



## BITDEFENDER GRAVITYZONE COMPARISON

### Choose the offer that best suits your needs

GravityZone is a business solution that can be installed locally or hosted by Bitdefender. Multi-layered protection with proven machine learning, advanced heuristics, anti-ransomware, powerful anti-exploit, signatures, Firewall and Device Control are included in each of the options below

Bitdefender GravityZone Business Security	Bitdefender GravityZone Advanced Business Security	Bitdefender GravityZone Elite Security	Bitdefender GravityZone Ultra Security	Bitdefender GravityZone Enterprise Security
Ideal for small businesses looking for simple, yet efficient security	Recommended to midsized companies looking for comprehensive protection	Recommended to companies looking for aggressive protection against sophisticated threats	Recommended to companies looking for an integrated next-gen endpoint protection & EDR platform that accurately protects against sophisticated cyber threats	Flexible solution for larger organizations with datacenters using virtualization

Management options	On premise / Cloud	On premise / Cloud	On premise / Cloud	On premise / Cloud	On premise only
<b>TYPES OF ENDPOINTS PROTECTED</b> <i>Consistent, next-gen defenses across any type of endpoints</i>					
<b>Physical and Virtual Workstations and Servers</b> State of the art security for end-user devices.	✓	✓	✓	✓	✓
<b>Server Security with Smart Centralized Scanning (VDI, DaaS) - on-premises or in the cloud. (Also available by CPU socket licensing.) Pro-VM, Pro-Cloud defenses with Smart Centralized Scanning for high performance and optimum user experience.</b>	●	✓	✓	✓	✓
<b>Mobile Devices</b> Device and platform agnostic mobile security.	●	(On-Premises Console Only) ✓	(On-Premises Console Only) ✓	(On-Premises Console Only) ✓	(On-Premises Console Only) ✓
<b>Microsoft® Exchange</b> Unrivaled defense against malware, spam & phishing attempts.	●	✓	✓	✓	✓
<b>IoT Devices</b> Agentless defenses that can detect threats for IIoT, IoMTs and other types of IoTs.	Available with the NTSA product	Available with the NTSA product	Available with the NTSA product	Available with the NTSA product	Available with the NTSA product
	SECURITY TECHNOLOGIES				
	PREVENTION MODULES				
<b>Local and Cloud Machine Learning</b> Predictive detection of unknown malware; Dynamic file analysis trained on billions of samples; Local machine learning trained on 80,000 malware features. Threat intelligence from over 500 million endpoints globally.	✓	✓	✓	✓	✓
<b>Advanced Anti-Exploit</b> Focuses on attack tools and techniques to detect both known and zero-day exploits that target popular software applications.	✓	✓	✓	✓	✓
<b>Automatic Disinfection and Removal</b> Automatically blocks confirmed threats through a set of predefined rules, including process termination, moving to quarantine or access blocking.	✓	✓	✓	✓	✓
<b>Network Attack Defense</b> Protects against threats that use network vulnerabilities.	✓	✓	✓	✓	✓
<b>Fileless Attacks Defense</b> Protects against attacks that attempt to write changes directly in memory.	●	✓	✓	✓	✓
<b>HyperDetect™ (Tunable Machine Learning)</b> Tunable machine learning layer, detects sophisticated threats.Blocks hacking tools, fileless attacks, zero-day malware and more.	●	●	✓	✓	Add-On
<b>Sandbox Analyzer</b> Sends suspicious files for detonation, analyzes & provides a verdict in real time. Detects zero-day & targeted attacks; Prevents real time attack prevention with auto-submit; Analyzes once enterprise-wide block.	●	●	✓	✓	Add-On
	DETECTION AND RESPONSE MODULES				
<b>Process Inspector</b> Behavior-based real time detection; Monitors all processes running in the operating system & if the process is deemed malicious, will terminate it. Formerly known as Advanced Threat Control (ATC).	✓	✓	✓	✓	✓
<b>Ransomware Mitigation</b> Creates a real-time back-up of the files before being modified by the suspicious process to mitigate the risk of losing data during advanced ransomware attacks.	✓	✓	✓	✓	✓
<b>Incident Visualization</b> Easy to understand visual guides highlight critical attack paths, easing burdens on IT staff.	●	●	✓	✓	Add-On
<b>Root Cause Analysis</b> Highlights the attack vector, the attack entry point, & how the attack originated. Helps pinpoint the origin node of attack, highlighted in the Incident page. The confidence score provides context for security events.	●	●	✓	✓	Add-On
<b>Anomaly Defense</b> Baselines system resources to spotlight unusual behavior based on MITRE threat techniques and Bitdefender's own research.	●	●	●	✓	Add-On
<b>MITRE Event Tagging</b> MITRE attack techniques and indicators of compromise provide up to the minute insight into named threats and other malware that may be involved.	●	●	●	✓	Add-On



