Sandbox Analyzer on Premise

With the advancements of sophisticated threats and the sheer overload of new malware appearing each year, sandbox malware analysis remains a key tool for your incident response and threat investigation teams. Bitdefender Sandbox Analyzer on Premise is a powerful and highly scalable next-gen sandbox security solution that enhances an organization's posture against advanced, sophisticated attacks while optimizing file-scanning traffic for effective cost containment.

The solution, powered by machine learning and behavioral analysis technologies, lets your security teams safely detonate suspicious files in a secure local environment that carefully mirrors your production environment, following a potential attack vector throughout its entire lifecycle. Once a potential threat is uncovered, your teams receive advanced visualization graphs and reports that enable complete visibility into the attack. Delivered as a virtual appliance that can be deployed on your premises, the solution can integrate into your existing security architecture or it can combine with additional Bitdefender security layers for enhanced, integrated security for lower TCO, and effortlessly scale up as your infrastructure evolves.

Advanced detection and visibility

Sandbox Analyzer on Premise features a complete array of Bitdefender's award-winning security technologies, combined with proprietary threat intelligence streams, that enable timely detection of advanced threats and ensure attacks are properly catalogued and described, and fully logged as they unfold.

- Combines in-house threat intelligence streams with proprietary machine learning and behavioral detection for maximum, real-time accuracy.
- Displays interactive visualization graphs of security incidents for in-depth forensics.
- Detects highly sophisticated, custom-built threats targeting specific environments using golden images as the detonation environment.

Compliant and effective

Building on proprietary multiple behavioral and machine learning technologies, Sandbox Analyzer on Premise effectively detects zero-day attacks and other sophisticated threats targeting your infrastructure exclusively through proprietary algorithms, keeping you secure and compliant.

- Prevention and detection are performed on your premises, with no files sent for scanning outside your network.
- Leverages AI and Bitdefender threat intelligence built from over 500 million endpoints worldwide to maintain accurate real-time detection on a local level.
- Reveals most advanced and evasive type of malware like APTs or C2s by incorporating anti-evasion and anti-fingerprint technologies.

Integrated, automated, scalable

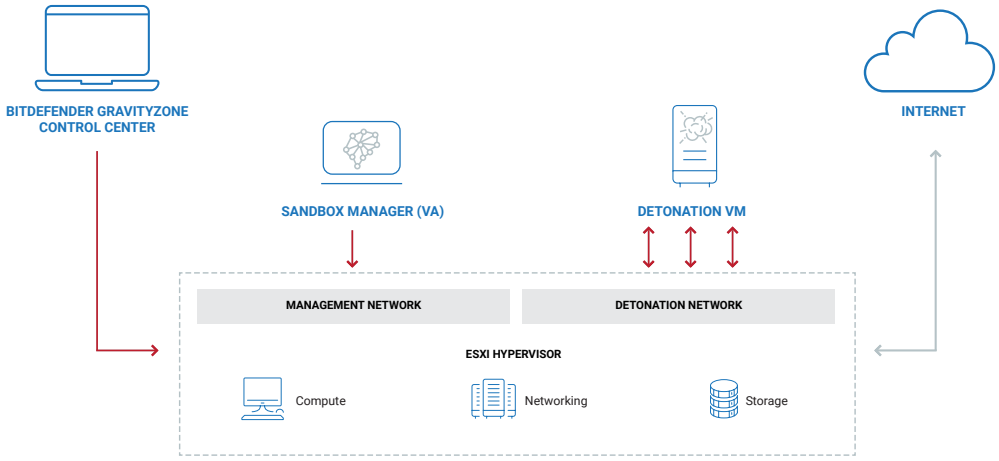
Sandbox Analyzer on Premise is deployed as a virtual appliance, further optimizing costs and improving ROI for your business, and it seamlessly plugs into existing Bitdefender deployments to ensure integrated, automated security on any endpoint across your infrastructure

PIONEERING MACHINE LEARNING

Thanks to our strong research focus since our inception (2001)??, we are one of the first security solutions to have successfully implemented machine learning to aid detection (2011), and we introduced the market's first tunable machine learning technology (2017). Today, we rely on dynamical analysis and multiple machine learning algorithms that augment our detection capabilities, combined with multiple prevention and detection technologies to effectively detect any threat at the network or endpoint level.

500 MILLION-ENDPOINT THREAT INTELLIGENCE NETWORK

Bitdefender achieves the highest detection rates through its rich, global threat intelligence gathered from the 500 million endpoints it helps protect. Our cloud processes over 11 billion requests per day and over 6 TB of data from 150 countries, maintaining an effective and globally balanced detection of advanced, emerging threats. The resulting knowledge is constantly fed into the On-Premises machine learning technologies to keep detection at its peak.



Features & Benefits

Award-Winning, Baked-In Technology

Bitdefender Sandbox Analyzer On-Premise is built entirely on award-winning, Bitdefender technologies and in-house threat intelligence data.

Powered by AI, behavioral analytics and threat intelligence

A next-gen sandbox solution, Bitdefender Sandbox Analyzer On-Premise features state-of-the-art machine learning, and behavioral analytics ensuring quick and accurate threat analytics and further forensic capabilities.

