ES

Endpoint Protection for Business

Buyer's Guide and Reviews

July 2019

IT Central Station
Unbiased reviews from the tech community

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

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station 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

AhnLab	AhnLab EPP
Avast Software	Avast Business Endpoint Protection
Barkly	Barkly
Bitdefender	Bitdefender GravityZone
Bitdefender	Bitdefender Hypervisor Introspection
Bromium	Bromium
Carbon Black	Carbon Black CB Defense
Carbonite	Carbonite Endpoint
Check Point	Check Point Endpoint Security
Cisco	Cisco AMP for Endpoints
Comodo	Comodo Advanced Endpoint Protection
CounterTack	CounterTack Predictive Endpoint Protection Platform
CrowdStrike	CrowdStrike
CyberArk	CyberArk Endpoint Privilege Manager
Cybereason	RansomFree
Cybereason	Cybereason Deep Detect & Respond
Cylance	Cylance
Cynet	Cynet
Deep Instinct	Deep Instinct
Dell EMC	Dell Data Protection - Endpoint Security Suite
Endgame	Endgame
enSilo	enSilo
ESET	ESET Endpoint Security
Faronics	Faronics Anti-Executable
Fortinet	FortiClient
HCL	BigFix
Ivanti	Ivanti Endpoint Security for Endpoint Manager
Ivanti	Lumension Endpoint Management and Security
J2 Global	VIPRE Endpoint Security
Kaspersky Lab	Kaspersky Endpoint Security
Malwarebytes	Malwarebytes
McAfee	McAfee Complete Endpoint Protection
Microsoft	Microsoft Windows Defender
Morphisec	Morphisec Moving Target Defense
Nehemiah Security	AtomicEye ASM
Nyotron	Nyotron PARANOID
OpenText	Guidance Software EnCase
Palo Alto Networks	Palo Alto Networks Traps
Panda Security	Panda Security Adaptive Defense
RSA	RSA NetWitness Endpoint
SentinelOne	SentinelOne
Sophos	Sophos EPP Suite
Sophos	Sophos Intercept X
SparkCognition	DeepArmor
Stormshield	Stormshield Endpoint Security
Symantec	Symantec Endpoint Protection (SEP)
Tanium	Tanium
Trend Micro	Trend Micro OfficeScan
Trend Micro	Trend Micro Smart Protection Complete
Trend Micro	Trend Micro ServerProtect
Webroot	Webroot SecureAnywhere Business Endpoint Protection

Top Endpoint Protection for Business Solutions

Over 352,246 professionals have used IT Central Station research. Here are the top Endpoint Protection for Business 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	Comparisons	Reviews	Words/Review	Average Rating
Number of views	Number of times compared to another product	Total number of reviews on IT Central Station	Average words per review on IT Central Station	Average rating based on reviews

Bar length

The total ranking of a product, represented by the bar length, is based on a weighted aggregate score. The score is calculated as follows: The product with the highest count in each area gets the highest available score. (18 points for **Reviews**, **Words/Review**, **Views** and **Comparisons**.) Every other product gets assigned points based on its total in proportion to the #1 product in that area.
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 18 (weighting factor) * 80% = 14.4. For **Average Rating**, the maximum score is 28 points awarded linearly between 6-10 (e.g. 6 or below=0 points; 7.5=10.5 points; 9.0=21 points; 10=28 points).
If a product has fewer than ten reviews, the point contribution for Average 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.
Reviews that are more than 24 months old, as well as those written by resellers, are completely excluded from the ranking algorithm.

1 Symantec Endpoint Protection (SEP)

67,329 views **36,772** comparisons **33** reviews **384** Words/Review **8.2** average rating

2 BigFix

29,476 views **14,059** comparisons **37** reviews **547** Words/Review **8.4** average rating

3 CrowdStrike

30,111 views **17,186** comparisons **10** reviews **395** Words/Review **8.6** average rating

4 Carbon Black CB Defense

36,959 views **19,143** comparisons **7** reviews **871** Words/Review **9.1** average rating

5 Microsoft Windows Defender

53,975 views **39,248** comparisons **1** reviews **515** Words/Review **8.0** average rating

6 ESET Endpoint Security

19,944 views **12,836** comparisons **10** reviews **282** Words/Review **8.3** average rating

7 Kaspersky Endpoint Security

16,609 views **11,023** comparisons **18** reviews **299** Words/Review **7.9** average rating

8 Palo Alto Networks Traps

20,696 views **13,325** comparisons **8** reviews **929** Words/Review **8.5** average rating

9 Cylance

44,562 views **23,280** comparisons **3** reviews **542** Words/Review **9.0** average rating

10 McAfee Complete Endpoint Protection

26,404 views **13,389** comparisons **10** reviews **236** Words/Review **7.4** average rating

