



GravityZone Elite Suite

An Integrated Endpoint Protection, Risk Management, and Attack Forensics Platform

GravityZone Elite safeguards your organization from the full spectrum of sophisticated cyber threats. With more than 30 machine learning-driven security technologies, GravityZone provides multiple layers of defense that consistently outperforms conventional endpoint security, as proven in independent tests. A single-agent, single-console platform for physical, virtual, mobile and cloud-based endpoints and email, GravityZone Elite minimizes management overhead while giving you ubiquitous visibility and control.

Next-Generation Endpoint Security, Evolved

WORLD'S STRONGEST PREVENTION

Automatically stop 99% of attacks with #1 ranked prevention that combines over 30 technologies, such as tunable machine learning, sandbox analyzer, anti-exploit and behavioral analysis



ATTACK FORENSICS AND VISUALIZATION

Gain insight into your threat environment and perform forensic analysis by zeroing in on attacks specifically aimed at your organization. Visualize the attack kill chain and perform required remediation

ENDPOINT HARDENING AND RISK MANAGEMENT

Strengthen security posture with integrated device- and application control, patching, encryption and other technologies. Leverage integrated Risk Management and Analytics to continuously assess, prioritize, and address misconfigurations and vulnerabilities

HyperDetect™ tunable machine learning blocks file-less attacks

Sandbox Analyzer enhances detection of targeted attacks

Anti-Exploit, Process Control, and Network Defense maximize efficacy

Web-Threat Protection, Application- and Device Control harden endpoints

NEW

Attack Forensics provides visibility and insight into attacks

NEW

Risk Management and Analytics helps control risk and reduce attack surface

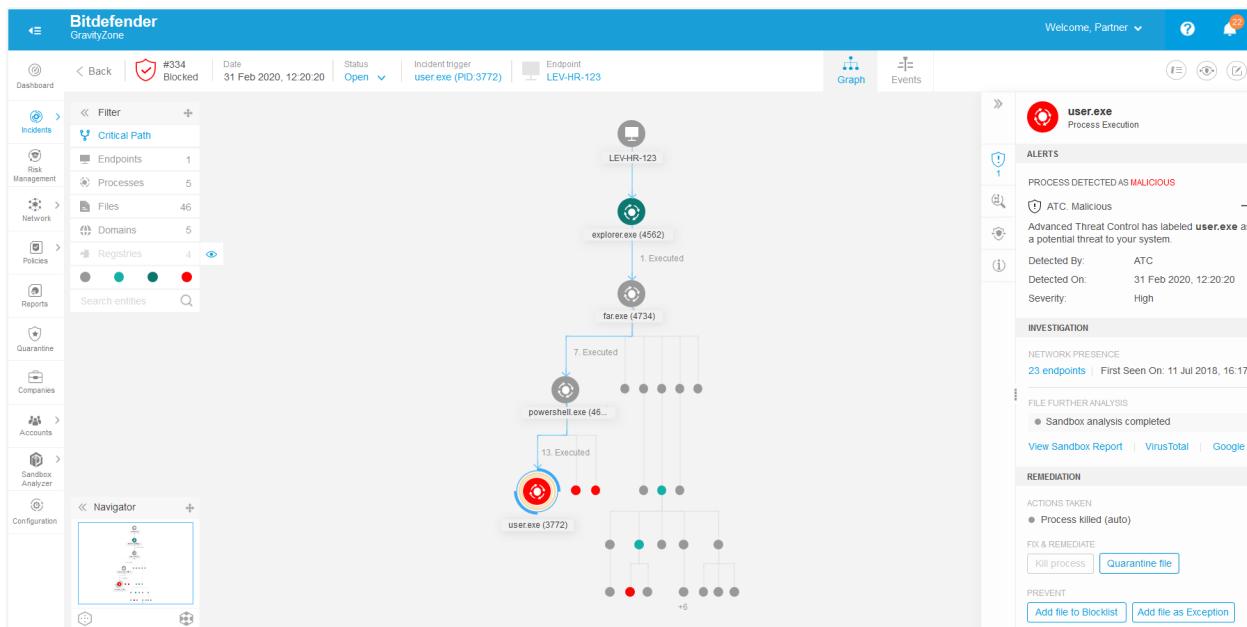
NEW

Patch Management, Encryption, and Email add-ons further strengthen security posture

Attack Forensics and Visualization

Enhance visibility into organization-specific threats. Understand the broader context of attacks on your endpoints with root-cause analysis and attack kill-chain visualization. Remediate threats detected by GravityZone prevention technologies (Antimalware, Sandbox, and Network-Attack Defense).

Analyze how an attack was engineered and zero in on its specific stages, machines, processes, files, web domains and other elements. Enhance GravityZone's automatic remediation capabilities with manual action, such as remotely running PowerShell commands on the infected machine, killing a process, quarantining a file or adding a file to a shared blocklist.



