MORPHISEC
Threat Protection for VDI

POWERED BY MOVING TARGET DEFENSE

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

The VDI Security Challenge

While virtual environments bring many benefits, improved security is not one of them. In fact, they widen the attack perimeter – a single successful attack on one virtual endpoint puts your entire VDI at risk. The fact that an image is isolated and reset at the end of each session, does not make it more resistant to end-user attacks and infections – by the time the system is rebooted, additional images on the server have already been infected.

Moreover, pooled VDI environments usually have long patching gaps as patch implementation involves the time-consuming process of creating and deploying a new golden image.

Like physical endpoints, virtual endpoints need protection, but unique constraints make traditional anti-virus and resource-intensive security solutions unsuitable for VDI environments:

- 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.
- 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.

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

Secure Your VDI Without Compromising Performance

Morphisec's Moving Target Defense technology adds a dedicated in-memory defense layer to secure your endpoints and servers for maximum VDI protection.

- Protects your VDI and business critical data from zero-days, fileless attacks and advanced, evasive malware
- Reduces your risk exposure without slowing down your systems or operations
- Stops attacks pre-breach before they can do any damage, with no IOCs or detection required
- Functions across virtual, physical or hybrid IT environments

KEY BENEFITS

PRESERVE YOUR VDI INVESTMENT

Does not lower VM density; no increase in VDI cost or complexity

STOP ADVANCED THREATS AND BROWSER-BASED ATTACKS

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

VIRTUALLY PATCH VULNERABILITIES

Keeps your VDI protected from vulnerability exploits when patches are not yet available or deployed

SET AND FORGET

Installs quickly with no system conflicts and zero maintenance – no databases, signatures or rules to update, no logs and alerts to analyze

SECURE WITHOUT DISRUPTING

Lightweight, stateless agent with minimal footprint with no run-time components and zero performance impact

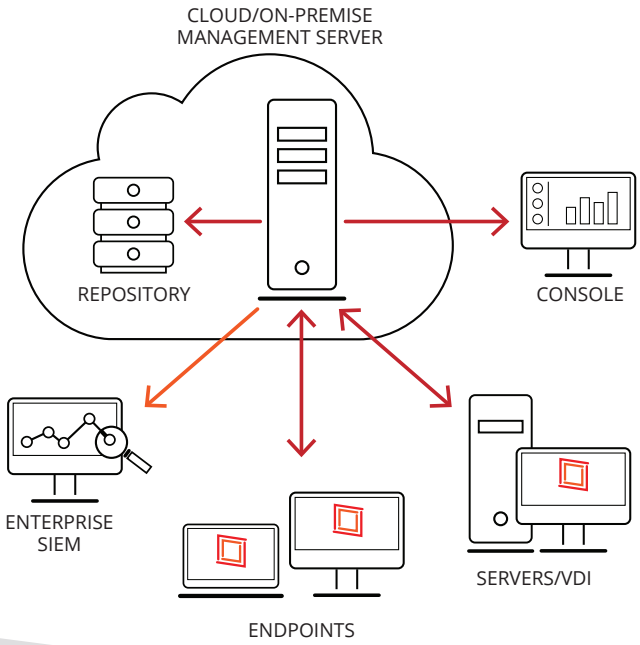
WORKS ON ANY VIRUTALIZATION PLATFORM

Supports all major VDI systems including Citrix VDI and MS VDI, both persistent and non-persistent (pooled), as well as Application Virtualization platforms such as Citrix XenApp

MORPHISEC
Moving Target Defense

Solution Infrastructure

Morphisec Endpoint Threat Prevention is a Windows Service application built on a highly-scalable, tiered architecture. It can support organizations of any size, in a single or multi-site configuration. Blocked attacks are logged, along with the full attack fingerprint, and reported to the Management Console or organizational SIEM for forensic analysis. All communication is encrypted, and connections between tamper-resistant agents and servers are mutually authenticated.



