aws marketplace

Bitdefender Security for AWS

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Bitdefender Security for AWS

Bitdefender Security for AWS Recap

Bitdefender Security for AWS provides robust protection and seamless integration for AWS environments, ensuring that your data and applications are secure from threats without compromising performance.

It is designed to address the complex security needs of cloud-based infrastructures. With advanced threat intelligence and automated protection features, it offers streamlined management of security tasks, reducing operational burdens. Its scalable architecture optimizes protection for any size infrastructure, delivering a comprehensive, tailored security solution.

What are the key features of Bitdefender Security for AWS?

- Advanced Threat Intelligence: Provides real-time detection and mitigation of threats.
- Automated Security Management: Streamlines processes to reduce manual workload.
- Scalable Architecture: Fits infrastructures of any size seamlessly.
- Seamless Integration: Easily integrates with existing AWS services to enhance security.

What benefits and ROI should be considered?

- Cost Efficiency: Reduces costs associated with manual security processes.
- Enhanced Security Posture: Strengthens the protection of AWS environments.
- Time Savings: Automates tasks to free up valuable time.
- Regulatory Compliance: Helps meet compliance requirements effectively.

Implementing Bitdefender Security for AWS across different industries shows significant improvements in security management. Companies in sectors like finance and healthcare leverage its features to enhance protection of sensitive data, ensuring compliance with industry standards. Its adaptability makes it a preferred choice for businesses with specific needs, providing peace of mind through scalable and efficient security measures.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Bitdefender Security for AWS has positively impacted my organization because whenever we plan to build on AWS, we follow integration processes and implement them properly, and after implementing Bitdefender Security for AWS, I saw specific outcomes such as easier monitoring and investigation, which makes the process much faster."

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

- "Bitdefender Security for AWS has positively impacted my organization by being a lightweight security agent that does not impact server performance."

Verified user

Sr. Security Consultant at a tech vendor with 10,001+ employees

- "The best features of Bitdefender Security for AWS are its EC2 workloads, called elastic compute cloud, which provide a solution from a single console to manage policy, deployment, and visibility across all platforms and across all AWS, so it was easy that way and it was good."

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

"The protection that it provides is valuable because the biggest problem that people and companies have been seeing in the last two or three years is scams and everything like that."

WayneMcgowan

System Administrator at a government with 1,001-5,000 employees

What users had to say about valuable features:

"The protection that it provides is valuable because the biggest problem that people and companies have been seeing in the last two or three years is scams and everything like that. You ought to protect yourself for security reasons. You want to make sure you protect critical things such as files or databases because there's so much hacking going on in the world.."

WayneMcgowan

System Administrator at a government with 1,001-5,000 employees

Read full review

"Bitdefender Security for AWS provides an agent-based solution that combines antivirus, endpoint detection and response and behavioral detection to reduce the risk of compromised production servers.

One of the best features of Bitdefender Security for AWS is its protection for EC2 workloads. It offers centralized management from a single console, allowing users to manage policies, deployments, and visibility across all AWS platforms. This centralized approach simplifies administration and improves efficiency.

The anti-malware and behavioral detection features are robust. For both Windows and Linux EC2 instances, Bitdefender provides strong detection capabilities against both known and unknown threats, helping to minimize false positives and accurately identify true positives. It also supports offloading scans to optimize performance.

Bitdefender Security for AWS helps secure servers running in AWS while reducing CPU and I/O consumption. Managing physical servers is often more complex since it may require additional hardware, such as memory expansions or system extensions, to maintain performance. In contrast, AWS environments benefit from Bitdefender's optimized performance, resulting in lower CPU and memory usage, as well as better handling of I/O loads.

From a security standpoint, this solution allows for easier management even under high resource consumption. Because it operates within AWS, performance remains stable, making it a reliable and efficient choice for cloud-based security operations.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"Bitdefender Security for AWS is a lightweight agent-based workload security solution that protects the EC2 instance with strong malware detection and low performance impact.

"The best features that Bitdefender Security for AWS offers include an advanced anti-malware solution, behavioral detection, a lightweight agent, scan offloading, and low performance impact.

"All features are valuable because protecting the endpoint means all points are very important, and they work in consolidation with each other.

