VMware Workspace Security VDI

Zero Trust security for VMware Horizon virtual desktops and apps

WHAT'S NEW

VMware Workspace Security VDI delivers a cohesive, intrinsically secure virtual desktop and application solution that has been built and fully tested by a single vendor. It is available as a subscription offering that provides a single, flexible entitlement to all VMware Horizon technology, services and deployment options: on premises, in the cloud, or for hybrid and multi-cloud use cases.

AT A GLANCE

VMware Workspace Security VDI delivers a more secure virtual desktop and application solution available for the distributed workforce by combining *VMware Horizon* and *VMware Carbon Black Cloud* into a single, unified solution. Horizon is a market-leading, modern platform for secure delivery of virtual desktops and apps across the hybrid cloud. With next-generation endpoint protection from VMware Carbon Black Cloud, IT can further improve security and help provide a Zero Trust access security model across users, apps and endpoints that empowers employees.

With the shift to a distributed workforce, desktop and application virtualization have been recognized as key technologies to enable end users to securely access corporate applications and data from any device and location. This accessibility, coupled with a dramatic rise in cyberattacks, requires the highest levels of security, which is complicated by distributed and increasingly complex environments. To keep up with these growing threats, organizations are employing a Zero Trust approach to security that incorporates device state, location and user behavior information to determine which, if any, corporate resources a user should be able to access in any given scenario and time.

Desktop and application virtualization have enabled organizations to reduce operational management costs, while providing high levels of control necessary to ensure compliance and achieve the highest security standards by keeping sensitive corporate apps and data in the data center and off the endpoint. Despite the inherently secure nature of virtual desktops and applications, just as for traditional desktops, there are still additional capabilities that can further improve security without compromising the end-user experience.

VMware Workspace Security VDI

VMware Workspace Security™ VDI delivers a highly secure virtual desktop and application solution for the distributed workforce by combining *VMware Horizon®* and *VMware Carbon Black Cloud™* into a single, unified solution. Horizon is a market-leading, modern platform for secure delivery of virtual desktops and apps across the hybrid cloud. VMware Carbon Black Cloud strengthens the combined solution with endpoint security capabilities in multiple categories, including threat identification, detection and response, auditing capabilities, and the ability to investigate data breaches. These capabilities are typically point solutions purchased separately, which often leads to a sprawl of agents, vendors, integration testing, updates, and patching issues that IT departments are challenged to eliminate. Alternatively, Workspace Security VDI delivers a cohesive, intrinsically secure virtual desktop and application solution across the hybrid cloud that has been designed and fully tested by a single vendor.

BENEFITS

- Delivers a single-vendor solution, tested and supported by VMware
- Streamlines routine operations and eliminates multiple security point products with comprehensive endpoint security from a single console
- Detects and blocks attacks, and predicts attacks that have never been seen before, via a holistic approach that leverages machine learning and behavioral models
- Provides fast, easy access to system state information to make quick, confident actions that harden systems and improve security posture

FIGURE 1: VMware Workspace Security VDI combines VMware end-user computing and security products.

An advanced level of endpoint security protection

Workspace Security VDI includes next-generation antivirus (NGAV) and behavioral endpoint detection and response (EDR) provided by VMware Carbon Black products to provide multilayer protection for Horizon virtual desktops and applications. Traditional antivirus solutions focus on signature-based attacks. Today's attackers can easily bypass these solutions with macro-based and memory-based attacks, as well as highly developed tools that target vulnerabilities associated with PowerShell scripting and remote logins. VMware Carbon Black Cloud takes endpoint security protection to an advanced level by analyzing entire event streams across files, processes, applications and network connections. This holistic approach to data collection powers machine learning and behavioral models to detect and block attacks, as well as predict attacks that have never been seen before. By leveraging policy-based controls, administrators can fine-tune their security environment, further enhancing the overall security posture of the organization.

These technologies help companies identify patterns as well as tactics, techniques and procedures (TTPs) that may be suspicious and turn them into attack visualizations that incident responders can quickly use. To remediate from anywhere in the world via VMware Carbon Black Cloud, a secure connection to the infected desktop can be created to pull or push files, kill processes, and perform memory dumps. An infected desktop that is based on VMware nonpersistent instant clone technology can simply be destroyed, and a new one can be immediately spun up from a known good image.

