Microsoft Security Suite

Buyer's Guide & Reviews

January 2024

PeerSpot

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

Thanks for downloading this PeerSpot report.

Note that this is a generic report based on reviews and opinions from the entire PeerSpot community. We offer a customized report personalized for you based on:

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

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

Get your personalized report here.

Contents

Vendor Directory

Microsoft	Microsoft Purview Audit		**Microsoft**	Azure Firewall
Microsoft	Microsoft Purview Communication Compliance		**Microsoft**	Azure Firewall Manager
Microsoft	Microsoft Purview Compliance Manager		**Microsoft**	Azure Front Door
Microsoft	Microsoft Purview Data Lifecycle Management		**Microsoft**	Azure Web Application Firewall
Microsoft	Microsoft Purview Data Loss Prevention		**Microsoft**	Microsoft Defender XDR
Microsoft	Microsoft Purview eDiscovery		**Microsoft**	Microsoft Defender External Attack Surface Management
Microsoft	Microsoft Purview Information Protection		**Microsoft**	Microsoft Defender for Business
Microsoft	Microsoft Purview Insider Risk Management		**Microsoft**	Microsoft Defender for Cloud
Microsoft	Microsoft Purview Records Management		**Microsoft**	Microsoft Defender for Cloud Apps
Microsoft	Microsoft Entra ID		**Microsoft**	Microsoft Defender for Endpoint
Microsoft	Microsoft Entra External ID		**Microsoft**	Microsoft Defender for Identity
Microsoft	Microsoft Entra ID Protection		**Microsoft**	Microsoft Defender for IoT
Microsoft	Azure Key Vault		**Microsoft**	Microsoft Defender for Office 365
Microsoft	Microsoft Entra Permissions Management		**Microsoft**	Microsoft Defender Threat Intelligence
Microsoft	Microsoft Entra Verified ID		**Microsoft**	Microsoft Sentinel
Microsoft	Microsoft Intune		**Microsoft**	Microsoft Purview
Microsoft	Azure Bastion		**Microsoft**	Microsoft Defender Vulnerability Management
Microsoft	Azure DDoS Protection			

Top Microsoft Security Suite Solutions

Over 752,108 professionals have used PeerSpot research. Here are the top Microsoft Security Suite vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

● **Views**

Number of views

● **Comparisons**

Number of times compared to another product

● **Reviews**

Total number of reviews on PeerSpot

● **Words/Review**

Average words per review on PeerSpot

● **Average Rating**

Average rating based on reviews

Bar length

The total ranking of a product in a category, represented by the bar length, is based on a weighted aggregate score. The score is calculated using the following factors:

ul>

li>**Comparisons Views**: the product with the highest number of comparisons with other products-in-the-category gets a maximum of **25 points**. Every other product gets assigned points based on its total in proportion to the #1 product in that ranking factor. For example, if a product has 80% of the number of comparison views compared to the product with the most reviews then the product's points for reviews would be 25 * 80%./li>

li>**Views**: We calculate the number of Views based on the percentage of category comparisons out of the total comparisons of the product./li>

ul>

li>For example, if a product has 100 Comparisons with other products in the category and a total of 1,000 Comparisons, the product will be assigned 10% of the total number of Views. If the product has a total of 2,000 Views, it will be assigned 200 Views for this ranking factor./li>

li>The product with the highest number of views gets a maximum of **25 points**. Every other product gets assigned points based on its total in proportion to the #1 product in that ranking factor./li>

li>For example, if a product has 100 Comparisons with other products in the category and a total of 1,000 Comparisons, the product will be assigned 10% of the total number of Views. If the product has a total of 2,000 Views, it will be assigned 200 Views for this ranking factor./li>

/ul>

li>**Reviews**: the product with the highest number of reviews gets a maximum of **15 points**. Every other product gets assigned points based on its total in proportion to the #1 product in that ranking factor. For example, if a product has 80% of the number of reviews compared to the product with the most reviews then the product's points for reviews would be 15 * 80%./li>

li>**Rating**: the maximum score is **25 points** awarded linearly between 6-10/li>

ul>

li>e.g. 6 or below=0 points; 7.5=7.5 points; 9.0=18 points; 10=25 points./li>

/ul>

li>**Words/Review**: the maximum score is **10 points** awarded linearly between 0-900 words/li>

ul>

li>e.g. 600 words = 4 points; 750 words = 7 points; 900 or more words = 10 points./li>

li>If a product has fewer than ten reviews, the point contribution for Rating and Words/Review is reduced: 1/3 reduction in points for products with 5-9 reviews, two-thirds reduction for products with fewer than five reviews./li>

/ul>

/ul>

Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

All products with 50+ points are designated as a Leader in their category.

Rankings for June 2023 and earlier used our previous ranking methodology. Learn more here.
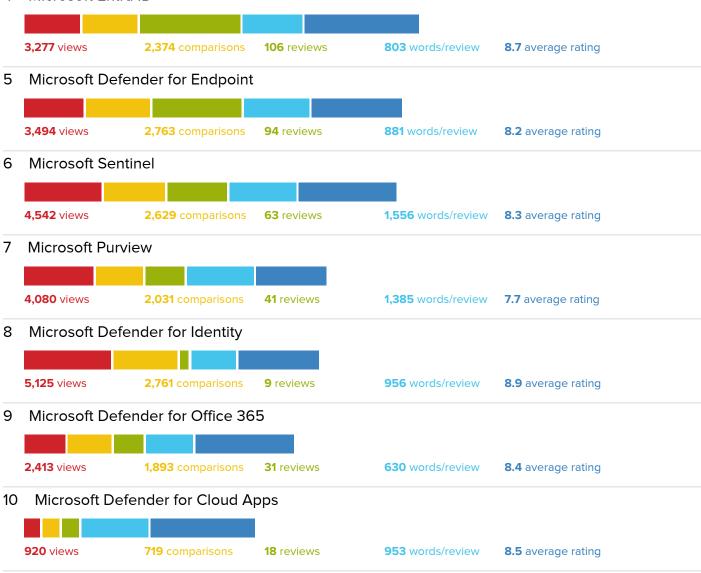
1   Microsoft Defender XDR

8,508 views   **6,376** comparisons   **53** reviews   **1,203** words/review   **8.4** average rating

2   Microsoft Defender for Cloud

9,849 views   **7,220** comparisons   **22** reviews   **1,016** words/review   **8.0** average rating

To read more reviews about Microsoft Security Suite, please visit: https://www.peerspot.com/categories/microsoft-security-suite

3 Microsoft Intune

5,997 views   **3,951** comparisons   **74** reviews   **634** words/review   **8.3** average rating

4   Microsoft Entra ID

3,277 views   **2,374** comparisons   **106** reviews   **803** words/review   **8.7** average rating

5   Microsoft Defender for Endpoint

3,494 views   **2,763** comparisons   **94** reviews   **881** words/review   **8.2** average rating

6   Microsoft Sentinel

4,542 views   **2,629** comparisons   **63** reviews   **1,556** words/review   **8.3** average rating

7   Microsoft Purview

4,080 views   **2,031** comparisons   **41** reviews   **1,385** words/review   **7.7** average rating

8   Microsoft Defender for Identity

5,125 views   **2,761** comparisons   **9** reviews   **956** words/review   **8.9** average rating

9   Microsoft Defender for Office 365

2,413 views   **1,893** comparisons   **31** reviews   **630** words/review   **8.4** average rating

10   Microsoft Defender for Cloud Apps

920 views   **719** comparisons   **18** reviews   **953** words/review   **8.5** average rating

Top Solutions by Ranking Factor

● Views

		VIEWS
1	Microsoft Defender for Cloud	9,849
2	Microsoft Defender XDR	8,508
3	Microsoft Intune	5,997
4	Microsoft Defender for Identity	5,125
5	Microsoft Sentinel	4,542

● Reviews

		REVIEWS
1	Microsoft Entra ID	106
2	Microsoft Defender for Endpoint	94
3	Microsoft Intune	74
4	Microsoft Sentinel	63
5	Microsoft Defender XDR	53

● Words / Review

		WORDS / REVIEW
1	Microsoft Purview Insider Risk Management	2,240
2	Microsoft Sentinel	1,556
3	Microsoft Purview	1,385
4	Microsoft Purview Information Protection	1,307
5	Microsoft Defender XDR	1,203

Microsoft Defender XDR

Overview

Microsoft Defender XDR is a comprehensive security solution designed to protect against threats in the Microsoft 365 environment.

It offers robust security measures, comprehensive threat detection capabilities, and an efficient incident response system. With seamless integration with other Microsoft products and a user-friendly interface, it simplifies security management tasks.

Users have found it effective in detecting and preventing various types of attacks, such as phishing attempts, malware infections, and data breaches.