## BITDEFENDER GRAVITYZONE COMPARISON

Bitdefender GravityZone Business Security	Bitdefender GravityZone Advanced Business Security	Bitdefender GravityZone Elite Security	Bitdefender GravityZone Ultra Security	Bitdefender GravityZone Enterprise Security
Ideal for small businesses looking for simple, yet efficient security	Recommended to mid-sized companies looking for comprehensive protection	Recommended to companies looking for aggressive protection against sophisticated threats	Recommended to companies looking for an integrated next-gen endpoint protection & EDR platform that accurately protects against sophisticated cyber threats	Flexible solution for larger organizations with datacenters using virtualization

### HARDENING AND RISK ANALYTICS MODULES

<b>Endpoint Risk Analytics</b> Assesses, prioritizes and hardens endpoint security misconfigurations and settings with an easy-to-understand prioritized list.	✓ (Cloud Console Only)	✓ (Cloud Console Only)	✓ (Cloud Console Only)	✓ (Cloud Console Only)	●
<b>Web Threat Protection</b> Scans incoming web traffic, including SSL, HTTP & HTTPS traffic, to prevent the download of malware to the endpoint. Automatically blocks phishing & fraudulent web pages. Displays search ratings signaling trusted and untrusted pages.	✓	✓	✓	✓	✓
<b>Device Control</b> Threats are often introduced into the company via removable devices. Choose which devices to allow to run, and decide what will be blocked or scanned automatically.	✓	✓	✓	✓	✓
<b>Application Control (Blacklisting)</b> Enables full visibility and control of running applications by blacklisting unwanted software. Helps limit the risk of malicious code running undetected.	✓	✓	✓	✓	✓
<b>Application Control (Whitelisting)</b> Provides full visibility and control of applications installed or running on company endpoints, and prevents the execution of any application not allowed by policy.	●	●	✓ (On-Premises Console Only)	✓ (On-Premises Console Only)	✓
<b>Firewall</b> Fully-featured two-way firewall that controls applications' access to the network and to the Internet. Furthermore, the firewall can protect the system against port scans, restrict ICS and warn when new nodes join a Wi-Fi connection	✓	✓	✓	✓	✓
<b>Smart Centralized Scanning</b> Allows up to 30% more virtual machines than traditional solutions by optimizing and centralizing scan tasks.	●	✓	✓	✓	✓

### EXTEND SECURITY WITH COMPATIBLE PRODUCTS

#### AVAILABLE ADD ONS

<b>Email Security</b> For all email clients, including Office 365	Available	Available	Available	Available	●
<b>Patch Management</b> Keeps OSes and applications up to date across the entire Windows install base	Available	Available	Available	Available	Available
<b>Full Disk Encryption</b> Protects data for the entire endpoint hard drive by leveraging the encryption mechanisms provided by Windows (BitLocker) and macOS (FileVault).	Available	Available	Available	Available	Available
<b>Security for AWS</b> Built for virtualization, offers flexible pricing, & scales to your size & needs for optimal return on investment	Available	Available	Available	Available	Available

#### COMPATIBLE PRODUCTS

<b>Hypervisor Introspection</b> Protects business sensitive data before they are exposed, by detecting and stopping in real-time the cyber attacks at the hypervisor level	●	(Compatible - On Premises Console Only)	(Compatible - On Premises Console Only)	(Compatible - On Premises Console Only)	Compatible
<b>Security for Storage</b> Complete security solutions for data storage protection for enterprise ICAP-compatible file-sharing and network storage systems	●	Compatible	Compatible	Compatible	Compatible
<b>Network Traffic Security Analytics</b> Cloud threat intelligence, machine learning & behavior analytics applied to network traffic to detect advanced attacks early and enable effective threat hunting	Compatible	Compatible	Compatible	Compatible	Compatible
<b>Sandbox Analyzer On-premises</b> Next-generation AI-powered on-premise sandbox with advanced detection, reporting & attack visibility	Compatible	Compatible	Compatible	Compatible	Compatible

Licensing	Bundle	Bundle	Bundle	Bundle	a la carte
-----------	--------	--------	--------	--------	------------

Data center licensing (Dedicated CPU licensing for virtual servers)	●	●	●	●	●
<b>Details</b>	Covers servers & desktops. Servers should account for less than 30% of total units	Covers desktops, servers and mobiles + Exchange mailboxes. Servers should account for less than 35% of total units.	Covers desktops, servers and mobiles + Exchange mailboxes. Servers should account for less than 35% of total units.	Covers desktops, servers and Exchange mailboxes. Servers should account for less than 35% of total units.	Each item can be purchased separately and can be activated based on its own license key.