GravityZone Risk Management

Problem Statement

Security risks have the potential to expose businesses to devastating cyberattacks. Among them: misconfigured policy settings in the operating system, unencrypted passwords, weak browser security settings, software vulnerabilities, and more. In addition, security vulnerabilities caused by human behavior can be equally as impactful, with the potential of leaking sensitive data, and opening up your network to ruinous hacks, data exfiltration, data ransoming, and asset destruction.

Security teams are struggling to gain visibility into these security risks in time to prevent a breach or cyber-attack and are faced with many challenges:

- Managing large numbers of users, including those working remotely requires an enormous amount of resources.
- Maintaining visibility into vulnerable applications is difficult without the right tools.
- Overseeing patches for the operating system and software is arduous to maintain.
- Understanding where to first prioritize their efforts is time-consuming and risky.

These challenges are exponentially worse for Managed Service Providers (MSP) and Managed Security Service Providers (MSSP), who are required to oversee the environments of numerous businesses.

Detection Overview

GravityZone Risk Management allows security teams to scan for, and identify risks associated with the Windows Operating System misconfigurations, vulnerable applications, and human-based behavior. The identification of risk is tailored to the company's industry. With the ability to configure routine scans, admins can be made aware of security risks on a daily basis, and they can then review these risks through a comprehensive Risk Management dashboard.

At-a-Glance

Advanced endpoint and human risk assessment available through GravityZone for Windows and Linux, help minimize cybersecurity risks through analysis, reporting, and remediation .

Key Capabilities

- **Complete visibility into security risks** – scan for risks associated with OS misconfigurations, application vulnerability, and user-behavior that can put businesses in peril
- **Comprehensive dashboard** – allows security teams to quickly identify and review high-risk users and devices and eliminates the frustration and confusion associated with managing security risks
- **Scheduled Risk Scans** – allows security teams to stay up-to-date on emerging security risks. As new security risks emerge, security teams will be able to stay on top of them and quickly remediate them
- **Fix security risks right from the GravityZone console** – many OS misconfigurations can be easily remediated right from the Risk Management Dashboard. With the addition of the GravityZone Patch Management add-on, security teams can patch vulnerable applications with a single click of a button on all affected systems

> *"We now see everything from a protection status at a glance via one console. Our staff has found GravityZone much easier to manage than other vendors' security solutions."*
>
> *Josh Gilliland, Security Team Lead, GEHA*

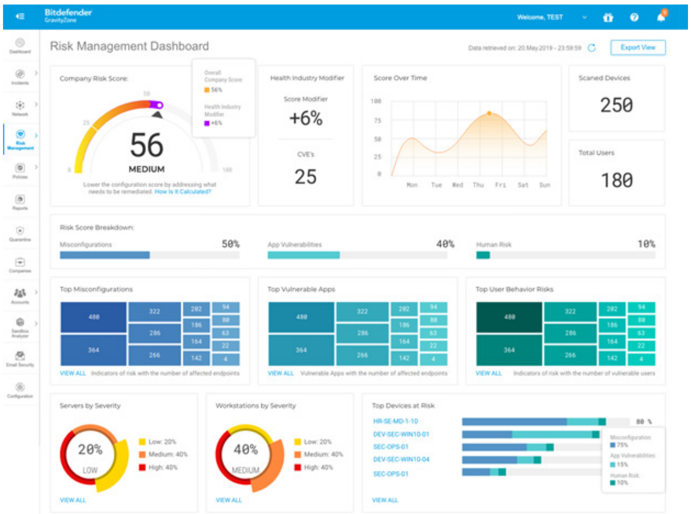


Figure 1.1: The GravityZone Risk Management dashboard gives you complete visibility into security risks, allowing admins to easily track high priority risks through a comprehensive scoring and categorization system

The Risk Management dashboard provides an easy-to-understand risk assessment score that grants admins an effortless way to determine which systems or users are at greater risk. The score fluctuates based on the number of risks identified in the risk scan, their severity, and whether the risk has been remediated. Along with the overall risk score, risks are further divided by categories – which we will discuss in detail in the next section – Server and Workstation security risks, Top Devices, and Top Users at risk. This allows security teams to quickly identify what companies, systems, and users they want to focus on first. This feature helps alleviate a lot of the confusion and torpidity associated with having to manage risks across a company or multiple companies.