Top Solutions by Ranking Factor

Views

SOLUTION		VIEWS
1	**Symantec Endpoint Protection (SEP)**	67,329
2	**Microsoft Windows Defender**	53,975
3	**Cylance**	44,562
4	**Carbon Black CB Defense**	36,959
5	**CrowdStrike**	30,111

Reviews

SOLUTION		REVIEWS
1	**BigFix**	37
2	**Symantec Endpoint Protection (SEP)**	33
3	**Kaspersky Endpoint Security**	18
4	**ESET Endpoint Security**	10
5	**McAfee Complete Endpoint Protection**	10

Words / Review

SOLUTION		WORDS / REVIEW
1	**Deep Instinct**	1,613
2	**Bromium**	1,282
3	**Palo Alto Networks Traps**	929
4	**Carbon Black CB Defense**	871
5	**Nyotron PARANOID**	839

Symantec Endpoint Protection (SEP)

See 40 reviews >>

Overview

Symantec Endpoint Protection is a powerful endpoint antivirus software solution, which provides multiple layers of protection against all types of known and unknown threats. Powered by SONAR and Symantec Insight, Symantec Endpoint Protection combines all the security tools that you could require into one proactive solution. It integrates antivirus, firewall, antispyware, intrusion prevention, application control and device control, and allows you to manage all of these tools centrally from one agent. Upgrades happen automatically, and the software offers seamless migration from previous versions.This solution maximizes the security and performance of physical and virtual systems, and is compatible with multiple operating systems, such as Wi... [Read More]

SAMPLE CUSTOMERS

Audio Visual Dynamics, Red Deer Advocate, Asia Pacific Telecom Co. Ltd., Kibbutz Ein Gedi, and AMETEK, Inc.

TOP COMPARISONS

Microsoft Windows Defender vs. Symantec Endpoint Protection (SEP) ... Compared 25% of the time [See comparison]
McAfee Complete Endpoint Protection vs. Symantec Endpoint Protection (SEP) ... Compared 11% of the time [See comparison]
ESET Endpoint Security vs. Symantec Endpoint Protection (SEP) ... Compared 7% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 31%
Comms Service Provider ... 10%
Insurance Company ... 9%
Non Profit ... 9%

COMPANY SIZE

1-200 Employees ... 39%
201-1000 Employees ... 23%
1001+ Employees ... 38%

VISITORS READING REVIEWS *

TOP INDUSTRIES

University ... 14%
Local Government ... 10%
Integrator ... 10%
Retailer ... 10%

COMPANY SIZE

1-200 Employees ... 46%
201-1000 Employees ... 20%
1001+ Employees ... 34%

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

Symantec Endpoint Protection (SEP)

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Cameron Mottus

There are a number of features that all work synergistically to be able to provide the protection. Originally, anti-virus was based on definition. About 10 years ago, the bad guys figured out how to get past that. So what they've been doing for the past 10 years is adding in additional features to help mitigate any of these other attack vectors that the hackers or malicious people have. So it's just a working together of all these components that makes it special. And then SEP itself fits into the Symantec ecosystem, and inter-operates with a number... [Full Review]

Leopold Dapa

We had to position Symantec in big companies like Telco and several banks. With this solution, you also get the Protection Suite, endpoint protection, SEP, and you also have the Mail Security and Messaging Gateway. It's really integrative and our customers find it very valuable. It addresses almost all of the challenges on security for endpoint messaging. Symantec is going to be used much more because of its features. [Full Review]

Imtiaz Hussain

In Symantec Endpoint Protection, the most valuable feature I like is the good performance. With Symantec, I always know this tool will be reliable and with the latest protection. [Full Review]

Subodh Sing

The fact that it has centralized management is the most valuable feature. In addition, the support from Symantec is very important. It is a global company and they give very good support. That is an important factor here because we are sitting in Africa and getting support on time can be a bit tougher. In this way, Symantec is a good fit for us. Also, the console is very user-friendly. It is easy to understand, easy to play with it, easy to make up policies. And you can customize your policies. It's not like there's a set of policies that has been s... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Leopold Dapa

We had a bank that we were working with and they had a challenge in which they needed to protect against vulnerability. They had previously used Kaspersky, we discussed and told them that Symantec is capable and is able to address their specific challenges. We gave them a trial version. When they started they found it very easy; not easy to implement but easy to use. We started with the headquarters here and later we also implemented it for all the subsidiaries in the region, in other countries. They have a centralized solution, so they can help oth... [Full Review]

Imtiaz Hussain

Symantec is top of all of the antivirus tools. I couldn't find any single incident that happened. Symantec was not the leader previously, McAfee and Kaspersky were. This is a new game. [Full Review]

Subodh Sing

Symantec, as an antivirus solution, makes things far better on the management and the vulnerability scanning sides. From a management point of view, it is good. [Full Review]