Detailed visualization & reporting tools

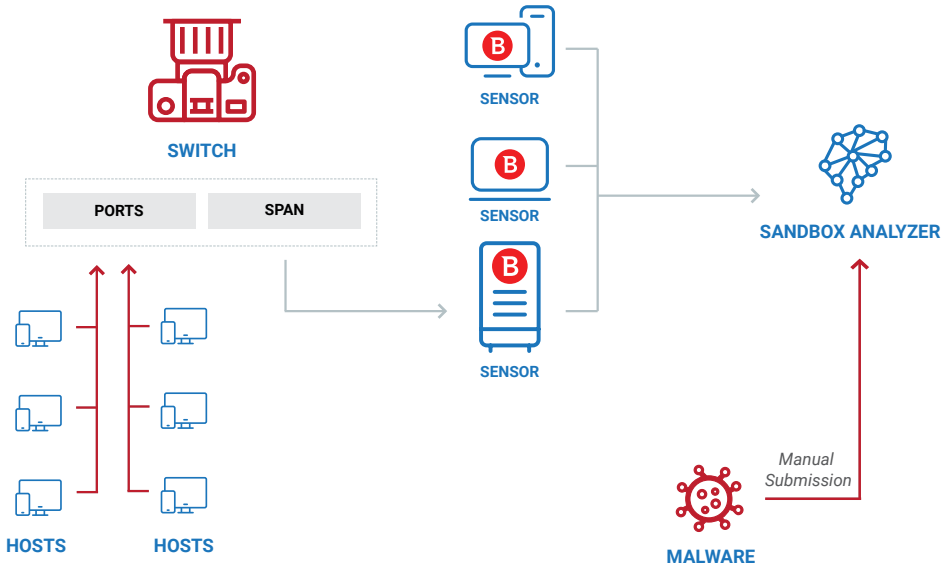
Bitdefender Sandbox Analyzer On-Premise features a uniquely comprehensive and elegant visualization chart that delivers a complete view of each detection and its underlying context. It can learn the threat behavior and provide a timeline display of the changes it tries to make to the system, display root-cause “tree” graphs, and even screenshots of the message or error the user “sees” as it is infected – such as the ransomware note.

Extended file support & tunable throughput

Bitdefender extends the range of files supported by the sandbox to make the solution effective against a wide range of attack vectors, including malicious applications, documents, archives, emails and scripts. Different detonation profiles allow the sandbox throughput to be managed by shifting resources to increase the number of samples that can be detonated per unit of time or to increase sandbox accuracy with the side effect of a lower throughput.

Automatic content selection and submission of files

The solution incorporates a mechanism that singles out suspicious files and eliminates redundant scanning, ensuring that only unknown, relevant files are submitted for analysis. The automatic submission of files is enabled by the built-in network sensors, ICAP protocol support, and through the integration with GravityZone: automatic submission from the endpoint agent or from the central quarantine.



Custom VM image support to replicate real-life configurations

Multiple golden image support enables admins to emulate different configurations on the sandbox instances, from production to executive golden image configurations. Different golden images can be used for parallel detonation to ensure that any attack that may manifest on your specific configurations or application environment will be detected in advance. Bitdefender Sandbox Analyzer On-Premise also includes a tool for inspecting a golden image against a specific set of requirements (mainly apps that need to be a part of the golden image) prior to actually using the golden image as a base for detonation VMs

Integrates with the security architecture in-place

The On-Premise Sandbox environment is managed using the Bitdefender's GravityZone rich UI and its functionality can be further leveraged using API's, thus ensuring seamless export of sandbox telemetry across 3rd party security solutions. The integration into the existing security architecture not only automates the submission of files but also enables autonomous response in case threats are detected.

Scalability

Delivered as a Virtual Appliance, Bitdefender Sandbox Analyzer On-Premise can easily scale up to support increasing file submission load, limited only by the underlying bare metal. Virtually unlimited scalability can be achieved by increasing the number of detonations VMs while maintaining centralized management of the entire sandbox network under a single management console.

Built and perfected in-house

Bitdefender Sandbox Malware Analysis On-Premises is built entirely on proprietary Bitdefender technologies and code further leveraging Bitdefender Advanced Threat Intelligence feeds.

Contact us

Evaluating Bitdefender Sandbox Analyzer On-Premise is free of charge and includes technical support. For any inquiries regarding the Bitdefender SDKs, please reach us at www.bitdefender.com/oem.

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 enterprise organizations 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

Founded 2001, Romania
Number of employees 1800+

Headquarters
Enterprise HQ – Santa Clara, CA, United States
Technology HQ – Bucharest, Romania

WORLDWIDE OFFICES
USA & Canada: Ft. Lauderdale, FL | Santa Clara, CA | San Antonio, TX | Toronto, CA
Europe: Copenhagen, DENMARK | Paris, FRANCE | München, GERMANY | Milan, ITALY | Bucharest, Iasi, Cluj, Timisoara, ROMANIA | Barcelona, SPAIN | Dubai, UAE | London, UK | Hague, NETHERLANDS
Australia: Sydney, Melbourne

Bitdefender-OEM-Premise-Datasheet-creat4587210x297-en_EN
07/05/2025, June 24, 2025 at 2:31 PM (5 days ago)