Process Inspector

Technical Brief

Overview

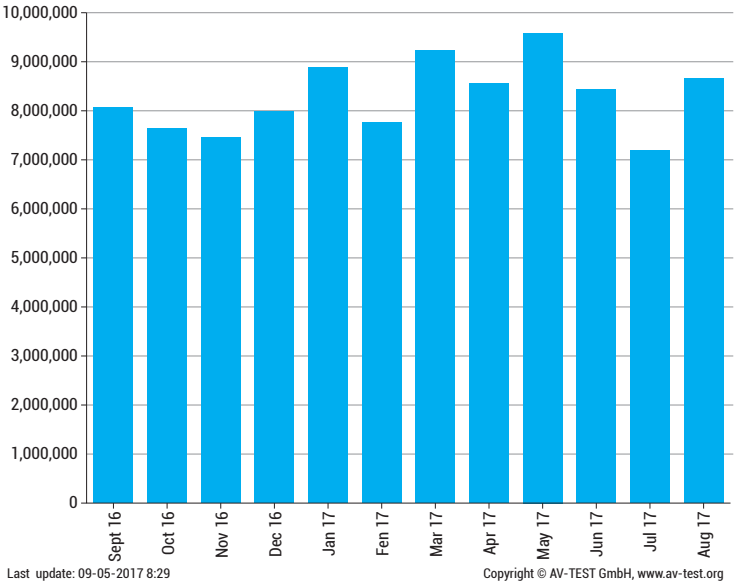
In the current cybersecurity landscape, threat actors are always probing and constantly switching tactics, making companies susceptible to malware incidents and outbreaks, business disruption and data breaches. Bitdefender GravityZone Endpoint Security Platform defends your endpoints from the full range of sophisticated cyber-attacks with high efficacy, low end-user impact and low administrative overhead. It consists of multiple layers of defense that erect obstacles for the bad guys to make sure they keep stumbling. Each layer is designed to stop specific types of threats, tools, or techniques, covering multiple stages of the attacks.

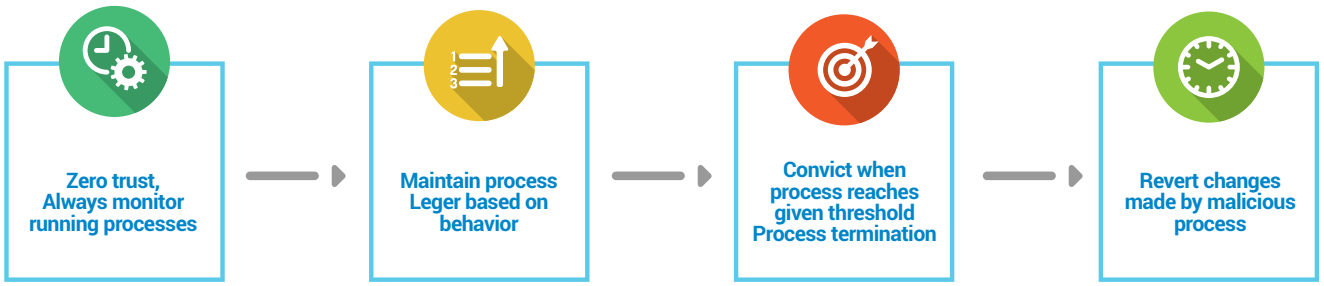
Bitdefender Process Inspector is part of GravityZone Endpoint Security platform. It is a behavior anomaly detection technology that provides protection against never-before-seen threats in on-execution stage.

Detection Stage	Technology Type	Threat Coverage
On-Execution	Behavior Anomaly detection	Obfuscated malware, Targeted attacks, Custom malware, Script-based attacks, Exploits, Delayed Malware, Memory Attacks, Process Injection, Privilege escalation, Fileless attacks (e.g. misuse of PowerShell), Ransomware

Understanding the importance of Bitdefender Process Inspector technology

With over 390,000 new malicious programs discovered every day, the need to protect your environment from zero-day and emerging threats is the 'New Normal' for today's security teams. Process Inspector is an on-execution protection layer that augments comprehensive pre-execution detection technologies in GravityZone Endpoint Security platform. It drastically reduces the risk of a new or emerging threat compromising a system. It operates on a 'zero-trust' model and monitors processes running in the OS using filters in user mode and kernel model. It looks for behavior specific to malware and assigns a score for each process based on its action and context. This is important because each process individually may not indicate malicious intent but a collective analysis provides more insight. When the overall score for a process reaches a given threshold, the process is reported as harmful and appropriate remediation action is taken, including the rollback of changes made by the malicious process on the endpoint.





Features

- Behavioral anomaly tracking: Active applications and processes are continuously monitored
  Some examples: Copying or moving files in System or Windows folders or disk locations with limited access ,Executing or injecting code in another process's space to run with higher privileges, Running files that have been created with information stored in the binary file, Self-replication, Creating an auto-start entry in the registry, accessing or executing illegal operations on registry locations that require elevated privileges, Dropping and registering drivers, Misuse of PowerShell - e.g. identify if powershell.exe is launched with several specific arguments, Ransomware specific detection- e.g. Removing backup files / shadow copies, Generating encryption keys and more
- Automatic Action: Automatically scores running processes and acts when a threat is detected
- Rollback/clean up: Maintains an audit trail of changes made by the process on the endpoint. When a threat is detected, it automatically kills the process and rolls back the malicious changes made by the process.
- Process Exclusion: Ability to exclude processes from monitoring
- Feedback loop with Bitdefender Global Protective Network (GPN): Threats detected by Process Inspector are instantly reported to Bitdefender's security cloud, the Bitdefender Global Protective Network (GPN), ensuring even systems on the other side of the globe will detect it.

Benefits

- Detect advanced attacks early and prevent breaches, reduce incident response costs and efforts
- Reduce threat hunting burden
- Process Inspector greatly increases detection rate of evasive or new malware, including fileless attacks, by enabling monitoring of a process for its entire lifetime, and relying on actual behavior characteristics instead of signatures or binary or code fingerprints
- Protection against obfuscated malware, targeted attacks, custom malware, script-based attacks, exploits, delayed malware, memory attacks, process injection, privilege escalation, fileless attacks (e.g. misuse of PowerShell), ransomware
- Automatic rollback of malicious changes on the system gives security teams peace of mind
- It is designed to work out of the box with little or no configuration and doesn't require enabling or writing complex rules
- Intelligent performance optimization for application and process monitoring ensures low system impact
- Insight gathered from Process Inspector detections is used to enhance machine learning models responsible for pre-execution detection
- It is part of a single, integrated endpoint security agent and central management platform, greatly reducing administrative burden. Customers don't need to deploy a mixture of endpoint security solutions

BD-NGZ-Dec05.20.17-1T-#
Bitdefender-2017-TechnicalBrief-ProcessInspector-creat-103-A4-en_EN-2