MORPHISEC
Moving Target Defense

DATA SHEET

MORPHISEC ENDPOINT THREAT PREVENTION

Protect your business from zero-days and advanced attacks that target your unpatched vulnerabilities. Morphisec's Moving Target Defense technology camouflages your applications and web browsers and traps any attempts at access. Your endpoints, once a site of weakness, become an impenetrable defense.

THE SECURITY GAP

Attackers are more sophisticated, creative and persistent than ever, releasing millions of malicious threats each year. They use their profound knowledge of the target environment to develop stealthy, highly-targeted attacks, most notably Advanced Persistent Threats (APT) and zero-days, while at the same time drawing from unpatched vulnerabilities as much as ten years old.

To add to the destructiveness, attackers use polymorphism, obfuscation, encryption and other advanced techniques to evade security mechanisms and avoid detection. Under the traditional Detection & Remediation paradigm – even with sophisticated behavioral-analysis based solutions – applications remain vulnerable from the time a new attack is launched until it is discovered, a solution developed, and a patch deployed.

TRADITIONAL AND "NEXT-GENERATION" SOLUTIONS

Endpoint protection solutions generally use one or a combination of the following:

- Tools that require knowledge of the attack's signature or an understanding of the attack's behavior or pattern, such as anti-viruses, gateways and Host Intrusion Prevention systems. Such systems are easily evaded by zero-days or polymorphic attacks.
- Next generation anti-viruses, utilizing static analysis and artificial intelligence or machine learning capabilities. These rely on known attack patterns, and can detect known attacks, but not zero-days.
- Application Control and similar tools. These require significant configuration effort – configured too tightly and they cause false positives and impact performance, too loosely frees employees to perform business unimpeded but attacks can go undetected.
- Containment solutions such as sandboxes. These can be a working solution for applications that do not need to immediately connect to the internal network, but are easily evaded by attackers specifically recognizing sandboxes.
- Detection and remediation tools. Often effective in detecting attacks, but they require intensive analysis to distinguish valid attacks from the numerous false-positive alerts, costing the organization time, resources and impairing efficient business.

MORPHISEC
Moving Target Defense

DATA SHEET

MORPHISEC'S RADICALLY DIFFERENT APPROACH

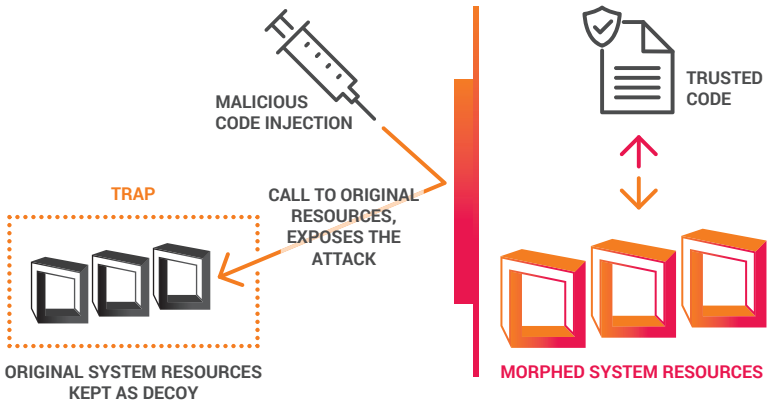
Morphisec shifts the security paradigm with proactive, early prevention that uses the hackers' tactics to beat them at their own game. Its Moving Target Defense technology morphs the runtime environment so authorized code runs safely while malicious code is blocked and trapped. By preventing attacks before a breach ever occurs, Morphisec changes the security economics, cutting costs and minimizing disruption and damage to business.

Morphisec Endpoint Threat Prevention protects your endpoints from all exploit-based, memory injection attacks in your endpoint 32-bit and 64-bit 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, with no false positives, via a lightweight, 2MB agent requiring no administration.

How it works:

1. As an application loads to the memory space, the polymorphic engine morphs the inner structure of the process, its calls to library functions, and library addresses. Each run is unique, per process and per process instance. This makes the memory unpredictable to attackers.
2. Simultaneously, the process is made aware of the legitimate morphed application structure. The application runs as usual with the morphed structure while Morphisec keeps a dummy of the original to use as a trap.
3. Malicious code fails to execute since it lacks knowledge of the new structure and cannot access any of the functions it needs: The kill chain is stopped as it begins. Attacks continue to target the original structure, unaware that it's now a decoy.
4. Attacks on the dummy structure are by definition malicious and find themselves trapped. Blocked attacks are logged and reported to the Morphisec Management Dashboard or the organizational SIEM, while rich forensic attack and memory data is sent to additional organizational systems for forensics analysis.

