

Bitdefender®

GravityZone

SOLUTION GUIDE

Do more with less: Streamlined Ransomware Protection for Lean IT Teams



All Rights Reserved. © 2025 Bitdefender. All trademarks, trade names, and products referenced herein are the property of their respective owners. The information contained in this document is confidential and only for the use of the intended recipient.

You may not publish or redistribute this document without advance permission from Bitdefender.

Ransomware remains one of the most relentless and costly threats organizations face today. Despite years of heavy investment in cybersecurity tools and awareness programs, companies continue to fall victim at an alarming rate.

According to [Verizon's 2025 Data Breach Investigations Report \(DBIR\)](#), ransomware incidents surged by 37% year-over-year, indicating that attackers are evolving faster than many defenses can keep pace. For IT and security leaders, this serves as a reminder that traditional, siloed defenses are no longer sufficient.

Part of the challenge lies in how ransomware capitalizes on gaps across the attack surface. Attackers thrive when teams fail to patch vulnerabilities, misconfigure systems, and stretch their resources too thin. This dynamic helps explain why larger enterprises with mature compliance programs (such as those in heavily regulated industries like finance) tend to perform better. Meanwhile, smaller organizations and lean IT teams often struggle to match that level of protection, which makes them prime targets.

The good news is that effective defense is not limited to enterprises with expansive security teams. Using the right mix of prevention, detection, response, and risk management techniques means that even lean IT teams can establish enterprise-grade ransomware protection.

Tracing Ransomware Challenges and Bitdefender's Solutions

Modern attackers frequently change their tactics to exploit weaknesses in your systems. For organizations opening with lean IT security teams, it's essential to understand how to defend effectively against these threats at every stage in the kill chain.

Initial Access & Prevention Layers

An effective ransomware protection strategy begins by addressing the growing attack surface and the rapid pace at which modern attackers operate. While some attackers wait weeks before launching an attack, many strike within hours of gaining entry. For lean IT security teams relying on manual, siloed defenses, it can be impossible to keep up with the speed of modern attacks. This is why a prevention-first approach is essential to stopping attackers before they gain a foothold in your organization.

Many modern ransomware groups use scanning tools to help them identify and exploit weaknesses at scale, thereby blurring the line between targeted and opportunistic attacks. A single overlooked patch or misconfiguration can quickly turn into an entry point for a much larger breach. For lean IT teams, defending against that stage can feel overwhelming.

Here are some of the ways Bitdefender can protect your organization at the Initial Access stage:

- Attackers are constantly scanning for weaknesses in your environment. [GravityZone External Attack Surface Management \(EASM\)](#) identifies vulnerabilities that attackers may exploit, including exposed assets and shadow IT.
- Attackers often hide malicious code within files that appear harmless. [GravityZone Sandbox Analyzer](#) detonates risky files in a secure environment to uncover hidden malicious behaviors.
- Ransomware often begins with a malicious email designed to trick your employees. [GravityZone Extended Email Security](#) prevents suspicious emails from reaching users' inboxes, and blocks ransomware, phishing, and BEC.
- Malicious traffic often masquerades as legitimate network activity. [GravityZone Network Attack Defense](#) uses deep packet inspection to detect suspicious traffic and block malicious protocols, reverse shells, and executable code in hidden traffic, even if it appears legitimate.

If an attacker successfully navigates this stage, they will typically attempt to establish a foothold in your organization and advance their attack.

Attack Progression & Detection

After gaining initial access, the attackers' goal shifts from entry to establishing footholds across your network. From here, they can attempt to access additional systems, install mechanisms to maintain persistent access, and test methods to gain further control.