SAMPLE CUSTOMERS

1. Accenture
2. Coca-Cola
3. Deloitte
4. ExxonMobil
5. General Electric
6. IBM
7. Johnson & Johnson
8. Kellogg's
9. L'Oréal
10. Microsoft (self-use)
11. Nestlé
12. Oracle
13. PepsiCo
14. Qualcomm
15. Rolls-Royce
16. Siemens
17. Target
18. Unilever
19. Verizon
20. Walmart
21. Xerox
22. Yahoo
23. Zara
24. Adobe
25. Boeing
26. Cisco
27. Disney
28. eBay
29. Ford
30. Google
31. HP
32. Intel

TOP COMPARISONS

Microsoft Defender for Cloud vs. Microsoft Defender XDR ... Compared 31% of the time [See comparison]

CrowdStrike Falcon vs. Microsoft Defender XDR ... Compared 29% of the time [See comparison]

Microsoft Purview Compliance Manager vs. Microsoft Defender XDR ... Compared 6% of the time [See comparison]

To read more reviews about Microsoft Security Suite, please visit: https://www.peerspot.com/categories/microsoft-security-suite

REVIEWERS *   **VISITORS READING REVIEWS** *

TOP INDUSTRIES   **TOP INDUSTRIES**

To read more reviews about Microsoft Security Suite, please visit: https://www.peerspot.com/categories/microsoft-security-suite

Microsoft Defender XDR

Top Reviews by Topic

VALUABLE FEATURES

Pekka Kahkipuro.

Its most significant advantage lies in its affordability. Being an integral part of the Microsoft Stack, it comes with a cost-effective package. Especially for higher education, there's an appealing pricing structure. [Full Review]

Michael Wurz

From the perspective of Microsoft 365 XDR, the main benefit is a single, centralized dashboard offering the holistic visibility organizations crave. This is particularly valuable when dealing with multiple vendors, as fragmentation can make achieving this visibility difficult. Microsoft 365 Defender shines when deployed within organizations heavily invested in the Microsoft ecosystem. For those heavily reliant on Defender products like Defender for Endpoint, Defender for Office, and now even Microsoft Sentinel, 365 Defender provides that coveted sin... [Full Review]

Matthew Madigan

The most valuable feature is probably the aggregation and correlation of the different telemetry points with Defender for Identity, Defender for Endpoint, and Defender for Cloud Apps. All of these various things are part of that portal. We've wanted that single pane of glass for years. We've become early adopters of almost all of the features that they offer through the portal, so we've become good at working through the leading-edge quality of the new features and deciding whether or not we want to implement something in production based on that. W... [Full Review]

Verified user

The most valuable aspect is that it comes included with the licensing, which is excellent. It provides a single pane of glass within the 365 admin interface, streamlining our experience by consolidating information in one place and eliminating the need to navigate through multiple interfaces. [Full Review]

Verified user

The incident threat response and its ability to facilitate effective remediation against threats are the standout features. I haven't encountered a similar level of comprehensive incident response in other solutions before. [Full Review]

Christopher Pelfrey

The most valuable aspect is undoubtedly the exploration capability. Given that we are consistently engaged in exploration, constantly seeking reasons for message delivery issues and searching for malicious attachments, the Explorer feature stands out as the primary and most beneficial tool for our needs. [Full Review]

ROOM FOR IMPROVEMENT

Pekka Kahkipuro.

The management features could be improved, particularly in terms of better integration with Intune, Microsoft's cloud-based management solution. Enhanced integration would contribute to a smoother user experience, and ease of use is a key aspect that could benefit from such improvements. [Full Review]

Microsoft Defender XDR

Verified user

Microsoft Defender XDR is not a full-fledged EDR or XDR. Any true XDR should be more powerful than what Microsoft is currently providing. For some public-facing companies, computers, and endpoint computers, we need additional security from CrowdStrike or other third-party XDR. Microsoft Defender XDR does not stop 100 percent of the lateral movement or advanced attacks. Our machines use both Microsoft Defender XDR and Crowdstrike and we have had instances where attacks were missed by Microsoft Defender XDR but caught by Crowdstrike. [Full Review]

Michael Wurz

Overall, the unified dashboard is a great step forward. However, for new users unfamiliar with Microsoft and these products, it can be overwhelming. The abundance of sub-dashboards and sub-areas within the main dashboard can be confusing, even if it all technically makes sense. While it's great for our technical teams and C-Suite to have access to a centralized risk dashboard, it needs to be simplified for less tech-savvy users. The numerous dashboards and interfaces, despite being unified, can be daunting for new users. Ideally, Microsoft could str... [Full Review]

Matthew Madigan

The advanced threat-hunting capabilities are phenomenal, and the security copilot enhances that, but some data elements could be better or have more context inside of the advanced tables themselves. The schemas feel a little limited to what they're building into the product. It's probably just a maturity thing. I imagine we'll see the features I want in the next year. Once you've onboarded your servers to Defender, they're housed on Azure. When those things are brought into the 365 Defender portal, I can see clearly that some of those are Azure reso... [Full Review]

Tony Van Swieten

I don't know if that is Defender's feature, but more active monitoring for data breaches would be beneficial. There could be a way to proactively monitor unusual activity versus just depending on viruses and malware. If the traffic seems unusual, it could detect anomalies and update us. It would help us stop malware attacks ahead of time. [Full Review]

Verified user

It would be highly beneficial if CoPilot could identify anomalies within the network and notify the IT team. For instance, if a user typically accesses around a hundred megabytes of data daily from familiar files and locations but suddenly diverges to an uncommon destination, uploading ten gigabytes of data to an unfamiliar website, that would be a significant anomaly. Pausing such activity and alerting the IT team for a human assessment would be a valuable feature to ensure security. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Pekka Kahkipuro.

It has consistently offered highly appealing academic pricing, with distinct rates for higher education and general educational purposes. This differential pricing is a significant factor and it influenced our choice to use Microsoft products. [Full Review]

Matthew Madigan

Data is expensive if we want to leverage the telemetry that exists within the 365 ecosystem and bring that into Sentinel. I can't pipe that data in without paying an ingestion cost. I know how much data exists in each one of the tables that are there, and it would cost a significant amount of money to bring that in. [Full Review]

Christopher Pelfrey

There has been a noticeable reduction in costs. We've managed to navigate it effectively through our enterprise agreement, and Microsoft's academic discounts have proven to be quite generous. The overall expense is significantly lower, approximately fifty percent less than what we would incur with a traditional enterprise license. [Full Review]

Microsoft Defender for Cloud   See 23 reviews >>

Overview

Microsoft Defender for Cloud is a comprehensive security solution that provides advanced threat protection for cloud workloads. It offers real-time visibility into the security posture of cloud environments, enabling organizations to quickly identify and respond to potential threats. With its advanced machine learning capabilities, Microsoft Defender for Cloud can detect and block sophisticated attacks, including zero-day exploits and fileless malware.

The solution also provides automated remediation capabilities, allowing security teams to quickly and easily respond to security incidents. With Microsoft Defender for Cloud, organizations can ensure the security and compliance of their cloud workloads, while reducing the burden on their sec... [Read More]

SAMPLE CUSTOMERS

Microsoft Defender for Cloud is trusted by companies such as ASOS, Vatenfall, SWC Technology Partners, and more.

TOP COMPARISONS

AWS GuardDuty vs. Microsoft Defender for Cloud ... Compared 18% of the time [See comparison]
Microsoft Defender XDR vs. Microsoft Defender for Cloud ... Compared 17% of the time [See comparison]
Prisma Cloud by Palo Alto Networks vs. Microsoft Defender for Cloud ... Compared 12% of the time [See comparison]

REVIEWERS *	VISITORS READING REVIEWS *
TOP INDUSTRIES	**TOP INDUSTRIES**
Computer Software Company ... 17%	Computer Software Company ... 24%
Financial Services Firm ... 13%	Agriculture ... 10%
Manufacturing Company ... 7%	Consumer Goods Company ... 10%
Government ... 7%	Recruiting/Hr Firm ... 10%
COMPANY SIZE	**COMPANY SIZE**
1-200 Employees ... 20%	1-200 Employees ... 27%
201-1000 Employees ... 14%	201-1000 Employees ... 11%
1001+ Employees ... 66%	1001+ Employees ... 61%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Defender for Cloud

Top Reviews by Topic

💡 VALUABLE FEATURES

Verified user

The entire Defender Suite is tightly coupled, integrated, and collaborative. This allows me to have more flexibility in the roles and responsibilities of my teams, the access to their tooling, and the ability to report accurately on the current threat posture. For example, if I have Sentinel and CloudApp, and someone closes an incident in CloudApp, it will also close in Sentinel. However, if I had CloudApp in Splunk, this would not be the case. This integration is what I like. [Full Review]

Nicolo-De Jesus

DSPM is the most valuable feature. It integrates with standard frameworks, so we can easily see if there are any gaps in our compliance with NIST standards. This allows us to identify areas for improvement and ensure that we are meeting all applicable requirements. [Full Review]

Ellwood S

I like that the solution shows me recent log-ins for certain servers and devices. It's pretty helpful to track down activities and identify or tie them to specific users. [Full Review]

Deshant Shukla

We find two things inside the Azure Security Center to be quite valuable. One is the recommendations, and the second is the regulatory compliance. Both help to keep everything running smoothly. This will give you the security score as well. You can try to get the highest security score, which is 100%. You can get there just from the recommendations from Microsoft. Not all the recommendations will be applicable on the enrollment side. Regulatory compliance is PCI compliance. There are multiple compliance options you can follow. Azure Defender helps i... [Full Review]

