Datasheet

Bitdefender
BUILT FOR RESILIENCE

GravityZone Sandbox Analyzer on-Premises

Next-generation, AI-powered sandbox with advanced detection, reporting and attack visibility

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.

Key capabilities

- **Integrates natively with Bitdefender technologies –** and through APIs with other security elements, integrated, automated, and scalable
- **Advanced detection and visibility –** combining in-house threat intelligence streams with proprietary machine learning and behavioral detection for maximum, real-time accuracy
- **AI, behavioral analytics, and threat intelligence –** incorporating state-of-the-art machine learning, neural networks and behavioral analytics that ensure quick and accurate containment
- **Multiple golden image support –** enables security teams to emulate different real-life configurations on the sandbox instances ensuring that any attack that may occur on your specific configurations or apps will be detected in advance
- **Automatic content selection and submission –** identifies suspicious files and automatically sends them for detonation by built-in network sensors, ICAP and protocol support. For increased efficiency, the sandbox incorporates a mechanism that eliminates redundant scanning

At-a-Glance

GravityZone Sandbox Analyzer is a security solution that enhances an organization's security posture against sophisticated or targeted attacks through advanced detection and reporting capabilities. Delivered as a virtual appliance, the solution can integrate into your existing security architecture or be combined with additional Bitdefender security layers. The solution can effortlessly scale up as your infrastructure evolves.

Key Benefits

- **Compliant and effective:** prevention and detection are performed fully on-premises, with no files sent for scanning outside your network
- **Nothing gets past us –** Bitdefender achieves the highest detection rates – via global threat intelligence gathered from 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

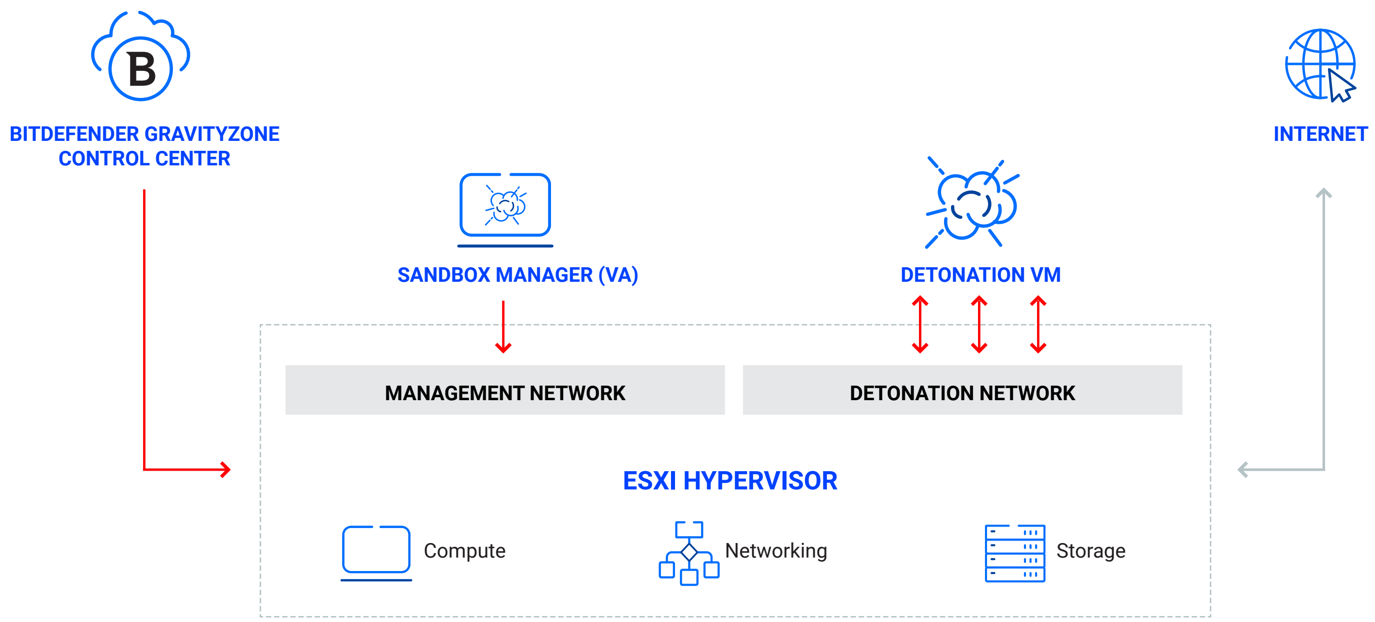
- **Continuously updated intelligence –** built entirely on proprietary Bitdefender technologies, leveraging Bitdefender Advanced Threat Intelligence so it is never out of date, and is constantly improved over time with new intelligence.

Detailed visualization and reporting tools

provide a comprehensive and easy-to-use visualization chart, that delivers a complete view of each detection and its underlying context. It learns the threat behavior, provides a timeline display of the system changes and even a screenshot of the message or error the user views as it is infected – such as a ransomware note.

Extended file support and tunable throughput

Bitdefender extends the range of file supported by the sandbox to make the solution effective against a wide range of attack vectors, like applications, documents, archives, emails and scripts. Different detonation profiles allow the sandbox throughput to be managed by shifting resources to increase the capacity or to increase the sandbox accuracy.



Bitdefender
BUILT FOR RESILIENCE

3945 Freedom Circle
Ste 500, Santa Clara
California, 95054, USA

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.

For more information, visit https://www.bitdefender.com.

Bitdefender-BSG-GZ-SandBoxAnalyzer-Datasheet-DEX4857-en_EN
CD-Feb/11/2022 • MD-Mar/22/2022