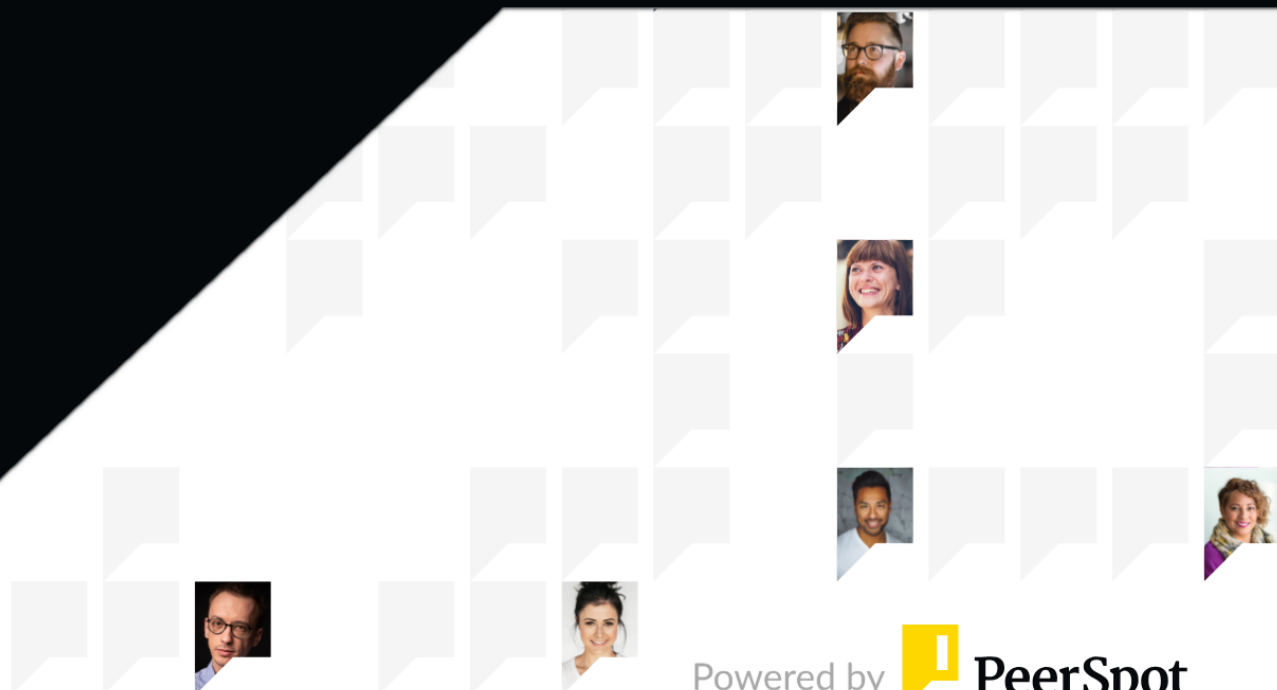


aws marketplace

IBM Security MaaS360 with Watson

**Reviews, tips, and
advice from real users**



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 16

ROI..... 17 - 19

Use Case..... 20 - 24

Setup..... 25 - 27

Customer Service and Support..... 28 - 29

Other Advice..... 30 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



IBM Security MaaS360 with Watson

IBM Security MaaS360 with Watson

Recap

IBM Security MaaS360 with Watson, a proven enterprise mobility management platform, provides seamless integration of security and productivity features powered by AI technology.

IBM Security MaaS360 with Watson helps organizations maintain secure access and management of mobile devices, applications, and content. Its AI capabilities improve threat intelligence, enabling IT departments to efficiently manage endpoints while ensuring robust data protection. Highly appreciated for its flexible deployment and ease of integration, this platform stands out for its AI-driven insights which aid in proactive security measures.

What are the key features of IBM Security MaaS360 with Watson?

- **AI-Powered Threat Management:** Enhance threat detection and mitigation using Watson's AI capabilities.
- **Comprehensive Device Management:** Manage devices across different operating systems from a unified interface.
- **Secure Containerization:** Safeguard corporate data in secure containers on mobile devices.
- **Advanced Analytics:** Provide valuable insights for improved decision-making and threat response.

What benefits and ROI can be expected from IBM Security MaaS360 with Watson?

- **Increased Efficiency:** Streamlined processes for IT teams resulting in time savings.
- **Enhanced Security:** Improved protection of corporate data and reduced risk of breaches.
- **Cost-Effectiveness:** Optimize operations potentially leading to cost savings over time.
- **Scalability:** Adaptability to evolving business needs.

