WHITE PAPER–MAY 2021

Best Practices for Securing VMware Horizon VDI with VMware Carbon Black Cloud

vmware®

Table of contents

Introduction

Over the past several years, the mission and vision of VMware have been to deliver any application on any device on any cloud in an intrinsically secure manner. Security can mean many different things depending on what is being protecting, including securing physical and virtual endpoints (such as virtual desktop infrastructure [VDI]), securing applications and data across public and private clouds, and securing workloads (be they physical, virtual or containerized).

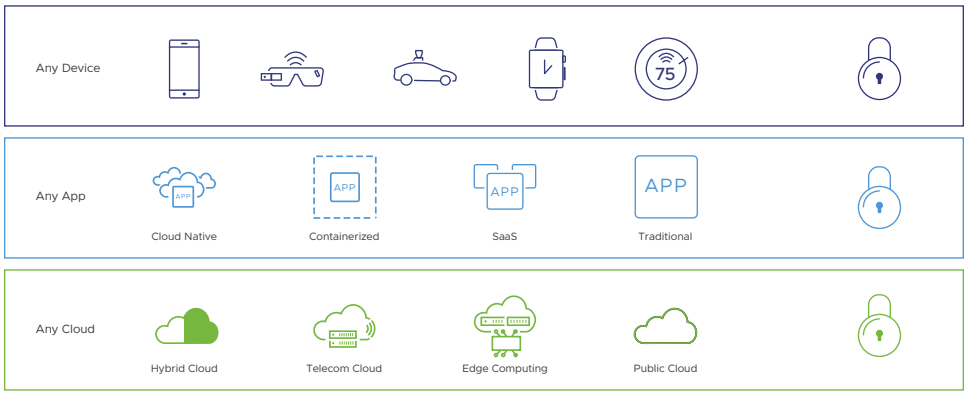

FIGURE 1: The VMware vision of the essential, ubiquitous digital foundation.

Intrinsic security means security is built in, not bolted on. It means security comes from a single vendor and is already architected into the technologies you're using. It means optimal performance, and it also means you have the same source of truth from IT, the security team, and the development team. VMware is known for doing things intrinsically: built-in storage, networking, compute, and now security.

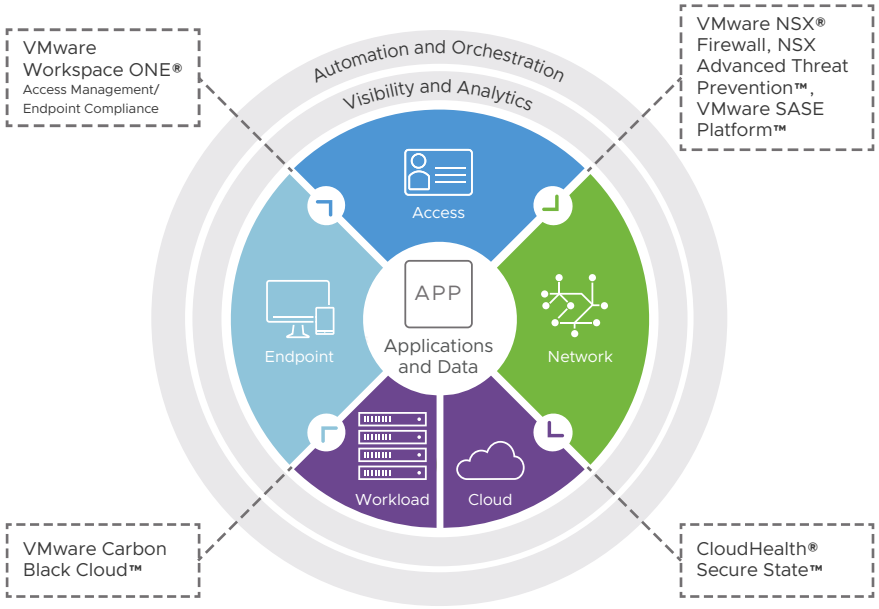

FIGURE 2: Intrinsic security from VMware secures critical applications and data.

With a continual increase in the distributed workforce, there is an increased demand for bandwidth in employees' homes as well as the need to access enterprise applications in remote locations. Using VDI is a fast and cost-effective method to ensure remote workers can access the applications they need from wherever they are.

In fact, VDI use might soon increase. Company leaders intend to shift some positions to remote permanently because of increased efficiencies. This is especially true among enterprises that already use virtual desktops compared to small and midsize businesses.

Better together: VMware Carbon Black Cloud and VMware Horizon VDI

Security optimization and architecture remain a persistent challenge in large-scale deployments. The traditional security approach is not suitable or sustainable for single-image management. The lack of context, intelligence, prevention, detection/response and recovery hinders efficiency, efficacy and the mitigation of risk.