Symantec Endpoint Protection (SEP)

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Cameron Mottus

They're just starting to get into this now, but I think they can do better - they're just starting out with I think is called the SEP Cloud Console. It has more limited functionality. It will be good once we can run SEP from the cloud. That would be good. [Full Review]

Leopold Dapa

The mobility solution should be improved. You need to separately purchase mobile, like a smartphone with Android and so on, you need to buy it separately with SAP, for example. It would be better for the user to use the same solution with all devices, even laptops, desktops, server and so on. They should also use the same endpoints for mobile devices. There are a few negative points. They should separate the feature for each separate solution for mobile devices. The second one is about the price, it's expensive. Finally, the third would be the compl... [Full Review]

Imtiaz Hussain

The device control level and application control level should improve. I am finding a lot of issues when I block the devices, like a printer or scanner. In the classes of the devices for the application control, the most important issue is the hashing. Nowadays all the vendors, like Cisco firewalls, are detecting threats with the hashes. Symantec has this option that we can block them always by the hashes but the problem is that sometimes Symantec detects these hashes and is not consistent. These two parts should improve. The rest is always awesome.... [Full Review]

Subodh Sing

We have talked to Symantec about a feature that is lacking. Any external device which is inserted into a computer should be subject to an auto-scan policy, to automatically scan it before accepting the device. Let's say I have a pen drive and there is a Trojan virus for which the signature is not updated. If the signature is not updated, then the system should automatically scan and understand that there is a foreign file and it should be blocked immediately. That is the one feature that I feel is missing. They need to make it more user-friendly, so... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Cameron Mottus

From a simplicity perspective, it's per user. Therefore, it makes it easy to do licensing. I'll be honest, I haven't really done licensing with Symantec for seven years. I just do professional services and we let our partners handle the licensing. [Full Review]

Mamonoor Rashid

Pricing and licensing for our country is very good. It's not that expensive and the endpoint security is very good. It's not as cheap as some others, but they are not as good. [Full Review]

SystemAdmin677

We receive a discounted price for this solution because we are a non-profit organization. There are no costs in addition to the standard licensing fees. [Full Review]

HCL BigFix [See 39 reviews >>]

Overview

IBM BigFix provides complete visibility and control into all endpoints through a single, unified platform. Enterprises can now bridge the bridge the gap between threat detection and response, drastically reducing remediation times and costs by consolidating best-in-class EDR, enterprise asset discovery, endpoint interrogation, rich threat intelligence, multi-platform patch management (90+ OS) and software distribution.

Security and operations teams can see, understand and act on all endpoint threats while proactively reducing the attack surface. ... [Read More]

SAMPLE CUSTOMERS

US Foods, Penn State, St Vincent's Health US Foods, Sabadell Bank, SunTrust, Australia Sydney, Stemac, Capgemini, WNS Global Services, Jebsen & Jessen, CenterBeam, Strauss, Christian Hospital Centre, Brit Insurance, Career Education Corporation

TOP COMPARISONS

SCCM vs. BigFix ... Compared 52% of the time [See comparison]
Symantec Endpoint Protection (SEP) vs. BigFix ... Compared 6% of the time [See comparison]
Tanium vs. BigFix ... Compared 5% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 21%
University ... 15%
Retailer ... 10%
Manufacturing Company ... 10%

COMPANY SIZE

1-200 Employees ... 5%
201-1000 Employees ... 16%
1001+ Employees ... 80%

VISITORS READING REVIEWS *

TOP INDUSTRIES

University ... 20%
Retailer ... 17%
Healthcare Company ... 17%
Wireless Company ... 7%

COMPANY SIZE

1-200 Employees ... 15%
201-1000 Employees ... 12%
1001+ Employees ... 73%

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

BigFix

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

MartinCarnegie

* Patching support: IBM BigFix supports most of the major OSs with natively packages patches. This includes Windows, MacOSX, Oracle Linux, Solaris, AIX, RedHat, Ubuntu and others. * Pre-packaged support for many third-party applications such as Adobe, Google, Mozilla, Sun (Java), WinZip, and others. * Near real-time view of the environment. Most systems will report their current patch state within 15 minutes. * The IBM BigFix console provides a single pane view into the entire environment. This also provides a common interface for taking actions, su... [Full Review]

Michelle McGough

The subscription patch content was the most useful because it made patching a lot easier, faster, and more successful than alternative options requiring prescans and custom code development. [Full Review]

Informat76c6

The custom content flexibility is the most important feature. Its ubiquity is also valuable. We've got very good adoption and it helps that it's one of the few tools that we have everywhere. [Full Review]

