MORPHISEC
Moving Target Defense

FACT SHEET

HOW ARE MORPHISEC AND EMET DIFFERENT?

EMET and Morphisec address the same problem, preventing exploits. The similarities end there. Here's a summary of their differences.

EMET - (Enhanced Mitigation Experience Toolkit) is a toolkit used for exploit prevention. It has several flaws, namely:

a) Rules must be defined. EMET uses a set of explicit, predefined rules to prevent specific types of attacks (rule per set of attacks)
b) Applications must be configured to work with it
c) EMET has compatibility issues with several applications as it blocks behaviors those applications require.
d) It requires a large amount of RAM, the system must be rebooted to apply any changes and it significantly impacts performance
e) It does not provide forensic information on blocked attacks (*)
f) It can be bypassed in Windows 7, 8 and 10 (**)

Morphisec takes a completely different approach:

a) No rules to define
b) No prior knowledge of the attack required - any access to non-morphed memory area is malicious by default
c) Application agnostic – works with all applications
d) Compatible with most existing security solutions
e) No run-time components and no performance penalty
f) Provides detailed forensic information that can be used by SIEMs or other security products
g) Provides insight into the current security status of the organization
h) Enterprise-grade security solution

* LACK OF FORENSIC INFORMATION

EMET is not intended to deliver visibility into organizational security or management of security events; it stops attacks without providing details. As a result, material insights are missing and organizations cannot form a holistic view. In comparison, Morphisec operates under the premise that an organization requires a continuous and lateral defense. Morphisec provides key attack forensic information such as timeline, organizational spread, user and application dimensions.

** BYPASSING EMET

In addition to the complexity of configuration, management, and performance degradation, EMET can be bypassed by various methods. For example:

- Executing 64bit shell-code inside 32-bit process
- Disarming EMET through unhooked methods
- Utilizing EMET.dll to bypass ASLR and hooking
- For interested readers, here are some links to documented EMET bypasses:
  - https://threatpost.com/latest-emet-bypass-targets-wow64-windows-subsystem/115224/
  - http://blog.sec-consult.com/2015/06/bypassing-microsoft-emet-52-neverending.html
  - http://blog.sec-consult.com/2014/11/bypassing-microsoft-emet-51-yet-again.html
  - https://bromiumlabs.files.wordpress.com/2014/02/bypassing-emet-4-1.pdf