This challenge arises primarily because the traditional approach does not allow the security solution any direct access to, or control of, processes in the individual desktop's memory. IT and security teams face numerous challenges when attempting to prevent, detect, respond to and troubleshoot performance issues while trying to determine their root causes within a VDI and virtualized environment. With so many moving parts and multiple agents deployed, solutions are often unmanageable or require additional effort to achieve an appropriate outcome.

The VMware Carbon Black Cloud™ platform features a single point of security configuration for all server, desktop, public and private cloud assets. It maintains centralized management of configurations and policies that are updated in real time. VMware Carbon Black Cloud also provides risk assessment and audit and remediation capabilities for testing and validating configuration changes that can resolve and improve performance issues, create better prevention policies, and attain hardening of systems. The platform validates whatever policy configuration the administrator makes and automatically adjusts to achieve the right level of security.

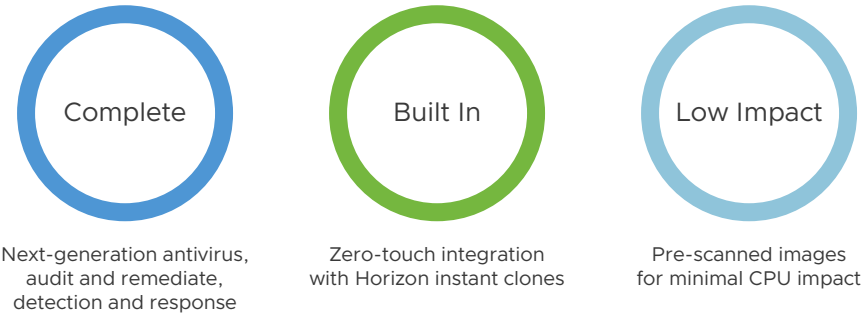

FIGURE 3: Features of VMware Carbon Black Cloud.

Our built-in, layered security approach is a necessity, especially in public and private clouds where advanced protection against breaches must not come at the expense of efficiency, virtual machine (VM) density, or performance. Organizations can leverage our intrinsic security capabilities specifically designed for virtualization and for the cloud, as opposed to legacy security solutions that introduce excessive latency with bloated agents that take up host and VM resources, reduce consolidation ratios, and drive-up costs. The VMware Carbon Black Cloud integration with the VMware Horizon® platform is critical for rapid deployments to maintain real-time VM inventory, facilitate security automation, and ensure compliance in environments that use nonpersistent desktops.

VDI reference architecture with VMware Carbon Black Cloud

Figure 4 shows the high-level logical architecture of the core Horizon components and indicates where VMware Carbon Black Cloud can be enabled in your infrastructure to secure the Horizon components.

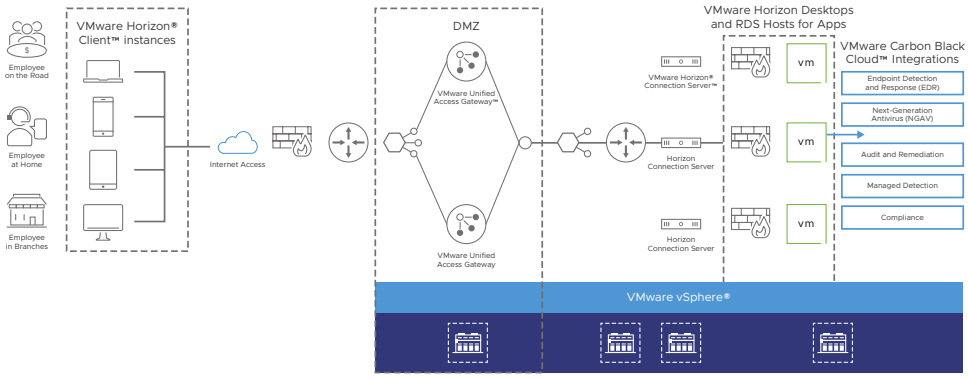

FIGURE 4: Architecture of the integration of Horizon and VMware Carbon Black Cloud.

Figure 5 shows the high-level logical architecture of the core Horizon components, Horizon Enterprise Edition components, and additional infrastructure components on which the VMware Carbon Black Cloud sensor can be installed to increase your overall security posture within the Horizon platform.