"Bitdefender Security for AWS provides anti-malware protection for AWS workloads, EC2 behavioral detection using machine learning and analytics, scan offloading to Bitdefender servers, centralized management via the GravityZone console, real-time threat detection, monitoring of file and memory processes, a pay-as-you-grow licensing model, and integration with the AWS EC2 API for visibility. These are great features.

"Bitdefender Security for AWS has positively impacted my organization by being a lightweight security agent that does not impact server performance. Bitdefender uses scan offloading, meaning heavy scanning tasks are performed outside the workload on dedicated security servers, which reduces CPU and memory usage on EC2 instances. For example, in production workloads, security scans do not significantly impact application performance because scanning is done outside the EC2 instance. This is especially useful for high-performance applications. Additionally, strong malware and behavioral detection provide antivirus and machine-learning-based detection for comprehensive protection.."

Verified user

Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

“Bitdefender Security for AWS offers features that are provided easily.

Bitdefender Security for AWS stands out mainly because it’s built specifically for AWS and keeps protection lightweight while still giving strong antimalware coverage for EC2 workloads.

One of its best features is **offloaded, hosted scanning**: instead of doing heavy scanning on each EC2 instance, the agent sends scan requests to dedicated Bitdefender-hosted Security Servers running in AWS, which improves performance and keeps CPU and memory usage low on your instances. This is especially valuable when you’re running performance-sensitive web or database tiers and don’t want traditional AV dragging them down.

Another strong point is the **centralized GravityZone Cloud Console**, which lets you manage Windows and Linux EC2 instances, apply policies, view security status, and generate reports from a single web interface without having to log into each account or region separately. That reduces operational overhead and makes it easier to maintain consistent security across multiple AWS accounts or tenants.

The **pay-as-you-go, pay-as-you-grow licensing model** is also a key advantage: you deploy the agent on EC2 instances and only pay for what you use, which matches nicely with AWS’s own consumption-based billing and lets you scale protection up or down as your workload changes. Combined with instant provisioning through EC2 API-style workflows, it removes deployment friction and avoids paying for idle capacity.

Finally, the solution is tuned for **cloud-native environments**, supporting both Windows and Linux EC2 instances and integrating cleanly with AWS cross-account access so you aren’t stuck managing long-term AWS credentials. For teams that want solid, low-impact antimalware coverage on AWS without heavy-on-box agents or complex licensing, these features are usually the main reasons they choose Bitdefender Security for AWS..”

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

Other Solutions Considered

"I have not used a different solution before Bitdefender Security for AWS as my use is based on customer requirements. Some customers may need a unified solution, so for them, I use CrowdStrike or sometimes SentinelOne. I move from one solution to another based on customer needs; it is not about migrating or selecting a solution.."

Verified user
Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

"Before selecting Bitdefender Security for AWS, we evaluated CrowdStrike Falcon Cloud Security and Trend Micro Deep Security as primary alternatives for EC2 workload protection, given our existing experience with both on endpoints and servers."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"It was my first time using Bitdefender Security for AWS for this specific type of policy. However, I have worked with several other security tools before. This one was a bit different. I used it for the first time in this project, but previously, I had experience with other tools such as antivirus, EDR, and XDR solutions.

I didn't evaluate alternative tools before choosing Bitdefender Security for AWS because it was already implemented when I joined the project. Therefore, I didn't get the opportunity to review or compare other options.

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"In many organizations that have written about Bitdefender Security for AWS, the product is used to replace or supplement more traditional, on-prem or legacy-style AV solutions that were difficult to manage at scale in AWS.

Typically, companies came from either a generic enterprise-AV platform (like older server-based antivirus suites) or basic, self-managed security stacks where they were manually installing and tuning agents on each EC2 instance. They switched to Bitdefender Security for AWS because it integrates tightly with AWS, scales automatically as new EC2 instances spin up, and uses off-loaded scanning so their workloads stay performant, which was a big pain point with the previous solutions that degraded server performance and required a lot of manual oversight.

From their perspective, the main reasons for switching were: lower operational overhead, better alignment with AWS's pay-as-you-go model, and the ability to manage everything from a single GravityZone-style console instead of juggling multiple tools and siloed policies.

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"In real-world use, teams that adopt Bitdefender Security for AWS typically evaluate a small set of other AWS-focused security or antimalware solutions before deciding, often comparing it with either native AWS services (like GuardDuty plus basic host-based AV) or other third-party cloud-security tools available on AWS Marketplace. The main differences usually come down to how much extra work you have to manage, how tightly the product integrates with AWS, and what type of protection you really need (pure antimalware vs full-stack CNAPP).

