Morphisec Protector for Horizon VDI

Secure VDIs Against the Most Dangerous Cyberattacks

"Morphisec instantly blocks the most dangerous cyberattacks without impacting precious Horizon VDI resources."

MORPHISEC

VMWARE HORIZON

VMware Horizon is a modern platform for secure delivery of virtual desktops and apps across the hybrid cloud, from the market leader in software-defined data center and digital workspaces. By leveraging unique integration with trusted VMware technology, Horizon helps IT efficiently deploy and scale virtual desktops and apps from a single control plane with rapid provisioning, automation, and simplified management to extend the best digital workspace experience to end users.

MORPHISEC UNIFIED THREAT PREVENTION PLATFORM

The Morphisec Unified Threat Prevention Platform secures VMware Horizon View virtual desktops through a deterministic approach to prevention that protects Horizon VDIs from zero days, evasive malware, and other damaging cyberattacks

Your Virtual Desktop Infrastructure Needs Protecting

Organizations adopting a dynamic mobile workforce are turning to VMware Horizon virtual desktop infrastructure (VDI) to support a fluid digital workspace optimized for greater mobility and provide low-cost access to a centralized suite of applications. Horizon VDI set-ups that need agile delivery of applications to new users are often found in healthcare settings like hospitals and clinics, financial services and also in hospitality and retail stores.

For all the benefits that VDI provides, individual virtual machines booted from the hypervisor still represents another endpoint that must be secured. This issue is particularly acute with the pooled, non-persistent model of VDI. Every time a new virtual machine is booted from the golden image, it needs to be born secure.

VDIs require significant memory to operate effectively. A resource-intensive antivirus solution consumes too much processing power to secure virtual desktops without increasing costs and complexity. What VMware Horizon View users need is a non-invasive security solution that can load quickly without consuming the process memory needed to operate the virtual desktop. That's where Morphisec comes in.

Morphisec's Unique Approach to VDI Security

The lightweight architecture of Morphisec, based on Moving Target Defense is highly optimized to protect Virtual Desktop Infrastructure (VDI) environments, safeguarding not only the individual virtual desktops, but also securing the underlying VDI server. Morphisec's Unified Threat Prevention Platform prevents the unknown threats that designed to evade detection.

By morphing the underlying application memory, Morphisec blocks the most dangerous cyberattacks before the executable of the attack can cause any damage. It does so in a deterministic manner, without generating false alerts to be analyzed, via a lightweight, 2MB agent requiring no administration, no CPU, or memory consumption that are common with other antivirus and EDR endpoint solutions.

With Morphisec deployed, VMware Horizon View users are protected from:

- Zero days
- Fileless attacks
- Unpatched vulnerabilities
- Evasive malware
- In-memory exploits

The Morphisec agent also does not require cloud/network updates or even an internet connection to be operational. Paired with its minimal memory consumption, this makes the Morphisec platform uniquely suited for securing virtual desktop infrastructure.

vmware®

"The Morphisec agent also does not require cloud/network updates or even an internet connection to be operational. Paired with its minimal memory consumption, this makes the Morphisec platform uniquely suited for securing virtual desktop infrastructure."

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation with its Moving Target Defense-powered Unified Threat Prevention Platform – placing defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits.

USE CASES

Securing VDI from advanced evasive malware for all organizations.

SEE OUR SOLUTIONS IN THE VMWARE MARKETPLACE

https://marketplace.vmware.com/vsx/solutions/morphisec-for-horizon-vdi-3-5

Morphisec + VMware = Better VDI Security

Morphisec's 2MB agent is extremely lightweight, consumes no CPU and enhances security without adding any performance overhead to VMware Horizon VDI solutions. Morphisec's agent is uniquely suited for non-persistent pooled virtual desktop infrastructure deployments. The platform's lightweight memory consumption enables VMware Horizon VDI users to create virtual desktops that are "born secure" without needing to constantly check a signature database or load a machine learning algorithm.

This creates a more secure virtual desktop environment, protecting mission critical VDIs from the most damaging cyberattacks. With Morphisec, VMware Horizon VDI customers can have confidence that their virtual endpoints are secure without the high memory consumption of other security solutions.

Morphisec's Moving Target defense architecture allows customers to deploy our agent in persistent and non-persistent (pooled) mode on the VDI server as well as inside the individual virtual machines, providing reliable protection for all VDI users. As a result, individual VDI virtual machines will remain protected even against zero-day threats without a known signature.

VMWare Horizon customers also benefit from Morphisec's single installation package that supports all Windows operating systems deployed on-premises and in the cloud, and works with both 32 and 64-bit OS flavors.
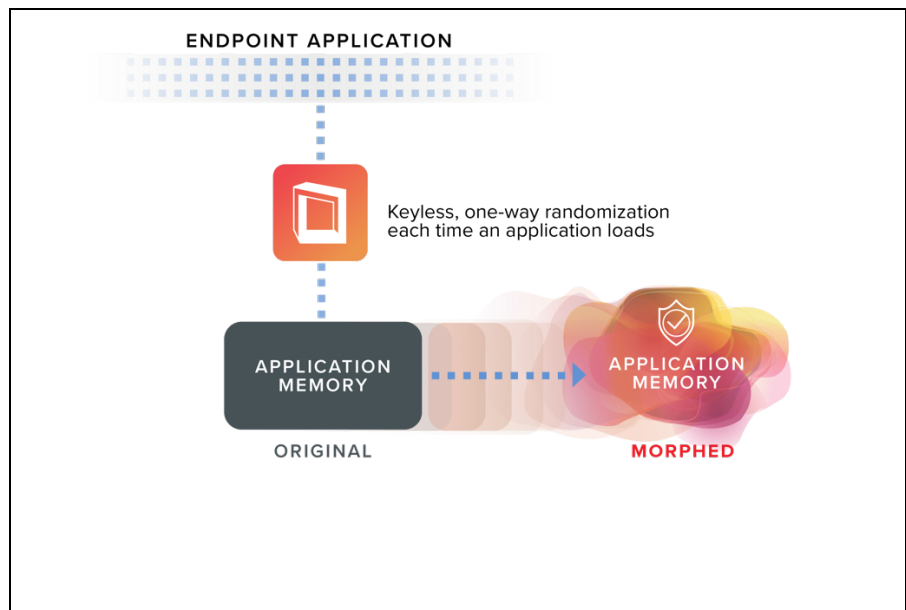

Figure 1: Morphisec morphs application memory to create a dynamic structure and prevent attackers from breaching the enterprise.

Call to Action

To learn more about how Morphisec and VMware Horizon View can enhanced VDI security, visit https://marketplace.vmware.com/vsx/solutions/morphisec-for-horizon-vdi-3-5 or contact Morphisec at info@morphisec.com

vmware®