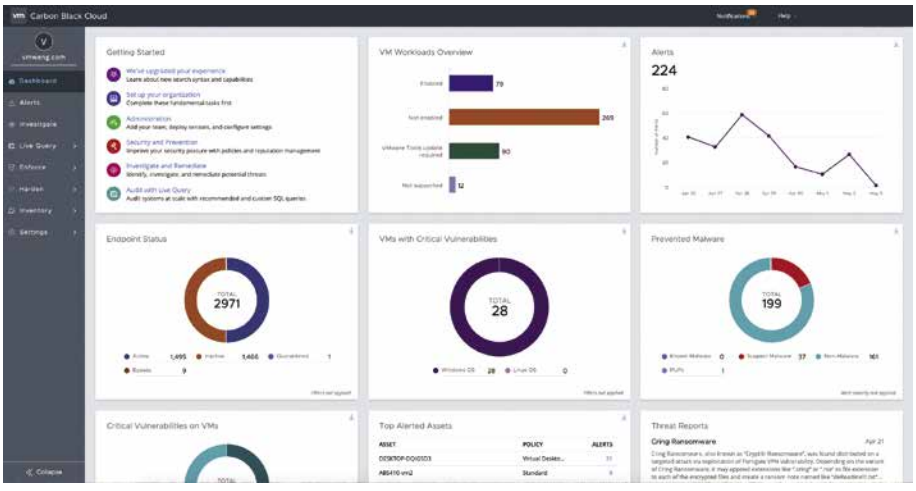

FIGURE 2: Using the VMware Carbon Black Cloud universal console, the solution applies behavioral analytics to events to streamline detection, prevention and response to cyberattacks.

Real-time audit and remediation

VMware Carbon Black® Cloud Audit and Remediation™ provides both IT and SecOps teams with faster, easier access to real-time virtual desktop data with the ability to change the system state of virtual desktops or endpoints across their organization. By providing administrators with real-time query capabilities from a cloud native endpoint protection platform, Carbon Black Cloud Audit and Remediation enables teams to make quick, confident decisions to harden systems and improve security posture. Unlike competing solutions, it provides the evidence that systems are configured and patched according to industry standards, which is required in highly regulated industries. Carbon Black Cloud Audit and Remediation closes the gap between security and operations, allowing administrators to perform full investigations and take action to remotely remediate endpoints, all from a single solution.

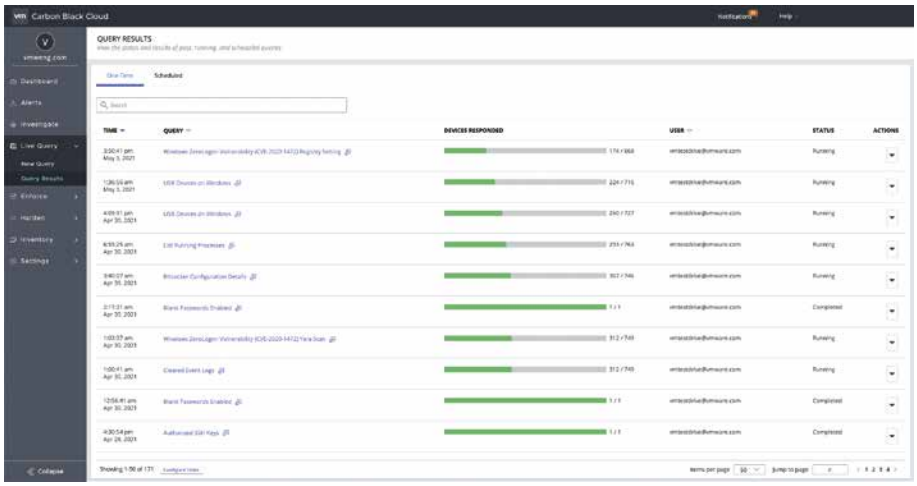

FIGURE 3: Carbon Black Cloud Audit and Remediation gives administrators the ability to easily create custom queries and return results from across all endpoints in their environment to a single cloud-based console.

Enable your future-ready workforce with enhanced Zero Trust security

Workspace Security VDI delivers a highly secure desktop and application virtualization solution that consolidates multiple endpoint security capabilities into a cohesive solution that has been tested end to end. Compared to legacy solutions, this modernized, lightweight approach significantly improves performance and protects against a new wave of attack vectors that traditional antivirus solutions cannot detect.

