MORPHISEC
Moving Target Defense

VDI SECURITY SOLUTION

MORPHISEC VDI SECURITY SOLUTION

Protect your Virtual Desktop Infrastructure (VDI) from zero-days and sophisticated advanced attacks. Morphisec Endpoint Threat Prevention leverages Moving Target Defense technology for a low-profile solution that helps secure your VDI without sacrificing any of its benefits.

THE SECURITY GAP IN VDI

Although Virtual Desktop Infrastructure (VDI) itself is not new, the emergence of cloud-hosted virtual desktop solutions has accelerated VDI adoption by enterprises and smaller organizations alike. And for good reason – a VDI environment provides flexible and reliable access for workers, and a centralized, efficient client infrastructure environment that's easier and more economical for IT departments to maintain and support. **However, while desktop virtualization brings many benefits, improved security is not one of them**. In fact, virtual environments widen the attack perimeter – an attack on a user's physical desktop can provide access to the central virtual desktop server.

The VDI Security Myth

Without a doubt, physical security in a VDI environment is greater: Because the laptop or PC does not contain any data, in the event of theft, no data is actually stolen. And since VDI minimizes data distribution, it is commonly used to protect against the threat of data leakage and theft in specific industries. VDI also makes data recovery easier in the event of a ransomware attack or other disaster.

Beyond these physical security benefits, as well as improved management of patching known vulnerabilities, virtual environments actually pose a greater security challenge. Security hazards such as remote access attacks and vulnerability exploits threaten both the physical desktop and the central virtual desktop server. The belief that because an image is isolated, and because an image is reset at the end of each session in a non-persistent or pooled mode, it is more resistant to end-user attacks and infections is misleading: By the time the system is rebooted, additional images on the server have already been infected. A single server can be accessed by many different users, all accessing their desktops and applications from a multitude of locations and devices. **To be considered secure, your VDI must be complemented with additional security layers, just like a traditional desktop environment.**

MORPHISEC VDI SECURITY SOLUTION

VDI Security Requirements

VDI is a complex environment to protect with many constraints that make traditional anti-virus and resource-intensive security solutions unsuitable:

1. The VDI itself requires substantial memory and CPU. Adding a resource heavy security solution can result in lower virtual machine consolidation ratios, immediately raising costs and complexity.
2. In addition, a pooled, or non-persistent environment restarts images from scratch every time. The image startup cannot support retrieving a set of attack signatures or other updates from a central server each time it boots up.

Inside the Memory Space:

The optimal security solution for VDI needs to be very lightweight and one that does not require updates.

Morphisec's Endpoint Threat Prevention protects your virtual desktops in a deterministic manner, with no false positives, via a lightweight, 1MB agent requiring no updates and no administration.

With Morphisec, your virtual endpoints are safe from all exploit-based, memory code execution in endpoint 32-bit applications such as browsers and productivity tools. It prevents evasive attacks, zero-days and attacks targeting known but unpatched vulnerabilities.

Morphisec Endpoint Threat Prevention seamlessly supports VDI environments such as Citrix VDI, VMware Horizon View and MS VDI, both persistent and non-persistent (pooled) running at the VDI level. It also supports Application Virtualization platforms such as Citrix XenApp.

Morphisec Moving Target Defense technology morphs the memory space so authorized code runs safely while malicious code is blocked and trapped. Advanced attacks are effectively stopped, and trapped, on their first attempts and without false positives.

BENEFITS AT A GLANCE

WORKS ON ANY VIRUTALIZATION PLATFORM: Supports VDI environments such as Citrix VDI, VMware Horizon View and MS VDI, both persistent and non-persistent (pooled) running at the VDI level. It also supports Application Virtualization platforms such as Citrix XenApp.

NEUTRALIZE ADVANCED THREATS: Prevents zero-days and advanced attacks, without requiring any prior knowledge of the threat form, type or behavior.

CLOSE PATCHING GAPS: Covers endpoint vulnerabilities exposed by gaps in patching cycles.

HASSLE-FREE: Installs on the fly with no maintenance required. No databases, signatures or rules to update, no logs and alerts to analyze.