Verified user

Defender is user-friendly and provides decent visibility into threats. We use multiple solutions in the Microsoft security suite, including Sentinel and Defender for Endpoint. They integrate smoothly to offer coordinated detection and response. Sentinel ingests data from our entire environment, allowing us to manage everything from one place. We don't need to go to multiple places to find information. Sentinel's capabilities are quite comprehensive. [Full Review]

📊 ROOM FOR IMPROVEMENT

Verified user

The documentation could be much clearer. I also think that Microsoft should stop rebranding everything constantly. I'm tired of every name changing every 90 days. It's ridiculous. I understand that they're coupling tools together but look at AIP. It has had over 14 names in the last five years. That's absurd. Microsoft needs to stop rebranding everything and stick with one brand. They can build them out from there. I like the fact that the dashboards are integrated, but I don't like that the CloudApp is now mapped to the Security dashboard. I hate t... [Full Review]

Hari Shankar

The remediation process could be improved. I have seen that Google has a similar Security Center, where they not only identify vulnerabilities but also provide the steps to fix them. If Microsoft Defender for Cloud could provide remediation steps for all vulnerabilities, it would be a significant enhancement. Currently, only some vulnerabilities have remediation steps available. [Full Review]

Microsoft Defender for Cloud

The product must improve its UI. Looking at multiple devices for the same issue or vulnerability is very cumbersome. The solution should provide built-in features related to trending and graphing over time. If it's already present, we haven't found it. It doesn't seem intuitive to find it quite as easily as some other tools with ready-to-go dashboards. [Full Review]

Ellwood S

The team is already working on one of the latest features, which is having migration techniques right on the portal available. It's possible to use it now. That's one good new feature. For MIM, they are still improving things on Azure Security Center. There are a few flaws in backend technologies. If you do not have the correct access to the system, you cannot access the files and most of the reported resources. For example, a general huge storage account, which is exposed for public access. If there are ten storage accounts available, you can see t... [Full Review]

Deshant Shukla

The solution's portal is very easy to use, but there's one key component that is missing when it comes to managing policies. For example, if I've onboarded my server and I need to specify antivirus policies, there's no option to do that on the portal. I will have to go to Intune to deploy them. That is one main aspect that is missing and it's worrisome. Defender for Cloud, as a solution, allows you to manage and protect servers from vulnerabilities without using Defender for Servers. I find it a bit weird, if you are to manage the antivirus for serv... [Full Review]

Kennedy Kolute

When there is a recommendation by Microsoft Defender that suggests using the Azure Logic App, the remediation step when a user takes action should be created automatically. Microsoft can improve the pricing by offering a plan that is more cost-effective for small and medium organizations. [Full Review]

Srikanth Matsa

PRICING, SETUP COST AND LICENSING

Our clients complain about the cost of Microsoft Defender for Cloud. Microsoft needs to bring the cost down. What we're doing to their detriment is simply lowering the amount of log retention we're keeping, which is not what I want to do. Storage is so cheap in every other aspect of Azure except for Log Analytics, which makes it even more difficult to explain to clients why we're charging them so much for terabytes of storage. In comparison, data lakes and storage accounts store terabytes of data for much less cost. [Full Review]

Verified user

The licensing cost per server is $15 per month. This is the same for SQL which is also $15 per server. It covers the Defender licensing as well. According to my experience, it's a good deal. [Full Review]

Deshant Shukla

There are improvements that have to be made to the licensing. Currently, for servers, it has to be done by grouping the servers on a single subscription and that means that each server is subject to the same planning. We don't have an option whereby, if all those resources are in one subscription, we can have each of the individual servers subject to different planning. There's no option for specifying that "Server A should be in Plan 1 and server B should be in Plan 2," because the servers are in the same subscription. That's something that can be ... [Full Review]

Kennedy Kolute

Currently, Microsoft offers only one plan at the enterprise level which is $15 per machine. This plan can be very costly for small and medium businesses and in some parts of the world, it is cheaper for an organization to hire a full-time security engineer instead. [Full Review]

Srikanth Matsa

Microsoft Intune

Overview

Microsoft Intune is a comprehensive cloud-based service that allows you to remotely manage mobile devices and mobile applications without worrying about the security of your organization's data. Device and app management can be used on company-owned devices as well as personal devices.

In an increasingly mobile workforce, Microsoft Intune keeps your sensitive data safe while on the move. Microsoft Intune makes it possible for your team members to work anywhere using their mobile devices. Microsoft Intune provides both the flexibility and the control needed for securing all your data on the cloud, no matter where the device with the data is located.

Microsoft Intune Device Management Key Features

With Microsoft Intune Device Management yo... [Read More]

SAMPLE CUSTOMERS

Mitchells and Buzzers, Callaway

TOP COMPARISONS

Jamf Pro vs. Microsoft Intune ... Compared 16% of the time [See comparison]
VMware Workspace ONE vs. Microsoft Intune ... Compared 14% of the time [See comparison]
ManageEngine Endpoint Central vs. Microsoft Intune ... Compared 8% of the time [See comparison]

REVIEWERS *	**VISITORS READING REVIEWS ***
TOP INDUSTRIES	**TOP INDUSTRIES**
Educational Organization ... 23%	Financial Services Firm ... 21%
Computer Software Company ... 13%	Computer Software Company ... 20%
Government ... 7%	Manufacturing Company ... 7%
Financial Services Firm ... 6%	Healthcare Company ... 5%
COMPANY SIZE	**COMPANY SIZE**
1-200 Employees ... 20%	1-200 Employees ... 36%
201-1000 Employees ... 33%	201-1000 Employees ... 14%
1001+ Employees ... 47%	1001+ Employees ... 49%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Intune

Top Reviews by Topic

VALUABLE FEATURES

Verified user

One of the most valuable aspects of Microsoft Intune is its seamless integration with Azure Active Directory, offering capabilities akin to Group Policy Objects. This integration provides a centralized platform for managing and enforcing policies, ensuring the stability of configuration data across devices, resembling the familiar functionalities of traditional group policies in an on-premises Active Directory environment. In utilizing Intune's endpoint privilege management feature, I've primarily focused on configuring VPN access and certificates, ... [Full Review]

Colin Jamieson

It is quite easy to manage. From what I have seen, it is very easy to check through. It is very basic. I do not need to be a rocket scientist to manage it. It takes a little bit of experience to set it up if you have never done it before. From a manageability point of view and ease of use, I would give it an eight out of ten rating. It is quite policy-enabled, so you can build pretty much any policy to manage remote endpoints. [Full Review]

Amel Benali

Its most valuable aspect is the seamless onboarding and offboarding of new users, whether it's for a computer or a mobile device. This process is remarkably straightforward. Additionally, while not explicitly security features, there are safeguards in place that enhance safety. For instance, if a user reports their computer as stolen, you can promptly lock it and erase all data remotely. This means you can secure the hardware even without physical possession of the device. It goes beyond safeguarding just the Microsoft 365 user account; it extends p... [Full Review]

Shrikant Pillay.

The system as a whole is immensely valuable, proving to be highly helpful and practical. There has been a noticeable increase in productivity for both my organization and clients. The primary factor contributing to this enhancement is the user-friendly nature of the platform, coupled with effective technical support. [Full Review]

Olusola Odediran

Intune plays a crucial role in ensuring the security of hybrid work environments and safeguarding data on both company-owned and BYO devices. While it functions seamlessly for mainstream devices, including Dimensional and others, there might be some challenges with certain brands of personal devices. However, overall, Intune provides a comprehensive platform where both corporate and partner devices can coexist securely. The utilization of Microsoft security signals, coupled with the impact of Intune on our organization's security, is a pivotal aspec... [Full Review]

Verified user

The most valuable feature of Intune is the central dashboard for compliance and policy management. It is also handy for asset management and it covers all the basics we need right now. [Full Review]

ROOM FOR IMPROVEMENT

Verified user

In terms of configuration, my experience with Intune is somewhat mixed. The configuration tool appears to be scattered throughout the Intune interface, requiring frequent navigation back and forth. The web interface, while functional, isn't particularly user-friendly, leading me to find PowerShell a preferable option. However, using PowerShell involves investing time in developing scripts. The challenge lies in the complexity of navigating between profiles and MDM configurations. Multiple windows need to be open simultaneously to grasp the overall c... [Full Review]

Microsoft Intune

Colin Jamieson

There could be more wizard-driven policy development or creation. Some of the policies can get quite complex. If they have a wizard that assists the administrators in creating the policy, that will be a great job. Microsoft South Africa should improve their support for Intune in terms of turnaround time. [Full Review]

Amel Benali

It would be beneficial to have a more straightforward understanding of Intune's capabilities, presented in a simplified manner. This way, one wouldn't need to be an Intune specialist or spend hours trying to grasp the intricacies of policies and functionalities. While I've used Intune extensively and have practical experience, I've found that to explore its full potential, significant time is needed for both understanding capabilities and seeking out relevant training. The current understanding of what actions or functionalities are available for co... [Full Review]

Shrikant Pillay.

