GravityZone™ Sandbox Analyzer On-Premises

With the advancements of sophisticated threats and the sheer overload of new malware appearing each year, sandbox security remains a key tool for your incident response and threat analysis teams. Bitdefender GravityZone™ Sandbox Analyzer On-Premises 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, enables your security teams to safely execute suspicious files in a secure local environment that faithfully mirrors your production endpoints, tricking attackers into believing they have reached their target. Once an advanced threat is uncovered, your teams are provided with advanced visualization graphs that enable complete visibility into the attack.

Delivered as a virtual appliance on 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

Bitdefender GravityZone™ Sandbox Analyzer On-Premises features a rich 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 prevented before 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 very sophisticated, custom-built threats targeting specific environments through golden image support.

Compliant and effective

Building on proprietary multiple behavioral and machine learning technologies, Bitdefender GravityZone™ Sandbox Analyzer On-Premises effectively detects zero-days attacks and other sophisticated threats targeting your infrastructure exclusively through in-house scanning, ensuring you remain secure and compliant.

- Prevention and detection are performed fully on-premises, with no files sent for scanning outside your network.
- Leverages AI and Bitdefender threat intelligence built from over 500 million users 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

Bitdefender GravityZone™ Sandbox Analyzer On-Premises is deployed as a virtual appliance, drastically optimizing costs and improving ROI for your business, and 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, we are one of the first security solution to have successfully implemented machine learning to aid detection back in 2007 and introduced the market's first tunable machine learning technology in 2017.

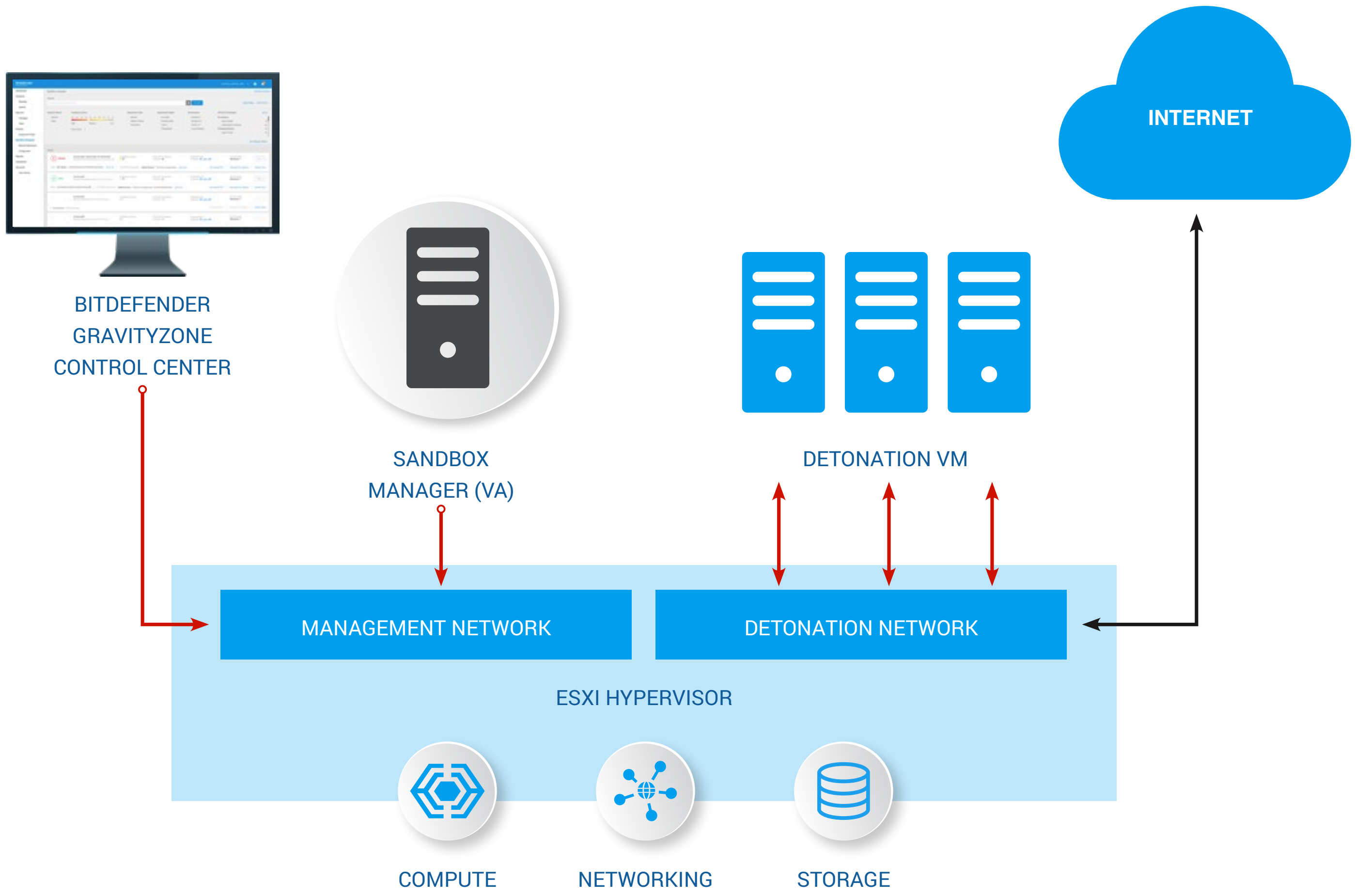
Today, we rely on dynamical analysis and dozens on machine learning algorithms to fuel our detection capabilities, which we combine with multiple prevention and detection technologies to effectively detect files at network and endpoint levels.