Here's how Bitdefender addresses some of the key challenges at the Progression & Detection stage:

- Attackers often try to compromise domain controllers to deploy ransomware more widely or lock you out of critical systems. [GravityZone XDR](#) detects unusual activity that is targeting these systems and helps you identify unusual behavior, even from privileged accounts, that would otherwise slip through unnoticed.
- Ransomware groups actively search for sensitive data and probe your defenses to gauge your organization's cybersecurity readiness. [GravityZone Network Traffic Analytics](#) is a key component of XDR, using integrated telemetry and analytics to help expose reconnaissance attempts, enabling you to respond quickly.
- Attackers often use legitimate tools, such as PowerShell, WMI/WMIC, and PsExec, to conceal their activities and complicate detection. GravityZone integrates [Identity Threat Detection and Response \(ITDR\)](#) within XDR to distinguish these deviations from normal user behavior, even when attackers are hiding behind trusted tools.

The secret to GravityZone's powerful detection is custom machine learning. Instead of relying on generic models, GravityZone trains models uniquely for each customer's environment. As a result, your model will gain a deep understanding of the activity patterns of your systems, enabling it to spot even subtle anomalies that could signal an attacker's presence. This capability gives your team more time to respond to suspicious activity, limiting potential damage and allowing you to move to containment more quickly.

Response & Containment

As soon as you detect a ransomware threat, it's important to act quickly to minimize damage as much as possible before the attack escalates. For lean IT teams, an effective ransomware protection strategy relies on a combination of automated and human-assisted response capabilities.

Here are some of the ways Bitdefender assists with Response & Containment:

- Attackers often rely on persistence techniques, such as privilege escalation and unauthorized changes, to maintain access. GravityZone continuously monitors for these activities and quickly cuts off access.
- Lean IT teams often struggle to strike a balance between speed and accuracy when responding to threats. GravityZone [EDR, XDR, and MDR](#) provide automated containment to ensure rapid containment across endpoints, servers, and networks.
- Security teams often struggle to piece together the fragmented alerts of an attack into a clear incident timeline. GravityZone provides real-time attack visualization by displaying a graphical map of the entire attack chain. This helps teams understand where it started, how it spread, and its impact.

GravityZone integrates prevention, detection, and response to help your organization shorten dwell time and stop ransomware more effectively. This can turn what could have been a full-scale ransomware crisis into a manageable incident.

The Value of a Comprehensive, Integrated Platform

Using a single consolidated platform to ward off attacks is far more effective than relying on multiple standalone tools. Unfortunately, many of the vendors that claim to offer an “all-in-one” solution fall short. They often lack true prevention capabilities and are too complex for lean teams to use effectively. The right platform should offer comprehensive protection, without adding hidden overhead.

We prioritized addressing this challenge when designing GravityZone, ensuring that our integrated security platform met the complexities and demands of lean IT teams. Instead of relying on analysts to manually piece together clues from various tools, GravityZone automatically correlates signals to build a comprehensive picture. The platform reduces reliance on manual detection, making it easier to identify genuine threats before they escalate.

It also provides your teams with detection and response capabilities that large enterprises with dedicated teams of highly specialized staff once enjoyed. At the same time, it eliminates the overhead of managing many fragmented tools.

Consolidating your security tools into an integrated security platform can lead to significant immediate cost savings. It can also help your organization save money in the long run by allowing your teams to spend less time on configuration and tool management, and more time on high-value security activities, such as incident investigation and risk reduction. Additionally, it allows your departments to simplify their training programs and can help reduce their licensing and maintenance costs.

Simplifying Detection and Response for Lean IT

Time is valuable for lean IT security teams. Unfortunately, traditional security approaches often leave analysts buried in raw logs and overwhelmed by numerous alerts. As a result, they have to waste time manually piecing events together before they can even begin to respond. This outcome is frustrating and can drastically increase dwell time, which provides more opportunities for attackers to wreak havoc.

GravityZone reduces this burden by automating the heavy lifting of detection and correlation. Instead of treating every alert in isolation, it collects signals and compiles them into a single, human-readable incident narrative. Automation helps filter out false positives, and clear, contextualized insights guide your organization’s analysts directly to the root cause.

This capability helps your teams to quickly understand what happened, how it happened, where it originated, and which systems are at risk. For small and mid-sized teams with limited staffing, it can make the difference between hours of manual investigation and a near-real-time response.