An area for improvement is the absence of seamless integration, particularly with external dashboards. Currently, to obtain an updated overview of devices not in compliance, we need to download the data, restricting visibility across other platforms like Power BI or third-party dashboards. This presents a challenge as we have to manually pull and manage the data, highlighting the need for enhanced integration with dashboard solutions. [Full Review]

Muhammad Javed

Microsoft Intune is not user-friendly to manage and has room for improvement. The detection and prevention of end-user data leaks from mobile devices can be improved. [Full Review]

Verified user

There is room for improvement, particularly on the Apple side. Enhancements for managing MacOS more comprehensively would be beneficial. While it is good, there are still features missing compared to the management capabilities we have for other operating systems. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Jon McWilliams

For organizations that are a Microsoft shop, the pricing is compelling. To buy it outright, it's two dollars a seat, which is cheap. The price is worth it. [Full Review]

Verified user

The pricing is inherently reasonable, as Microsoft leverages market insights to maintain the total cost of ownership at around ninety to ninety-five percent of what would be incurred in an on-premise scenario. Microsoft products inherently benefit from economies of scale and global reach, making them cost-effective. [Full Review]

Colin Jamieson

It comes as a bundle, so you do not really know what the prices are. Microsoft does not break it down to the user cost for us. It is just bundled with our E5 license. [Full Review]

Microsoft Entra ID

Overview

Secure access to any app or resource from anywhere

Take advantage of adaptive identity and network access controls to secure access to any app or resource for every user or digital workload across your entire environment.

Protect and verify every identity

Implement consistent security policies for every user—employees, frontline workers, customers, partners—as well as apps, devices, and workloads across multicloud and hybrid.

Provide only the access necessary

Discover and right-size permissions, manage access lifecycles, and ensure least privilege access for any identity.

Simplify the user experience

Reduce IT friction and improve the hybrid workforce experience with seamless access to any resource, single sign-on, user self-service ... [Read More]

SAMPLE CUSTOMERS

Microsoft Entre ID is trusted by companies of all sizes and industries including Walmart, Zscaler, Uniper, Amtrak, monday.com, and more.

TOP COMPARISONS

Google Cloud Identity vs. Microsoft Entra ID ... Compared 7% of the time [See comparison]
Microsoft Intune vs. Microsoft Entra ID ... Compared 7% of the time [See comparison]
Yubico YubiKey vs. Microsoft Entra ID ... Compared 6% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Educational Organization ... 24%
Computer Software Company ... 12%
Financial Services Firm ... 9%
Government ... 6%

COMPANY SIZE

1-200 Employees ... 18%
201-1000 Employees ... 32%
1001+ Employees ... 49%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 15%
Computer Software Company ... 14%
Healthcare Company ... 6%
Educational Organization ... 6%

COMPANY SIZE

1-200 Employees ... 33%
201-1000 Employees ... 14%
1001+ Employees ... 54%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Entra ID

Top Reviews by Topic
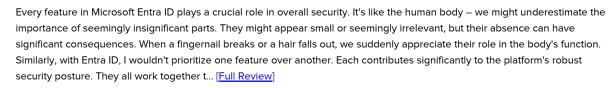
💡 VALUABLE FEATURES

Arun Govind

The most valuable feature of Microsoft Entra ID is its security options, where we can provide highly effective security for user accounts during authentication. We have a conditional access policy in place, along with modern authentication methods that can be configured in various ways to meet organizational requirements. These methods may include phone calls, SMS, or even passwordless authentication, which is the most convenient and secure method introduced by Microsoft. This includes Windows Hello for business and certification-based authenticatio... [Full Review]

Dumebi Chukwueme ka

Every feature in Microsoft Entra ID plays a crucial role in overall security. It's like the human body – we might underestimate the importance of seemingly insignificant parts. They might appear small or seemingly irrelevant, but their absence can have significant consequences. When a fingernail breaks or a hair falls out, we suddenly appreciate their role in the body's function. Similarly, with Entra ID, I wouldn't prioritize one feature over another. Each contributes significantly to the platform's robust security posture. They all work together t... [Full Review]

Verified user

The most valuable features of Microsoft Entra ID are the login and the conditional access pieces. The login helps me identify who went where, why, and what problems they may have encountered. The conditional access allows me to control the flow of user access. [Full Review]

Trevor Mulanax

The most valuable feature of the solution is its ability to delegate roles to each individual resource, which is great. I think the aforementioned feature is better done in the solution itself than with an actual local AD. [Full Review]

📊 ROOM FOR IMPROVEMENT

Arun Govind

There are several limitations that Microsoft is currently facing. Since I work with global customers daily, they often come up with new ideas. However, these ideas are sometimes hindered by Microsoft's limitations. As a result, many people are turning to third-party tools or services, even from vendors that are not as reputable as AWS or GCP. I have personally made similar suggestions to my product team, especially regarding the vendors that users are attempting to rely on. For instance, certain organizations prefer to restrict the use of mobile pho... [Full Review]

Nagendra Nekkala.

The role-based access control can be improved. Normally, the role-based access control has different privileges. Each role, such as administrator or user, has different privileges, and the setup rules for them should be defined automatically rather than doing it manually. [Full Review]

Dumebi Chukwueme ka

Microsoft Entra ID can make improvements in two key areas. The first is to upgrade Workday and SuccessFactors integration to OAuth 2.0. Currently, these HR applications use basic authentication for inbound provisioning to Entra ID, while integration with other IDPs utilizes OAuth 2.0. Many organizations request the adoption of OAuth 2.0 for Entra ID as well, considering its enhanced security. The second is to provide clearer communication about features under public review. Features under public review should have comprehensive documentation outlini... [Full Review]

To read more reviews about Microsoft Security Suite, please visit: https://www.peerspot.com/categories/microsoft-security-suite

Microsoft Entra ID

Verified user

The private access is the next big thing for us, and that's one feature I'm going to try in public preview and probably move towards. There is no great solution in the cloud for Conditional Access authentication and RADIUS-type authentication. [Full Review]

Trevor Mulanax

I wish transitioning from Microsoft Active Directory to Microsoft Entra ID was a little easier, and I didn't have to learn so many new concepts. I faced difficulties from Micorosft's end and during the transition from Microsoft Active Directory to Microsoft Entra ID. Sometimes, some of Microsoft's documentation could be a little outdated. The product doesn't meet the organization's niche requirements, especially in our environment. Microsoft Entra ID is not a very standard product. When I think about the trade-off I have had to go for to get the afo... [Full Review]

Verified user

Allowing for more customization would be very useful. There is a limited metadata capability. When you look at a user, there are only six pieces of information you can see, but organizations are way more complex, so having that metadata available and being able to use that for dynamic user groups and other policies would be very helpful. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Arun Govind

Entra's pricing is somewhat higher compared to AWS. With AWS, we have the ability to access EC2 servers, which are essentially virtual machines, for free for a duration of up to one year, specifically the basic virtual machine instances. However, Entra does not offer a similar option. If we are utilizing any form of virtual machine on Entra, we must begin payment after one month of complimentary usage. Unlike AWS, Entra does not provide access to basic virtual machine instances for educational or testing purposes. Furthermore, there is a discernible... [Full Review]

Dumebi Chukwuemeka

The cost of Entra ID depends entirely on our organization's specific needs and use cases. For smaller organizations, like a local supermarket, it might be quite affordable with the basic free tier or a lower-tiered license. However, larger, multi-national companies with complex requirements may incur higher costs due to the need for additional features and advanced licensing tiers like P1 or P2. Instead of simply labeling it as cheap or expensive, it's important to consider our specific scenario and what functionalities we require. Different models ... [Full Review]

Verified user

Everything costs money in a tough market. As a nonprofit, we have A5 licenses for nonprofits in education, so we at least have some reduced costs. Looking at Copilot and a bunch of other features that are coming out, we'll have to seriously consider that cost-to-value ratio. [Full Review]

Verified user

Pricing could always be better. You pay the premium for Microsoft. Sometimes, it is worth it, and at other times, you wish to have more licensing options, especially for smaller companies. [Full Review]

Jay Ved

It is good. We have Office 365 E3, and then that is tied in with Azure Active Directory. I believe that we only have to pay for our technician-level access or IT department access for Azure Active Directory Premium, which I am sure they call Entra Premium P2 licensing, so it is not a very large cost. We just adopted that, and that gives us a lot of insights into user security that we would not otherwise have. [Full Review]

Microsoft Defender for Endpoint

Overview

Microsoft Defender for Endpoint is a comprehensive security solution that provides advanced threat protection for organizations. It offers real-time protection against various types of cyber threats, including malware, viruses, ransomware, and phishing attacks. With its powerful machine-learning capabilities, it can detect and block sophisticated attacks before they can cause any harm. The solution also includes endpoint detection and response (EDR) capabilities, allowing organizations to quickly investigate and respond to security incidents. It provides detailed insights into the attack timeline, enabling security teams to understand the scope and impact of an incident. Microsoft Defender for Endpoint also offers proactive thre... [Read More]

SAMPLE CUSTOMERS

Petrofrac, Metro CSG, Christus Health

TOP COMPARISONS

Intercept X Endpoint vs. Microsoft Defender for Endpoint ... Compared 10% of the time [See comparison]
Symantec Endpoint Security vs. Microsoft Defender for Endpoint ... Compared 9% of the time [See comparison]
CrowdStrike Falcon vs. Microsoft Defender for Endpoint ... Compared 5% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Educational Organization ... 21%
Computer Software Company ... 13%
Government ... 8%
Financial Services Firm ... 7%

TOP INDUSTRIES

Financial Services Firm ... 19%
Computer Software Company ... 16%
Energy/Utilities Company ... 7%
Manufacturing Company ... 7%