BigFixAddb6e

Some of the most valuable features are its: * Ease of use * The fact that it's a single port access across the board. There's only one firewall to be required. * The user community is great, very helpful. * There's not a lot of overhead to the client. There's a bit of set up to do but it's pretty simple once it gets running to maintain it. It basically maintains itself. As such for as big of a system, it only requires a little manpower. There's only a couple of people that have to manage it. My impressions of peer to peer file transfer in relation t... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

MartinCarnegie

Our primary use for IBM BigFix is around patching and reporting on Microsoft Windows servers. We are also using the reporting capabilities for patching state on AIX, Solaris, and Red Hat Linux. These reports are being presented to the Safeguards groups and are being used to report MSA compliance for our server environment. IBM BigFix has provided our Windows server team more flexibility for scheduling the deployment of patches in their environment which has caused them a lot of issues in the past. Also with the near realtime reporting, the server te... [Full Review]

Michelle McGough

I used this product at several organizations during my career as an Endpoint Management SME from a small Windows-only fleet to extreme sized heterogeneous empires containing various Nix distros, Windows, and macOS. The more varied and complex the requirements, the better BigFix fit the bill while other solutions faded in the background. When the customer needed the capability to have high visibility over their fleet followed by fulfilling the need to address all issues found in that fleet: BigFix was able to perform. Having built-in continuous deliv... [Full Review]

Informat76c6

BigFix has enabled us to have a highly successful endpoint patching program for the past decade. It's been enormously successful there. It's also become a core part of many of our business processes, from compliance monitoring of endpoints, encryption management, key escrow, and local administrator password escrow. It's built into our inventory. It's very much everywhere. We do use BigFix as a system of investigation in the instance of lost and stolen devices to get an idea of what sort of data was possibly on it. It is an integral part of our compl... [Full Review]

BigFix

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

MartinCarnegie

IBM has been heavily focused on adding and improving features to the tool, especially with new components like IBM BigFix Detect. While all these new features are great and provide useful information, IBM has not focused on the Web Reports capabilities. This is not to say that the Web Reports is bad, but at this time, it is currently the weakest part to me. IBM has also introduced the BigFix Web UI, which is a start to addressing the web based reporting. I believe that this is going to be the direction to modernize the web reporting capabilities alo... [Full Review]

Michelle McGough

With great power and flexibility comes a somewhat overwhelming thick console. In environments without well-designed workflows, it was sometimes difficult to bring up junior staff to high proficiency. This is being addressed in WebUI but for customers that don't invest in workflow development or staff education the ramp-up time can take longer than necessary. [Full Review]

Informat76c6

Network traffic is one of our current pain points. BigFix's high performance and high availability in our environment easily overwhelms our high-performance firewalls. Every time we push out patches to our entire population, it makes the firewalls very unhappy for about an hour and slows down some of our core enterprise apps. We're working to identify ways to fix that. We think that BigFix provides mechanisms for spreading out that load over time. We're going to be deploying that soon which will hopefully take care of the problem. Bandwidth is never... [Full Review]

BigFixAddb6e

I'd like to see: * More visibility * Better reporting * I'd like for it to be more futuristic, for it to be less plain Windows looking with a little more pizazz. * Better integration, with the different applications within BigFix. Instead of sometimes feeling like four or five different applications, they need to be integrated a little better within themselves. * Better folder structure internally. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

MartinCarnegie

IBM BigFix comes with many different packages depending on the functions that are required. IBM BigFix Patch is the most basic package which provides the ability to patch almost any operating system with many third-party applications. It also provides the capability to create custom content such as software packages (called Fixlets), inventory scans (called Analysis) and create custom reports. All of the other IBM BigFix packages also provide patches. When purchasing, buying with other IBM tools provided us with a very good discount in pricing. Also... [Full Review]

Michelle McGough

I would advise someone considering this solution to take advantage of everything offered by the seller and sales engineer - they always seemed eager to help me be successful to reach my goals and were very generous with their time and advice. The BigFix community is also very rich and generous. It was a rare occasion when I had to "invent a wheel." Most custom solutions that I needed were already developed by IBM or available from the community - in some cases, I needed to tailor what was offered but this was not difficult. [Full Review]

Endpoint84a2

License management isn't quite as easy as it should be to deal with the licensing. You need to take the server down to import the new licenses which I find to be annoying. [Full Review]

CrowdStrike [See 11 reviews >>]

Overview

Falcon sensor (small and light) and cloud (big and powerful) work seamlessly to deliver real-time protection and visibility -- yes, even when the sensor is not connected to the internet. The simplicity of CrowdStrike's architecture finally gives you the freedom to replace and retire the complicated, performance-robbing security layers that clutter your environment.

This architecture lies at the heart of Falcon, CrowdStrike's pioneering cloud-delivered endpoint protection platform. It both delivers and unifies next-generation antivirus, endpoint detection and response (EDR), managed threat hunting, security hygiene and threat intelligence. Using its purpose-built cloud native architecture, the Falcon Platform collects and analyzes more than... [Read More]

SAMPLE CUSTOMERS

Rackspace Inc.