IBM Security MaaS360 with Watson implementations span various industries including healthcare, finance, and education. In healthcare, it ensures secure management of devices that access sensitive patient data while complying with regulations. In finance, it helps manage mobile endpoints accessing sensitive financial information, enhancing data security. Education institutions use it to manage and monitor devices used in learning environments, ensuring a safe and controlled digital landscape.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Everything since we started using IBM Security MaaS360 with Watson has been phenomenal, especially security, which has improved overall on our devices and our data.”



Hehic Faith

Information Technology Manager at DuPont

- ✓ “IBM Security MaaS360 with Watson has had a positive impact on our organization by improving device security, streamlining endpoint management, and reducing the time spent on routine IT tasks.”



Varun Mehra

collaboration support engineer at a retailer with 11-50 employees

- ✓ “IBM Security MaaS360 with Watson has positively impacted our organization by improving our security posture through effectively managing and securing mobile devices, apps, and content.”



Diana Yegon

Senior Software Developer at Radical FANATICS

- ✓ “IBM Security MaaS360 with Watson significantly reduced deployment time, improved consistency across the managed devices, and made supporting a remote workforce much easier.”



Nikita B

Senior Business Manager at Fidelix

- ✓ “Some of the most useful features in IBM Security MaaS360 with Watson are the centralized device management, security policy enforcement, application management, and compliance monitoring.”



Anumula Hitesh

Senior Business Development Executive at Digitaltrack

- ✓ “IBM Security MaaS360 with Watson is a reliable solution for device management, security, and compliance; it provides strong centralized control and helps simplify endpoint administration, and while there is room for improvement in reporting and end-user experience, it has been a valuable platform for the organization.”



Sohan Hadke

Cyber Security Analyst at Digitaltrack



“IBM Security MaaS360 with Watson has impacted my organization positively by giving us control for the cybersecurity of mobile devices, which is a very strong aspect.”



Martins Zeipe

IT Security Expert at ALSO Finland Oy

What users had to say about valuable features:

“The best features IBM Security MaaS360 with Watson offers include managing devices remotely while providing the location and also being able to manage the applications and some policies remotely.

“When managing applications and policies remotely, all of them are equally useful for me.

“IBM Security MaaS360 with Watson helps keep track of the iPads we manage, which positively impacts my organization.

“Keeping track of everything keeps things organized, which has helped my team and organization significantly..”

Verified user

[Read full review](#)

IT Support Specialist at a tech services company with 51-200 employees

“I consider the best features offered by IBM Security MaaS360 with Watson to be the fact that all secure applications are contained in a container, and that when a user's device might have been compromised or the user left the company, I could directly delete the container and remove all corporate applications and configurations.

“Regarding the secure container feature and the ease of deleting corporate information, I found it quite simple to manage on a day-to-day basis; the tool is quite intuitive. Once I manage to group the devices, I then apply policies to each group and it is easy to manage. IBM Security MaaS360 with Watson has positively impacted my organization by being able to protect mobile devices. The protection of mobile devices has improved as we did not have many security problems, but we wanted to prevent them because these devices are normally used within the workplace and are not taken outside. Since we are a public organization and users do not take the devices outside, we do not have the risk of them being lost or stolen, but we wanted to make sure that they did not fall into anyone's hands and could compromise corporate information..”

Verified user

[Read full review](#) 

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

One of the best features of IBM Security MaaS360 with Watson is the ability to correlate security events from multiple sources into a centralized single-level incident instead of reviewing logs from firewall, active directory, endpoint, and server separately. The platform provides a unified view that makes investigations much faster. IBM Security MaaS360 with Watson also combines in-store endpoint detection and response, EDR, XDR, and logs management into a connected workflow, helping analysts investigate and respond more efficiently.

For day-to-day operations, IBM Security MaaS360 with Watson serves as a central platform for monitoring security events across the environment. We use it for debugging forensic investigations and monitoring VPN events before taking action.

“IBM Security MaaS360 with Watson has strong endpoint visibility and security analysis. The mobile device management model helps us by collecting and correlating endpoint security events with data from firewalls to identify systems, VPN, and other security tools. This gives our security team better visibility into expected activity and helps us investigate incidents more recently. .”