NO PERFORMANCE DISRUPTION: Lightweight, state-less agent with minimal footprint, no run-time components or performance penalty, and no false positives.

REAL-TIME PROTECTION: Blocks and traps attacks pre-breach, before they can do any damage.

SOLUTION INFRASTRUCTURE

The Morphisec Endpoint Threat Prevention Solution employs an enterprise class, multi-tier architecture, which is highly scalable in terms of data and endpoints. Its components consist of:

Endpoint Protector

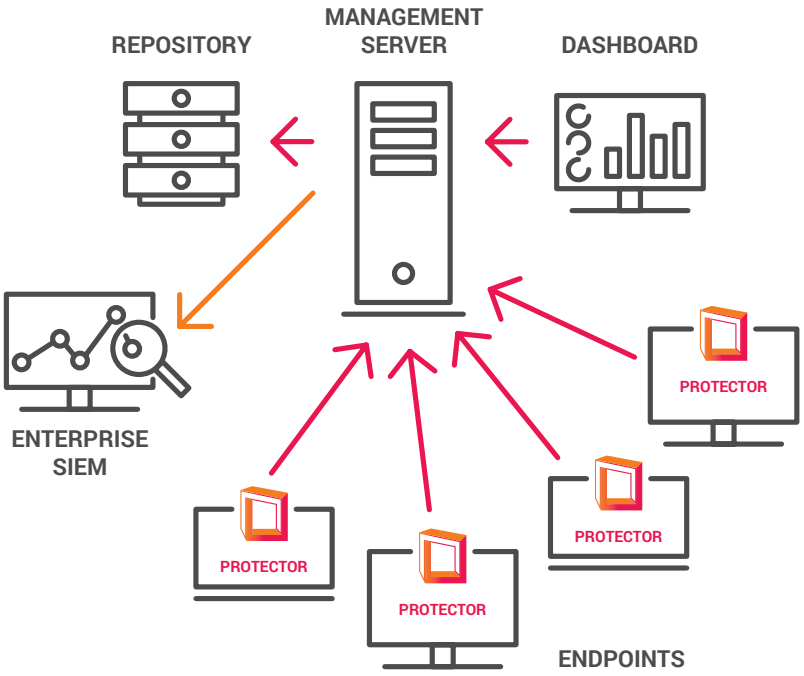
The solution centerpiece, Protector, runs autonomously on Windows-based virtual endpoints and servers, and securely communicates with an on-premise or cloud-based Management Server for reporting purposes. Protector safeguards commonly attacked applications out of the box – such as MS Office programs and web browsers – and its application agnostic nature makes it easy to add any other application.

MORPHISEC
Moving Target Defense

VDI SECURITY SOLUTION

Management Server

This component is a highly scalable set of services that can support an organization of any size, from a few endpoints up to tens of thousands, in a single or multi-site configuration. It supports complex and heterogeneous IT environments, with a structure designed to deliver fault tolerance while providing high availability. The Management Server, delivered as on-premise or cloud-based, handles management and tracking of all the endpoint Protectors, SIEM integration and dashboard generation.



Dashboard

A clear, powerful dashboard, with a set of role-based, customizable views, lets users:

Manage Protectors

- Manage endpoint *Protectors*
- Define policies and assign them to *Protector* groups
- Track *Protector* state

View Attack Data

- Get real-time visibility into attacks
- View current organizational attack status at a glance
- View high level attack information
- Gain additional insights for conducting forensic analysis
- Correlate attacks with other attacks on your organization
- Easily filter, sort and report information

Suitable for Enterprises and SMBs

Morphisec adapts to the unique business needs of both large and smaller organizations, protecting systems, intellectual property and brand without impeding operations. The solution integrates seamlessly with the organizational deployment systems and SIEMs that larger corporations rely on. Yet it does not require daily maintenance or rule setting, and the forensic data captured is not necessary for solution operation. So SMBs with limited resources get the same level of protection as the big enterprises.

Robust Self-Protection

Security applications themselves are an increasingly popular attack target for malware. Morphisec's robust self-protection includes tamper-resistant Protectors, validated servers and encrypted communication, all which use proprietary, state-of-the-art technology.

To learn more about Morphisec visit our website or call us at 1-617-209-2552!