TOP COMPARISONS

Cylance vs. CrowdStrike ... Compared 25% of the time [See comparison]
Carbon Black CB Defense vs. CrowdStrike ... Compared 13% of the time [See comparison]
Microsoft Windows Defender vs. CrowdStrike ... Compared 7% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 39%
Government ... 13%
Retailer ... 9%
Energy/Utilities Company ... 7%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Energy/Utilities Company ... 43%
Comms Service Provider ... 14%
Insurance Company ... 14%
Hospitality Company ... 14%

COMPANY SIZE

1-200 Employees ... 27%
201-1000 Employees ... 9%
1001+ Employees ... 64%

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

CrowdStrike

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Nachiket Sathaye

The EDR feature of CrowdStrike is fantastic. Also, in comparison to other solutions, it can connect remotely, so our security analysts can get into the system directly and do manual analysis as well. I also like the overall reports. They are crisp and to the point. [Full Review]

Kunal Gupta

* It can connect to host and isolate it from the network if needed; this feature helps us to investigate the endpoint without visiting the endpoint and then testing. * It saves time and helps to contain the threat in less time. * complete visibility into the endpoint [Full Review]

Secu8765

When something is detected you can log into the GUI and you can get very specific details about what happened. It's very helpful for investigating incidents and this sort of thing. [Full Review]

Ahmad Hasan

The features that we have found most valuable are the detection functions. You cannot rely on the signature based detections anymore. You need something to look after signature-less attacks. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Nachiket Sathaye

First, it is a production from known and unknown interests. Second, it has an extremely low footprint, so it has minimal impact on the user endpoints in terms of CPU and memory usage. The tamper protection of the CrowdStrike agent is extremely good even if the user is having admin rights and he tries to disable these CrowdStrike services. The CrowdStrike service will respawn itself. It is practically impossible to tamper with these services. If I managed to craft some malware that would shut down the services, CrowdStrike will respond itself, and it... [Full Review]

Kunal Gupta

* CrowdStrike is a SaaS-based solution which means it can be operated from anywhere, which gives the admins access to control the endpoints from multiple endpoints. * It has a very low footprint, using 1-2 % CPU and around 40 Mb of RAM, and the agent size is small and easy to deploy as well. * It has segregation of roles at various levels for the analysts, admins, SMEs, etc. [Full Review]

SeniorAsd84b

This solution has made the lives of the IT staff much easier, compared to the previous one. This is the lightest client available that is compatible with different versions of the OS. [Full Review]

CrowdStrike

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Nachiket Sathaye

There are a couple of issues with the compatibility to some of the operating systems. But, I see that there are a lot of things in the pipeline. They have a roadmap, and continuously are improving. Within the last three months I have seen lot of new features in the overall CrowdStrike suite. A couple of things were on the cosmetic part. CrowdStrike needed some improvements on the report functionalities, specifically the dashboard functionalities. Technically there a lot of things also coming from a visual perspective. There are a couple of things th... [Full Review]

Kunal Gupta

The current version of Falcon does not support DLP which is a may be a good to have in a EDR Solution. It must be included in the future version if possible. There must be a on-premise versions. MDM is also coming soon must also have ability to be controled from same dashboard. [Full Review]

Erik Sobel

It probably needs more integration with firewall vendors. It needs integration with other technologies. It doesn't play well with anything else. It is more of a standalone solution. Therefore, integration with other technologies would be great. [Full Review]

Secu8765

The GUI can use improvement, it's cloud-based so sometimes the interface can be a bit slow. The interface could use a little bit more speed. When I change the policies for some users, I would like to have an option to apply that policy immediately. Right now, I have to wait for the users to connect to the cloud to take the new policy. I would like for them to develop the ability to have an option to apply the post the policy immediately. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Kunal Gupta

The setup of CrowdStrike is very simple. It supports all three platforms (Windows, MacOS, Linux), and it has support for the specific version of the above OS. Which means sometimes, a particular OS won't be compatible with the CrowdStrike version. [Full Review]

Fadhullah Iskandar Roy

Purchasing the product through the AWS Marketplace is just a click away. Since we were using the on-premise version of the product, we continued on the cloud by purchasing it through the AWS Marketplace. I would like them to further reduce the price, because it is quite pricey at the moment. [Full Review]

Carbon Black CB Defense

See 7 reviews >>

Overview

CB Defense is an industry-leading next-generation antivirus (NGAV) and endpoint detection and response (EDR) solution. CB Defense is delivered through the CB Predictive Security Cloud, an endpoint protection platform that consolidates security in the cloud using a single agent, console and data set. CB Defense is certified to replace AV and designed to deliver the best endpoint security with the least amount of administrative effort. It protects against the full spectrum of modern cyber attacks, including the ability to detect and prevent both known and unknown attacks. CB Defense leverages the powerful capabilities of the CB Predictive Security Cloud, applying our unique streaming analytics to unfiltered endpoint data in order to predict, ... [Read More]