Sonusingh Singh

Customer Support Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“IBM Security MaaS360 with Watson offers several best features, including the separation of work and personal profiles, which ensures that work-related information such as emails and documents is contained within a work profile, while personal data remains private, preventing any overlap. Additionally, it provides granular monitoring capabilities that block and restrict numerous activities, and a partnership with TeamViewer for quick remote access. There is also the remote wipe feature, which allows me to erase data from any device remotely when necessary.

“While all the features are equally important, the separation of work and personal profiles stands out because many organizations do not provide mobile phones when employees start, leading to the BYOD (bring your own device) method. This ensures that company data is kept separate and secure within its own container.

“IBM Security MaaS360 with Watson includes both basic and advanced capabilities of a complete MDM or UEM solution and allows for policy customization to optimize results. IBM Security MaaS360 with Watson positively impacts my organization, especially across various sectors such as finance, telecom, and healthcare, with numerous client success stories showcasing their satisfaction with the solution I have implemented..”

Mustafa Kashif

Presales Consultant And Solutions Engineer at Trillium Information Security Systems

[Read full review](#) 

“The best features IBM Security MaaS360 with Watson offers are ease of use, user interface, and wide possibilities to configure a mobile device as needed. I can configure not only mobile phone devices but also desktops or PCs.

“What makes the user interface of IBM Security MaaS360 with Watson stand out to me is the main dashboard where I can see all the alerts and what is happening with my mobile devices, mobile endpoints, or other devices. Additionally, there is a wide possibility to create specific policies for Windows, macOS, or Android devices.

“There is also good integration with TeamViewer, which I use on an everyday basis to remotely connect to Android devices at any location.

“IBM Security MaaS360 with Watson has impacted my organization positively by giving us control for the cybersecurity of mobile devices, which is a very strong aspect.

“I can share specific outcomes that show how gaining this control with IBM Security MaaS360 with Watson has helped my organization. We have seen that we have limited possible threats from someone installing something not secure on their mobile phones. We can deploy our internal applications in a secure container to user mobile phones, and we can see in the alerts when something is not happening as it should, for example, on the mobile phones. Then, we take actions from the cybersecurity team to react to those possible incidents. Additionally, in the usual use cases, if a user loses their phone or the mobile device is stolen, we can erase remotely all the data from that mobile device or block that mobile device from accessing our internal IT resources, programs, or applications.

“Regarding IBM Security MaaS360 with Watson's AI capabilities, I think it has many functions and features regarding security and how we could improve the security for the endpoints and end devices, mobile end devices when we are using IBM Security MaaS360 with Watson with AI possibilities. AI automatically provides different kinds of notifications of threats or possible configuration needs, so there is more automation available.

“I think that IBM Security MaaS360 with Watson is reliable, and everything works as it should..”

“The features I find most valuable in IBM Security MaaS360 with Watson are its unified endpoint management capabilities, policy-based device management, application deployment, compliance monitoring, and the Watson-powered security insights. Having a single console to manage Android, iOS, Windows, and macOS devices has made administration much simpler because I no longer have to rely on multiple tools for different operating systems. The automated enrollment process and policy-based management ensure that every device receives the correct security settings, application, Wi-Fi and VPN profile, and compliance rules as soon as it is enrolled, which has reduced manual configuration and improved consistency across the organization.

“I also appreciate the remote management features such as device lock or selective wipe, full wipe, and troubleshooting, as they allow me to respond quickly if a device is lost, stolen, or an employee leaves the company. Another feature that stands out is the Watson integration, which provides intelligent insights by identifying devices that may present security risks or compliance issues, helping me prioritize remediation instead of manually reviewing every endpoint.

“The feature I rely on the most is the centralized device management combined with policy-based compliance enforcement because it is the one my team interacts with almost every day. In a typical enterprise environment, there are hundreds or even thousands of devices connecting from different locations, and manually checking whether each one meets the organization's security requirements simply is not practical. With IBM Security MaaS360 with Watson, I can define security policies once and have them applied consistently across all managed devices, whether they are corporate-owned or part of a BYOD program. The dashboard gives me a quick view of device health, compliance status, encryption, operating system version, and any policy violations, so I can identify potential issues before they become security incidents. This has made routine administration much more efficient because I spend less time on manual audits and more time addressing genuine exceptions.