Inside the Memory Space:



BENEFITS AT A GLANCE

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

CLOSE PATCHING GAPS: Constant management of security patches wastes time, dollars and resources, and delays increase risk. Morphisec covers endpoint vulnerabilities exposed by gaps in patching cycles.

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

NO PERFORMANCE DISRUPTION: Extremely lightweight agent active only at load-time, minimal footprint, no run-time components or performance penalty, and no false positives.

AUTONOMOUS: Protects employee machines in and outside the company network.

REAL-TIME PROTECTION: Blocks and traps attacks pre-breach, before they can do any damage. Protection does not depend on server connectivity.

CHANGE ATTACK ECONOMICS: Turns the tables so the attacker must now chase the target. Eliminates the costs associated with hunting for attacks, investigating false positives and damage remediation.

SOLUTION INFRASTRUCTURE

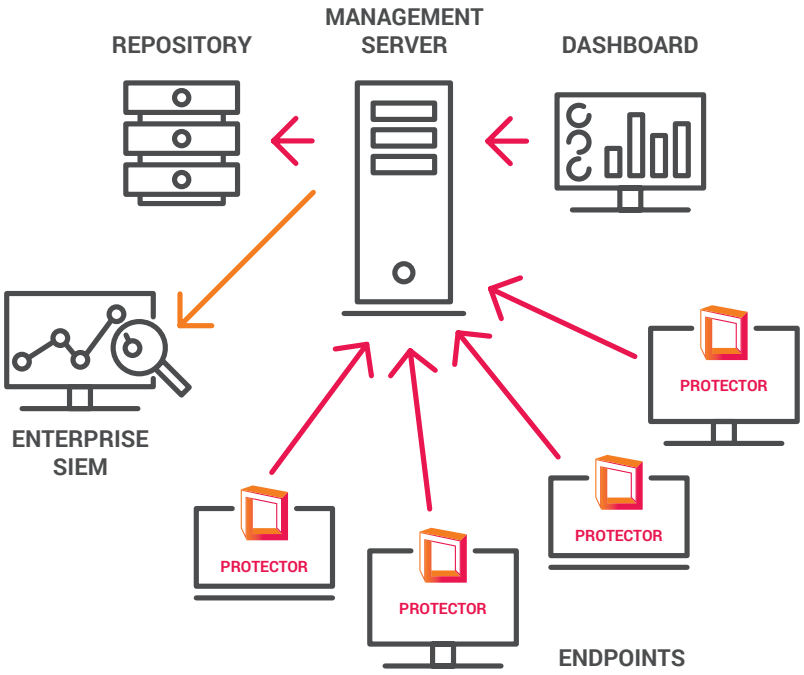
The Morphisec Endpoint Threat Prevention Solution employs an enterprise class, multi-tier architecture, which is highly scalable in terms of data and endpoints. Its components consist of:

Endpoint Protector

The solution centerpiece, *Protector*, runs autonomously on Windows-based endpoints and servers, physical or virtual, 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 or all applications used by the customer.

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 Medium Businesses

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 businesses with limited resources get the same level of protection as the big enterprises. And because Morphisec has zero performance impact at run-time, it easily supports endpoints that require high performance and cannot afford rapid changes.

Being very lightweight and not requiring updates, makes Morphisec an optimal security solution for VDI. 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.

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.

TECHNICAL REQUIREMENTS

Endpoint Protector	Management Server On-Premise
Hardware Requirements	
Hardware recommended by Microsoft to run the software below.	■ Intel 64-bit Pentium 2 CPU 8 core hyperthreading, Recommended RAM 8G, minimal 4G. ■ Disk size: Recommended 1T, minimal 250 G ■ Disk: Recommended: Raid 5 with backup. Minimal: Raid 0
Software Requirements	
A physical or virtual image running the following: ■ Microsoft Windows 7 (32-bit and 64-bit) ■ Microsoft Windows 7, Service Pack 1 (32-bit and 64-bit) ■ Microsoft Windows 8, 8.1 ■ Microsoft Windows 10 ■ Microsoft Windows Server 2008 R2, 2012/2012 R2, 2016 ■ Microsoft .net 4.5 or above	■ A physical or virtual image running Microsoft Windows Server 2012 R2

ABOUT MORPHISEC

Spearheaded by leading Israeli security experts, Morphisec provides the ultimate threat prevention by making sure attackers never find the targets they seek.

Morphisec fundamentally changes the cybersecurity scene by shifting the advantage to defenders, keeping them ahead of attacks with moving target defense.

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