CYLANCE

CylancePROTECT+ MemoryProtection

Memory Protection Without Configuration Complexity

CylancePROTECT is the world's first math- and machine learning-based endpoint protection product that detects previously "unknown" malware and prevents it from executing. It operates by analyzing potential file executions for malware in less than 100 milliseconds. PROTECT detects and prevents file exploitations from delivering their malicious payloads in both the Operating System (OS) and memory layers.

PROTECT's memory protection abilities are similar to those found in modern host intrusion prevention systems, but without the configuration complexity. Memory protection adds an additional layer of security and strengthens the OS's basic protection features like data execution prevention, address space layout randomization and enhanced mitigation experience toolkit.

In many breach events, a benign process is initially exploited by malicious payload code. The most common incidents involve a user browsing to a malicious website or a user executing a malicious document. When this occurs, the attacker's payload code executes in the memory of the browser or application without attempting to create or execute a new malicious executable. When deployed on servers, PROTECT's memory protection capabilities prevent the exploitation of many of the most common classes of vulnerabilities, such as exploits for buffer overflows and uses-after-free.

CylancePROTECT's memory protection module is comprised of an agent dynamic-link library loaded into each protected process, and a service component to supply configurations, receive information, and respond to events. The agent hooks various user-mode application program interface (API) functions in order to maintain state and watch for certain hard-coded behaviors considered to be indicative of a compromise. Whenever such a behavior is detected, an event is communicated to the service before the hooked API function is allowed to complete. The service then responds with an action for the agent to take, such as:

- Ignore the violation and let it execute
- Alert on the violation, but let it execute
- Block the violation and send an alert
- Terminate the process completely

These actions are easily configured in a policy maintained by the PROTECT administrator. The memory protections are effective for both 32- and 64-bit processes and are designed to protect without imposing a heavy performance overhead.

+1 (877) 973-3336
sales@cylance.com
www.cylance.com
18201 Von Karman, Ste. 700, Irvine, CA 92612

CYLANCE