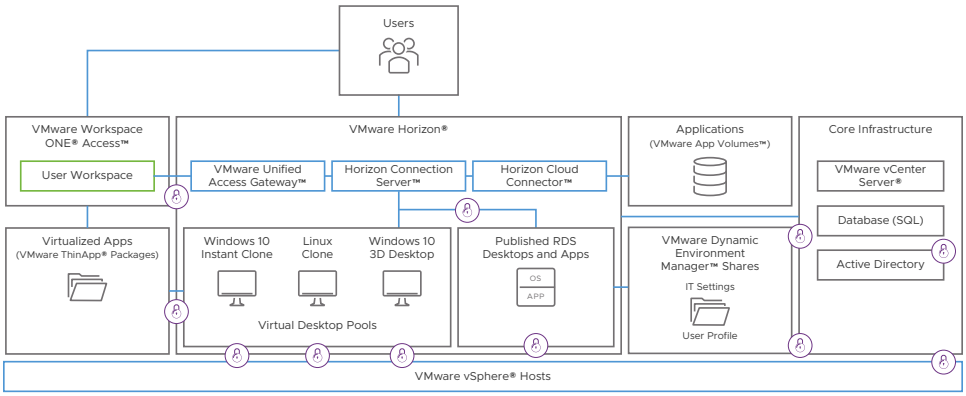

FIGURE 5: Architecture of where the VMware Carbon Black Cloud sensor can be installed on Horizon components.

Figure 6 depicts the virtual desktop OS and where the VMware Carbon Black Cloud sensor would reside within the desktop OS. This setup would be deployed on the golden VM image used to create either persistent or nonpersistent desktop pools.

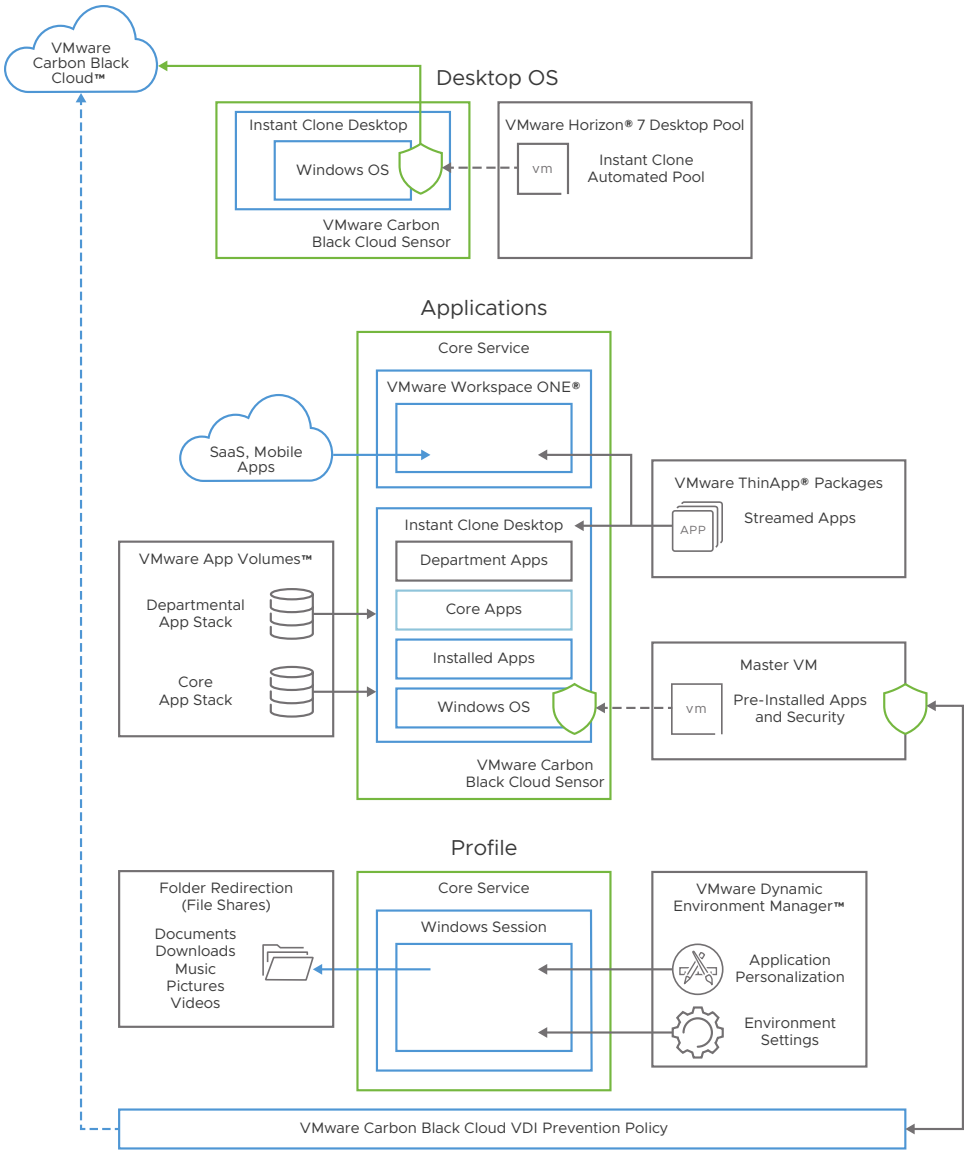

FIGURE 6: Architecture of where the VMware Carbon Black Cloud sensor would reside within a virtual desktop OS.