“One additional feature that deserves mention is the reporting and analytics capability. I use it regularly to monitor compliance trends, track device inventory, and identify endpoints that need attention before they become larger security

issues. The reports are useful during internal security reviews and audits because they provide a centralized view of device status without having to collect information from multiple systems. I also appreciate that the platform supports a wide range of operating systems, which means I can manage different device types from a single console instead of maintaining separate management tools. The Watson-powered insights are another valuable addition because they help prioritize potential risks instead of overwhelming administrators with raw data. That said, I think the user interface could be more intuitive in certain areas, especially when configuring advanced policies or troubleshooting deployment issues. Some workflows require navigating through multiple menus, which can slow down new administrators. Even with those limitations, the overall feature set has helped me standardize endpoint management, improve security, and reduce the amount of manual effort required to support users across the organization..”

Nikita B

Senior Business Manager at Fidelix

[Read full review](#) 

Other Solutions Considered

“Before choosing IBM Security MaaS360 with Watson, I evaluated other options, specifically looking at Microsoft-offered solutions for mobile device management..”

Martins Zeipe

IT Security Expert at ALSO Finland Oy

[Read full review](#) 

“Before choosing IBM Security MaaS360 with Watson, I considered MobileIron as an option in the market, but we ultimately chose IBM Security MaaS360 with Watson..”

Verified user

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

[Read full review](#) 

“I previously used Miradore a lot; it's a product of Finland. It is simple for basic configurations but lacks a lot of security features. I used it because it was cheaper, and the client was not willing to pay more than a specific budget, so I recommended that..”

Yawarkhan Khan

Systems Engineer at a consultancy with 1-10 employees

[Read full review](#) 

We evaluated several other solutions including Microsoft Sentinel and Splunk Enterprise Security and compared them based on event collection, threat detection, integration capability, ease of deployment, scalability, and total cost of ownership.

Sonusingh Singh

Customer Support Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“Before adopting IBM Security MaaS360 with Watson, we used a basic mobile device management solution that provided core device management capabilities but lacked advanced security, compliance, and analytics features. We switched to IBM Security MaaS360 with Watson because we needed a more comprehensive platform with stronger security controls, better policy management, centralized administration, and AI-driven insights. The ability to manage multiple device types from a single console and improve compliance visibility were also key factors in our decision to migrate..”

Varun Mehra

collaboration support engineer at a retailer with 11-50 employees

[Read full review](#) 

“I did not previously use a different solution before working with IBM Security MaaS360 with Watson.

“Before choosing IBM Security MaaS360 with Watson, I evaluated other options, including Samsung Knox and Microsoft Intune. However, both solutions had issues, with Samsung Knox favoring Samsung devices and lacking functionality for iOS, while Microsoft Intune was less effective for iOS and quite expensive compared to IBM Security MaaS360 with Watson, which provides greater value..”

Mustafa Kashif

Presales Consultant And Solutions Engineer at Trillium Information Security Systems

[Read full review](#) 

ROI

Real user quotes about their ROI:

Organizations typically see a strong return on investment with IBM Security MaaS360 with Watson through improved analyst efficiency and reduced incident response time.

Nitin Yadav

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

[Read full review](#) 

“I have definitely seen a return on investment with IBM Security MaaS360 with Watson, particularly with time saved when reacting to different kinds of cybersecurity incidents..”

Martins Zeipe

IT Security Expert at ALSO Finland Oy

[Read full review](#) 

“Regarding return on investment, I can share relevant metrics with you, such as cost savings on mobile data, but this was not within my responsibilities..”

Kevin Fredo

Analista de TI at a energy/utilities company with 10,001+ employees

[Read full review](#) 

“I have not seen any return on investment from implementing IBM Security MaaS360 with Watson, as those of us who administered it still needed to administer it afterward; management became easier, but it did not mean any staff reduction or return on investment. I do not know that figure..”

Verified user

[Read full review](#) 

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

“Specific outcomes and metrics that show how IBM Security MaaS360 with Watson has helped my clients include reduced data leaks, improved compliance, and significant time savings in managing devices. Clients report that they now effectively manage employees, block and restrict data sharing, and monitor unauthorized activities on devices, which increases their overall visibility and security..”