From a comparison standpoint, solutions like **AgileBlue Cloud Security** or similar CNAPP-style tools tend to be stronger in **cloud-native detection and posture management**: they offer broader visibility across AWS, Azure, and GCP, along with CSPM and more aggressive threat-hunting-style analytics, but they're often more complex and licensing can be heavier for teams that only care about basic antimalware on EC2. In contrast, **Bitdefender Security for AWS** is more focused: it shines when you want low-impact, off-loaded scanning across mixed Windows and Linux EC2 instances, pay-as-you-go AWS Marketplace billing, and simple centralized management in GravityZone, but it doesn't try to replace a full-fledged cloud-native detection and response (CDR) or XDR platform.

Another common alternative teams look at is **traditional / on-prem AV products adapted for AWS**, or home-grown scripts plus generic AV agents. Those usually feel more familiar but become hard to scale, cause more performance drag, and don't integrate cleanly with AWS automation or Marketplace billing. Bitdefender wins there on ease of deployment, auto-scaling with EC2, and staying lightweight, but it's still a narrower solution compared with products that combine antimalware, EDR, and cloud-security posture checks in one suite.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

ROI

Real user quotes about their ROI:

"I have observed reduced infrastructure costs and CPU usage due to the scan offloading feature of Bitdefender Security for AWS, resulting in a fifteen to twenty-five percent reduction in compute overhead. There is also an improvement in threat detection accuracy, with a twenty-five to forty percent enhancement due to machine learning and behavioral detection. Furthermore, I note a twenty to thirty percent improvement in SOC efficiency and a thirty percent faster incident response time.."

Verified user

Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

"Yes, many organizations report seeing a positive ROI with Bitdefender Security for AWS, though it tends to show up more in operational efficiency, risk reduction, and cloud-cost alignment than in flashy headline numbers.

Bitdefender itself highlights that the solution is designed for virtualization and cloud environments, with flexible, pay-per-hour pricing through AWS Marketplace, which typically produces immediate cost savings versus traditional on-prem-style AV licenses that force you to over-buy capacity upfront. Because the agent footprint is small and scanning is offloaded to Bitdefender-hosted servers, teams often see less performance degradation on EC2 instances, which indirectly reduces the need to oversize instances or license more compute just to tolerate heavy-on-box scanners.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

Use Case

“My main use case for Bitdefender Security for AWS is to protect cloud workloads like EC2 workload, Windows, Linux, and other similar environments.

“For a specific example of how I use Bitdefender Security for AWS to protect my workloads, I used it to protect the EC2 workload running in the AWS environment from malware and other threats at the endpoint level..”

Verified user

Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

"My main use case for Bitdefender Security for AWS is primarily for investigation purposes.

"Bitdefender Security for AWS is mainly used to protect Windows and Linux EC2 instances running on AWS by adding a lightweight, cloud-based antimalware layer that doesn't slow them down. Organizations typically adopt it when they want dedicated security for their EC2 workloads without managing heavy on-box scanners, especially in environments where they're already using AWS Marketplace for billing and need something that scales automatically with their instance count. It's also commonly used by security teams or MSSPs who manage multiple AWS accounts, because the solution lets them manage policies, view events, and monitor protected workloads from a single GravityZone console, then forward alerts into their existing SIEM or XDR setup.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"I primarily used Bitdefender Security for AWS for SOC policy tuning and other SOC-related tasks. Our work involved integrating Bitdefender with different environments and fine-tuning security policies to enhance malware threat protection.

Bitdefender Security for AWS provides comprehensive protection for cloud-based infrastructures. It covers endpoint, network, and identity security, making integration easier across cloud environments. After integration, we fine-tuned detection policies and monitored activity logs. Any detections—such as malware, lateral movements, or suspicious DNS activity—were forwarded to our SIEM or XDR for analysis and response.

As part of both the SOC and incident response teams, I worked on integrating Bitdefender Security for AWS with other security tools. This integration helped streamline alert management, reducing false positives through continuous policy optimization.

