Bitdefender®

PRODUCT PRESENTATION

English Version Only

Sandbox Service

Business Challenges

As cybercriminals develop more sophisticated campaigns 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.

Solution Overview

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. Powered by machine learning algorithms and the latest AI techniques, the tool is highly efficient at detecting malware, advanced persistent threats (APTs) and malicious URLs.

Key Benefits:

The Sandbox Service offers multiple functionalities for malware analysis. It can serve as an independent tool for analyzing files, generating comprehensive analysis reports. Additionally, it can be integrated into out-of-band solutions that automatically examine all network traffic files, triggering alerts whenever malware is detected. Furthermore, the technology can be integrated with inline solutions, e.g., for mail traffic it can analyze all emails and their attachments.

- 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;
- Using the multiple-award-winning Bitdefender cloud technologies, all results are checked across known threats in an extensive array of online repositories;
- The file is not analyzed on the endpoint, eliminating the risk associated with allowing a potentially malicious file to run on the endpoint and removing 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.

Most advanced detection

At Bitdefender, we've been working on machine-learning algorithms since 2009, constantly developing and training them to identify new and unknown threats. Artificial Intelligence and machine learning are essential to combat a threat landscape that is larger and more sophisticated than ever. Bitdefender has years of experience in perfecting these technologies, and the results clearly show better detection rates with fewer false positives.

Bitdefender holds patents in all major areas of interest: machine-learning, antispam/anti-phishing/antifraud, antimalware, virtualization.

Multi-layer next-gen detection for advanced and zero-day threats:

- Network level layer
- On-Access layer
- Pre-execution stage
- During execution stage
- Post-execution stage

Innovative prefiltering

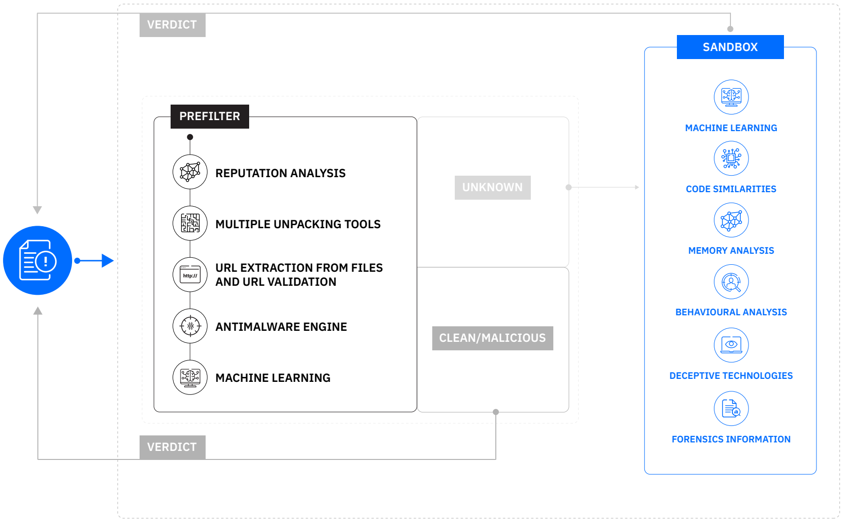
Leveraging the latest advancements in machine learning and state-of-the-art technologies, Bitdefender Sandbox prefilter serves as an intelligent gatekeeper, employing advanced algorithms to precisely filter files for detonation.

By harnessing machine learning capabilities, it continuously learns from extensive data sets, enabling it to accurately identify potential threats or clean files with remarkable precision and speed. This breakthrough technology not only enhances the effectiveness of Bitdefender Sandbox Service but also brings significant cost reduction benefits.

With our prefilter technology, organizations can proactively defend against emerging and sophisticated cyber threats, while simultaneously optimizing resource allocation and reducing operational expenses.

CLOUD PREFILTER

CLOUD PREFILTER IS USED TO PRE-ANALYZE THE FILE BEFORE SUBMITTING TO SANDBOX. REDUCE THE NUMBER OF DETONATED FILES



At-a-Glance

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 next generation sandbox service acts as a ‘real target environment’ for potentially 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.

Features

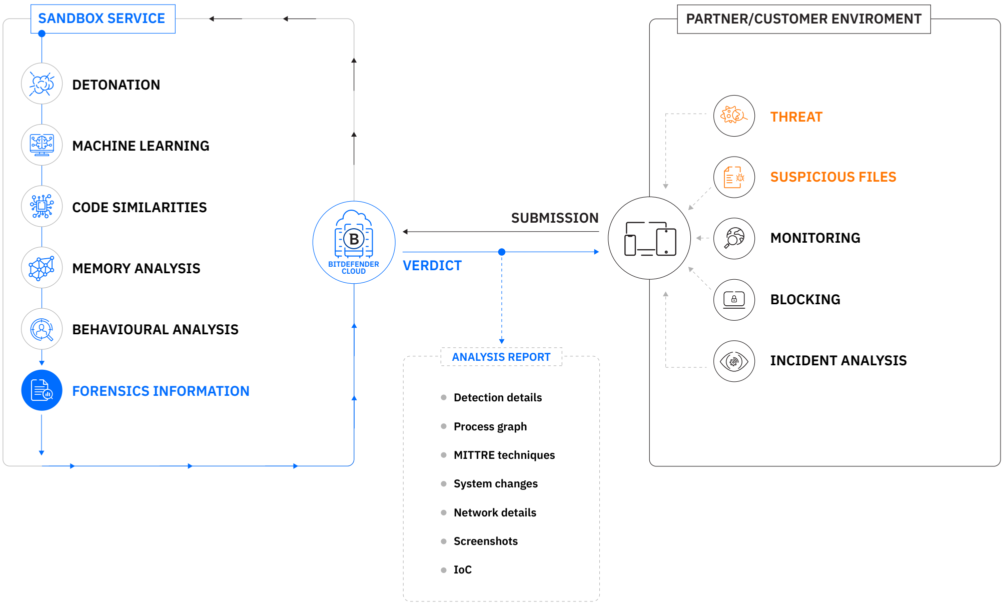
Bitdefender Sandbox service combines the latest threat analysis with powerful emulation tools to ensure that files are inspected using real-time intelligence along with comprehensive detection techniques:

- → Provides advanced threat protection and zero-day exploit detection;
- → High end prefiltering technology
- → Uses 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:

→ Best in class detection
→ Advanced anti-evasion technologies
→ Innovative prefiltering (edited)
→ Comprehensive analysis report
→ MITTRE ATT&CK framework support
→ Highly Scalable infrastructure
→ Easy API integration
→ Tailored privacy options



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 www.bitdefender.com/oem

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, business, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers over 400 new threats each minute and validates around 40 billion daily threat queries. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence, and its technology is licensed by more than 150 of the world's most recognized technology brands. Launched in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com