Through the analysis of the risk details in the dashboard, we provide a clear understanding of the risk, along with relevant remediation actions. Security teams can also immediately deploy patches using the Bitdefender GravityZone Patch Management add-on right from the Risk Management Dashboard.

Response Overview

By reviewing systems for several indicators of risk, GravityZone Risk Management can help identify and mitigate potential security weak points caused by OS misconfiguration, vulnerable apps, and user behavior. A Risk Scan can be triggered individually on any system from the GravityZone console, or periodically, configured through a policy. Once the risk scan completes, an overall Risk Score is provided based on the identified risks and the Health Industry Modifier selected. Security teams can swiftly identify the systems and users that are most at risk.

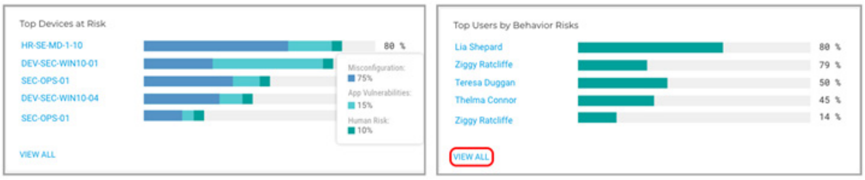
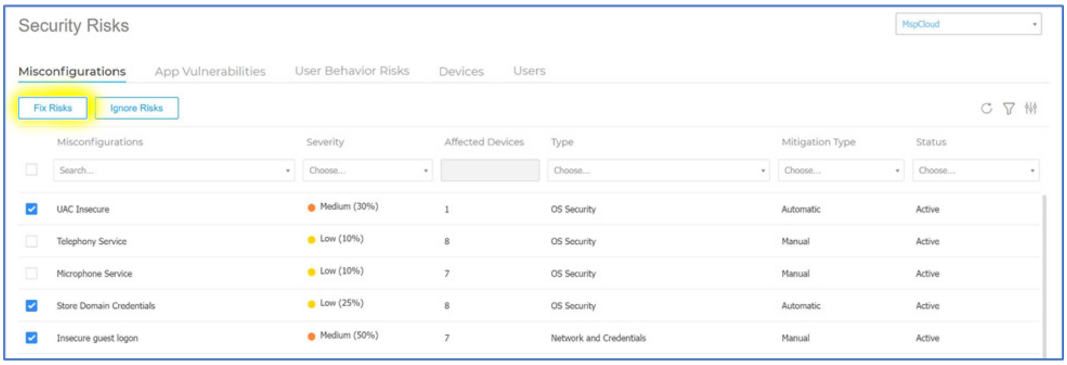


Figure 2.1: The Risk Management console makes it very easy to prioritize the top "at risk" devices and users. Many risks can be fixed directly from the Bitdefender Risk Management dashboard, making mitigation fast and efficient.

Multi-Tenant Risk Management

MSPs and MSSPs managing multiple companies can use the “Companies” view to quickly determine which business they manage is most at risk, and immediately start resolving the highest severity risks.



☐	Misconfigurations	Severity	Affected Devices	Type	Mitigation Type	Status
	Search...	Choose...		Choose...	Choose...	Choose...
☑	UAC Insecure	● Medium (30%)	1	OS Security	Automatic	Active
☐	Telephony Service	● Low (10%)	8	OS Security	Manual	Active
☐	Microphone Service	● Low (10%)	7	OS Security	Manual	Active
☑	Store Domain Credentials	● Low (25%)	8	OS Security	Automatic	Active
☑	Insecure guest logon	● Medium (50%)	7	Network and Credentials	Manual	Active

Figure 3.1: Security teams will be able to immediately fix Misconfiguration risks with the push of a button from the GravityZone Risk Management Dashboard.

A Risk Score breakdown provides an overview of the top identified risks in three separate categories:

Misconfigurations

Identifies Risk associated with the Windows operating system— these includes issues with local and group policies, vulnerable services, computer configuration settings, and more.

