AimPoint Group

FINANCIAL IMPACT ASSESSMENT

SPONSORED BY Bitdefender

GravityZone Platform and MDR

Bitdefender customers quantify their **financial and operational savings** with the GravityZone cybersecurity platform and MDR service

Key Findings of This Study

GravityZone cybersecurity platform

By using the Bitdefender GravityZone cybersecurity platform, organizations can expect these annual savings per 1,000 employees*:

$67,548
on IT and security staff time

$32,021
on direct expenses

for a total annual saving of

$99,569
per 1,000 employees

GravityZone Managed Detection and Response (MDR)

By deploying GravityZone Managed Detection and Response (MDR) in conjunction with the platform, organizations can expect these annual savings per 1,000 employees*:

An additional $79,976
on IT and security staff time

plus $135,356
on the cost of after-hours security coverage

for an additional annual saving of

$215,332
per 1,000 employees

* Figures have been adjusted to model results for 1,000 employees.
Readers can adjust the figures down or up based on the size of their own organization.

Overview of the Research

Integrated cybersecurity platforms offer far-reaching benefits for hard-pressed information technology and security teams responsible for reducing vulnerabilities in endpoints, reviewing a torrent of alerts, and protecting against hundreds of cyber attacks. Many of these teams have also turned to to a managed detection and response (MDR) service that provides 24×7×365 threat monitoring and immediate access to cybersecurity experts for specialized knowledge and proven action plans.

The solutions also provide financial and operational benefits that save time and money. These include automating security processes, eliminating false positive alerts, reducing spending on overlapping security tools, and providing uninterrupted attack response at a fraction of the cost of hiring staffers for after-hours shifts.

But how big are the financial and operational benefits in the real world? In what areas do they produce the greatest savings? Are the savings large enough to move the needle by offsetting most or all the cost of the platform and services?

To answer these questions, AimPoint Group interviewed IT and cybersecurity managers at four organizations that work with the Bitdefender GravityZone cybersecurity platform and MDR service. They have between 250 and 1,800 employees, and all have lean IT and security teams whose members have multiple responsibilities.

We asked the managers to estimate time and direct expense savings attributable to the platform and services compared to their organization's experience before deploying GravityZone. We then averaged and adjusted the figures to show savings per 1,000 employees. You can scale the results down or up to see the impact on your organization. The findings are summarized in the appendix.

Financial and operational benefits include saving time and money by:

- Automating security processes
- Eliminating false positive alerts
- Reducing spending on security tools
- Providing 24×7×365 attack response at low cost

Profiles of the Organizations

Industry	People working on cybersecurity	Key security challenges
Manufacturing	Cybersecurity tasks shared by an IT team of three Time spent on security = 2 FTEs	• Unified visibility across IT and OT environments • Vulnerability and patch management at scale • Limited after-hours (24×7×365) security coverage
Non-profit	Cybersecurity tasks shared by several IT and help desk staff Time spent on security = 1 FTE	• Budget constraints requiring cost-effective security • Resource-intensive vulnerability and patch management • High operational impact of false positive alerts
Local government	One full-time cybersecurity person with support from several IT and help desk staff Time spent on security = 2 FTEs	• Assuring the continuity of mission-critical public services • Budget constraints requiring cost-effective security • Fragmented security tools and limited operational visibility
Engineering services	One full-time cybersecurity person with support from three system admins Time spent on security = 2.5 FTEs	• Securing a highly distributed workforce across multiple locations • Vulnerability and patch management across widely dispersed regions • High alert volumes creating unsustainable investigation and triage overhead

FTE = Full-time equivalent (amount of work typically performed by one full-time employee)

Financial Benefits of the Cybersecurity Platform

The person primarily responsible for cybersecurity at each organization was asked to estimate time and direct expense savings attributable to the GravityZone platform and MDR service when compared to the security tools and services in place before Bitdefender solutions were deployed. The estimates of hourly savings were converted to weekly and annual dollar savings based on fully loaded compensation (base pay plus benefits and bonuses) of $75 per hour.

None of the organizations reduced staff based on the hours saved. Rather, they reallocated the time to have team members work on neglected security tasks and other high-value IT projects. The managers believe that the value to their organization of that extra work is equal to or significantly greater than the simple hourly savings imply.

This section of the report discusses savings from GravityZone. Additional savings from MDR are covered in the next section.

TIME SAVED ON PREVENTION AND PATCHING

To maintain a strong security posture and prevent attacks from reaching systems and applications, cybersecurity teams must manage a range of time-consuming activities. These include scanning for vulnerabilities, applying software patches to servers and endpoints, fixing misconfigurations, and managing access. Prevention also includes assessing risks, prioritizing remediation activities, and other steps to reduce and harden the organization's attack surface.