COMPANY SIZE

1-200 Employees ... 23%
201-1000 Employees ... 31%
1001+ Employees ... 46%

COMPANY SIZE

1-200 Employees ... 40%
201-1000 Employees ... 16%
1001+ Employees ... 43%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Defender for Endpoint

Top Reviews by Topic

💡 VALUABLE FEATURES

Verified user

It has Kusto Query Language (KQL), so we can use our own queries to find anything. We can get real-time updates. It is not just signature-based. It provides results based on behavior and successors. It analyzes the behavior and the process. With that, we can achieve greater results that other products do not offer. [Full Review]

Mike LaRochelle

The most valuable aspect lies in its automation capabilities, particularly within security automation. It contributes to more efficient time management for us and it provides an efficient way to keep track of user actions and maintain a secure and well-monitored system. [Full Review]

Mark Foust

I like that Defender is integrated and doesn't have a third-party payload trying to advertise subscription renewal. I don't get spam because of it. Regarding visibility, no one has their finger in as many operating systems as Microsoft. No one has the platform or deployment profile that Microsoft has. Microsoft can outshine any third-party vendor when it comes to visibility. [Full Review]

Drake Scott

Microsoft Defender for Endpoint's WCS function, a content filtering solution, has proven to be the most useful, stable, and reliable option for our current needs. [Full Review]

📊 ROOM FOR IMPROVEMENT

Verified user

We need better support to learn about the product. Documentation is available, but we need some kind of training program so that we can get a better understanding of the product. [Full Review]

Doug Kinzinger

Defender should be more accessible for small and medium-sized businesses. You have some organizations that maybe have a hundred employees, and they're focused on making their widgets. That's their nine-to-five every day. They're not thinking about that security side, but maybe they're already invested in 365 or the Azure ecosystem and having Defender as an add-on makes sense from a price perspective. It's easy to deploy, but it could be easier for some of those smaller businesses to onboard endpoints. The onboarding and deployment could be more user... [Full Review]

Mark Foust

The interface isn't necessarily intuitive to a nontechnical person. You can get stuck in the little endpoint security portal. Sometimes, if you uninstall a competitive product, the end user doesn't always know if it's running or if they're protected even though it's silently running. There could be a notification, widget, or something that's resident on the screen for at least a bit, especially if you're doing remote support. You want to talk them through it, but sometimes, we're not allowed to look at the PCs we support. I'd like them to improve vi... [Full Review]

Microsoft Defender for Endpoint

Vili Nurminen

Microsoft Defender for Endpoint's licensing is confusing. It has conflicting information on the website. We also faced integration issues with other systems. It makes laptops slower than traditional antivirus systems. [Full Review]

Verified user

The product itself does not necessarily need improvement, but the support and implementation of the product are the disaster cases. Instead of being able to go back to Microsoft and ask how to do something, we have to work with a vendor who does not exactly know how to do that and has to go to Microsoft to say, "How do we do this?" so that they can answer our questions. There are a lot of things in relation to various compliance standards such as CIS. The primary levels of support of Microsoft do not know or cannot implement that. Working through ve... [Full Review]

Drake Scott

Defender for Cloud Apps is one of the most significant products that Microsoft could improve. We've encountered several limitations with Defender for Cloud Apps, such as the inability to create custom cloud applications and add URLs. These features would be valuable for the scoping feature in Defender for Cloud Apps, as each application can currently only have one scope. It cannot have multiple scopes, meaning that an application cannot be blocked for some device groups and allowed for others. This is another limitation we've encountered frequently.... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Doug Kinzinger

Defender's pricing is competitive. There are ways to negotiate a better price with Microsoft or your reseller as your business grows. You can say, "Hey, I bought 365 Business, then E3, and E5. Now, I'm buying Defender, so give me bulk pricing." There are opportunities to save as you grow that wouldn't exist if you picked a different vendor. [Full Review]

Mark Foust

Defender is typically bundled with 365 packages that the customers are already buying. We haven't done an in-depth ROI for right. Often, we leave the customer to make those decisions even though we can point to tools like that on the web or allow an analyst tool to do that type of work. [Full Review]

Verified user

I recently switched from education to private business, and all I can say is that private business licensing from Microsoft is not cheap until you hit certain quantities or scale. That does not mean that it is not comparable to other industries. It is similar pricing, but it is still crazy to me how much you pay for a client. I feel it is high, but it is in line with other vendors. [Full Review]

Drake Scott

The base price for an E5 license, which includes Enterprise Mobility + Security E5, is $57 per user per month. However, there are additional costs for certain security features, such as Premium Threat and Vulnerability Management and Insider Risk Management. [Full Review]

Naman Verma.

The product is very cheap compared to other options. It's very affordable, which is why Microsoft is gaining a foothold in terms of client acquisition. [Full Review]

Microsoft Sentinel

Overview

Microsoft Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution that lets you see and stop threats before they cause harm. Microsoft Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Eliminate security infrastructure setup and maintenance, and elastically scale to meet your security needs—while reducing IT costs. With Microsoft Sentinel, you can:

- Collect data at cloud scale—across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds

- Detect previously unc... [Read More]

SAMPLE CUSTOMERS

Microsoft Sentinel is trusted by companies of all sizes including ABM, ASOS, Uniper, First West Credit Union, Avanade, and more.

TOP COMPARISONS

AWS Security Hub vs. Microsoft Sentinel ... Compared 17% of the time [See comparison]
IBM Security QRadar vs. Microsoft Sentinel ... Compared 12% of the time [See comparison]
Splunk Enterprise Security vs. Microsoft Sentinel ... Compared 8% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Computer Software Company ... 16%
Financial Services Firm ... 10%
Government ... 9%
Manufacturing Company ... 7%

COMPANY SIZE

1-200 Employees ... 24%
201-1000 Employees ... 16%
1001+ Employees ... 60%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 23%
Computer Software Company ... 11%
Manufacturing Company ... 9%
Healthcare Company ... 6%

COMPANY SIZE

1-200 Employees ... 33%
201-1000 Employees ... 22%
1001+ Employees ... 44%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Sentinel

Top Reviews by Topic

💡 VALUABLE FEATURES

Harman Saggu

The most valuable feature is the alert notifications, which are categorized by severity levels: informational, low, medium, and high. This allows us to prioritize and address alerts based on their urgency. For instance, we would immediately address high-severity alerts. This feature, along with the ability to create playbooks, significantly enhances our workflow. [Full Review]

Joseph Messina

The analytic rule is the most valuable feature. It allows us to assess the various use cases we've developed and then automate those processes accordingly. I consider it a force multiplier. It empowers a small team to achieve a significant impact, whereas previously, I would have relied on multiple individuals. By utilizing it, we can accomplish more with fewer resources. [Full Review]

Sachin Paul

The features that stand out are the * detection engine * integration with multiple data sources. And while it does not give the tools to detect and investigate, it provides the ability to integrate multiple tools together on the platform. This is very important for us. Sentinel provides very good integration with Microsoft Power Apps and Power Automate. That is a very handy feature. It provides a good user interface for an operations analyst and makes it easy for an ops analyst to do incident analysis and investigations. [Full Review]

Nagendra Nekkala

The product can integrate with any device. It has connectors. So, we do not have big issues in building connectors. Microsoft Sentinel gives us a unified set of tools to detect, investigate, and respond to incidents. It also helps us recover things. It is very important to our organization. It centralizes our total threat collection and detection and generates investigation reports. [Full Review]

Verified user

It has a lot of great features. The integrations on offer are very good. They have a lot of frequent updates on the integrations as well. We also use other Microsoft products with it, such as Active Directory and Defender for Endpoint and Identity. Everything is well integrated together. The integration itself is seamless. Its connectors are helpful. We get good logs from the solution. Threat visibility is good so far. We are able to prioritize threats based on many factors. The comprehensiveness of the solution is good. [Full Review]

📊 ROOM FOR IMPROVEMENT

Harman Saggu

I would like Microsoft to add more connectors for Sentinel. Microsoft Sentinel should provide an alternative query language to KQL for users who lack KQL expertise. [Full Review]

Hari Shankar

I would like Sentinel to have more out-of-the-box analytics rules. There are already more than 400 rules, but they could add more industry-specific ones. For example, you could have sets of out-of-the-box rules for banking, financial sector, insurance, automotive, etc., so it's easier for people to use it out of the box. Structuring the rules according to industry might help us. They could also add some more connectors. Sentinel has 120 connectors, including most of the essential data ones, but they could add some more legacy connectors. [Full Review]

Microsoft Sentinel

Joseph Messina

While I appreciate the UI itself and the vast amount of information available on the platform, I'm finding the overall user experience to be frustrating due to frequent disconnections and the requirement to repeatedly re-authenticate. Microsoft needs to address these usability issues to enhance the user experience. [Full Review]

Nagendra Nekkala

The AI capabilities must be improved. The product must efficiently leverage the AI capabilities for threat detection and response. The product does not provide auto-configuration features. So, we need to do configuration, policy changes, and group policies ourselves. If AI can do these functions, it will be easier for the customers. [Full Review]