SAMPLE CUSTOMERS

Netflix, Progress Residential, Indeed, Hologic, Gentle Giant, Samsung Research America

TOP COMPARISONS

Cylance vs. Carbon Black CB Defense ... Compared 17% of the time [See comparison]
CrowdStrike vs. Carbon Black CB Defense ... Compared 11% of the time [See comparison]
SentinelOne vs. Carbon Black CB Defense ... Compared 7% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 19%
Manufacturing Company ... 14%
Venture Capital & Private Equity Firm ... 9%
Writing And Editing Position ... 8%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 50%
1001+ Employees ... 50%

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

Carbon Black CB Defense

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Karthik Balakrishnan

Carbon Black Defense has a higher detection ratio because it's cloud-based and it also does a lookup to virus total, so it is out of like 65 vendors that are normally listed in virus total, if there are any kind of hits out of those, in that case, it is getting recognized as a known Malware or a suspected Malware. Under these categorizations, we are able to see a spike in the detection ratio. It is enlightening us with respect to what are the programs that are generally used in our environment and how they are compliant with our environment. [Full Review]

Darrick Kristich

The biggest feature out of Carbon Black is its ability to dive in with more depth. You can look at the entire kill chain and understand, not only if an alarm or identified incident is truly a true security issue versus a false positive, and it allows us to backtrack and figure out why it actually happened and how it got into the environment. It also helps us determine what other things may have been impacted along with it, from an asset standpoint. It allows us to go into more depth than a more traditional antivirus, like Symantec. Symantec is more ... [Full Review]

Andre B.

I think something that is the most valuable is the time-lining capability for any breach activity. It gives us the ability for us to actively threat hunt. This is not something where it's a passive response tool where we watch things happen. In contrast, it actually does some heuristics, and some behavioral analysis, and we're able to do some prevention with it as well. I think that's really the strongest attribute, and it makes this a more aggressive tool than others. [Full Review]

Brody Wright

* The software uses very few resources; it is almost invisible to the end user. * Behavioral Monitoring stops known malicious events before they even begin. * The whitelist: Being a Casino, we have some odd software packages. Being able to whitelist them is a must. * The option to quarantine a device and use the cloud-based portal to gain a “shell” on the infected machine. With this, we can dump the entire system memory to a machine in our lab, then run analysis. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Karthik Balakrishnan

It has improved the number of alerts or the number of threat events that we are able to recognize in our environment. And it also highlights the usage of potentially unwanted programs. So these are the ways in which that highlighted the possible vectors through which we can have an incident happening in our environment. That is one thing that we have seen. In addition, the detection ratio compared to that of a typical anti-virus and the EDR solution or the next gen AV as they call it, is on the ratio of one to ten when you compare it with a Symantec... [Full Review]

Andre B.

We've integrated it with Splunk, with ThreatConnect, and a couple of others. It has a lot of modules for integration that has streamlined our ability to respond and decrease the amount of time for response, but also allowing us not to have to pivot to so many tools where we can actually work from more of a single pane of glass perspective. [Full Review]

Brody Wright

During the company’s transition, we had a memory scraper infiltrate our network, and with the help of Carbon Black, we isolated the outbreak to a few point of sale machines.. We saw a step-by-step account of how the software was introduced into the environment, the host it originated from, and the destination address it was connecting too. Carbon Black stopped the spread in its tracks. [Full Review]

Carbon Black CB Defense

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Karthik Balakrishnan

It is still evolving, as we see. We started using the version 3.0. We've been migrating and upgrading as well, laterally, until version 3.2. So, we have been seeing a lot of improvements in general in terms of bug fixes and in terms of what are the things that we had encountered. I think they can probably bring in because there is a little bit of a gap between the native Antivirus solutions like Symantec or McAfee. So, you really can't say whether an end user will not be able to judge whether it's a Malware-free software that they are downloading or... [Full Review]

Darrick Kristich

Symantec needs more investigative features out-of-the-box. Though, they are using the Advanced Threat Protection add-on to correct some of this. It is also not quite as feature-rich as some of the more advanced MDR platforms out there. Carbon Black needs to do a better job of proving their platform in the industry, and providing a bit more access to do industry testing with real world examples to help prove their platform. In additional, they have been actively porting over a lot of features from some of their other products, and they should continu... [Full Review]

Andre B.

