Bitdefender
Sandbox Service

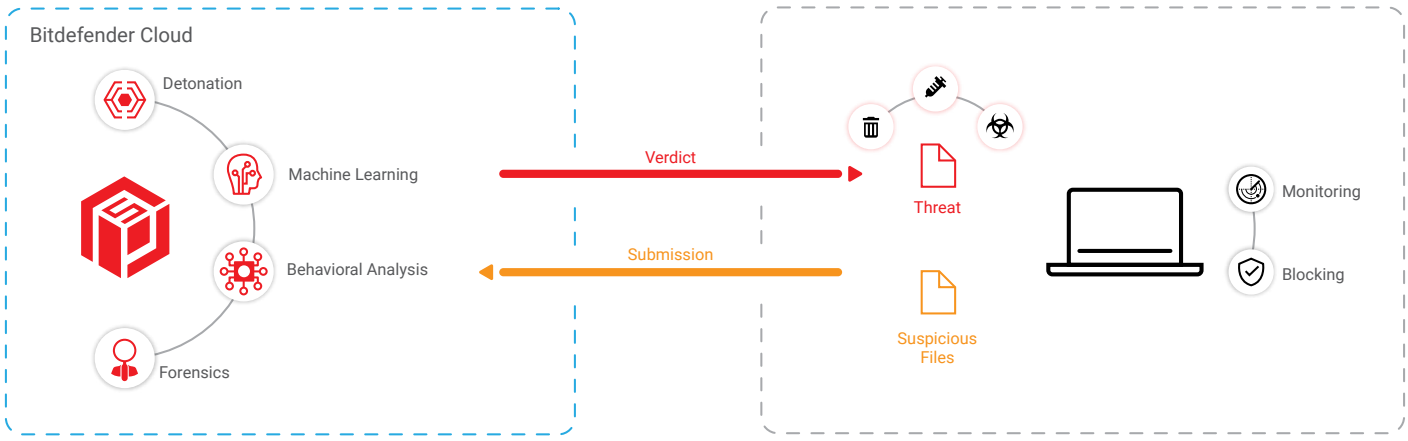
Stop evasive zero-day threats

As cybercriminals develop new and more sophisticated malware to remain elusive, the cost and complexity of managing such threats is growing exponentially. Zero-day malware has become more prevalent than ever, often bypassing known techniques and existing security layers. Businesses of all sizes are facing zero-day exploits, targeted attacks, and advanced persistent threats that have never been seen before, and are specifically designed to evade traditional malware defenses.

Bitdefender's Sandbox service protects against breaches and data loss from today's evasive zero-day threats and sophisticated attacks by providing a highly scalable and powerful environment to run in-depth, sophisticated analysis of unknown or suspicious programs and files. The tool is highly efficient at detecting malware, advanced persistent threats (APTs) and malicious URLs, offering insight into new threats and helping mitigate risks.

How the Sandbox service works

A powerful layer of protection against stealthy attacks, the Sandbox service analyzes suspicious files in depth, detonates payloads in a contained virtual environment hosted by Bitdefender, analyzes their behavior, reports malicious intent and provides actionable insight. The Sandbox service acts as a 'real target environment' for potential malicious files, where everything is carefully crafted so a potential threat acts as it would in the wild, making it a powerful tool against targeted malware attacks and malware infiltration.



- Files accessed by end users are first analyzed with Bitdefender's award-winning antimalware technologies; strong machine learning and behavior detection technologies ensure that only files that require further analysis get sent to the Sandbox;
- The files are detonated in the Sandbox and monitored for signs of malicious activity; self-protection mechanisms are in place and every evasion attempt by a piece malware is properly marked and the files are flagged;
- The Sandbox service analyzes the files by leveraging purpose-built, advanced machine learning algorithms, decoys and anti-evasion techniques, anti-exploit and aggressive behavior analysis;
- Through the use of the highly awarded Bitdefender cloud technologies, all results are checked across known threats in an extensive array of online repositories; and all in just a few minutes;
- Since the file is not analyzed on the endpoint, this eliminates the risk associated with allowing a potentially malicious file to run on the endpoint and also removes any performance implications;
- If the verdict is malicious, the service also updates Bitdefender's Global Protective Network (cloud threat intelligence service), ensuring that the new threat is blocked globally, and Bitdefender does not have to detonate the same file again.

The Sandbox service can be used as a standalone analyzer where the files are sent and a report of the analysis is provided. It also can be used in out-of-band solutions aimed at analyzing all network traffic files automatically and setting alarms when malware is found. The technology can also be used as an inline solution, e.g. for mail traffic, where all emails with attachments are analyzed and, if clean, forwarded to the intended recipients.

Features

Bitdefender Sandbox combines the latest threat analysis with powerful emulation tools to ensure that files are inspected using real-time intelligence along with comprehensive detection techniques:

- Provides advanced threat protection and zero-day exploit detection;
- Utilizes Bitdefender's global Cloud intelligence to detect malware;
- Leverages purpose-built, advanced machine learning algorithms, aggressive behavior analysis, anti-evasion techniques and memory snapshot comparison to detect threats;
- Analyzes a broad range of targets (emails, documents, application files…);
- Delivers in-depth reporting on malware behavior and enables early visibility into valuable indicators of compromise (IOC);
- Helps uncover malicious files including polymorphic and other threats designed for undetectable targeted attacks;
- Is extremely easy to integrate; no effort needed to install and set-up locally, as it is a web service.

Benefits

The Sandbox service augments the protection against targeted malware attacks and malware infiltration:

- Detects advanced attacks early and prevents breaches, reducing incident response costs and efforts;
- Reduces threat-hunting burden;
- Greatly increases the detection rate of elusive threats in the pre-execution stage, including APTs, targeted attacks, evasion techniques, obfuscated malware, custom malware, ransomware;
- Provides a complete solution for quickly integrating advanced emulation-based malware analysis;
- Ensures continuous protection and maximum performance against rapidly evolving advanced threats.

FREE evaluation

Evaluating the Bitdefender Sandbox service is free of charge and includes technical support.

Contact us

For more information regarding the Sandbox service or any of the Bitdefender security technologies, please reach us at oemsales@bitdefender.com

About Bitdefender Technology Licensing

Bitdefender provides end-to-end cyber security solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and has become a provider of choice for leading Independent Software Vendors (ISVs), hardware vendors, service providers and marketing companies looking to integrate security technologies into their products and services. Today, Bitdefender has over 150 technology partners worldwide. More information is available at www.bitdefender.com/oem

Bitdefender