The solution secures EC2 instances directly from the Bitdefender console and includes advanced features such as anti-malware protection and behavioral threat detection. It is especially beneficial to SOC teams for its ease of policy management and scalability, making it a reliable solution for maintaining a secure AWS environment.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The initial setup for Bitdefender Security for AWS is generally straightforward, not overly complex, as long as you're already familiar with AWS and basic agent-based security tools. You start by subscribing through the AWS Marketplace, creating a GravityZone Cloud account, and then integrating AWS EC2 into GravityZone using a cross-account IAM role so the console can discover and manage your instances without having to hand-roll long-term AWS credentials. From there, you either install the Bitdefender Security for AWS agent (BEST) manually on each EC2 instance or use remote-push methods via GravityZone, and then adjust the security-group rules to allow the required ports so the agent can talk back to the Bitdefender Security Servers and Control Center. Most teams report that once the AWS integration and ports are in place, rolling protection out across a fleet of Windows and Linux EC2 instances feels clean and repeatable, more like a scripted cloud-security setup than an old-school on-prem AV rollout.."

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

Read full review

Customer Service and Support

“My experience with customer support for Bitdefender Security for AWS has been very good. I reached out during troubleshooting or detection-related queries, and they provided excellent support. I would rate customer support for Bitdefender Security for AWS a nine out of ten..”

Verified user
Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

“The support team for Bitdefender Security for AWS is good, actually. It's really very good in support. They always give immediate acknowledgment and also try to resolve it very quickly. Even regarding escalations, I didn't see any escalations related to these support cases because every time they provide us good services. .”

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"Customer service and technical support for Bitdefender Security for AWS tend to be viewed as solid and responsive, especially if you come in through AWS Marketplace or an authorized partner. Many customers highlight that the support staff is familiar with both AWS and the GravityZone-based architecture, which helps when troubleshooting issues around agent-to-control-center connectivity, permissions, or environment-specific quirks.

If you hit problems, Bitdefender offers documented knowledge-base articles and support channels tailored to the AWS offering, and AWS-Marketplace-linked customers often report that issues are resolved in a reasonable timeframe, without the kind of long-run frustrations that some see with legacy-style security vendors. Some negative reviews do exist, but they are typically about edge-case configurations or billing misunderstandings rather than systemic unreliability, suggesting that the overall support experience is generally positive as long as you're clear about your environment and expectations.

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

Other Advice

“It works well as long as you set it right. You have to be careful with Bitdefender. It's different when you use it on laptops and desktops, but on servers, it's not the same. You need to make proper settings on it for what you ought to exclude. The problems it was causing were mainly because they didn't set it up properly. When you start putting it on things, you have to make sure you don't include certain things and that you make proper rules and settings to say go scan this or that. When you're installing anything like this on desktops, laptops, servers, or anything else, you want to make sure that you have done the research first and that you know what to include or exclude.

Overall, I'd rate it an eight out of ten..”

WayneMcgowan
System Administrator at a government with 1,001-5,000 employees

Read full review

"When I joined the project, it was already in place. I didn't review what had been implemented previously or what was new. However, what I observed is that, from a policy perspective, the process of creating and fine-tuning policies worked very well. We were able to create templates and policies effectively, which improved the overall configuration.

When you create clear policies and rules, your false positives are automatically reduced, and your threat protection becomes stronger. During behavioral analysis, the system can easily identify situations that typically generate false positives. Using behavioral detection features helps differentiate between true positives and false positives, which is very useful.

The solution is completely cloud-based, and we use AWS Cloud. Bitdefender Security for AWS helps us create effective rules and policies. Implementing these policies and rules also reduces the need for manual intervention by employees.

Overall, I would rate Bitdefender Security for AWS a seven out of ten.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"Bitdefender Security for AWS offers good detection capabilities that arise from its use of artificial intelligence and machine learning. There may be some initial tuning required, but once that is done, it performs quite well, reducing alert fatigue and minimizing false positive detections.

"Bitdefender Security for AWS is deployed in my organization only for public cloud environments specifically for AWS.

"I did not purchase Bitdefender Security for AWS through the AWS marketplace; it is from a partner.

"I advise others looking into using Bitdefender Security for AWS to proceed if they have workloads on AWS and certain budget constraints because this solution offers a good licensing model and is cost-effective, along with decent performance and threat coverage protection. I would rate this product an eight out of ten overall.."

Verified user
Sr. Security Consultant at a tech vendor with 10,001+ employees

Read full review

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944