Improving Security Posture with Risk Management and Patch Control

A strong security posture depends on proactively identifying and mitigating vulnerabilities before attackers can exploit them. Features like Risk Management, Prioritized, High-Impact Security Remediation (PHASR), and integrated patching capabilities can give your organization the tools to do this effectively. These capabilities help reduce your exposure and speed up remediation.

- [GravityZone External Attack Surface Management \(EASM\)](#) helps you proactively identify, monitor, and secure all of your internet-facing assets to prevent attacker exploitation. It provides you with complete control over your external attack surface by showing you all publicly exposed IPs, ASN reports, expiring or expired certificates, vulnerable public services, and open ports, so you can view your organization from an attacker's perspective. It also helps you uncover potential spoofing and fraudulent impersonations of your organization by showing you instances of similar domains to your organization.
- [GravityZone PHASR](#) further strengthens your security posture by dramatically reducing your attack surface. It identifies risks at the user level and restricts both unused applications and atypical but high-risk applications, helping to shrink the attack surface by up to 95%. PHASR also mitigates attacks that rely on Living-off-the-Land (LOTL) techniques, which use legitimate tools like PowerShell to evade detection.
- [GravityZone Patch Management](#) is designed to boost your resilience by automating the deployment of software updates and security patches across your endpoints and servers. The platform reduces the manual effort required to track, test, and deploy patches, thereby minimizing the windows of vulnerability that attackers often exploit.
- [GravityZone XDR](#) unifies detection and response across your environment, enabling lean IT teams to quickly identify and contain attacks without requiring extensive security expertise.

The combined effect of these capabilities helps lean IT security teams to track risk scores across your environment and monitor improvements over time. Additionally, it can help you demonstrate compliance with internal policies and external regulations.



The Importance of Independent Evaluations

Independent evaluations can provide an objective view of a solution's effectiveness by highlighting strengths and exposing potential weaknesses. Analyst reports and third-party tests offer concrete evidence of how your platform performs in real-world scenarios.

Choosing ransomware solutions that consistently perform well in independent evaluations gives you confidence that the technology can effectively detect, prevent, and respond to threats. Strong results in areas such as threat detection, attack chain visibility, and actionable reporting demonstrate that the platform can quickly identify threats and provide your team with clear insights to respond effectively.

[AV-Comparatives](#) and [MITRE](#) are two examples of trusted independent evaluators that provide objective information on the effectiveness, efficiency, and ROI of security solutions. Reading leading industry evaluations from top analyst firms, such as Gartner and Forrester, can also provide an objective understanding of the available options.

Independently validated technology reduces your risk and operational uncertainty, which is especially important for lean IT security teams. Instead of wasting time verifying alerts, they can focus directly on responding, resulting in faster and more effective outcomes.

Modern Ransomware Protection for Lean IT Security Teams

As ransomware evolves and attacks become more sophisticated, adequate ransomware protection must evolve accordingly. For lean IT teams, the challenge is balancing comprehensive defense with limited resources, without adding to alert fatigue.

Bitdefender GravityZone is designed to help teams overcome this challenge by unifying prevention, protection, detection, and response across the entire environment. Its extended prevention layers, integrated telemetry, automated incident analysis, and risk management features reduce manual effort, improve time-to-response, and strengthen your overall security posture.

For mid-market teams, this means faster, more accurate threat detection, simplified operations, and measurable improvements in risk management, all without the complexity of managing multiple standalone tools. Independent evaluations consistently demonstrate GravityZone's effectiveness, so you can have confidence that you are being protected by proven technology.

Experience the full capabilities of Bitdefender GravityZone with a [free trial](#) and see firsthand how it can simplify your security operations.

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry's most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 200 of the world's most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world.

Release Date: October 2025

For more information, visit <https://www.bitdefender.com>.

Romania HQ

Orhideea Towers
15A Orhideeor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

US HQ

111 W. Houston Street,
Suite 2105, Frost
Tower Building,
San Antonio, Texas
78205, USA