Mustafa Kashif

[Read full review](#) 

Presales Consultant And Solutions Engineer at Trillium Information Security Systems

“From an operational standpoint, I saw several measurable improvements after implementing IBM Security MaaS360 with Watson. The average time required to provision and configure a new employee's device dropped from around two to three hours to less than an hour because application, security policies, email profiles, and device settings were applied automatically during the enrollment. Routine endpoint management tasks that previously required manual intervention were reduced significantly, allowing my IT team to spend more time on strategic security initiatives instead of repetitive administrative work. I also noticed roughly a 35% to 40% reduction in endpoint-related support tickets, particularly those related to device configuration and policy compliance, since users receive standardized configurations from the start. My device compliance rate consistently stayed above 95%, giving me much better visibility into which devices met corporate security requirements and allowing me to address non-compliant endpoints before they become security risks..”

Nikita B

Senior Business Manager at Fidelix

[Read full review](#) 

Use Case

Our main use case for IBM Security MaaS360 with Watson is to provide capability for centralized security monitoring and instant detection. We collect logs from firewall, network, VPN gateway, and Windows to a single platform to enrich alerts with intelligence and provide context, helping prioritize investigations.

Sonusingh Singh

Customer Support Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“My main use case for IBM Security MaaS360 with Watson is managing iPad devices remotely.

“For example, we ensure to follow the procedure or process to get the MDM installed on the iPads and get them registered to our account to manage iPad devices remotely. It came in handy when we would try to locate devices remotely when they were lost or stolen, which highlights my main use case..”

Verified user

IT Support Specialist at a tech services company with 51-200 employees

[Read full review](#) 

“I use IBM Security MaaS360 with Watson primarily as an MDM solution on mobile devices in my organization. A concrete example of how I use this tool as an MDM on mobile devices is using corporate devices to access applications that connect to our internal networks through the IBM Security MaaS360 with Watson module that allows access to our corporate network..”

Verified user

[Read full review](#) 

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

“My main use case for IBM Security MaaS360 with Watson is mobile device security and specific features tailored to my company.

“I use IBM Security MaaS360 with Watson for mobile device security in my company to allow specific devices where only a specific webpage could be opened and nothing more. All other features on those mobile phones need to be disabled and not accessible to the users. IBM Security MaaS360 with Watson is a good solution for accomplishing this.

“Another use case for IBM Security MaaS360 with Watson involves specific locations. When a mobile phone or mobile device leaves a specific location like headquarters, all the data on the mobile device is automatically erased or deleted..”

Martins Zeipe

[Read full review](#) 

IT Security Expert at ALSO Finland Oy

“IBM Security MaaS360 with Watson is primarily used by clients to block data sharing on employees' mobile phones because confidential company data is stored on these devices, and companies want to restrict sharing, screenshots, and recording. The overall goal is to block any data sharing and prevent insider threats, with companies typically preferring a cloud-based solution that manages all mobile devices, laptops, and endpoints.

“A specific example of how clients use IBM Security MaaS360 with Watson to block data sharing or prevent insider threats involves the use of policies within IBM Security MaaS360 with Watson. By simply enabling these policies on a mobile device, clients can effectively block data sharing.

“Clients also use IBM Security MaaS360 with Watson as an endpoint management solution, which integrates and enrolls with Windows systems as well as other platforms beyond just Android and iOS, allowing patch management and a comprehensive unified endpoint management system. It has a vast array of use cases, including screenshot blocking, geolocation, and more, along with customization and integration with third-party platforms such as SIEM and ServiceNow, making it a complete solution backed by IBM..”

Mustafa Kashif

Presales Consultant And Solutions Engineer at Trillium Information Security Systems

[Read full review](#) 

“My primary use case for IBM Security MaaS360 with Watson has been to centralize, manage, and secure all corporate-owned and BYOD mobile devices across the organization while ensuring compliance with my internal security policies. I use the platform to enroll and manage Android, iOS, Windows, and Mac devices, deploying business applications remotely, enforcing password and encryption policies, configuring Wi-Fi and VPN settings, and performing actions such as remote lock or wipe whenever a device is lost or an employee leaves the company. Before implementing IBM Security MaaS360 with Watson, device management was largely manual with different teams following different processes, making it difficult to maintain consistent security standards and track device compliance. As my workforce became more mobile and remote, I needed a solution that could provide centralized visibility and control without requiring users to be connected to the corporate network.

“IBM Security MaaS360 with Watson helped me standardize endpoint management by automating device enrollment, applying security policies based on user role, and monitoring compliance from a single console. I also found the Watson-powered insights useful for highlighting potential security risks, identifying non-compliant devices, and providing recommendations that help me prioritize my remediation efforts. While the product has significantly improved my operational efficiency and reduced the time spent on routine administration, there is still a learning curve when configuring advanced policies, and some integrations with legacy environments require additional planning and testing. Overall, it has become an important part of my endpoint security strategy by giving me better visibility, stronger governance, and a more consistent approach to managing devices across the organization.

