Workspace Security VDI

Coordinated Endpoint Protection for Horizon Virtual Desktops

AT A GLANCE

VMware Workspace Security VDI enhances the security of virtual desktops with a combined VMware Horizon and Carbon Black Cloud solution.

With next-generation endpoint protection from VMware Carbon Black, IT can improve security of virtual desktops and support a Zero Trust access security model across users, apps and endpoints.

WHY ZERO TRUST

Zero Trust validates security state prior to granting access to corporate resources. Continuous verification of device and desktop state and location and user behavior, paired with adaptive policies, can help determine and put into effect the level of access that a user should have in any given situation.

Workspace Security VDI not only helps ensure that connected devices and desktops are secure, but also provides critical information that informs Zero Trust policies so that organizations can evaluate and automatically respond to risk.

Desktop virtualization helps organizations increase productivity, reduce operational overhead, and provide controls necessary for security and compliance. Despite the inherently secure nature of virtual desktops and applications, vulnerabilities exist. Virtual desktop and application security can be improved by implementing Carbon Black Cloud solutions in virtual environments.

Workspace Security VDI: Horizon Virtualization paired with Carbon Black Cloud Security

VMware Workspace Security VDI combines VMware Horizon and VMware Carbon Black Cloud into a single solution that provides Horizon virtual desktops with extended security. VMware Carbon Black specialized endpoint protection includes threat identification, detection and response, auditing capabilities, and the ability to investigate data breaches. Workspace Security VDI is a cohesive and secure virtual desktop and application solution.

Endpoint Protection for Persistent and Non-Persistent Virtual Desktops

Three levels of endpoint protection for Horizon virtual desktops are available. The most comprehensive security is provided by Workspace Security VDI Advanced, which includes NGAV (Next-generation AntiVirus) and Behavioral EDR (Endpoint Detection and Response) as well as Audit and Remediation. This solution is appropriate for both persistent and non-persistent desktops and is recommended for persistent desktops because of their increased exposure to threats. More detail below in the section "Workspace Security VDI Offerings."

Ongoing protection via NGAV and behavioral EDR

VMware Carbon Black Cloud with NGAV (next-generation antivirus) and behavioral EDR (endpoint detection and response) takes a comprehensive approach to protection by analyzing event streams across files and processes. Data is collected and machine learning and behavioral models are employed to not only detect and block known threats, but also to prevent never-seen-before attacks. Behavior analysis allows administrators to analyze patterns over time.

vmware®

Policy-based controls allow administrators to fine-tune their security environment and further enhance the organization's security posture.

Threat detection and intelligence, automated watchlists, and integrations with the rest of your security stack help organizations scale detection and response across the enterprise.

Real-time audit and remediation

VMware Carbon Black Cloud Audit and Remediation allows IT and security teams to audit the current system state to track and harden the security posture. With this solution, IT and SecOps teams can access virtual desktop data with real-time query capabilities from the Carbon Black cloud native endpoint protection platform and respond with script-based adjustments to virtual desktops across their organization. Additionally, compliance reporting indicates which instances are configured and patched according to industry standards, which is required in highly regulated industries.

Enable your future ready workforce with enhanced Zero Trust security

By leveraging the rich VMware ecosystem, Workspace Security VDI can be incorporated in a broader security program that provides protection from the endpoint to the cloud, across networking and data center workloads.

Workspace Security VDI offerings

VMware Workspace Security VDI protection for virtual desktops is available as a subscription offering, which 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. Choose from these subscription licenses:

VMware Workspace Security VDI Audit

- **VMware Workspace Security VDI Audit with Horizon Universal Subscription:** Horizon desktop for on-premises or cloud deployment and Carbon Black Audit and Remediation

- **VMware Workspace Security VDI Audit with Horizon Subscription:** Horizon desktop delivery for cloud deployment and Carbon Black Audit and Remediation

VMware Workspace Security VDI Essentials

- **VMware Workspace Security VDI Essentials with Horizon Universal Subscription:** Horizon desktop delivery for on-premises or cloud deployment and Carbon Black Next Generation Antivirus (NGAV) and Behavioral Endpoint Detection Response (Carbon Black EDR)

FIND OUT MORE

For more information, visit
https://www.vmware.com/security/workspace-security.html

For information or to purchase VMware products, call 877-4-VMWARE, visit www.vmware.com, or search online for an authorized reseller. For detailed specifications and requirements, refer to the product documentation.

- **VMware Workspace Security VDI Essentials with Horizon Subscription:** Horizon desktop delivery for cloud deployment and Carbon Black Endpoint Standard, which includes Next Generation Antivirus (NGAV) and Behavioral Endpoint Detection Response (Carbon Black EDR)

VMware Workspace Security VDI Advanced

- **VMware Workspace Security VDI Advanced with Horizon Universal Subscription:** Horizon desktop delivery for on-premises or cloud deployment and Carbon Black Next Generation Antivirus (NGAV), Behavioral Endpoint Detection Response (Carbon Black EDR) and Carbon Black Audit and Remediation
- **VMware Workspace Security VDI Advanced with Horizon Subscription:** Horizon desktop delivery for cloud deployment and Carbon Black Next Generation Antivirus (NGAV), Behavioral Endpoint Detection Response (Carbon Black EDR) and Carbon Black Audit and Remediation

The Workspace Security VDI solutions listed above are also available via the Subscription Upgrade Program for Horizon (HSUP). Please note that Carbon Black protection for Horizon perpetual deployments are not included in the above subscription licenses.

Coordinated endpoint protection

Workspace Security VDI extends advanced security in the Anywhere Workspace to persistent and non-persistent virtual desktops. VMware endpoint protection across all hybrid work environments is available via Carbon Black Cloud for Windows, Mac, and Linux devices; and Workspace ONE Mobile Threat Defense for Android, iOS, and Chrome OS devices.

For more information, contact your sales representative or reach out to VMware at https://www.vmware.com/company/contact_sales.html.