Verified user

We've seen delays in getting the logs from third-party solutions and sometimes Microsoft products as well. It would be helpful if Microsoft created a list of the delays. That would make things more transparent for customers. In some instances, the customer reports that they suspect malware on a computer, and one of their IT guys noticed it. There is a five to ten minute delay before we can see it and respond. As a security company, we don't want the customer to be the first one to identify the threat. However, we must deal with delays from the vario... [Full Review]

Santhosh I

The UEBA part needs improvement. They need to bring other log sources to UEBA. The reporting could be more structured. There are no reporting modules or anything. It's only the dashboard. Therefore, when a customer requests a report, you need to manually pull the dashboard and send it to the customer for the reporting. However, if there was a report or template there, it would be easier to schedule and send the weekly reports or monthly executive reports. The log ingestion could be improved on the connector layer. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Hari Shankar

I am not involved on the financial side, but from an enterprise-wide use perspective, I think the price is good enough. We have bundled pricing with Azure Monitor Log Analytics. We would be using Log Analytics Workspace even if we didn't have Sentinel, and we would need to pay a separate license for IBM QRadar or Splunk. It optimizes costs when we use both in our digital estate. [Full Review]

Joseph Messina

Microsoft Sentinel can be costly, particularly for data management. While Microsoft provides various free offerings to attract users, these benefits can quickly become overwhelmed by escalating data management expenses if proper precautions are not taken. I don't think it's Microsoft engaging in underhanded tactics. I believe the issue lies with customers not paying close enough attention to what they're enabling. Initially, they're excited and eager to incorporate everything, but before they realize it, they've incurred unexpected costs. Azure Moni... [Full Review]

Sachin Paul

The licensing cost is available on the Microsoft Azure calculator. It depends on the size of the deployment, the size of the data ingestion. It is consumption-based pricing. It is an affordable solution. [Full Review]

Nagendra Nekkala

The product is costly compared to Splunk. When we pay for the product, we also have Azure Monitor Log Analytics as part of the package. It is economical for us. [Full Review]

Microsoft Purview

Overview

Microsoft Purview is a unified data governance solution that helps you understand all of your on-premises, multi cloud, and software-as-a-service (SaaS) data and maintain control over its usage. With the Microsoft Purview solution, you can create a detailed, up-to-date map of your data landscape with sensitive data classification, automated data discovery, and end-to-end data lineage. Not only does it enable data curators to easily secure your data, but it also allows data consumers to find valuable, trustworthy data.

Microsoft Azure Purview is designed with:

Data Map: Microsoft Purview Data Map provides the foundation for data discovery and effective data governance. Azure Purview Data Map is a cloud-native PaaS service that captur... [Read More]

SAMPLE CUSTOMERS

TOP COMPARISONS

Collibra Governance vs. Microsoft Purview ... Compared 16% of the time [See comparison]
Alation Data Catalog vs. Microsoft Purview ... Compared 13% of the time [See comparison]
Informatica Axon vs. Microsoft Purview ... Compared 9% of the time [See comparison]

REVIEWERS *	VISITORS READING REVIEWS *
TOP INDUSTRIES	**TOP INDUSTRIES**
Financial Services Firm ... 14%	Financial Services Firm ... 26%
Computer Software Company ... 13%	Computer Software Company ... 13%
Government ... 9%	Insurance Company ... 9%
Insurance Company ... 7%	University ... 9%
COMPANY SIZE	**COMPANY SIZE**
1-200 Employees ... 20%	1-200 Employees ... 32%
201-1000 Employees ... 14%	201-1000 Employees ... 20%
1001+ Employees ... 66%	1001+ Employees ... 48%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Purview

Top Reviews by Topic

💡 VALUABLE FEATURES

Satya Vinayan

The user interface is highly intuitive and user-friendly. I appreciate it because it provides a unified solution. Everything can be managed in one place, from scanning sources to making assets available. The access includes comprehensive metadata information, presented in a non-technical manner for easy comprehension of the asset's nature. The visualization it offers is quite clear. Additionally, it creates a lineage based on data processing, allowing for workflow authorization and control over metadata modifications or other activities. It caters t... [Full Review]

Afeez Olaboye

The custom classifications are one of the most valuable features. For instance, if we want to block the transfer of card details, there are many pre-built samples for different countries that we can easily use in Purview, eliminating the need to create our classifications which makes the work easier. [Full Review]

Mohammad Kassab

No single feature stands out as the best because the most effective approach involves combining multiple features. For example, when using information protection, labeling, and classification, a multi-step process is necessary. First, we must classify our data, which requires a thorough understanding of our environment and the nature of the data itself. Once classified, we can apply labels and establish rules governing data sharing through information protection measures. The final step involves implementing and configuring a Data Loss Prevention so... [Full Review]

Rajesh Yad

Data segregation is the most valuable feature. This provides clear visibility into the hierarchy of data flow, including its destinations, loading points, and table updates. [Full Review]

Hanuman Devineni

The most valuable features are lineage, data cataloging, glossaries, and the new access delegation feature. This feature will make it quicker to delegate access to all the data with a single request button. On Azure, it's definitely important that Purview delivers data protection across multi-platform environments. It gives us complete visibility of where our security data resides and what types of data we have. This is useful because we store data across multiple platforms, including databases, storage, spreadsheets, Excel, CSS, and caching. Purvie... [Full Review]

Daniël Zadrosz

I really like the entire system for auto-labeling content. It's a very refined system. I use the Keyword Query Language to define refined string-based metadata, and then I can really go deep into the specific data with the specific properties labeled in such and such a way. That's a very good basis for the use cases that I have. That gives me a lot of leeway and a lot of freedom to really enclose a lot of specific use cases. Another thing I'm very much a fan of is the notion of machine-learning-based labeling. However, as with syntax, which I'm a bi... [Full Review]

📊 ROOM FOR IMPROVEMENT

Satya Vinayan

Enhancing the tool's capability to connect to multiple sources would be valuable. Also, when data is transformed in other systems, the tool should capture the relevant metadata and generate lineage for those systems as well. Thirdly, addressing limitations, such as relying on Apache Atlas for mitigation, should be handled within the Microsoft tool itself rather than external dependencies like Apache Atlas. [Full Review]

Microsoft Purview

Purview needs to improve its DLP capabilities for removable devices such as external drives and USB devices. The custom data classification for the African region needs to be improved. [Full Review]

Afeez Olaboye

I've been working closely with Microsoft support on issues with the Microsoft Purview Information Protection scanner's on-premises services. While it's a solid tool, there's still room for improvement in my opinion. I've submitted numerous recommendations, from solutions to address specific problems to the implementation of new features like bulk scanning across multiple servers, not just individual paths. I've also encountered a high number of false positives in the classifier and made suggestions for resolving them. Microsoft support is currently ... [Full Review]

Mohammad Kassab

While Microsoft Purview offers data protection across multi-cloud and multi-platform environments, granting access in such complex settings can be lengthy and expensive. Every scan we perform incurs a charge, making exploration quite costly. I would like to have complete video documentation for training. [Full Review]

Rajesh Yad

I have some concerns about the separation of roles in Purview from the Microsoft tenant, as well as how they interact with the security portal and endpoint manager. Certain permission issues or protracted permission updates could arise due to suboptimal configuration, potentially extending the expected timeframe. [Full Review]

Francisco Montilla

As we are looking at Purview as an enterprise-level tool, there are two areas where I still see that there is something that can be improved. One is about disaster recovery. Purview has not matured in the way of building the tool without having disaster recovery. We don't have disaster recovery or high availability. If anything goes wrong, like, there are any changes happening, and I want to roll back, there is no way that I can roll back in the existing system. For example, I have a data source in which one of the users has dropped or deleted the d... [Full Review]

Hanuman Devineni

PRICING, SETUP COST AND LICENSING

I consider it cost-efficient because of the metrics it provides. With each scan being incremental, avoiding redundant scans of the same object, the tool offers a way to manage costs effectively. [Full Review]

Satya Vinayan

While Purview's standard pricing might not be accessible to most small businesses, we were fortunate to benefit from the educational pricing which made it a financially viable option for our needs. [Full Review]

Francisco Montilla

Since it's more consumption-based, the pricing looks good, but we should have a few options to limit Purview. In terms of usage or size and limit the price. Right now, we don't have control over it because it depends on the volume of data IT stores and the number of users being used concurrently. So those are a few areas we don't have control over because it's completely on the consumption base now. [Full Review]

Hanuman Devineni

Microsoft Defender for Identity

Overview

Microsoft Defender for Identity is a comprehensive security solution that helps organizations protect their identities and detect potential threats. It leverages advanced analytics and machine learning to provide real-time visibility into user activities, enabling proactive identification of suspicious behavior.

With its powerful detection capabilities, it can identify various types of attacks, including brute force, pass-the-hash, and golden ticket attacks. The solution also offers rich reporting and alerting capabilities, allowing security teams to quickly respond to incidents and mitigate risks. By continuously monitoring user activities and providing actionable insights, Microsoft Defender for Identity helps organizations strengthen t... [Read More]

SAMPLE CUSTOMERS

Microsoft Defender for Identity is trusted by companies such as St. Luke's University Health Network, Ansell, and more.