By leveraging the rich VMware ecosystem, Workspace Security VDI can be incorporated in a broader security program that intrinsically layers security solutions from the endpoint to the cloud, across networking and data center workloads. For example, VMware Workspace ONE® Access™ establishes and verifies end-user identity with multifactor authentication, and serves as the basis for conditional access and single sign-on for Horizon virtual desktops and apps. Additional security features are woven into VMware technologies across the network and supported by Horizon, such as network micro-segmentation with *VMware NSX® Data Center*, software-defined load balancing with *VMware NSX Advanced Load Balancer™*, secure remote access with VMware Unified Access Gateway™, and high-performance branch access with *VMware SD-WAN™*. These intrinsic elements help implement a Zero Trust security model across users, devices, networks and data that empowers employees without sacrificing security.

FOR MORE INFORMATION OR TO PURCHASE VMWARE PRODUCTS

Call 877-4-VMWARE (outside North America, +1-650-427-5000), visit *vmware.com/security/workspace-security*, or search online for an authorized reseller. For detailed specifications and requirements, refer to the product documentation.

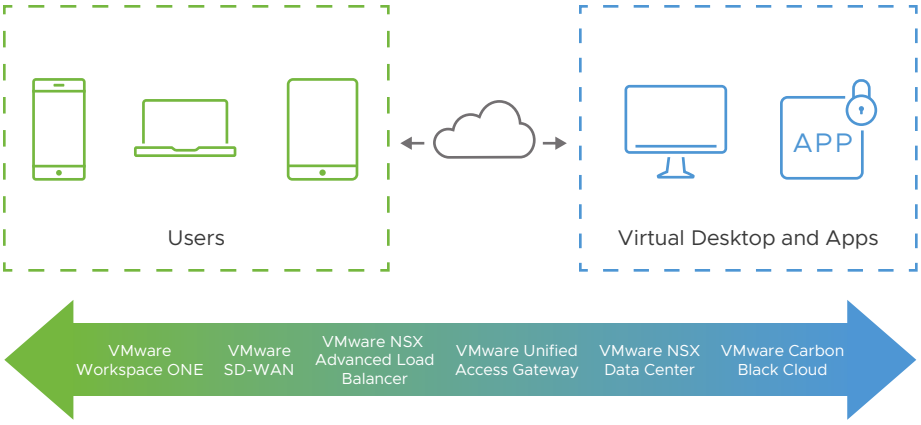

FIGURE 4: Workspace Security VDI leverages the VMware ecosystem to deliver a broader security program.

Make the move today

VMware Workspace Security VDI is available as a subscription offering that provides a single, flexible entitlement to all Horizon technology, services and deployment options: on premises, in the cloud, or for hybrid and multi-cloud use cases. You can choose from the following subscription licenses.

VMware Workspace Security VDI Audit

- VMware Workspace Security VDI Audit™ with Horizon Universal Subscription – Horizon desktop and application delivery for on-premises or cloud deployment, and Carbon Black Cloud Audit and Remediation
- VMware Workspace Security VDI Audit with Horizon Subscription – Horizon desktop and application delivery for cloud deployment, and Carbon Black Cloud Audit and Remediation

VMware Workspace Security VDI Essentials

- VMware Workspace Security VDI Essentials™ with Horizon Universal Subscription – Horizon desktop and application delivery for on-premises or cloud deployment, NGAV, and VMware Carbon Black® EDR™
- VMware Workspace Security VDI Essentials with Horizon Subscription – Horizon desktop and application delivery for cloud deployment, and VMware Carbon Black Cloud Endpoint™ Standard, which includes NGAV and Carbon Black EDR

VMware Workspace Security VDI Advanced

- VMware Workspace Security VDI Advanced™ with Horizon Universal Subscription – Horizon desktop and application delivery for on-premises or cloud deployment, NGAV, Carbon Black EDR, and Carbon Black Cloud Audit and Remediation
- VMware Workspace Security VDI Advanced with Horizon Subscription – Horizon desktop and application delivery for cloud deployment, NGAV, Carbon Black EDR, and Carbon Black Cloud Audit and Remediation

Workspace Security VDI is eligible for the Subscription Upgrade Program for Horizon. In addition, VMware Carbon Black Cloud supports Horizon perpetual deployments and may be purchased separately.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 873107aq-so-vmw-ws-sec-vdi-uslet 5/21