Combating the Scourge of Fileless Attacks

What Is a Fileless Attack?
Fileless attacks originally described threats existing and operating exclusively in volatile memory. The term later evolved to include threats that maliciously utilize legitimate system resources without writing new files on disk. Today, any cyber attack using fileless elements within the attack chain may also be described as fileless.

These kinds of attacks can be recognized by the following traits:

- **Memory Resident**
  Malware is memory resident instead of residing on disk.

- **Script Based**
  Script-intensive malware uses techniques to launch itself and to assist with attacks.

- **Exploits Resources**
  Malware exploits resources like PowerShell, WMI, and other legitimate Windows admin tools to conduct activities.

- **System Registry**
  Malware achieves persistence through modification of the system registry.

How do you combat a fileless attack?
The key to defeating fileless malware is to deny it system resources, such as with a combination of tools found in CylancePROTECT® and CylanceOPTICS®.

**Script Management**
Decide when, where, and how scripts are used.

By injecting itself into the script interpreter, CylancePROTECT Script Control gains insight into both script activity and the script path before execution. Questionable script activity is either blocked or sends an alert to the system administrator.

**Memory Exploitation Detection and Prevention**
Deny fileless attacks a space in which to operate.

A DLL is loaded into each protected process and a service component provides management capabilities. The agent hooks into user-mode API functions and monitors them far signs of compromise, then suspends suspicius functions and provides a choice of follow-on actions.

**Context Analysis Engine (CAE)**
Empower each endpoint with threat detection and response capabilities.

Allow each endpoint to act as a virtual SOC, responding to threats with predetermined processes. Impose rules on a catalog of system behaviors including PowerShell, WMI, and browser-specific actions that fileless attacks rely on to operate.

Prevention is possible.
Sophisticated threats require advanced solutions, which is why BlackBerry Cylance invests heavily in artificial intelligence and predictive security technology. For a better understanding of fileless threats and ways you can prevent them, visit: www.cylance.com/fileless.