“One real-world scenario where IBM Security MaaS360 with Watson proved especially valuable was during the onboarding of remote employees. Earlier, every new laptop and mobile device had to be configured manually by my IT team before it could be shipped, which was time-consuming and often delayed the onboarding process. After implementing IBM Security MaaS360 with Watson, I created standardized enrollment and security policies so that once a device was assigned to a user, it automatically received the required corporate applications, Wi-Fi and VPN configuration, email settings, password policies, and security restrictions

during the enrollment process. This allowed employees to receive their devices directly, sign in with their corporate credentials, and start working with minimal IT intervention.

“I also use the Watson-powered insights to monitor device compliance and quickly identify devices that were missing security updates or had settings that did not meet my corporate policy. Instead of waiting for users to report issues, my IT team could proactively address them before they became security risks. There are still a few legacy applications that require manual configuration, but for the majority of users, IBM Security MaaS360 with Watson significantly reduced deployment time, improved consistency across the managed devices, and made supporting a remote workforce much easier.

“Another way I have been using IBM Security MaaS360 with Watson is for ongoing compliance monitoring and day-to-day endpoint security management, rather than just device enrollment. As my employees install updates, travel, or switch networks, the platform continuously checks whether their devices still comply with my security policies. If a device falls out of compliance, for example, if encryption is disabled, the operating system is outdated, or a required security setting is changed, I can identify the issue quickly and take appropriate action before it becomes a security concern. I have also used the platform to manage application updates, retire devices when employees leave the organization, and remotely troubleshoot common issues without asking users to bring their devices into the office. This has reduced the administrative workload for my IT team and improved the overall user experience, especially for the employees working remotely..”

Nikita B

Senior Business Manager at Fidelix

[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.

My advice to others looking into using IBM Security MaaS360 with Watson would be to invest time in proper planning and tuning during the initial setup. The platform is very powerful, but it delivers the most value when your sources are well-integrated and your use cases are clearly defined. Focus on a good setup.

Nitin Yadav

[Read full review](#) 

Network & Security Engineer at Arrow PC Network Pvt.Ltd.

“I did not handle the costs, initial setup, or licensing of IBM Security MaaS360 with Watson. I did not manage the cost side; they renewed the licenses, but I do not know the price or that aspect..”

Verified user

[Read full review](#) 

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

“The pricing and licensing for IBM Security MaaS360 with Watson were reasonable for the features provided, setup was straightforward, and the cloud-based deployment helped reduce infrastructure costs, making it a good value for organizations looking for centralized device management and security..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“My experience with pricing, setup cost, and licensing indicates that cost can be a challenge, especially for large organizations managing a large number of devices. However, for my case and for our organization, the price is cost-effective and very affordable. The setup was straightforward since it can be used by anyone, even those who are non-technical users..”

Diana Yegon

Senior Software Developer at Radical FANATICS

[Read full review](#) 

“For others looking into using IBM Security MaaS360 with Watson, I advise that the new device setup and deployment are fairly easy. However, getting off the ground with the initial setup is a bit tough and it needs to be easier to get going. Training a new device manager is not straightforward, as it requires too much tutorial to get someone proficient in changing, adding, and deleting devices. It can take considerable time learning all of those processes..”

Hehic Faith

[Read full review](#) 

Information Technology Manager at DuPont

“IBM Security MaaS360 with Watson is deployed as a public cloud solution in my environment. Since it is delivered as a SaaS platform, I do not have to manage or maintain any on-premises infrastructure for the endpoint management system itself, which has reduced administrative overhead for my IT team. I access the management console through the cloud to enroll devices, enforce security policies, deploy applications, monitor compliance, and perform remote administrative actions across Windows, Android, iOS, and macOS devices. The cloud-based deployment has been particularly beneficial for supporting remote and hybrid employees because devices can be managed securely from virtually anywhere without requiring a VPN connection to the corporate network. The initial setup required careful planning around user groups, security policies, and integration with my identity management platform, but once those were in place, ongoing administration became much more streamlined..”

