber threats escalating and adapting to target new vulnerabilities beyond the traditional perimeter. Secure your digital workspace by combining access, device, and application management with analytics, leveraging a framework of trust across the entire ecosystem and using insights from collected data to make the right security decisions.

Learn more about Workspace ONE Trust Network at www.vmware.com/products/workspace-one/security.

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMW-WP-CMPRHENSIVE_APPROACH_SECURITY_WRKPLC-USLET_103
3/18