The IT and security managers interviewed for this report estimated that their organizations saved **between 6 and 10 hours weekly** on prevention activities.

The managers singled out vulnerability management and patching as the largest source of these savings. They highlighted the GravityZone platform's patch management capabilities to automate vulnerability tracking, target patches at relevant endpoints, and apply them with minimal human intervention and very high reliability.

> "We use Bitdefender patch management. We set it and it just does its thing. The new patches come in and they get applied."
>
> — Jason Kraai, Corporate Senior Systems Administrator, GPI (Greenman-Pedersen, Inc.)

Results

Normalizing the average time savings for the four organizations to show the results for a typical organization with 1,000 employees results in savings of 7.1 hours per week. At $75 per hour of fully loaded costs, that works out to:

Saving on prevention and patching of $533 weekly, or $27,716 annually.

TIME SAVED ON MONITORING, TRIAGE, ATTACK INVESTIGATION, AND RESPONSE

Organizations that quickly detect, analyze, and contain attacks can minimize attacker dwell time, reduce the blast radius of incidents, limit financial exposure from data theft and ransomware, and maintain system availability for business processes. But to achieve those goals, defenders must continually monitor alerts from security, network and systems management tools and perform triage. They must investigate incidents to determine the seriousness of the attacks, their points of impact, and their spread inside the organization. They must also execute containment steps such as quarantining employee systems compromised by malware and blocking communication with suspicious servers on the internet.

The managers interviewed for this report estimated that their organizations saved between **2 and 22 hours weekly** on monitoring, triage, investigation, and response.

They emphasized a dramatic reduction in the number of false positive alerts which allowed them to focus on the high-priority alerts while freeing up time to perform additional high-value activities. They also discussed how they saved time and made better decisions by being able to view in one console security data from many sources rather than having to collect and manually correlate data from multiple security tools.

Some of the managers also pointed to GravityZone's capability to automatically execute containment measures according to pre-defined rules, without human intervention.

Results

Normalizing the average time savings for the four organizations to show the results for a typical organization with 1,000 employees results in savings of 8.1 hours per week. At $75 per hour of fully loaded costs, that works out to:

Savings on monitoring, triage, investigation, and response of $608 weekly, or $31,616 annually.

Closing the window faster

The figures above are for hours of work saved. Interviewees also pointed out that GravityZone dramatically reduces the *elapsed time* for investigation and containment. That means attackers have a much shorter window to perform reconnaissance on the network, disseminate ransomware, and find and exfiltrate data. The result: reduced costs related to stolen data, disruption of business processes, fines for data breaches, and reputational damage.

> "GravityZone eliminates almost all our false positive alerts and presents us with only the alerts that need attention and the information we need to take action."
>
> — Sai Ravichandran, Director, Information Technology, Morton Arboretum

> "Before GravityZone, we'd be spending half our time doing triage. We had to collect data from four or five different systems, put all of it together, and see what it meant. Now, with Bitdefender, when we get a notification, we click on it and it tells us what the issue is that has been detected. All that information is in a single spot. It appears in a mouse click."
>
> — Jason Kraai, Corporate Senior Systems Administrator, GPI (Greenman-Pedersen, Inc.)

TIME SAVED ON TOOL ADMINISTRATION AND POLICY MANAGEMENT

Every hour spent on administrative tasks is one less hour available to prevent or mitigate costly cyberattacks. Yet cybersecurity tools must be monitored to ensure they are working and correctly configured. Time is also required to specify policies and rules to control actions the tools take under different circumstances, and those rules and policies need to be updated based on evolving threats and new business requirements.

Two of the managers interviewed for this report estimated that their organizations saved **4 and 5 hours weekly** on security tool administration and policy management. They cited GravityZone's dramatically better ease of use for administration and effective automation of policy updates to endpoints.

> "Bitdefender's solutions are light-years easier to manage than comparable products on the market."
>
> — Senior Cybersecurity Analyst, City Government

Results

Normalizing the average time savings across the four organizations to show the results for a typical organization with 1,000 employees results in savings of 2.1 hours per week. At $75 per hour of fully loaded costs, that works out to:

Savings on tool administration and policy management of $158 weekly, or $8,216 annually.

DIRECT EXPENSES SAVED

Organizations that use an integrated cybersecurity platform to consolidate security functions can eliminate license costs for redundant and overlapping security tools.

The interviewed managers estimated that their organizations discontinued software licenses totaling **between $8,900 and $67,230 annually.**

Software products mentioned as being phased out included:

- Vulnerability management
- Patching
- "Security utilities"
- SIEM
- Standalone endpoint detection and response (EDR)

One manager stated that the GravityZone platform reduced his company's cyber insurance premiums by about $10,000 annually.

