

**Bitdefender**  
BUILT FOR RESILIENCE

 **IPSYSTEMS, INC.**  
ALL ABOUT DATA SECURITY



# Experience More Than 30 Layers of Machine Learning-driven Security Technologies

Get to Know Bitdefender GravityZone Business Security Premium

The threat environment today has evolved. Most of the time, IT teams turn to multiple endpoint security solutions just to future-proof sensitive business data against unprecedented threats. But with Advanced Persistent Threats (APT) being more sophisticated than ever, and with ransomware still on the rise, it's become a task for security teams everywhere to find the perfect security tool. In addition to that, it becomes twice as hard when human error is added into the equation.

However, there's an endpoint security solution that can help your organization have ironclad defenses against existing and emerging cyber attacks.

## Introducing Bitdefender GravityZone Business Security Premium!

**Formerly known as Bitdefender GravityZone Elite Security**, Business Security Premium is an endpoint security solution that defends your organization with several layers of machine learning-driven security technologies, world-class attack forensics and visualization, and analytics driven system hardening. What's more, it covers physical, virtual, mobile, and cloud-based endpoints—even emails.

## Get to Know Its Capabilities

The technologies inside Business Security Premium provide the perfect balance between performance and efficient defense. It's proven as a consistent outperformer compared to conventional endpoint security solutions based on independent tests. Here's how this solution does it:

- **Strengthens Your Attack Surface with Human Risk Analytics**

Create a foolproof attack surface with Bitdefender's Human Risk Analytics. With this feature, you will have the power to oversee user actions and behaviors which can be the cause of breach. The Human Risk Analytics continuously monitors, prioritizes, and addresses end-point risks coming from misconfigurations and user-generated vulnerabilities. Not only does it look at user-by-user, but it also lets you view your company's overall Risk Score.



- **Efficiently Prevents Ransomware Attacks with Ransomware Prevention and Mitigation**

Defend your organization against ransomware attacks with a built-in prevention and mitigation response feature in Bitdefender's Management Console. The global leader in cybersecurity knows that to beat ransomware you must understand the attack's kill chain to map out defenses. Hence, this feature also consists of automatic, up-to-date tamperproof backup copies of user files, without using shadow copies; and blocking and prevention capabilities such as:

- o Fileless Attack Defense
- o Network Attack Defense
- o Advanced Anti-Exploit
- o Machine Learning Anti-Malware

Moreover, it includes multiple detection layers like:

- o Process Inspection
- o Registry Monitoring
- o Code Inspection
- o HyperDetect™
- o User and System Risk Mitigation Technology



- **Tells You How the Exploit Happened with End-to-end Attack Forensics**

Gain a 360-degree view of your organization's threat landscape with End-to-end Attack Forensics. Through this, you can reveal more context on attacks and how the endpoints are exploited. This way, your IT team can zero in on specific threats and take corrective action.

- **Prevents Targeted Threats with Network Attack Defense**

Build an ironclad wall between threats and your system with Network Attack Defense. Business Security Premium can help detect and prevent network vulnerability attacks such as brute force attacks, password stealers, and lateral movement before they're executed. This capability is also crucial as a source of information that's needed for EDR incident correlations.



# Learn More About the Technology Architecture Behind It

Take a look at the technology architecture that makes Business Security Premium the standout choice in the security industry:

- **HyperDetect™**

Improving your defenses against threats like fileless attacks, targeted malware, ransomware, and more is the reason why Bitdefender developed HyperDetect™. It's a security layer that's included in the Endpoint Security Platform which improves your defenses through machine learning and heuristic analysis. These enables you to identify threats that traditional endpoint security solutions miss. HyperDetect™ also contains stealth attack detection technology that allows your IT team to stay one step ahead of cybercriminals.

- **Sandbox Analyzer**

Detecting targeted attacks towards your organization is enhanced with Bitdefender's Sandbox Analyzer. Built by in-house machine learning and behavioral fact-finding models, the Sandbox Analyzer takes an in-depth view of suspicious files, detonates payloads in a contained virtual environment hosted by Bitdefender, analyzes their behavior and reports malicious intent.

- **Exploit Defense**

Fending off zero-day threats and providing an extra layer of protection should be a crucial step in your organization's defense plan. Exploit Defense delivers an extra layer of protection from attacks that leverage memory and vulnerable applications such as browsers, document readers, media files, and runtime (i.e. Flash, Java). Advanced anti-exploit technology along with machine learning hardens your vulnerable applications and reduces the attack surface.