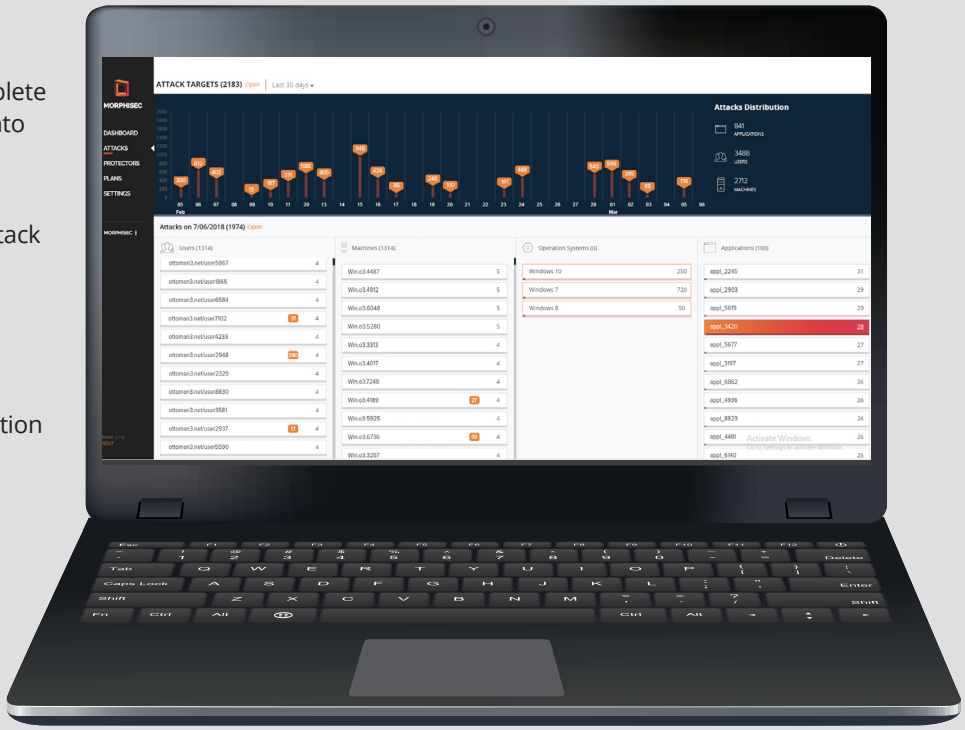
Key Components

MANAGEMENT SERVER

On-premise or cloud-based, the Management Server handles endpoint agent management and tracking, SIEM integration and dashboard generation.

MANAGEMENT CONSOLE

The Management Console provides complete system control and immediate visibility into organization threats via clear, powerful, customizable dashboards.



- Organizational risk posture based on attack and exploit prevention volume and customizable KPIs.
- Forensics and analytics for enhanced intelligence and drill-down.
- Automated reporting and threat prevention notification.
- VDI instances no longer in use are automatically decommissioned so that “ghost endpoints” do not appear.

AGENT

All prevention functions are performed autonomously by our lightweight 2 MB DLL Protector endpoint agent.

- Prevent attacks without prior knowledge — no need to update rules, signatures or databases, and no learning algorithms.
- Runs in all virtual environments, whether on-premise or cloud-based.
- Fully application agnostic — safeguards all your applications without tedious configuration.
- No runtime components and securely communicates with the Management Console for reporting and tracking purposes only.

The Only Viable Advanced Attack Prevention for Your VDI

Morphisec protects virtual endpoints from all known and unknown exploit-based, memory injection attacks in applications such as browsers and productivity tools. It prevents evasive attacks, zero-days and attacks targeting known but unpatched vulnerabilities. It does so in a deterministic manner, without generating alerts to be analyzed, via a lightweight, 2MB agent requiring no administration.

Morphisec Moving Target Defense technology continuously and randomly morphs the memory space so attacks simply cannot execute. Authorized code runs safely while threats are immediately stopped and rich forensic information is captured for teams who need it. No detection or hunting required.

Suitable for Enterprise and Mid-sized Business

Morphisec adapts to the business needs of organizations of all sizes, protecting systems, intellectual property and brand without impeding operations. Enterprise-critical features include auditing capabilities, Active Directory integration and seamlessly integrating with organizational deployment systems and SIEMs.

Morphisec's unparalleled prevention capabilities, however, do not depend on the forensic data captured. So businesses with limited resources get the same level of protection as large enterprises. The system does not require daily maintenance or rule setting. And because Morphisec has zero performance impact at run-time, it easily supports endpoints that require high performance and cannot afford rapid changes.

Supported VDI Platforms

Morphisec Endpoint Threat Prevention is a CitrixReady partner and seamlessly supports all major VDI systems including Citrix VDI, VMWare Horizon and MS VDI, both persistent and non-persistent (pooled) running at the VDI level. It also supports Application Virtualization platforms such as Citrix XenApp.

Third Party Partnerships and Integrations

- **CitrixReady partner:** Certified against the latest versions of Citrix XenApp and Citrix XenDesktop, and Citrix Azure
- **OPSWAT bronze partner:** Tested by Opswat for quality, false positives, and compatibility with over 1,000 devices from 40+ leading access control vendors
- **RSA Netwitness partner:** Certified interoperability with RSA Netwitness
- **Splunk Technology partner:** Certified Splunk Enterprise SIEM integration
- **IBM Global partner:** Certified integration with IBM QRadar SIEM
- **Additional SIEM Integrations:** McAfee Enterprise Security Manager, HP Arcsite, Rapid7 InsightIDR

"Our defense in depth security mandated Advanced Threat Prevention across our physical and VDI infrastructures. Morphisec's combination of high prevention efficacy with the lowest TCO and zero impact on user experience, made our choice clear."

— Adrian Asher, CISO, London Stock Exchange

Third-party Validation

ESG Enterprise Strategy Group

"Morphisec improves security efficacy, while streamlining security operations by reducing security alert volumes and freeing up staff to focus on more pressing strategic initiatives."

— FROM ESG REPORT ON ADVANCED PREVENTION FOR ENDPOINT SECURITY

SE Labs Gartner CRN *CRN NAMES MORPHISEC ONE OF THE TOP 10 CYBERSECURITY STARTUPS OF 2018*

MORPHISEC Moving Target Defense

www.morphisec.com