Sandbox Analyzer
Technical Brief

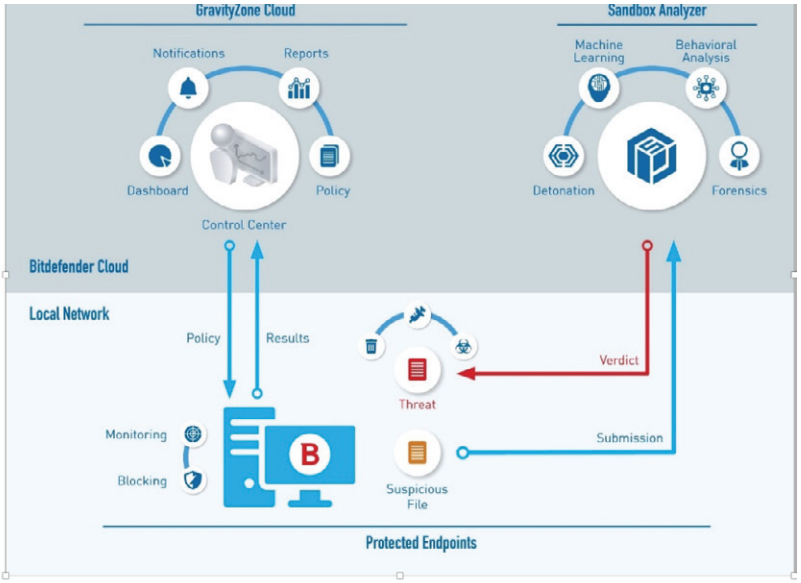
Overview

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 Sandbox Analyzer is part of the GravityZone Endpoint Security platform. It provides pre-execution detection of advance attacks by automatically sending files that require further analysis to cloud sandbox and taking remediation action based on the verdict.

Detection Stage	Technology Type	Threat Coverage
Pre-Execution	Detonator (Sandbox)	APTs, Targeted Attacks, Evasion techniques, Obfuscated Malware, Custom Malware, Ransomware

Understanding the importance of Sandbox Analyzer



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 always at risk of outbreaks and breaches from these elusive threats. Sandbox Analyzer is designed to detect and stop these elusive threats and prevent breaches early, before a malicious file can even run on the endpoint (pre-execution detection). It achieves this through cloud-based sandboxing technology. Each time an unknown portable executable (PE) is accessed by the end user, Bitdefender first applies machine learning and HyperDetect technology to determine if the file is malicious. Bitdefender will then automatically send files that require further analysis to cloud sandbox. The sandbox will analyze the file by leveraging purpose-built, advanced machine learning algorithms, decoys and anti-evasion techniques, anti-exploit and aggressive behavior analysis. Since the file is analyzed in a sandbox environment instead of on the endpoint, Bitdefender GravityZone can perform in-depth analysis without worrying about performance implications and it eliminates the risk associated with allowing a potentially malicious file to run on the endpoint. Bitdefender will either allow or block execution of the file on the endpoint based on administrative policy. If the verdict is malicious, Bitdefender will also update Global Protective Network (Bitdefender's cloud threat intelligence service). This will ensure that all Bitdefender customers can receive protection from this newly identified threat and Bitdefender doesn't have to detonate the same file again.

Features

- Automatic submission of files from the endpoint for sandbox analysis. Bitdefender GravityZone's additional prevention layers - Machine Learning-based Threat Detection and HyperDetect ensure that only files that require further analysis get submitted to the sandbox.
- Automatic remediation based on verdict: enterprise-wide and global blocking of newly detected threats
- Leverages purpose-built, advanced ML algorithms, aggressive behavior analysis, anti-evasion techniques and memory snapshot comparison to detect threats
- Covers a broad range of file types, including: Microsoft Office, Adobe Flash applets, Adobe Reader, Java applets, Portable Executable files (PEF)
- End User alert when sandbox analysis is performed
- Supports 'Monitor' and 'Blocking' mode
- Ability to manually submit files
- Gain early visibility into valuable indicators of compromise (IOC)
- Delivers in-depth reporting on malware behavior
- Support for physical and virtual endpoints (Bitdefender Gravity Zone - Security for Virtualized Environments (SVE)

Benefits

- Detect advanced attacks early and prevent breaches, reduce incident response costs and efforts
- Reduce threat-hunting burden
- Sandbox Analyzer greatly increases the detection rate of elusive threats in the pre-execution stage, including APTs, targeted attacks, evasion techniques, obfuscated malware, custom malware, ransomware
- Automatic submission of PEs from the endpoints to a cloud-based sandbox service dramatically reduces administrative burden normally associated with sandboxing technology.
- Bitdefender's strong machine learning and behavior detection technologies ensure that only files that require further analysis get submitted to the sandbox.
- In-depth reporting gives the security administrator visibility into malware behavior
- Support for both 'Monitor' and 'Block' mode allow security administrator the necessary flexibility
- 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-IT-#
Bitdefender-2017-TechnicalBrief-SandBoxAnalyzer-creat2103-A4-en_EN-2