Results

Normalizing the average expense savings for the four organizations to show the results for a typical organization with 1,000 employees results in a:

Reduction in direct expenses of $32,021 annually per 1,000 employees.

Minimizing tool sprawl

Interviewees described other advantages of consolidating on an integrated platform: one management console instead of several, one agent per endpoint to deploy instead of several, complete data in one place for analysis and reporting, and less time negotiating contracts and onboarding vendors.

What about cyber insurance premiums?

All the managers interviewed agreed that GravityZone had reduced their cyber insurance premiums by demonstrating to the insurer that their organization had deployed recommended security technologies and best practices. However, only one had enough information to state a specific figure (savings of $10,000 annually). Because there was only one data point, we did not include insurance expenses in this analysis, but it is likely that most organizations will get a significant reduction.

Financial Benefits of the MDR service

MDR services combine monitoring and incident response services with access to cybersecurity specialists in disciplines such as threat research, detection engineering, threat hunting, and incident root cause and impact analysis. They enhance an organization's IT and cybersecurity efforts by:

- Ensuring 24×7×365 security coverage to detect and contain attacks quickly during non-business hours
- Executing "pre-approved actions" (PAAs) to contain attacks at the earliest possible moment (for example, blocking malicious files from executing on endpoints, isolating infected host systems, or disabling access rights for compromised user accounts)
- Providing analysis, threat intelligence, and practical experience that accelerate and improve triage, response, and containment
- Sharing expertise and recommendations on how to protect against emerging threats, harden an organization's attack surface, and improve security processes

Advantages of a single, cohesive team

GravityZone MDR, used by all four organizations interviewed in this report, has an advantage over many other MDR offerings. A single, cohesive team owns threat research, the MDR technology stack, and GravityZone platform and detection engineering. This enables superior insights into security context, threats, exposure, risks, and information assets. It also facilitates a new level of data correlation and analysis that goes well beyond what other MDR providers can supply. As a result, organizations experience many fewer incidents and can react much faster when incidents do occur.

TIME SAVED BY MDR MONITORING, TRIAGE, ATTACK INVESTIGATION, AND CONTAINMENT ACTIVITIES

The managers interviewed for this report estimated that their organizations saved **between 2 and 45 hours weekly** from the MDR service monitoring, triage, investigation, and containment activities.

They highlighted:

- The ability of the MDR SOC to contain most attacks immediately through the use of "pre-approved actions" (PAAs)
- How MDR experts help the organization's team analyze and recover from complex attacks like ransomware rapidly and effectively by providing contextual information, threat intelligence, analysis, and recommended action plans (see the example below).

Several also commented on time savings from automatically generated monthly management reports and periodic threat hunting efforts included as part of the MDR offering. Some mentioned help identifying security weaknesses and performing risk assessments.

> "The MDR service gives us peace of mind, because we know they give us the appropriate support and monitoring and handle things before they become a problem. And knowing that there is someone there when we have questions is a big relief."
>
> — Sai Ravichandran, Director, Information Technology, Morton Arboretum

Results

Normalizing the average time savings for the four organizations to show the results for a typical organization with 1,000 employees results in savings of 20.5 hours per week. At $75 per hour of fully loaded costs, that works out to:

Savings from MDR monitoring, triage, investigation, and containment activities of $1,538 weekly, or $79,976 annually.

Responding to major ransomware attacks – before and after

One manager compared his organization's responses to two major ransomware attacks, one before deploying the GravityZone platform and MDR service, and one after.

In the earlier attack, 4 or 5 IT and security people worked 12-hour days for *two weeks* to collect information, analyze the attack, isolate compromised systems, block paths to suspicious external websites, and perform other necessary containment and remediation actions.

In the later attack, the same 4-5 people also worked long hours– but the equivalent results were achieved in *three days*.

EXPENSE SAVINGS FROM 24×7×365 COVERAGE

One of the managers interviewed for this report stated that it was becoming "unacceptably risky" for his organization to operate without comprehensive 24×7×365 security coverage. Adopting GravityZone MDR enabled him to avoid hiring one or two additional team members to staff an after-hours late shift.

To count or not to count savings from after-hours coverage?
The other three managers interviewed for this report agreed that after-hours security coverage from the MDR service has been a major benefit to themselves and their team. However, because they believe their organization would not consider hiring additional staff for after-hours coverage, regardless of the risk, they did not estimate a specific amount of savings.

Whether or not you choose to attribute savings to comprehensive round-the-clock security coverage, keep in mind that 35%-40% of incidents that require a response occur during or close to non-business hours.[1]

35%-40% of incidents that require a response occur during or close to non-business hours.[1]

Estimated savings and results

Estimated savings for an organization that otherwise would have needed to increase its staff to provide after-hours coverage were 37.7 hours per week.