In some areas one of the big issues for me is responsiveness to issues that arise with the solution. There are some components that leave a bit to be desired and/or that are bugs, or that even if it's a feature update request. These kinds of things are not the fastest company to respond to those. We did have a bug that was persistent for it's now going on two months and it hasn't been fixed. That is one of the drawbacks. This is really impacting what we need to do with it. But, the bigger issue is the organizational responsiveness to clients. In add... [Full Review]

Brody Wright

It works the way we want and how we want. For one improvement, an easier integration with an AlienVault USM appliance would be good. The directions for Splunk are spot on, but it is difficult to find anything on integration with AlienVault, [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Karthik Balakrishnan

I just told you the price point that's one of the factors, basically because that is what the higher management gave us as an input. But, we didn't play a major role in terms of deciding. That was done by another person from the organization. So, that was just a communication that we received. So, that's how much I know about it. [Full Review]

Darrick Kristich

The licensing costs are comparable between the two products. If you're purchasing the product, they're both typically a traditional license model with an annual type fee or multiyear. The fees are the cost of the professional services to get the system up and running. It depends on the size of the environment. The size and complexity are what it really comes down to. It will be relatively consistent with whether it was MSSP versus a direct purchase. Carbon Black might be a touch more expensive. They tend to get a premium for their capabilities. They... [Full Review]

Jayandra Wickramasinghe

The cost is a considerable factor, but the benefit factor is the most important. When you compare it with other products, the price is high. Carbon Black will negotiate the price. [Full Review]

Microsoft Windows Defender

See 3 reviews >>

Overview

Windows Defender Pro is your first line of defense against spyware and other unwanted software. And in Windows 7, it's easier to use, with simpler notifications, more scanning options, and less impact on your computer's performance.

SAMPLE CUSTOMERS

Al-Imam Mohammad Ibn Saud Islamic University, Auckland Transport, Erste Bank Group, Urban Software Institute, NJVC, Sheraton Hotels and Resorts

TOP COMPARISONS

Symantec Endpoint Protection (SEP) vs. Microsoft Windows Defender ... Compared 30% of the time [See comparison]
Sophos EPP Suite vs. Microsoft Windows Defender ... Compared 8% of the time [See comparison]
ESET Endpoint Security vs. Microsoft Windows Defender ... Compared 7% of the time [See comparison]

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 43%
201-1000 Employees ... 14%
1001+ Employees ... 43%

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

Microsoft Windows Defender

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Ibikunle Imam

The malware features are most valuable for us because if you have an application that attacks, it is defended. It gives you a prompt and doesn't allow you to launch that app. If there's an application that has suspicious malware you downloaded from the internet, it gives you a prompt to prevent the application from launching. Microsoft Windows Defender moves it to the recycle bin automatically. [Full Review]

ITsece56457

One of the most valuable features of this product is the ability to "set it and forget it." I don't go in and make any changes to the settings. Another value add is the size of the user base, which is fairly large because it's a free MS product. I would imagine that it would be quite competitive since a blacklisting solution such as this is only as good as the threat intelligence it receives. I'm pretty sure that if the tool discovers something foreign and malicious it will upload that information back to Microsoft. The value of the tool is inherent... [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Ibikunle Imam

We are no longer buying a separate antivirus with Windows 10 Server Enterprise. We are no longer buying antivirus solutions where there is no compatibility with Windows 10. [Full Review]

ITsece56457

I'm working as a private contractor. In this regard, you can say this tool ensures I'm working with a product that gets updated regularly without me having to remember to do it. Since it's a Microsoft product, I'm confident that it requires a low use of system resources. The benefit of that being that my computer isn't constantly being drained. [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Ibikunle Imam

Microsoft Windows Defender doesn't have a game mode. Other antivirus software (like BitDefender) have something known as a game mode. If you want to play a game, just enable the game mode to allow certain traffic without needing to configure it. Windows Defender doesn't have that. There's no Windows Server edition for Windows Defender as part of the distribution. [Full Review]

ITsece56457

I'm sure the premium product has extra features, like listing questionable websites. Defender is just an antivirus product. It would be nice to have a paid upgrade that would provide additional screening of the day-to-day activities. [Full Review]

Microsoft Windows Defender

Continued from previous page

Defendwind
677

There were a few detections that are not picked up, and then Microsoft picks up on that and they update it. That's just a normal thing you go through based on every antivirus solution. You're always going to have viruses and signatures that are coming out. So, I wouldn't say it's the perfect solution because if you're looking at next-generation behavioral based things, for example, if you're going to use ATP, that's when you can get more methods out of it. With Defender, if you pay more you can get the ATP component, which is sold separately by Micr... [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Ibikunle
Imam

It's free because it comes with Windows. It's a free solution. We're not paying any license. That's why it's better than Bitdefender, McAfee, or Norton. It's free. [Full Review]

ESET Endpoint Security

See 10 reviews >>

Overview

Comprehensive multilayered security, combining machine learning and human expertise. Enables organizations to:Protect against RansomwareBlock Targeted AttacksPrevent Data BreachesDetect Advanced Persistent ThreatsStop Fileless attacks