# Get a Closer Look at the Features It Has To Offer

## RISK ANALYTICS AND HARDENING



**ENDPOINT  
RISK ANALYTICS**



**PATCH  
MANAGEMENT**



**FULL-DISK  
ENCRYPTION**



**THREAT  
PROTECTION**



**APPLICATION  
CONTROL**



**DEVICE  
CONTROL**

## PREVENTION



**EXPLOIT  
DEFENSE**



**FILELESS  
ATTACK DEFENSE**



**LOCAL & CLOUD  
MACHINE LEARNING**



**EMAIL  
SECURITY**



**MALICIOUS PROCESS  
MONITORING**



**TUNABLE MACHINE  
LEARNING**



**NETWORK  
ATTACK DEFENSE**



**FIREWALL**



**AUTOMATED  
SANDBOX ANALYSIS**



**AUTOMATIC  
DISINFECTATION &  
REMOVAL**

## ATTACK FORENSICS AND VISUALIZATIONS



**KILL  
CHAIN**



**ROOT CAUSE  
ANALYSIS**



**REMOTE COMMAND  
SHELL**



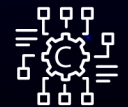
**DASHBOARDS  
& REPORTS**



**NOTIFICATIONS**



**SIEM  
INTEGRATION**



**API SUPPORT**

## REPORTING AND INTEGRATION

# Time to Switch To An Industry-recognized Endpoint Security Solution



MITRE | ATT&CK®



## Check if Your Endpoints are Compatible with Business Security Premium

### Supported Operating Systems:

- Windows 10 November 2021 Update (21H2) Windows 10 May 2021 Update (21H1) Windows 10 October 2020 Update (20H2), Windows 10 May 2020 Update (20H1), Windows 10 November 2019 Update (19H2), Windows 10 May 2019 Update (19H1), Windows 10 October 2018 Update (Redstone 5), Windows 10 April 2018 Update (Redstone 4), Windows 10 Fall Creators Update (Redstone 3), Windows 10 Creators Update (Redstone 2), Windows 10 Anniversary Update (Redstone 1), Windows 10 November Update (Threshold 2), Windows 10 (RTM, version 1507), Windows 8.1, Windows 8, Windows 7
- Ubuntu 14.04 LTS or higher, Red Hat Enterprise Linux / CentOS 6.0 or higher, SUSE Linux Enterprise Server 11 SP4 or higher, OpenSUSE Leap 42.x, Fedora 25 or higher, Debian 8.0 or higher, Oracle Linux 6.3 or higher, Amazon Linux AMI 2016.09 or higher
- macOS Monterey (12.x) macOS Big Sur (11.x), macOS Catalina (10.15), macOS Mojave (10.14), macOS High Sierra (10.13), macOS Sierra (10.12)
- Windows 10 IoT Enterprise, Windows Embedded 8.1 Industry, Windows Embedded 8 Standard, Windows Embedded Standard 7, Windows Embedded Compact 7, Windows Embedded POSReady 7, Windows Embedded Enterprise 7
- Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2



## Control Center Minimum Hardware Requirement

- T CPU: 4 vCPU with 2 GHz each
- Minimum RAM memory: 6 GB recommended
- 40 GB of free hard-disk space
- Internet access for updates and communication with remote and mobile endpoints.

## Endpoint Hardware Requirements

- Minimum: 2.4 GHz single-core CPU
- Recommended: 1.86 GHz or faster Intel Xeon multi-core CPU
- Minimum free RAM: 512 MB
- Recommended free RAM: 1 GB
- HDD Space: 1.5 GB of free hard-disk space

## GravityZone Control Center (On-premise Console)

GravityZone Control Center is delivered as a virtual appliance and is available in the following formats:

- OVA (compatible with VMware vSphere, View)
- XVA (compatible with Citrix XenServer, XenDesktop, VDI-in-a-Box)
- VHD (compatible with Microsoft Hyper-V)
- Support for other formats and virtualization platforms may be provided on request.

# Have Your Frequently Asked Questions About Business Security Premium, Answered

## • Why do you need next-gen endpoint security capabilities?

Enterprise data breaches continue to become more prevalent and damaging. Hackers constantly perfect their attacks to evade traditional antivirus solutions. Your business needs a next-gen endpoint security solution that delivers more than basic prevention and hardening.

## • Why choose Bitdefender GravityZone Business Security Premium?

To reinforce your organization's security posture, the endpoint security solution needs to not only identify and stop threats, but also harden defenses, reduce risks, and uncover the nature of threats. GravityZone Business Security Premium delivers all of this in a single package.

## • What types of devices and endpoints are compatible with GravityZone Business Security Premium?

GravityZone Business Security Premium provides 360-degree protection on desktops, servers (physical and virtual), mobile devices (on-premise only), and Microsoft Exchange mailboxes. It covers any OS (Windows, Mac, Linux) and all virtual platforms.

GOT ANY MORE QUESTIONS?  
**TALK TO A BITDEFENDER EXPERT TODAY!**

 +63 (2) 8638 – 3264

 [inquiry@ipsystems.ph](mailto:inquiry@ipsystems.ph)

 [www.ipsystems.ph](http://www.ipsystems.ph)