ESG Technical Validation First Look

Efficient Efficacy with Morphisec Advanced Threat Prevention Platform

Date: February 2019 **Author:** Jack Poller, Senior Analyst

Cybersecurity Challenges[1]

53% have a *problematic shortage of cybersecurity skills*.

40% believe *strengthening cybersecurity* will drive the **most technology spending** in their organization over the next 12 months.

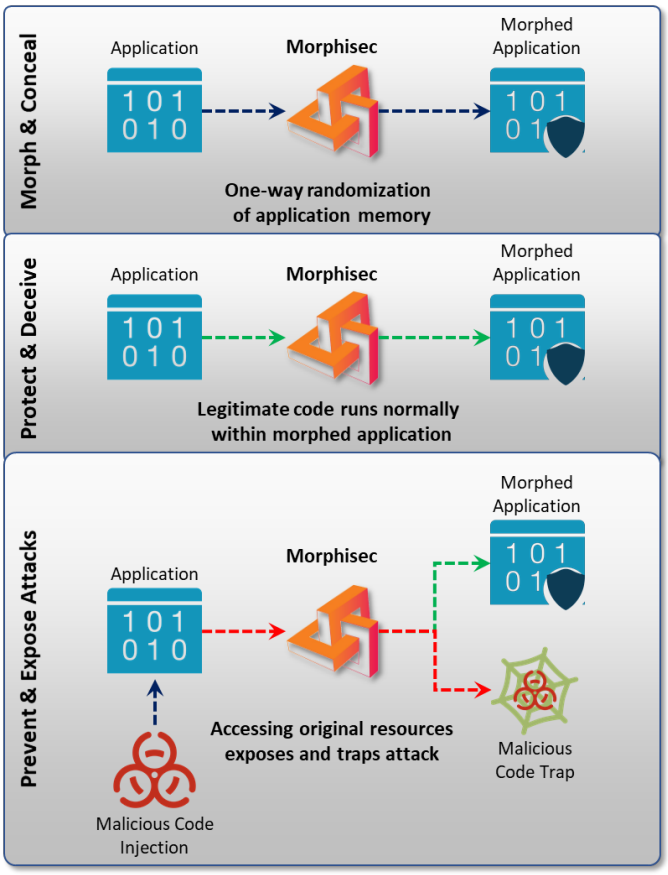
The ever-increasing volume and velocity of threats has made cybersecurity one of the top IT concerns. However, IT's drive to improve the business' security posture is complicated by the global cybersecurity skills shortage. As a result, organizations evaluating their options for strengthening cybersecurity are seeking more efficient and effective tools. Indeed, according to ESG research, 46% of surveyed IT and cybersecurity decision makers ranked effectiveness as the most important consideration when investing in cybersecurity products or services—by far the most often cited consideration.[2]

Morphisec Advanced Threat Prevention Platform

Morphisec, an Israeli-based cybersecurity vendor, provides advanced threat prevention defenses while maintaining operational simplicity. ESG validated its Threat Prevention Platform and this First Look provides preliminary results based on a comprehensive set of testing criteria including accuracy, efficacy, and operational efficiency.

Key Observations

- Morphisec covers an expansive range of unknown attacks and exploits with a prevent-first approach.
- Morphisec deploys and operates with efficiency.
- Morphisec significantly alleviates false positives and alert fatigue with a high level of preventive accuracy.
- Morphisec was effective in preventing fileless, zero-day exploits, and evasive malware without the need for IOCs.



How Does Morphisec Work?

Morphisec designed its platform to prevent fileless, zero-day exploits and evasive malware at the earliest stage of attack without the need for IOCs. Using a lightweight, small-footprint agent that deploys into existing security infrastructure, Morphisec blocks threats pre-execution, preventing damage and lateral movement.

Morphisec's "moving target defense" employs attacker stealth tactics—deception, obfuscation, modification, and polymorphism—to preemptively prevent attacks. When an application loads into memory, Morphisec's polymorphic engine employs keyless, one-way randomization to transform the process structure, relocating libraries, functions, variables, and other data segments.

[1] Source: ESG Research Report, *2019 Technology Spending Intentions Survey*, February 2019.
[2] Source: ESG Master Survey Results, *Cybersecurity Landscape: The Evolution of Enterprise-class Vendors and Platforms*, October 2018.