The screenshot displays the Bitdefender GravityZone interface. On the left, a sidebar navigation includes 'Dashboard', 'Incidents' (selected), 'Risk Management', 'Network', 'Policies', 'Reports', 'Quarantine', 'Companies', 'Accounts', 'Sandbox Analyzer', and 'Configuration'. The main area shows an 'Attack Tree' for a process named 'user.exe (3772)' on endpoint 'LEV-HR-123'. The tree shows the following sequence of events:

- 1. Executed: explorer.exe (4562)
- 2. Executed: far.exe (4734)
- 3. Executed: powershell.exe (46...)
- 4. Executed: user.exe (3772)

Each node is represented by a circular icon with a progress bar. To the right of the tree, a detailed threat card for 'user.exe' is shown:

- ALERTS:** PROCESS DETECTED AS **MALICIOUS**
- Detected By:** ATC
- Detected On:** 31 Feb 2020, 12:20:20
- Severity:** High
- INVESTIGATION:** NETWORK PRESENCE: 23 endpoints, First Seen On: 11 Jul 2018, 16:17
- FILE FURTHER ANALYSIS:** Sandbox analysis completed
- REMEDIAL ACTIONS:** Process killed (auto)
- PREVENT:** Kill process, Quarantine file
- Fix & Remediate:** Add file to Blocklist, Add file as Exception

GravityZone Elite Attack Forensics and Visualization: Attack Tree

Endpoint Risk Management and Analytics

Actively reduce your organization's attack surface by continuously assessing, prioritizing, and addressing endpoint risk coming from misconfigurations and application vulnerabilities.

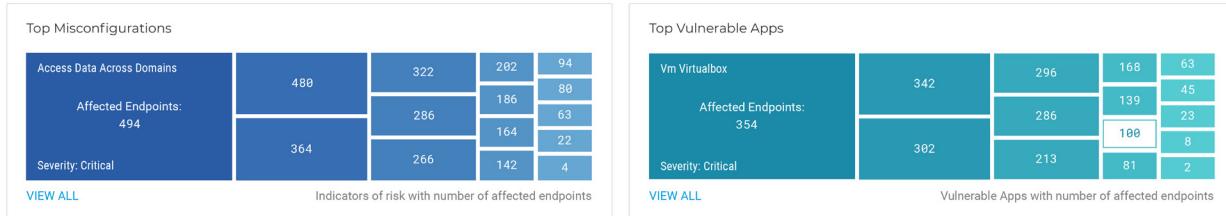
- View your overall Company Risk Score and understand how various misconfigurations and application vulnerabilities contribute to it:



GravityZone Elite Risk Management Dashboard: Company Risk Score and Its Components

Endpoint Risk Management and Analytics (Continued)

- Assess prioritized misconfigurations and application vulnerabilities across your organization's endpoint estate:



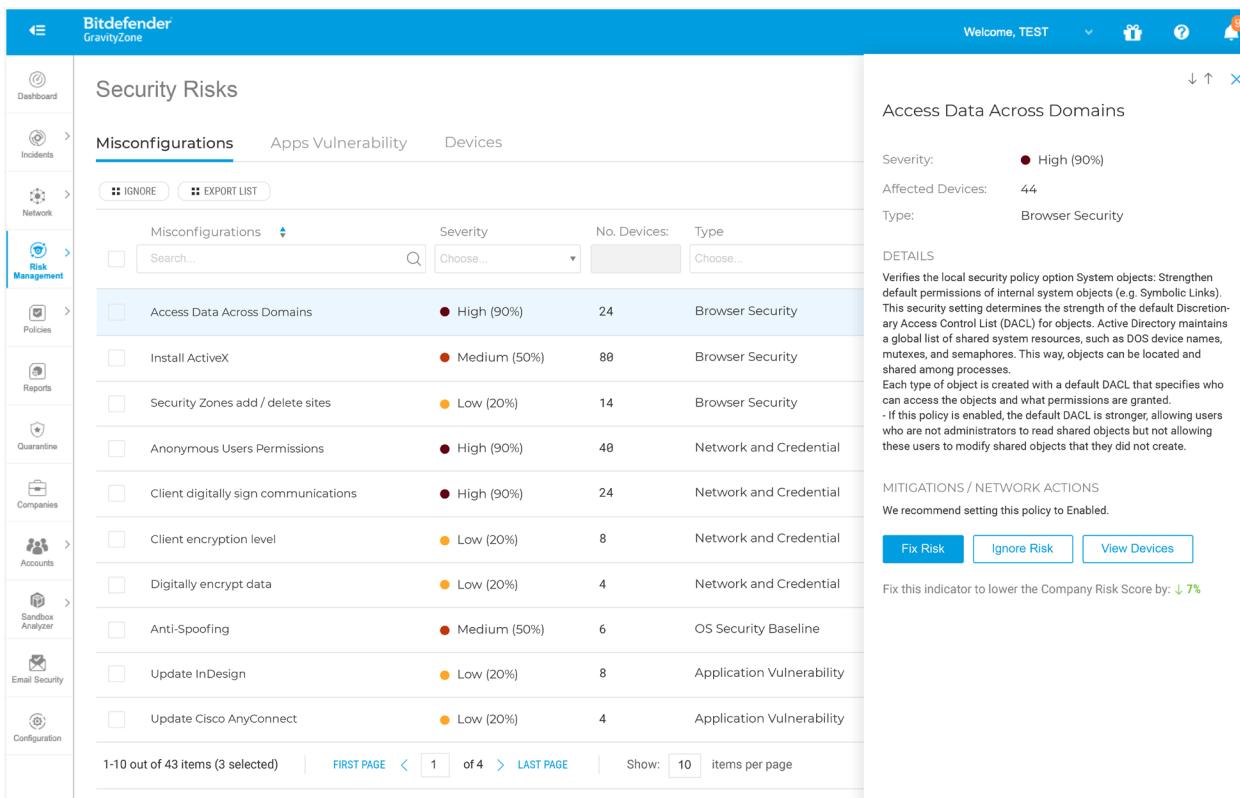
GravityZone Elite Risk Management Dashboard: Misconfigurations and Vulnerable Apps