App Vulnerabilities

Provides visibility into applications installed on the managed endpoints that have been identified to contain some security risk associated with the Common Vulnerabilities and Exposure system (CVE).

User Behavior Risk

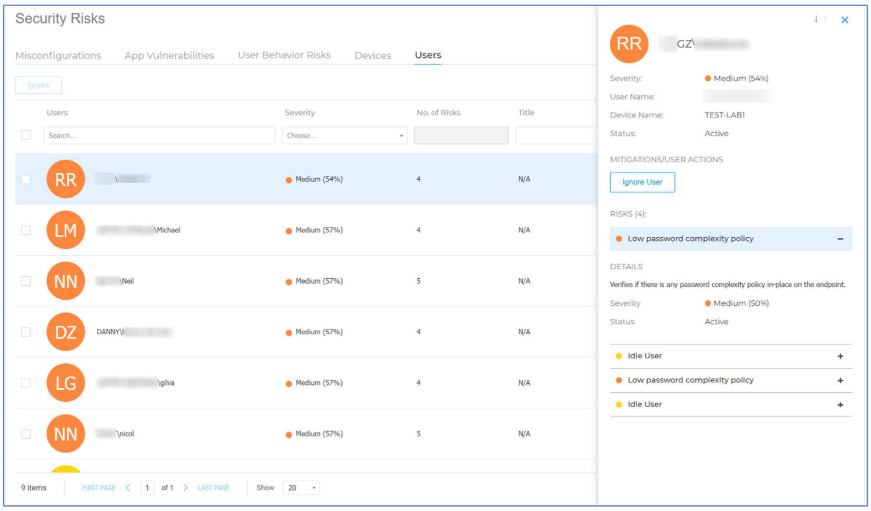
Tracks user activity that can potentially compromise a business’ security. The User Behavior tracking can be disabled if so desired, for security teams who wish to not use this feature.

GravityZone Risk Management identifies applications installed on the managed endpoints that have a known security vulnerability which can be compromised by an exploit technique. This allows security teams to target those applications that pose the highest security risk first. With the inclusion of GravityZone Patch Management, they can quickly and easily patch those applications with a simple press of a button.

The security teams can also choose to Ignore the risk, view a list of the devices where the hazardous application is installed, or review the CVE in greater detail to better understand the risk that is posed.

Risky User Behavior Identified

User Risk review allows the security teams to identify those users who have exhibited some behavior that is a potential security risk. The dashboard provides them with details on why the behavior identified is risky, and the security teams can then choose to take immediate remediation action, or simply ignore the risk.   For security teams that choose to enable this feature, they will have unique visibility into several indicators of risk such as: users having passwords with low complexity or using the same password across multiple sites, SMB connections with plain text authentication, identifying users that have used infected external storage devices, and more.



Security Risks

□	Users	Severity	No. of Risks	Title
□	Search...	Choose...		
□	RR [redacted]	● Medium (54%)	4	N/A
□	LM [redacted]\Michael	● Medium (57%)	4	N/A
□	NN [redacted]\Neil	● Medium (57%)	5	N/A
□	DZ DANNY\[redacted]	● Medium (57%)	4	N/A
□	LG [redacted]\gilva	● Medium (57%)	4	N/A
□	NN [redacted]\nicol	● Medium (57%)	5	N/A

RR GZ\[redacted]

Severity:	● Medium (54%)
User Name:	[redacted]
Device Name:	TEST-LAB1
Status:	Active

MITIGATIONS/USER ACTIONS

RISKS (4):

● Low password complexity policy −

DETAILS

Verifies if there is any password complexity policy in-place on the endpoint.

Severity	● Medium (50%)
Status	Active

● Idle User +

● Low password complexity policy +

● Idle User +

Figure 4.1: Using the Risk Management Dashboard, security teams can quickly review those users whose behavior has the potential to compromise the security of the systems

With GravityZone Risk Management, Security teams now have a powerful, comprehensive tool to help identify and remediate security vulnerabilities in their businesses. The tool allows them to swiftly recognize the high-priority risks they need to target first, providing a robust prevention piece that saves them time, resources, and potentially spares them from a potentially disastrous cyber-attack.

Bitdefender
BUILT FOR RESILIENCE

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