TOP COMPARISONS

Microsoft Entra ID Protection vs. Microsoft Defender for Identity ... Compared 32% of the time [See comparison]
Microsoft Defender for Office 365 vs. Microsoft Defender for Identity ... Compared 15% of the time [See comparison]
Microsoft Entra Verified ID vs. Microsoft Defender for Identity ... Compared 7% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Computer Software Company ... 16%
Financial Services Firm ... 14%
Government ... 9%
Manufacturing Company ... 7%

COMPANY SIZE

1-200 Employees ... 17%
201-1000 Employees ... 17%
1001+ Employees ... 67%

COMPANY SIZE

1-200 Employees ... 22%
201-1000 Employees ... 16%
1001+ Employees ... 62%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Defender for Identity

Top Reviews by Topic

VALUABLE FEATURES

Nagendra Nekkala.

It gives us visibility into advanced behavior activities. It'll show a history of logins or events. It's efficient, and it provides all of the investigation reports, which is an advantage for us. It also helps us prioritize threats across the company. It helps us detect the exact timing of incidents, and we'll see them when they happen. It helps us adhere to our SLAs. We can see threats and if they are of higher or lower severity. We can find the types of malicious events, see what's happening, see what actions are taken, and understand what is happ... [Full Review]

Dumebi Chukwueme ka

Microsoft Defender for Identity provides excellent visibility into threats by leveraging real-time analytics and data intelligence. With features like SecureScore and SecureScan, it offers a holistic view of security across both on-premises and cloud environments. A high SecureScore indicates strong security, while a low score signals potential threats. This makes it easy to detect and address security issues promptly. [Full Review]

Matthew Bouwer

The most valuable aspect is its connection to Microsoft Sentinel and Defender for Endpoint, and giving exact timelines for incidents and when certain events occured during an incident. It's good to know when a sign-on occurred, especially if it was outside the usual time, and whether the sign-on was from Australia, because our users don't usually sign on from outside Australia. And for prioritizing threats, we get alerts that are low or high severity and that tells us what need to do within our SLA, and what we prioritize in terms of further escalat... [Full Review]

Emeka Ndulu

The feature I like the most about Defender for Identity is the entity tags. They give you the ability to identify sensitive accounts, devices, and groups. You also have honeytoken entities, which are devices that are identified as "bait" for fraudulent actors. Once these devices have been tagged, they give you alerts about when a malicious actor tries to explore the vulnerability that you created. You can monitor what the attacker is going after. Entity tagging is a big win for Defender for Identity. There is a connection between the cloud, Defender... [Full Review]

Bikram S.

The feature I like most is that you can create your own customized detection rules. It has a lot of default alerts and rules, but you can customize them according to your business needs. For example, we have a prevention mechanism through a policy where, if anyone tries to access something and gives the wrong credentials three times, that account will automatically be deactivated for the next half hour. Also, you can integrate Defender for Identity with any SIEM platform, like Splunk, QRadar, and all top SIEMs, and create your own dashboards and rep... [Full Review]

Bala Krishna

Almost all the features are valuable. The solution offers excellent visibility into threats. Defender for Identity helps prioritize threats across our enterprise, which is essential for any identity and access management product. The solution's threat intelligence helps us prepare for potential threats and take proactive steps before they hit. We've tested various scenarios over the past months, including our major security concerns, a valuable exercise that helps us to protect our system. [Full Review]

ROOM FOR IMPROVEMENT

Nagendra Nekkala.

The tracking instance needs to be configured appropriately. They need to be able to identify more vulnerabilities in order to increase the efficiency of the solution. [Full Review]

Microsoft Defender for Identity

Dumebi Chukwuemeka

One potential area for improvement could be exploring flexibility in the installation of Microsoft Defender for Identity agents. Currently, it is mandatory to install the agent on the on-premises environment, and considering if there could be more flexibility in deployment might be worth exploring. [Full Review]

Reynaldo Ruiz Flores

Microsoft should look at what competing vendors like CrowdStrike and Broadcom are doing and incorporate those features into Sentinel and Defender. At the same time, I think the intelligence inside the product is improving fast. They should incorporate more zero-trust and hybrid trust approaches. They need to build up threat intelligence based on threats and methods used in attacks on other companies. [Full Review]

Matthew Bouwer

Defender for Identity gives us visibility, but we often get false positives from Azure that take us down the garden path. We go through 30 incidents each day and most of those are false positives or benign positive alerts. Occasionally, we get true positive alerts. Also, while the threat protection from Microsoft is very comprehensive for certain threat alerts, for new things we sometimes have to create new alerts to try to get them into the pipeline and we've had mixed results with that. There is also room for improvement in how the threat intellig... [Full Review]

Emeka Ndulu

An area for improvement is the administrative interface. It's basic compared to other administrative centers. They could make it more user-friendly and easier to navigate. [Full Review]

Iñaki Martinez Urricelqui

The logs are not too clear when you search in Azure Identity. And when you are working in a priority IP address, Identity is not able to know that those IPs are from the company. It sees that the IPs are from Taiwan or Hong Kong or India, even though they are internal IPs, resulting in a lot of false positives. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Bala Krishna

The product is costly, and we had multiple discussions with accounting to receive a discounted rate. However, on the open market, the tool is expensive. You can purchase Defender for Identity as an add-on to an E3 license, and it comes included with an E5 license. I think those with the E3 and add-on aren't benefitting, and it's a better deal for those with E5 licenses; however, the price difference between E3 and E5 is significant. If we can get E5 at a discounted price, that's likely the most cost-effective way of accessing the product. We use a m... [Full Review]

Microsoft Defender for Office 365

Overview

Microsoft Defender for Office 365 is a comprehensive security solution designed to protect organizations against advanced threats in their email, collaboration, and productivity environments. It combines the power of Microsoft's threat intelligence, machine learning, and behavioral analytics to provide real-time protection against phishing, malware, ransomware, and other malicious attacks.

With Microsoft Defender for Office 365, organizations can safeguard their email communication by detecting and blocking malicious links, attachments, and unsafe email content. It employs advanced anti-phishing capabilities to identify and prevent sophisticated phishing attacks that attempt to steal sensitive information or compromise user credentials.

T... [Read More]

SAMPLE CUSTOMERS

Microsoft Defender for Office 365 is trusted by companies such as Ithaca College.

TOP COMPARISONS

Proofpoint Email Protection vs. Microsoft Defender for Office 365 ... Compared 19% of the time [See comparison]
Mimecast Advanced Email Security vs. Microsoft Defender for Office 365 ... Compared 16% of the time [See comparison]
Microsoft Exchange Online Protection (EOP) vs. Microsoft Defender for Office 365 ... Compared 7% of the time [See comparison]

REVIEWERS *

VISITORS READING REVIEWS *

TOP INDUSTRIES

Computer Software Company ... 17%
Financial Services Firm ... 8%
Government ... 7%
Manufacturing Company ... 7%

TOP INDUSTRIES

Manufacturing Company ... 17%
Computer Software Company ... 17%
Comms Service Provider ... 10%
Energy/Utilities Company ... 7%

COMPANY SIZE

1-200 Employees ... 29%
201-1000 Employees ... 19%
1001+ Employees ... 52%

COMPANY SIZE

1-200 Employees ... 42%
201-1000 Employees ... 16%
1001+ Employees ... 42%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Defender for Office 365

Top Reviews by Topic

VALUABLE FEATURES

Nagendra Nekkala.

Defender is a SaaS platform, so it offers more flexibility. Managing the permissions is easier. The solution's automated detection and response features are scalable. It's a unified solution that doesn't just cover Microsoft products. We're a multi-cloud shop, and having that coverage is critical. It also includes the latest IAM features like two-factor and multifactor authentication, giving us the most robust solution. [Full Review]

Verified user

Threat Explorer is an invaluable tool for me, and it plays a crucial role in helping me discern the origins of various email campaigns, pinpointing where they emanate from, and identifying the individuals within our organization who are affected. The convenience of having a centralized location for extracting comprehensive data is particularly noteworthy. With Threat Explorer, I can efficiently manage and mitigate the impact of these campaigns by removing problematic emails from mailboxes, all in one centralized location, eliminating the need to nav... [Full Review]

Jamie LeClair

I work in my company's IT department, so I use all of the products under Office 365 daily, including Microsoft Word, Microsoft PowerPoint, Microsoft Teams, and all the other components in the product. My company can't make it through a day or go by without using the products offered under Office 365. Some of our manufacturing workers may use Office 365 a lot less, but it is still necessary for things like Microsoft Outlook and Exchange. I found Microsoft Teams to be the most valuable feature of the solution, along with all of the products and featur... [Full Review]

Verified user

Microsoft Defender for Office 365 helps people to work remotely. It is a secure solution. We don't need to use our company's computers or get VPN connections to the networks. I can control how they share screens and what they send to the devices. It keeps our organizations confidential and sensitive information safe. [Full Review]

Verified user

The solution does a thorough job of examining emails for malicious content and examines the URLs and potential malicious content in emails. It offers peace of mind with more real-time updates as far as what they're looking for as opposed to a signature-based solution. It's probably the most valuable feature in my mind. I've deployed it for a couple of clients in a 365 environment and it seems to be a pretty solid solution. [Full Review]

ROOM FOR IMPROVEMENT

Verified user

There's room for improvement regarding the time frame for retrieving emails. Currently, the limitation allows users to go back only thirty days when pulling emails or conducting related actions. Enhancing this capability to extend the timeframe, perhaps to sixty or ninety days, would be beneficial. [Full Review]

