MORPHISEC
Server Threat Prevention

Your server is one of the most strategic layers in your organization's infrastructure; it's also a prime target for hackers. Morphisec is built on Moving Target Defense to proactively prevent the most dangerous attacks on your physical and virtual servers, without reliance on signatures, attack patterns or behavioral analysis.

Protect Your Servers No matter Where They Run

Morphisec Server Threat Prevention provides the strongest protection for your physical or virtual servers, whether running on-premise or in the cloud. Attackers can use readily available malware toolkits and other means to gain access to your servers, steal administrator credentials, launch malware, and move undetected through your network. Virtualized environments are particularly at risk as they don't have the security capabilities of physical servers, and compromised virtual server credentials provide immediate unchecked privileges for all virtual machines. Morphisec employs patented Moving Target Defense technology to block attacks against both physical and virtual servers and safeguard administrative credentials.

Prevent Attacks on Administrators

Administrators run common user applications while logged into the server. They browse to sites to download patches or tools, and access documents and other important information. Unfortunately, these files and applications may also contain exploited vulnerabilities and threats. In such cases the attack vector is even more critical than on an endpoint, since an attacker can gain administrative privileges directly on a server inside the data center.

Stop Lateral Movement Breaches

Servers are also vulnerable to exploits such as the Server Message Block (SMB), the transport protocol used by Windows machines for numerous purposes such as shared access to files, printers and serial ports, and communication with remote Windows services. When this vulnerability is exploited for example, an encrypted payload containing the stager for the malware may be loaded on the remote machine. The service then uses the vulnerability to gain access to a remote machine and deliver the malware payload.

Once inside, the attacker can move laterally, stealing credentials to infiltrate other servers. Hackers create and sustain persistent access across the network, gaining higher privileges as they move. This, in turn, enables them to have access to servers, which contain valuable corporate information.

KEY BENEFITS

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 servers protected from vulnerability exploits when patches are not yet available or deployed

SET AND FORGET

Rapid, easy rollout with no system conflicts and zero maintenance – no databases, signatures or rules to configure and update, no logs and alerts to analyze

NO SYSTEM IMPACT

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

MAINTAIN BUSINESS CONTINUITY

Minimizes organizational risk while preserving ongoing operations with no interruptions for updates or scans

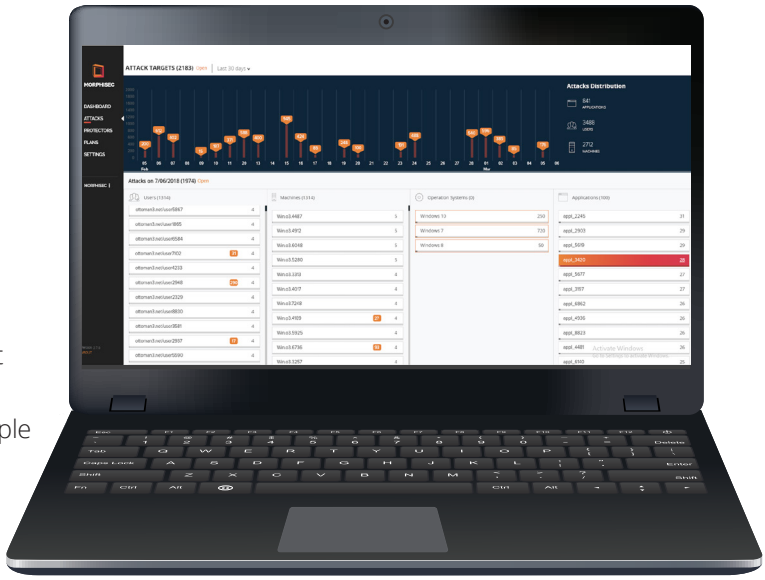
CUT SECURITY OPERATIONAL COSTS

Does not generate false alerts, no need to investigate, analyze or re-mediate. Blocks attacks pre-breach, before they can do any damage

MORPHISEC
Moving Target Defense

Secure Virtual Application Servers

Despite the accelerated adoption of virtualized platforms and cloud-based solutions, security for these environments remains inadequate. Most endpoint security solutions require updates and consume CPU resources that make them unsuitable for virtualized environments, while VDI vendor security solutions don't provide enough protection. At the same time, virtual environments face substantially more risk as more people in various roles have access to the server, thereby increasing the threat exposure.



Simple to Rollout and Operate

Morphisec's Server Threat Prevention is rapidly deployed, with rollout is measured in hours and days. The solution requires near zero maintenance and needs no configuration or tuning, ensuring very low ongoing costs. There is no monitoring or collection of personal data, a big plus for privacy aware companies.

As Morphisec does not generate false positives, there is no associated alert fatigue or wasting resources on attacks that never occurred.

Morphisec is extremely lightweight and does not require updates, making it optimal for VDI environments. Morphisec Server Threat Prevention is a CitrixReady partner and seamlessly supports all major VDI solutions such as 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.

Moving Target Defense for Maximum Protection

Morphisec Server Threat Prevention is the only solution based on Moving Target Defense, which prevents the execution of evasive unknown threats and zero-days that other technologies can miss.

Moving Target Defense technology morphs the runtime environment so authorized code runs safely while malicious code is blocked and trapped. By preventing attacks before a breach ever occurs, Morphisec changes the security economics, cutting costs while minimizing disruption and damage to business.

Morphisec Server Threat Prevention protects your servers from all exploit-based, memory injection attacks in your endpoint 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, easy to install 2MB agent requiring no administration.

Schedule a demo: demo@morphisec.com

MORPHISEC
Moving Target Defense

www.morphisec.com

© 2018 Morphisec Inc.