- Get a risk snapshot for servers and end-user devices, and review the most-exposed endpoints:



GravityZone Elite Risk Management Dashboard: Risk Severity by Endpoint Type

- Leverage convenient filtering options to search through indicators of risk and zero in on specific misconfigurations, vulnerable applications, or individual devices. Mitigate risk by taking recommended actions:



Security Risks

Misconfigurations

Misconfigurations	Severity	No. Devices	Type
Access Data Across Domains	High (90%)	24	Browser Security
Install ActiveX	Medium (50%)	88	Browser Security
Security Zones add / delete sites	Low (20%)	14	Browser Security
Anonymous Users Permissions	High (90%)	40	Network and Credential
Client digitally sign communications	High (90%)	24	Network and Credential
Client encryption level	Low (20%)	8	Network and Credential
Digitally encrypt data	Low (20%)	4	Network and Credential
Anti-Spoofing	Medium (50%)	6	OS Security Baseline
Update InDesign	Low (20%)	8	Application Vulnerability
Update Cisco AnyConnect	Low (20%)	4	Application Vulnerability

Access Data Across Domains

Severity: High (90%)

Affected Devices: 44

Type: Browser Security

DETAILS

Verifies the local security policy option System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links). This security setting determines the strength of the default Discretionary Access Control List (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. This way, objects can be located and shared among processes.

Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted.

- If this policy is enabled, the default DACL is stronger, allowing users who are not administrators to read shared objects but not allowing these users to modify shared objects that they did not create.

MITIGATIONS / NETWORK ACTIONS

We recommend setting this policy to Enabled.

Fix Risk **Ignore Risk** **View Devices**

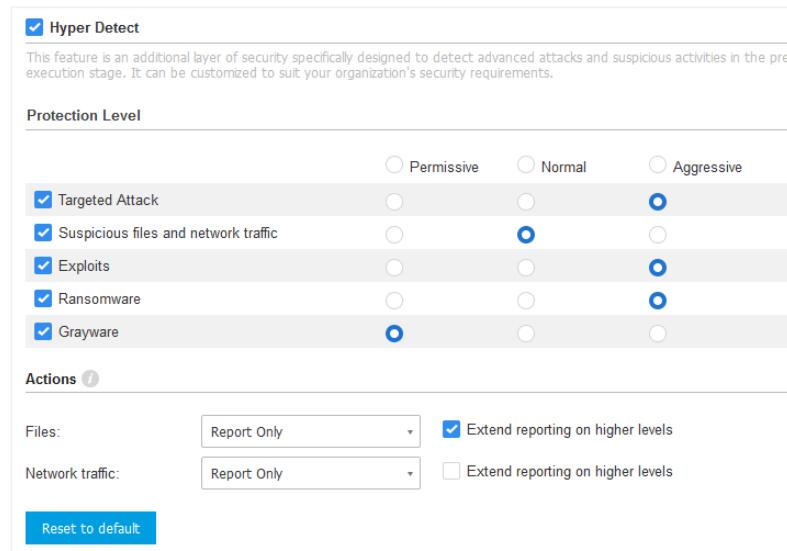
Fix this indicator to lower the Company Risk Score by: ↓ 7%

GravityZone Elite Security Risks Section: Indicators of Risk with Mitigation Recommendations



HyperDetect Tunable Machine Learning

Leverage HyperDetect's machine learning models and stealth attack-detection technology to stop polymorphic threats, obfuscated malware, file-less and script-based attacks and other suspicious activities before they can run on the endpoint (pre-execution). Adjust the detection-aggressiveness level to ensure visibility into high-impact threats and minimize noise from low-risk, low-probability infections.



GravityZone Elite: HyperDetect Configuration Menu

Bitdefender GravityZone: A Leader in Endpoint Protection



"GravityZone provided the highest levels of reliable security without slowing down computers and impacting the users' experience. Operationally, GravityZone also stood out because it provides a central view of our infrastructure and is easy to manage."

— Matt Ulrich, Network Administrator
Speedway Motorsports

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