Kishan Kishto

Microsoft Defender for Office 365 should improve the troubleshooting tools. It's unclear whether the device is blocked at the firewall level or at the device itself. The granularity needed for troubleshooting is currently lacking. From my perspective, Microsoft should address this issue to benefit many users who likely share the same sentiment. [Full Review]

Microsoft Defender for Office 365

Jamie LeClair

It seems like Microsoft has begun to roll out products before they are fully baked. Microsoft wants its well-paying customers to finish testing some of its half-baked products, find bugs, and report bugs back to Microsoft's team, which is a little frustrating for those who have to manage it and roll it up to thousands of people across the organization. I would say that Microsoft should release or launch better or fully baked products before going ahead with the GA phase. [Full Review]

Gordon McGowan

Microsoft Defender for Office 365 must improve the overall management style, including the GUI. It also needs to change the filters so that it is easy to whitelist and blacklist data. [Full Review]

Verified user

This is not really a defined product. You have to go to a lot of different places to enable things so it would be nice if you could go to one tab that says 365 Defender for Office 365 or something similar. You would be able to make all the settings and changes there, rather than having to go to lots of different places in the admin center to get it configured. Configuring Defender for Office 365 is not as easy as I would like but with some research and patience, you can tweak the solution to meet your needs. There are some pretty good articles onlin... [Full Review]

Oksana Kosukhina.

They have moved features from one console to another. Things have been moved around in the interface and it takes me time to find where certain features are. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Jamie LeClair

I know that the product is incredibly expensive. I know that my company has high expectations from Microsoft because of the high cost. I also know that Microsoft delivers tremendous value for our company in terms of productivity and collaboration. With Copilot coming along, the value Microsoft provides to my company will be even higher than what it was previously, owing to the productivity gain and the reformulation of how we work because of AI. [Full Review]

Chris-Atkinson

The pricing is too much compared to other security products that do the same things. The product is very expensive. I have a hard time demonstrating more value out of it. [Full Review]

Tolu Omolaja

For small and medium organizations, the pricing might not be affordable. Although Microsoft Defender for Office 365 is a good product; something all organizations should have. However, the question is, can all organizations afford it? For large enterprise organizations, they can definitely afford it, but for small and medium organizations, they might struggle to cover the expenses. [Full Review]

Sandor Nilsson

The pricing has become expensive. Some customers want to use a monthly payment, but Microsoft recently changed its license policies. So we are encouraging most users to pay annually. [Full Review]

Microsoft Defender for Cloud Apps   See 17 reviews >>

Overview

Microsoft Defender for Cloud Apps is a comprehensive security solution that provides protection for cloud-based applications and services. It offers real-time threat detection and response, as well as advanced analytics and reporting capabilities. With Defender for Cloud Apps, organizations can ensure the security of their cloud environments and safeguard against cyber threats. Whether you're running SaaS applications, IaaS workloads, or PaaS services, Microsoft Defender for Cloud Apps can help you secure your cloud environment and protect your business from cyber threats.

Microsoft Defender for Cloud Apps Benefits:

Provides comprehensive security for cloud applications

Integrates with other Microsoft security tools

Easy to use and de... [Read More]

SAMPLE CUSTOMERS

Customers for Microsoft Defender for Cloud Apps include Accenture, St. Luke's University Health Network, Ansell, and Nakilat.

TOP COMPARISONS

Cisco Umbrella vs. Microsoft Defender for Cloud Apps ... Compared 22% of the time [See comparison]
Zscaler Internet Access vs. Microsoft Defender for Cloud Apps ... Compared 22% of the time [See comparison]
Netskope vs. Microsoft Defender for Cloud Apps ... Compared 12% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Computer Software Company ... 16%
Financial Services Firm ... 12%
Manufacturing Company ... 8%
Government ... 7%

COMPANY SIZE

1-200 Employees ... 21%
201-1000 Employees ... 14%
1001+ Employees ... 65%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Educational Organization ... 27%
Financial Services Firm ... 18%
Construction Company ... 9%
Energy/Utilities Company ... 9%

COMPANY SIZE

1-200 Employees ... 28%
201-1000 Employees ... 28%
1001+ Employees ... 45%

* Data is based on the aggregate profiles of PeerSpot Users reviewing and researching this solution.

Microsoft Defender for Cloud Apps

Top Reviews by Topic

VALUABLE FEATURES

Verified user

The product's most valuable feature is SQL database. It notifies us even in case of false positives when people log in after a long time and when we're out of compliance with the security baseline. [Full Review]

Maymin Moe

Shadow IT discovery is the feature I like the most. Defender for Cloud Apps provides excellent threat visibility. The solution helps us prioritize threats across our enterprise. We use all Microsoft security products. I had no problems integrating or managing them. Microsoft's security solutions work together natively to deliver coordinated detection and response. We use Sentinel to ingest security data, which is essential. Sentinel allows us to investigate and respond to threats from one place. I like Sentinel because we can collect logs and data t... [Full Review]

Verified user

The most valuable feature is its policy implementation. Even public websites are directed to the Microsoft Net proxy, where we can establish policies to determine whether to block, authorize, or manage devices. [Full Review]

Jagadeesh Gunasekaran

The most valuable feature is the alerting system. Microsoft Defender for Cloud Apps covers all relevant cloud applications, such as OneDrive, shared drives, and specific directories. If we want to monitor a specific SharePoint directory, specific folder permissions, or specific VIP groups, all inherent features are available. [Full Review]

Edward-Walton

Defender integrates with MDE, and there's no agent, so everything happening on the endpoint is reported back to Defender. Defender for Cloud Apps is tightly integrated with Defender for Identity. The solution provides excellent visibility into threats. I rate Defender for Cloud Apps an eight and a half out of ten for visibility. I use all of Microsoft's security products, and they work together natively to deliver coordinated detection and response. Each solution is outstanding by itself, and I can coordinate between them by pumping the alerts and i... [Full Review]

ROOM FOR IMPROVEMENT

Verified user

I would like more customization of notifications. Currently, you either get everything or you get limited information. I would like to have something in between where we can customize the data that is included in notifications. That is one thing. The comment field also needs improvement. If you want to generate a workflow within the organization for a notification that occurs, the comment field is not visible to the next person who logs in. They should make that a little more visible. They should make the history more available to the next person I ... [Full Review]

Waseem Alchaar

There could be more granular roles that are out of the box included in the product. I guess it would help people who aren't as savvy. Right now, I have to create many custom models for different use cases. It would be great if roles were more geared towards specific use cases to cover multiple aspects. In a case where a role is for a security admin, it could grant roles that are needed and not too many unnecessary roles. For example, it gives the security admin some access to the compliance portal, but the executive may not need that access. So it c... [Full Review]

Microsoft Defender for Cloud Apps

Maymin Moe

Defender for Cloud Apps is primarily useful for Azure apps. It has limited capabilities for applications based on other cloud platforms. Microsoft security products are excellent in the detection phase, but they should have more features for the response component. I would like to see a mobile app for managing Defender for Cloud Apps. We currently use the cloud dashboard, but it would be nice if Microsoft offered more solutions for managing the product. [Full Review]

Verified user

Currently, we are only able to utilize the policies for blocking threats. I would prefer to have filtering options incorporated within the policies, enabling the solution to perform tasks beyond mere blocking or allowing. [Full Review]

Edward-Walton

Defender for Cloud Apps could come with more configured policies out of the box. Also, integration could be easier. Integration is moderately difficult because Microsoft hasn't developed a solution that unifies device onboarding and management. You have to use Intune to manage devices and Defender for Endpoint to enforce policies. They need to fix their integration, but I believe they will straighten it out by the end of the year. [Full Review]

Sunil V Jainapur

Defender could integrate better with multi-cloud and hybrid environments. It requires some additional configuration to ingest data from non-Azure environments and integrate it with Sentinel. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Verified user

Where we are right now, this is an acceptable pricing. I would like to see more transparency given to the end user. The end user given to us is via the cloud service provider. There are different programs and license models. Some include this, and some include that. It is all over the place. There can be a little more consistency or simplification in the pricing so that your parts list is not ten pages long, and you are not trying to determine, "If I have an E3, does this cover that?", or "Do I need to pay separately for the license?" Simplification... [Full Review]

Verified user

We utilize the Microsoft E5 licensing, which encompasses the entire Microsoft suite; however, it is costly. Furthermore, there are supplementary expenses associated with add-on modules. [Full Review]

Jagadeesh Gunasekaran

Microsoft offers bundle discounts and a pay-as-you-go option. We can also get an additional discount of 30 to 40 percent if we commit to a certain number of GB per day. [Full Review]

Sachin Vinay

The pricing is in the middle. It isn't too cheap or expensive compared to other antivirus or security products. It is priced according to industry standards. [Full Review]

About this report

This report is comprised of a list of enterprise level Microsoft Security Suite vendors. We have also included several real user reviews posted on peerspot.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About PeerSpot

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created PeerSpot to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

PeerSpot helps tech professionals by providing:

- A list of enterprise level Microsoft Security Suite vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

PeerSpot
244 5th Avenue, Suite R-230 • New York, NY 10001
www.peerspot.com
reports@peerspot.com
+1 646.328.1944