Nikita B

[Read full review](#) 

Senior Business Manager at Fidelix

Customer Service and Support

“Customer support for IBM Security MaaS360 with Watson is good; they are very responsive and fast responders. I barely call them, but whenever I have, I had a good experience with them..”

Yawarkhan Khan

Systems Engineer at a consultancy with 1-10 employees

[Read full review](#) 

“Customer support has been contacted on a few occasions and the experience has generally been positive, with the support team being responsive and helpful in resolving issues in a timely manner and providing guidance when needed..”

Sohan Hadke

Cyber Security Analyst at Digitaltrack

[Read full review](#) 

“My experience with the technical support of IBM Security MaaS360 with Watson has not been very good. We did not have major complications in management, but when we had to deal with some problems, I had some difficulty until I managed to find a person who really knew the tool, a person who was in Ireland, but the rest of the support was not very easy..”

Verified user

[Read full review](#) 

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

“The customer support for IBM Security MaaS360 with Watson has generally been good, with the support team being knowledgeable and responsive, especially for critical issues. We have found the documentation, knowledge base, and support resources helpful for resolving common questions and configuration challenges. While response times can vary depending on the complexity and priority of the issue, overall, the support experience has been positive and has helped us maintain smooth day-to-day operations..”

Varun Mehra

[Read full review](#) 

collaboration support engineer at a retailer with 11-50 employees

Other Advice

“I would advise others looking into using IBM Security MaaS360 with Watson to use the educational library that is available because it is really helpful. I gave this product a review rating of ten..”

Verified user

IT Support Specialist at a tech services company with 51-200 employees

[Read full review](#) 

“I use [Microsoft Azure](#) as the cloud provider for my IBM Security MaaS360 with Watson deployment. There are no improvements needed for IBM Security MaaS360 with Watson that I have not already mentioned. My overall rating for this product is 8..”

Martins Zeipe

IT Security Expert at ALSO Finland Oy

[Read full review](#) 

“My advice to other companies considering implementing IBM Security MaaS360 with Watson is to be clear that the matter of containers is not something that currently aligns with how vendors are distributing applications or managing their configurations, so perhaps the issue of containers needs to be reconsidered. I gave this product a rating of 8..”

Verified user

Administrador De Sistemas De Ti at a tech services company with 201-500 employees

[Read full review](#)

“IBM Security MaaS360 with Watson is very good in terms of security, especially in today's world in the age of AI. It is very specific and performs multiple verifications, so it's pretty tight. You can configure it with an LDAP and have all those features, which makes it highly secure. Regarding IBM Security MaaS360 with Watson's AI capabilities, I think it offers high-level security for mobile users in a corporate environment.

“Regarding the accuracy and reliability of IBM Security MaaS360 with Watson's AI capabilities, it is accurate in terms of geolocation, in deploying apps, and in general ease of access.

“The specific outcome I've seen with IBM Security MaaS360 with Watson is adding a geolocation feature to restrict the device to a specific zip code or GPS location, as if you go beyond that point, the phone may not work. The device becomes useless outside that range, which is good for people who want to use it inside the corporate area, and I find that pretty cool.

“I would advise anyone looking into using IBM Security MaaS360 with Watson that if you are not willing to compromise on security, then definitely this is your number one product to go for, because in today's world, security is everything. The more secure you are, the better for you, and the less trouble you will have.

“I give IBM Security MaaS360 with Watson a rating of 10 out of 10..”

Our advice to others considering IBM Security MaaS360 with Watson is to objectively understand which log sources and security tools you want to integrate before implementation. IBM Security MaaS360 with Watson delivers the most value when there is comprehensive visibility across the environment, including firewalls, identity services, VPN, endpoint, and cloud workloads.

We find IBM Security MaaS360 with Watson has a moderate learning curve. New users with a basic understanding can pick up basic functions quickly, but becoming familiar with advanced features such as AI correlation rules, custom searches, and automation requires more hands-on experience. In our experience, security and IT professionals with a solid background adapt relatively quickly, while administrators responsible for the initial entering and training need more time to become comfortable with the platform's extensive feature set, which is one of its strengths but also contributes to the learning curve.

“We would describe the reporting and analytics capabilities of IBM Security MaaS360 with Watson as very strong. The platform provides a detailed dashboard, customizable reports, and helps the security team monitor threats and investigate incidents to support compliance requirements. IBM Security MaaS360 with Watson has been effective in detecting and responding to threats in real-time. The arrangement of collecting logs from the firewall, VPN gateway, security solution, and other log sources facilitates connected activities that help analysts quickly identify potential incidents. In our experience, threats such as suspicious login attempts, unusual network activity, and policy violations are detected properly, allowing the security team to begin investigations without having to manually collect logs from multiple systems.

