MORPHISEC
Moving Target Defense

WHAT'S NEW – V.2.0

MORPHISEC ENDPOINT THREAT PREVENTION

WHAT'S NEW IN VERSION 2.0

The threat landscape evolves constantly and rapidly. Today, 40% of cyberattacks can no longer be stopped by detection solutions at the network or endpoint, whether signature, behavior or AI based. In the first half of 2017 alone, organizations have had to cope with a slew of new tactics: a surge in evasive, fileless attacks, record breaking attack propagation speeds and the rise of 64-bit attacks. Version 2.0 of Morphisec's flagship solution, released in July 2017, gives security teams the answer to tackle these trends as well as unknown threats to come.

Unlike the complex and still inadequate solutions coming from incumbent and new vendors alike, Morphisec upholds the concept of a simple, effective, cost-efficient prevention stack. Whether you use Defender, any anti-virus, an EDR or a NewGen tool, Morphisec provides the crucial memory-defense layer that these solutions lack. It prevents the most dangerous and destructive threats while preserving business efficiency and reducing operational risk. Version 2.0 of Morphisec Endpoint Threat Prevention brings simpler administration and provides broader protection for all 32 and 64bit applications running on Windows workstations and servers, whether physical or VDI. Expanded threat intelligence capabilities give security teams instantaneous visibility into threats and business risks and the means to share these findings across departments and stakeholders.

HIGHLIGHTS OF THIS VERSION INCLUDE:

- **Protection for a broader range of environments and attack vectors**
  - **Protection for 64-bit applications**
  - **Morphing of additional memory sections** provides expanded protection including prevention of Eternal Blue / Double Pulsar
- Revamped attack dashboards
- More efficient distribution of security intelligence across stakeholders
- Streamlined console-based administration

EXPANDED SYSTEM AND ATTACK COVERAGE

Fileless, or in-memory, attacks hijack legitimate OS applications and processes to carry out their malicious work, leaving no detectable traces. They are one of the fastest growing and most effective threat vectors – according to the 2016 Verizon Data Breach Report, 53% of successful breaches do not involve malware. Morphisec's memory morphing technology was developed specifically to prevent these types of attacks, without affecting existing applications. The 2.0 release of Morphisec Endpoint Threat Prevention (ETP) extends this model to prevent 64-bit attacks and new attack vectors, including DoublePulsar.

- **PREVENTS 64-BIT ATTACKS.** 64-bit Windows operating systems now make up a majority of the OS market. As users transition to 64-bit applications, attackers are developing more and more 64-bit threats. Morphisec ETP now protects all 64-bit applications so whether browsing in Google Chrome or using 64-bit Excel, you are protected.

- **ADDITIONAL SPECIFIC, TARGETED MEMORY MORPHING** provides protection against a wider range of attacks, including attacks exploiting the **Eternal Blue vulnerability** or establishing the **DoublePulsar backdoor** used in spreading WannaCry, "Petya/notPetya" and other threats. Morphisec ETP prevents the **initial infiltration as well as its propagation** – stopping both payload execution and the kill chain along the delivery framework – with no knowledge needed of the threat form, type or behavior.

- **New hardening mechanisms** provide better protection for Morphisec components.

FROM DATA TO INSIGHT

ATTACK DASHBOARDS

Revamped Attack-Overview and Single-Attack-View dashboards deliver better and deeper attack insight in a more readily visible manner. Understand organizational threats and assess risks with minimal time spent interacting with the Morphisec management console.

- View high level attack information at a glance
- Slice and dice attack data for easier and more thorough analysis
- Access richer attack information, including:
  - Parent process information
  - Command line string
  - SHA256 signature, replacing the previous MD5 hash
  - Contextual information about similar attacks
- Define custom time frames for the attack time filter in addition to pre-defined periods

ATTACK REPORTS

Version 2.0 of Morphisec ETP contains new Attack Report capabilities to facilitate security collaboration across the organization. Keep stakeholders in various departments informed of attacks prevented by Morphisec along with relevant details. Define custom email lists and schedule Attack Reports for automatic distribution.

MANAGEMENT AND CONFIGURATION - SIMPLER THAN EVER

DASHBOARDS

Dashboard upgrades improve flexibility and further simplify configuration and management. Changes include more filter control in the Protector dashboard and usability enhancements, such as flagging of mandatory input fields and explanatory text for selected fields.

CONSOLE-BASED ADMINISTRATION

Access administration settings via the Management Console for even easier and quicker configuration and management:

- SIEM settings
- Active Directory configuration
- Report distribution configuration
- Protector uninstall settings
- Manage repository server connection

SIEM

Enhanced Morphisec ETP SIEM integration seamlessly fits with any organizational SIEM view and process:

- Support for Common Event Format (CEF)
- Custom select attack fields to be retrieved by the SIEM for further correlation or analysis

MANAGEMENT SERVER INSTALLATION

An improved Management Server installer incorporates streamlined installation of default configurations.