VDI security best practices

The best practices listed in this section allow you to increase your security posture, decrease dwell time, and limit lateral movement by isolating access to sensitive resources. Usage of sensitive resources should not be mixed with other types of usage, such as personal or corporate access, that is exposed to the public internet. Public and private cloud security must be agile and mapped in real time to the infrastructure management plane. Other security features must also be built into the platform.

One the most dangerous attack vectors in any system is people. We are not only talking about employees clicking links and opening files received from known or unknown senders. This attack vector can also include IT admins who configure their systems in ways that leave gaps for attackers to abuse because the admins lack understanding of how to mitigate risk within their environment.

USING VMWARE DYNAMIC ENVIRONMENT MANAGER

If you are leveraging VMware Dynamic Environment Manager™, you can also enable privilege elevation. You can remove the administrator privilege from domain users and still allow users to start certain applications as administrators. With privilege elevation, a user can start certain preconfigured applications, which the VMware Dynamic Environment Manager agent runs elevated on the local desktop, as if the user is a member of the administrators group.

The following best practices apply to VDI environments:

- Forbid any type of local authorization using domain policies. This can be especially useful for virtual desktops, which are created and deleted on demand. The task of fixing a faulty machine, which could require a local login procedure, is not an option.
- Ensure you log out as administrator from your golden VM images. A common attack technique, once a machine is compromised because the admin forgot to log out, is to dump passwords. The attacker now has those credentials and could potentially hop into an actual data center resource outside of your VDI environment. Horizon admins should regularly update the golden VM image with the latest security updates and then roll them out to updated desktop pools. Elimination of these vulnerabilities can be seen and verified within the VMware Carbon Black Cloud console.
- Reduce to a minimum a user's ability to run unsolicited applications whenever a business process allows it, perhaps going as far as deploying a default deny scenario. Given the known specifics of particular industries where VDI technology is most popular, such as healthcare and insurance, the implementation of such a scenario can be undertaken without much resistance.
- Rule out the use of Java and other command interpreters, including PowerShell and even CMD.EXE, if business processes do not explicitly rely on them. Java remains one of the most exploited components of any system, and script chains are gaining in popularity as a legitimate way of circumventing detection and even application control mechanisms.
- If the network configuration permits, use network segmentation and/or identity-based segmentation if you are leveraging VMware NSX® Data Center for Desktop within your Horizon environment. Also, enforce user-based access controls to isolate VMs from one another. In the majority of business scenarios, there is no need for VMs to see one another on the network. VMs only need access to particular servers and network services—and to the internet, if required. Such a configuration can considerably reduce the possibility of infection spreading.
- Leverage a security framework and common principles, such as Zero Trust, the principle of least privilege, or defense in depth. You must also always take into account the rapidly changing threat landscape. VDI protection should not be in any way inferior to defenses used for physical machines, especially if the environment includes accessing the public internet.
- All these protective layers provide much greater levels of security in defense of endpoints which, virtualized or not, remain the primary targets for attackers. Keep in mind that every additional security layer requires additional context and configuration, which our platform alleviates because this functionality is built in.
- Our architecture and platform also ensure high availability. In the event of loss of connectivity or a disaster recovery event, the additional security layers will not leave the machines unprotected. In addition, the system event data obtained can be stored locally for later analysis after re-establishing connection.
- We re-engineered the VMware Carbon Black Cloud sensor to be fully aware of all of the unique requirements of virtualization, and the specifics of VDI in particular, including mechanisms such as machine migration and instant clones. The VMware Carbon Black Cloud sensor is easily embedded into VM templates, allowing instant protection after clone activation.

Conclusion

VDI can be an important ingredient for protecting remote workers. Combined with VMware Carbon Black Cloud, it can offer an incredibly secure solution to the security challenges of a distributed workforce. VMware Carbon Black Cloud is optimized for the virtual desktop and the supporting infrastructure by being built to have a small footprint and yet have full prevention capabilities. With an intrinsic approach, VDI use goes beyond legacy solutions leveraging behavioral detection to protect against ransomware and fileless malware.

Whatever the future holds, VMware solutions help you to stay nimble and prepared to meet the next challenge. With the right balance of automation and control, you are equipped to meet rapid changes and evolving demands while helping employees stay secure, connected and productive.

For more information:

- Read *Intrinsic Security: A New Approach*
- Visit *pathfinder.vmware.com*
- Read the *VMware Carbon Black Cloud endpoint protection datasheet*

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Item No: 856901aq-wp-bp-hzn-vdi-crbn-black-cld-uslet 5/21