Bitdefender®

Hyper Detect
Technical Brief

Multi-Stage Detection Techniques: **1.** Machine Learning   **2. Hyper Detect**   **3.** Sandbox Analyzer   **4.** Memory Protection   **5.** Process Inspector

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 HyperDetect is part of the GravityZone Endpoint Security platform. It contains machine learning models and stealth attack detection technology. It is an additional layer of security specifically designed to detect advanced attacks and suspicious activities in the pre-execution stage.

Detection Stage	Technology Type	Threat Coverage
Pre-Execution	Machine learning	Zero-days, advanced persistent threats, Obfuscated malware, Fileless attacks (Misuse of PowerShell, WMI etc.), credential stealing, targeted attacks, Custom malware, Script-based attacks, Exploits, Hacking tools, Suspicious network traffic, Potentially Unwanted Applications, Ransomware

Understanding the importance of HyperDetect

Threat actors take an existing threat and make minor modifications to the code in attempt to bypass customer's existing signature-based defenses. Many security tools have evolved today to detect at least some of these polymorphic threats. However, attackers who are more determined, patient and skilled will invest time and money to create an entirely new threat. These threats could target an industry or an organization or, in some cases, even an individual. Organizations are constantly at risk of outbreaks and breaches caused by these elusive threats since they can bypass signatures, heuristics and rudimentary machine learning technologies. HyperDetect is designed to detect and stop these elusive threats early, before they can run on the endpoint (pre-execution detection). It achieves this through a combination of tunable machine learning models and stealth attack detection technology. It can be customized to suit your organization's security requirements.

Features

- Sophisticated machine learning models (local and cloud) and stealth attack detection technology that includes:
    - Detection of potential misuse of PowerShell such as: File-less shell code/ Download & Execute (download and execute file from local or remote location), credential theft (invoke-mimikatz, out-minidump), powersploit commands (invoke shell code , port scan, dll injection, get keystrokes , add-persistence), stealth techniques (encoded commandline, eg:Base64 encoded, execution policy bypass, non-interactive mode), launch by browsers/unusual executables (ex: IIS), evasion attempts.
    - Known Packer detection
    - Detection of files not created by a known compiler (Visual Studio, Delphy, etc.)
    - Detection of files not packed with a known packer
    - Ability to search for several strings within the file that might indicate ransomware
    - Detection of Unwanted tools that can be used in APT attacks such as shelter, tools for dumping passwords from memory tools for network mapping and tools for brute-forcing
    - Detection of URLs generated for specific exploits
    - Detection of suspicious execution tree e.g. PowerShell that executes a suspicious file
    - Detection of suspicious command lines
    - Detection of Potential Unwanted Applications
- Tunable Detection
    - Ability to configure Detection Classifiers: Targeted Attacks, Suspicious Files and Network traffic, Ransomware, Exploits, Grayware, Configuration of the sensitivity of the machine learning models: 'Permissive', 'Normal' and 'Aggressive'
- Configuration of HyperDetect in 'Report only' mode or 'Enforcement' mode
- Ability to detect and report at a certain level and block (enforce) at a different level; e.g. Block at 'Normal' level but continue to report at 'Aggressive' level
- Easy exception management - Ability to exclude processes and applications directly from events

Benefits

- Detect advanced attacks early and prevent breaches, reduce incident response costs and efforts
- Protection from fileless attacks
- Reduce threat-hunting burden
- HyperDetect greatly increases the detection rate of elusive threats in the pre-execution stage, including zero-days, advanced persistent threats, obfuscated malware, fileless attacks (Misuse of PowerShell, WMI etc.), credential stealing, targeted attacks, custom malware, script-based attacks, exploits, hacking tools, suspicious network traffic, Potentially Unwanted Applications, ransomware
- Availability of local machine learning models ensures that cloud connectivity is not required for detection
- HyperDetect's unique ability to detect and report at a certain level and block (enforce) at a different level, as well as the ability configure aggressiveness of each detection classifier, allow administrators to customize defense based on their organization's threat profile, risk tolerance and security needs.
- Provides early visibility into suspicious activities
- 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