500 MILLION ENDPOINTS THREAT INTELLIGENCE NETWORK

Bitdefender achieves the highest detection rates through to 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 worldwide, 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 maintain detection at its peak.



Features & Benefits

Award-Winning, Baked-In Technology

Instead of incorporating third-party technologies, which can be discontinued or outdated in time, Bitdefender Sandbox Analyzer On-Premises is built entirely on award-winning, internally-developed Bitdefender technologies and in-house threat intelligence streams.

Powered by AI, behavioral analytics and threat intelligence

A next-gen sandbox solution, Bitdefender Sandbox Analyzer On-Premises features state of the art machine learning, neural networks and behavioral analytics ensure quick and accurate containment.

Detailed visualization & reporting tools

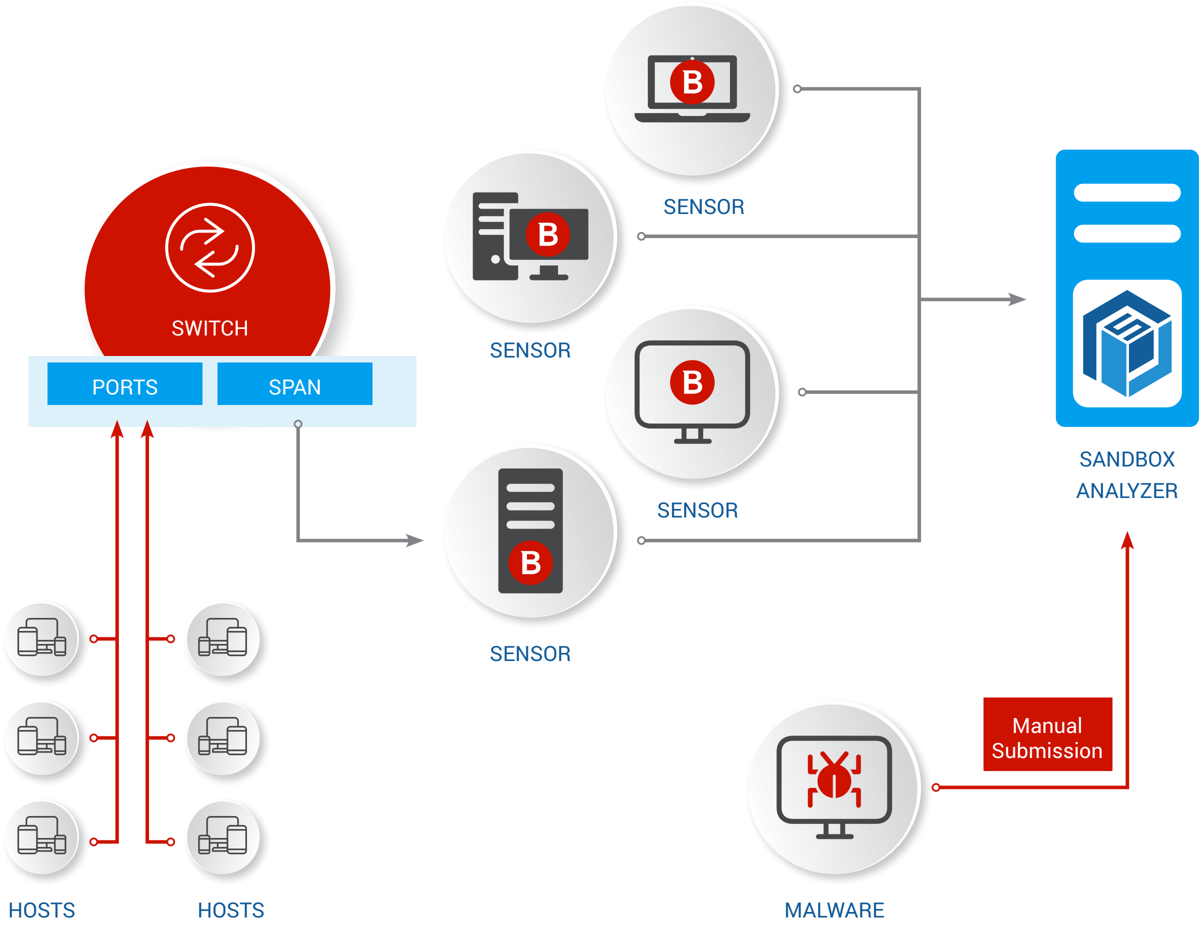
Bitdefender Sandbox Analyzer features a uniquely comprehensive and elegant visualization chart, which delivers a complete view of each detection and its underlying context. It can learn the threat behavior and provide timeline display of the changes it is trying to make to the system, tree graphs, and even a screenshot of the message or error the user views as it is infected – such as the ransomware note.

Extended file support & tunable throughput

Bitdefender extends the range of file supported by the sandbox to make the solution effective against a wide range of attack vectors, including malicious applications, document, 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 the 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 apps will be detected in advance. GravityZone™ Sandbox Analyzer On-Premises also includes a tool for inspecting a golden image against Golden Images requirements, before start using it.

Integrates with the security architecture in-place

The on-premises sandbox integrates natively with GravityZone and, through API's, ensures broad integration with 3rd party security solutions. The integration into the security architecture not only automates the submission of file but also enables autonomous response in case threats are detected.

Vertical and horizontal scalability

Ran as a virtual appliance, Bitdefender Sandbox Analyzer can easily scale up to support increasing streams of data that can be supported by the dedicated hardware host. Virtually unlimited scalability can be achieved by increasing the number of sandbox instances while maintaining a centralized management of the entire sandbox network under a single console (GravityZone).

Built and perfected in-house

Instead of incorporating third-party technologies, which can become discontinued or outdated in time, Bitdefender Sandbox Analyzer On-Premises is built entirely on proprietary Bitdefender technologies and leverages Bitdefender Advanced Threat Intelligence

Looking to test the solution for yourself?

Visit www.bitdefender.com/sandbox to learn more about the solution and request a POC today.

Bitdefender is a global security technology company that provides cutting edge 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 is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on. More information is available at http://www.bitdefender.com.