At $75 per hour, that works out to:

Savings on 24×7×365 security coverage of $2,603 weekly, or $135,356 annually.

Why on-call coverage after hours is risky

Several of the interviewed managers expressed serious reservations about the common practice of designating one team member to be on call outside of business hours, receiving alerts by email or text. They would often miss these alerts while living their normal lives or sleeping. The result is that they don't respond for hours, or even until the next morning, giving attackers a long window to cause damage. Also, unless alerts are very accurately filtered before being sent, the on-call staff member is often bombarded by duplicate and irrelevant alerts, causing stress and a tendency to check emails and texts even less frequently.

1 Bitdefender MDR SOC statistics

Stress Reduction and Increased Employee Satisfaction

Another topic that emerged consistently in interviews was the positive impact of the GravityZone platform and MDR service on stress levels, work-life balance, and peace of mind for both the managers interviewed and others participating in cybersecurity activities.

The GravityZone platform, by slashing the number of false positive alerts and automating security processes, reduces the feeling of being overwhelmed by boring routine tasks and provides more time for high-value activities.

GravityZone MDR gives IT and cybersecurity team members confidence that they are backed up by world-class specialists who will make them more productive and reduce the chances of bad decisions.

24×7×365 security coverage improves work-life balance by minimizing the inconvenience and stress of being on call when at home and during leisure activities.

Some of the managers interviewed intimated that they felt relieved of the fear that a missed alert or a mistake might result in an incident costing millions of dollars.

While the managers could not put monetary values on stress reduction and improved employee satisfaction, it is very likely they result in significant savings by preventing burnout and turnover among IT and cybersecurity personnel.

Some managers intimated that they felt relieved of the fear that a missed alert or a mistake might result in an incident costing millions of dollars.

Putting the Pieces Together

It is now widely recognized that integrated cybersecurity platforms and MDR services can simplify the lives of lean IT and cybersecurity teams and dramatically improve security outcomes. But very little data has been available on where, why, and how much they help organizations save time and money.

This report begins to fill that gap by providing estimates of the savings by front-line managers at a small but diverse sample of real organizations. Those figures, adjusted to show average savings per 1,000 employees, are shown in the appendix.

In addition, our discussions with IT and cybersecurity managers demonstrate that their organizations benefited the most from:

- Consolidating security capabilities into a single platform
- Automating routine security operations, especially endpoint patching
- Slashing the number of alerts to triage
- Reducing investigation effort through higher-quality detections
- Simplifying tool administration
- Containing many attacks immediately with pre-approved actions
- Augmenting internal teams with expert-led MDR services
- Reducing stress on IT and cybersecurity team members

> "Bitdefender GravityZone and MDR are probably the most valuable of all our security tools. Of all the areas of cybersecurity, the ones that Bitdefender covers concern us least."
>
> — Jason Kraai, Corporate Senior Systems Administrator, GPI (Greenman-Pedersen, Inc.)

About GravityZone and MDR

The GravityZone platform simplifies security operations across the complete cyber threat lifecycle. It reduces risk with tooling optimized for lean IT and security teams by consolidating prevention, protection, detection and response on a single platform. It is underpinned by trusted, innovative security technology that consistently leads independent evaluations and powers the world's security ecosystems.

GravityZone MDR was built for the era of AI-enabled security overload. It reduces incidents and enables lean IT and security teams to trust every response and prove their security posture.

GravityZone MDR combines complete platform, engineering and threat research ownership for native, contextual exposure and threat insights from Bitdefender experts. Customers achieve AI-led machine-speed detection and containment, combined with human judgment, validation and arbitration, to ensure response accuracy and attack containment 24×7×365.

Together, they provide stronger security outcomes, lower operational overhead, and more time for lean IT and security teams to focus on strategic initiatives while reducing the risk and impact of successful attacks.

Appendix: Average Savings Per 1,000 Employees

GRAVITYZONE PLATFORM	Hours saved weekly	Cost savings*	
		Weekly	Annual
Prevention, including patch management	7.1	$533	$27,716
Monitoring, triage, investigation, and attack containment	8.1	$608	$31,616
Tool administration and policy management	2.1	$158	$8,216
Subtotal	17.3	$1,299	$67,548
Direct expenses for software subscriptions	--	--	$32,021
Total annual savings			**$99,569**

MDR SERVICE	Hours saved weekly	Cost savings*	
		Weekly	Annual
Monitoring, triage, investigation, and attack containment	20.5	$1,538	$79,976
After-hours security coverage	34.7	$2,603	$135,356
Total annual savings		$4,141	**$215,332**

*Assumes fully loaded compensation (base salary plus benefits and bonuses) of $75/hour