

Bitdefender Sandbox Service

As cybercriminals develop more sophisticated campaigns to remain elusive, the cost and complexity of managing threats is growing. Zero-day malware has become more prevalent than ever, often bypassing traditional security measures.

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. It's a highly scalable and powerful environment to run in-depth, analysis of unknown or suspicious programs and files. Powered by advanced logging, realistic environments, and AI models, the tool is highly efficient at detecting malware, advanced persistent threats (APTs), and malicious URLs.

Features

- ↳ **Award-Winning Detection:** Detonations in the Bitdefender Sandbox can detect APTs, zero-days, and other sophisticated threats
- ↳ **Realistic Environments:** That simulate real endpoints, to ensure samples behave as they would in the wild.
- ↳ **Evasion Detection:** Through kernel-level logging and evasion mitigations that ensure samples are fully detonated.
- ↳ **Comprehensive Report:** That helps researchers analyze malware, extract relevant IoCs and stay ahead of modern threats.

At-A-Glance

Bitdefender's Sandbox is a powerful, realistic and secure environment to detonate potentially malicious files. Whether you need a sandbox for improved detection, or malware analysis, our service can help.

Benefits

- ↳ **Quick Detonation:** The Bitdefender Sandbox adapts sample execution time to its behavior. This ensures we fully detonate malware, while also returning a verdict as fast as possible.
- ↳ **Flexible Integration:** The sandbox is available in the cloud, or on-prem. It can be queried via a REST API, GUI, or the Bitdefender OEM portal.
- ↳ **Cost-saving:** Cloud prefilter can be employed for quicker verdicts, saving time and money for the partner.
- ↳ **Useful for SOC Analysts:** Detailed breakdown of how samples behave, including file changes, processes affected and actions, network activity, timeline visualization, and MITRE mapping of malicious activity.

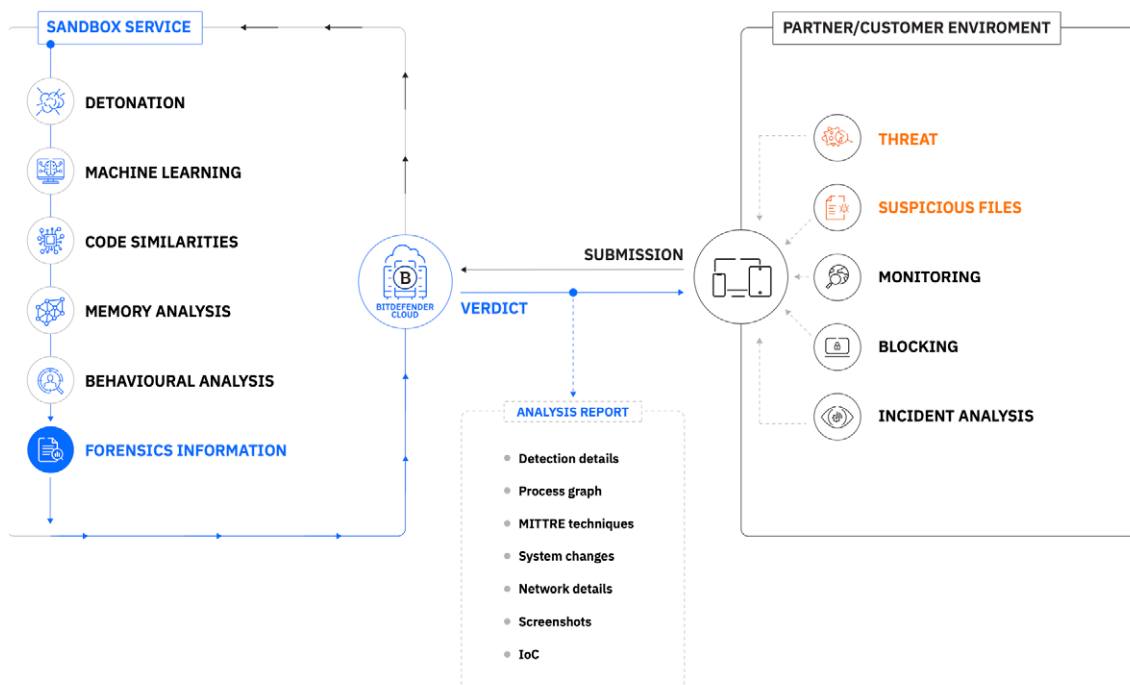
How The Sandbox Service Works

To access the highly scalable service, partners can submit a sample via API, or the OEM portal. The analysis can take a few seconds to a few minutes, depending on the service used (prefilter and/or detonation) and the file's behavior.

By default, files that receive a definite verdict from our prefilter don't get sent to the sandbox, to save costs and time. However, API calls can be customized to force detonation in the sandbox, or bypass prefiltering entirely.

When a file makes it to the sandbox, it's detonated in a fine-tuned virtual machine that simulates every aspect of a regular endpoint. The detonation has a dynamic execution time, running for as long as it's needed to extract all the relevant data from the sample.

Then, a comprehensive report is returned to the client. It includes in-depth behavioral analysis, event logs, network activity mapping, MITRE references, a list of extracted IoCs, file similarities, and more.



Alternatively, samples can be submitted via the IntelliZone portal, our one-stop shop for security researchers to consult advanced threat intelligence and use the sandbox service.

FREE Evaluation

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



Contact us

For more information regarding Sandbox Service please reach us at
<https://www.bitdefender.com/oem/contact-us.html>