“We have found the AI-generated output in IBM Security MaaS360 with Watson to be mostly accurate and reliable, especially for alert enrichment, event collection, and threat prioritization. It helps provide valuable context by incorporating threat intelligence. This makes investigations more efficient and reduces the amount of manual analysis required.

“We would describe the integration capabilities of IBM Security MaaS360 with Watson as one of its strong features. It integrates well with a wide range of security and IT tools including firewall, VPN gateway, endpoint protection platform, email

security solution, cloud service, and custom data sources. This enables us to centralize security events and investigate incidents from a single platform instead of working across multiple consoles. Our overall rating for this product is three out of five. .”

Sonusingh Singh

Customer Support Engineer at Arrow PC Network Pvt Ltd

[Read full review](#) 

“My advice to organizations considering IBM Security MaaS360 with Watson is to spend time planning the implementation before rolling it out across the entire company. Start by understanding your device landscape, security requirements, and compliance policies. Then begin with a small pilot group to validate application deployment, device enrollment, and policy enforcement before expanding it to all the users. This helps identify compatibility issues and fine-tune configurations without disrupting the wider organization. It is also important to organize devices and users into logical groups from the beginning because a well-structured policy framework makes ongoing administration much easier as the environment grows. I would also recommend taking advantage of the automation and compliance features instead of relying on manual processes, as that is where the platform delivers the most value.

“From my experience, the AI capabilities in IBM Security MaaS360 with Watson are designed to assist administrators rather than replace their decision-making, and that is something I appreciate from both a governance and security perspective. The Watson-powered insights help identify devices that may be at risk, highlight unusual behavior, and recommend actions based on the security posture of the environment, but the administrator still has full control over whether those recommendations are acted upon. That balance is important because endpoint management often involves business-specific policies that require human judgment. I also appreciate that the platform maintains detailed audit logs and role-based access control, making it easier to track administrative actions and

ensure accountability. From a governance standpoint, it supports compliance by continually monitoring device status and enforcing security policies before the devices are allowed to access corporate resources.

“That said, I would appreciate even greater transparency into how certain AI recommendations are generated, along with more detailed explanations of the potential impact of recommended actions.

“Based on my experience, the AI capabilities in IBM Security MaaS360 with Watson have generally been accurate and reliable when it comes to identifying potential security risks, highlighting non-compliant devices, and providing recommendations for endpoint management. The insights are based on actual device telemetry, compliance data, and security events, so in most cases, the recommendations are relevant and help my IT team prioritize what needed attention first. I found it particularly useful for reducing the time spent manually reviewing large numbers of endpoints because it brings the most important issues to the forefront. That said, I do not think AI recommendations should be applied without verification, especially in large or complex environments where there are many custom policies, legacy applications, or business-specific expectations that the platform does not fully understand. I would rate my overall experience with IBM Security MaaS360 with Watson as an eight out of ten..”

Nikita B

Senior Business Manager at Fidelix

[Read full review](#) 

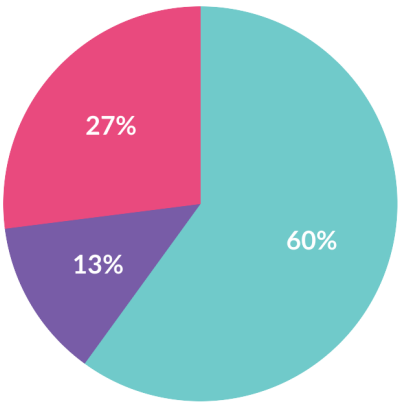
Top Industries

by visitors reading reviews

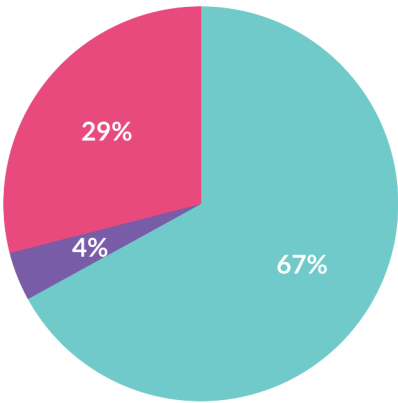


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

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