Each application instance is uniquely mutated, cloaking the application and making application memory unpredictable to attackers. Legitimate application code is updated with the location of its resources while a lightweight skeleton of the original application structure is maintained as a trap.

Malicious code injected into the application targets the original memory structure and gets captured by Morphisec, while the transformed application runs normally using the transformed application memory. Attacks are prevented, trapped, and logged, along with rich forensic data for analysis.

Morphisec's moving target defense neutralizes advanced attacks and browser-based threats at the earliest stage, independent of threat type, technique, or behavior. Deploying Morphisec provides real-time protection and comprehensive patch gap coverage by preventing exploitation of unpatched vulnerabilities. The Morphisec agent is active only at application load time, providing security without impacting performance and requiring no management.

ESG Validation Highlights

ESG validated Morphisec's capabilities and we were impressed with Morphisec's ability to instantly prevent a broad range of network, email, web, and physical threats without impacting performance.

Moving Target Defense

- ESG observed Morphisec's advanced prevention capabilities across detonated attacks and exploits of various threat categories. Our test environment used a C2 server dynamically generating attacks targeted at an up-to-date Windows 10 Enterprise workstation running Windows Defender and a popular commercial antivirus solution.
- The advanced attack started with a phishing email directing the target user to a website. The site automatically downloaded a VBS script, which passed Defender and AV scanning. The script used a variety of TTPs, including dot-net process hollowing to give the attacker a shell running on the target system. Leveraging additional TTPs, the attacker erased all traces of its presence from the system while gaining local administrator privilege, and then moved laterally to attack the domain controller, gaining domain administrator privilege.
- After installing Morphisec on the target, we retried the same attack. This time, Morphisec immediately prevented the process hollowing attempt and displayed a Win10 notification. The attack failed benignly, preventing infection or damage to the system, with no interruptions in operations or impact on performance.
- Morphisec's moving target defense prevented advanced attacks from crucial attack vectors, including email, web, fileless/in-memory, malware, scripts, and kernel. These attacks employed a variety of TTPs, including exploitation, macro, OLE code injection, reflective loading, exploit kits, drive-by campaigns, code injection, process hollowing, self-modifying code, and user-mode code injection from the kernel.
- ESG observed that Morphisec's threat prevention effectiveness reduced or eliminated the need to monitor web and network traffic for threats. Process monitoring could also be eliminated since Morphisec protected processes from buffer, integer, and stack-heap overflow and overrun; type confusion; use-after-free; and other exploitation methods.
- While static and runtime detection require known data to classify similar attacks, Morphisec quickly prevented unknown attacks when the attacks tripped over Morphisec decoys placed during code morphing at the launch of each process instance—attack detection was not necessary for prevention of the attack.
- We could see from Morphisec's attack analytics that the system captured extremely detailed, forensic intelligence including the full execution stack and memory access.

First Impressions

The traditional approach to strengthening cybersecurity is to layer on more tools to address perceived or existing weaknesses. This approach fails as it forces organizations to expend more scarce resources—time, money, effort, and, most importantly, staff—and creates an ever-more complicated environment. Instead, organizations need to focus on tools that are effective at preventing threats and have efficient implementations.

ESG's testing showed Morphisec to be both efficient and effective when tested against a range of advanced threats in multi-stage targeted attack campaigns. Tested threat vectors included ransomware, trojans, RATS, malware, downloaders, and others targeted at endpoints, web, and email. Threats were blocked pre-execution, preventing memory infiltration and lateral movement. ESG observed that in all cases the termination of malicious processes occurred in real time giving operators an immediate preventative capability against unknown, fileless, and zero-day threats.

The lightweight, small-footprint Morphisec agent demonstrated exceptional efficiency, installing quickly and running only at application instance launch, imposing no application performance penalty. Prevented threats were logged with a trove of forensic data. Morphisec's moving target defense deployed decoy code, ensuring that all detections and preventions were valid. This feature avoids false positive alerts and alert fatigue.

Morphisec's moving target defense—randomizing, morphing, and moving memory resources to prevent advanced attacks—obviates the need for separate detection and prevention solutions. If you're searching for an efficient and effective threat prevention solution, ESG suggests you consider Morphisec.