Morphisec Unified Threat Prevention

PROTECT AGAINST THE UNKNOWN WITH MOVING TARGET DEFENSE

POWERFUL PROTECTION THAT'S DECEPTIVELY SIMPLE

Today's advanced cyberattacks hit quickly and are engineered to evade detection-based forms of defense. Security teams and their tools are left trying to constantly catch up. Morphisec doesn't have to.

Morphisec's Unified Threat Prevention platform, based on patented Moving Target Defense technology, prevents unknown advanced threats at the earliest stage of attack, with no detection required. It blocks zero-day exploits, evasive malware and fileless attacks pre-execution, without the need for IOCs — before any damage happens.

Morphisec deploys easily into existing security infrastructure, does not generate alerts for analysts to chase, and does not impact system or network performance. It safeguards PCs, servers and virtual desktop infrastructure (VDI) from the most dangerous threats, while also protecting your security bottom line.

BUILT TO DEFEAT FILELESS ATTACKS

Fileless, in-memory attacks evade detection by co-opting legitimate system resources and are 10x more likely than malware attacks to breach your company. Morphisec pre-emptively prevents such attacks by making these resources inaccessible.

EARLIEST-STAGE, PROACTIVE THREAT PREVENTION

Morphisec's Moving Target Defense is an offensive prevention technology that shifts the balance of power to defenders by making attackers do the chasing. Its polymorphic engine continuously and randomly moves and morphs memory resources so attacks simply cannot execute. Threats are immediately stopped and deterministically revealed as malicious. Rich forensic information is captured for teams who need it.

- Prevent advanced threats and zero-days immediately and completely. No detecting, guessing or hunting for missed attacks.

- Set it and forget it. Non-invasive agent with zero performance degradation and no updates required.

- Reduce false-positives. No alert fatigue or wasting resources on attacks that never occurred.

- Replace legacy antivirus with a far more secure alternative at no additional cost via Morphisec's Defender AV integration.

BENEFITS

STOP ADVANCED UNKNOWN THREATS
Prevents attacks at the earliest stage, independent of threat type, technique or behavior

VIRTUALLY PATCH VULNERABILITIES
Keeps your organization protected from vulnerability exploits when patches are not yet available or deployed

CUT SECURITY OPERATIONAL COSTS
Does not generate false alerts, no need to investigate, analyze or remediate

GET REAL-TIME END-TO-END VISIBILITY
Optics into all endpoint events and full chain of attack

COMPENSATING CONTROL
Acts as a Windows 7 compensating control for compliance purposes

SIMPLE TO OPERATE
Single agent works on and offline, installs quickly, requires no management and has zero performance impact

MORPHISEC
Moving Target Defense
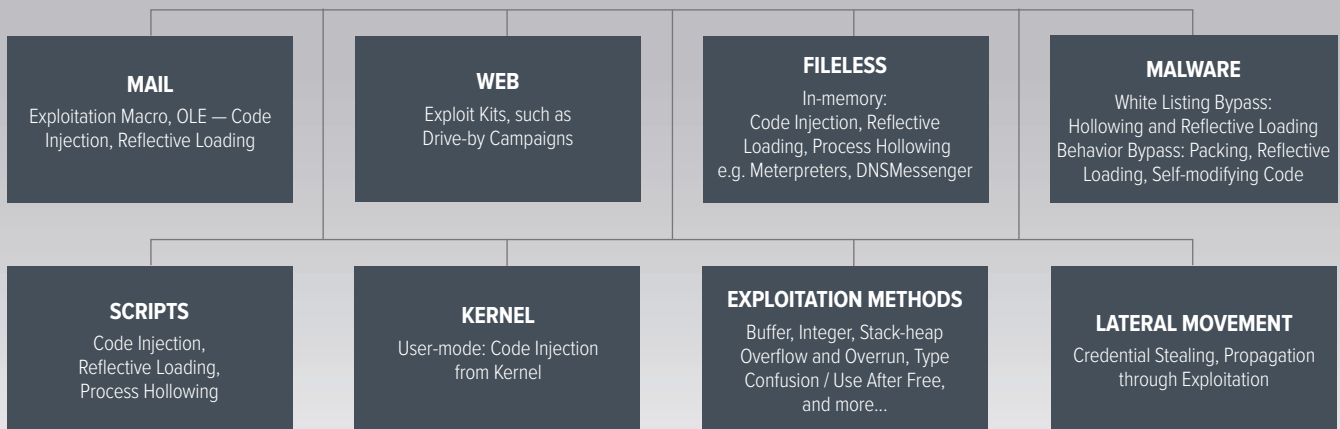
SECURITY THAT MAKES IT DEPARTMENTS HAPPY

Cut your security risk without cutting into business operations or productivity. Morphisec is built from the ground up to align business and security needs.

Morphisec Unified Threat Prevention is a single agent solution with no run-time components and zero performance impact. It runs autonomously so your endpoints are always protected, even when not connected to your company's network. An on-premise or cloud-based management console provides end-to-end visibility into organization threats and effortless control over settings and functionality.

- Prevent threats without continuous monitoring or generating reams of data.

- Reduce IT complexity and protect business continuity.

- Protect in-between patching cycles; employ as a Windows 7 compensating control.

- Gain visibility into all endpoint attacks including Microsoft Defender AV events.

- View full attack timeline and correlate events to make smarter, faster decisions.

- Easily deploy across virtual, physical or hybrid IT environments.

PREVENTS THE MOST ADVANCED ATTACK VECTORS

MAIL
Exploitation Macro, OLE — Code Injection, Reflective Loading

WEB
Exploit Kits, such as Drive-by Campaigns

FILELESS
In-memory:
Code Injection, Reflective Loading, Process Hollowing e.g. Meterpreters, DNSMessenger

MALWARE
White Listing Bypass:
Hollowing and Reflective Loading
Behavior Bypass: Packing, Reflective Loading, Self-modifying Code

SCRIPTS
Code Injection, Reflective Loading, Process Hollowing

KERNEL
User-mode: Code Injection from Kernel

EXPLOITATION METHODS
Buffer, Integer, Stack-heap Overflow and Overrun, Type Confusion / Use After Free, and more…

LATERAL MOVEMENT
Credential Stealing, Propagation through Exploitation

Schedule a demo now: demo@morphisec.com

MORPHISEC
Moving Target Defense

www.morphisec.com

© 2019 Morphisec Inc.