SAMPLE CUSTOMERS

ERSTE Group Bank, Miller Solutions, Wesleyan University, The Hospital Center of Luxembourg, Deer Valley USD, SPAR, Industrial Federal Credit Union, Honda, City Hall of Palmela, Hays CISD, Lester B Pearson School Board

TOP COMPARISONS

Symantec Endpoint Protection (SEP) vs. ESET Endpoint Security ... Compared 24% of the time [See comparison]
Microsoft Windows Defender vs. ESET Endpoint Security ... Compared 18% of the time [See comparison]
Bitdefender GravityZone vs. ESET Endpoint Security ... Compared 8% of the time [See comparison]

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 50%
201-1000 Employees ... 14%
1001+ Employees ... 36%

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

ESET Endpoint Security

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Jayandra Wickramasinghe

* ESET SysInspector: Provides full details of the process and modules loaded with path and risk levels. * Two-way firewall: Advanced level endpoint firewall, which helps to block unwanted and malicious traffic. * Trusted Network Detection: Provides strict protection when clients connect to an unauthorised network. * HIPS: Detects threats based on system behaviour and provides tampering protection for registry, processes, and files. * Centralised management: Visualised, central, advance management, server console. [Full Review]

Matija Dabic

What is great about ESET is the ERA Web Console through which we can pull various reports, and monitor and administer all clients and servers. In addition, the console is easy to use. The most valuable feature for us is the ability to create custom reports. Also, they are not exclusively related to antivirus and group synchronization from AD, so we can have the same group structure on AD and ESET. Another feature that we like is setting the GUI of ESET Endpoint Security/ESET File Security to silent mode because some servers and clients can have perf... [Full Review]

Edson Siqueira

The most valuables features are that it is a lightweight antivirus with a lightweight heuristic scan, web filter, bi-directional firewall, and device restriction that works well. [Full Review]

Michael Varga

The CLI Scanning is used for scanning our corporate storage (endpoint) for malware that our onboard scanner (MS Endpoint) misses. Personal experience with the real-time scanner was excellent and we wanted to create a second layer of detection on our systems, without going through the expense and trouble of running a second AV on our systems. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Jayandra Wickramasinghe

ESET Endpoint Security helps to improve our organisation's security. ESET Endpoint Security provides a smart level of security with a low system footprint, low bandwidth usage, and smooth performance while doing security operations. However, in some cases, ESET Endpoint Security was unable to provide 100% protection against zero day attacks. [Full Review]

Matija Dabic

ESET is recognized as one of the best in the security field. It provides a high level of security and the ERA Web Console increases productivity because we can do all we need to do with clients from one central place. And we have plenty of options for those clients. [Full Review]

Edson Siqueira

As ESET is a lightweight antivirus and gives us the most useful features that we need on an endpoint, we are comfortable after installing it. You don't need to worry about the machine becoming slow after installing it, and there are other features to protect the user machine as well. [Full Review]

ESET Endpoint Security

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Jayandra Wickramasinghe

ESET Endpoint Security does not have application control. ESET should consider giving it application control. Also, it needs to improve the temper protection and provide more detection capabilities (e.g., more behaviour base). [Full Review]

Matija Dabic

They need to improve licensing for VMs. When ESET is uninstalled from a VM, the seat stays on the license management server. We have to manually delete the seat from that server because it doesn't know how to handle it. I contacted exclusive ESET support here in Croatia and they told me there is no solution for this yet. [Full Review]

Edson Siqueira

The heuristic of ESET is not so effective in standard mode. We have to implement some policies on it to have good protection against malware like Zero-Day and ransomware. I think that such policies should be implemented by default on the product or by the automatic updates. [Full Review]

Michael Varga

From our perspective, no real issues with the application. Personally, I use it on my desktop/laptop/tablet and have had no issues with signature or application updates. I hope to convince our Application team to adopt it over our MSEPP solution but due to the difference in price, it's it's not likely. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Lilly Froud

If you are running a small business and don't need an over-the-top product, ESET is a good product. Cost-friendly and easy to manage for a small number of devices on the network. Phone support has been marvelous. [Full Review]

Marek Galik

Pricing per month, for security services as apps in CEE pricing: up to €2 monthly is OK. With pricing around €5 per month you have to provide really strong value as it is already at the level of one quarter of a telco bill. [Full Review]

Kaspersky Endpoint Security

See 19 reviews >>

Overview

Kaspersky Endpoint Security is a multi-layered endpoint protection platform, based on true cybersecurity technologies. This tightly integrated solution combines fully scalable protection capabilities for physical, virtual and cloud-based endpoints including desktops, servers, mobile devices and embedded systems. Every endpoint can be managed through one unified console, giving you a complete security overview, no matter how extensive your infrastructure. Kaspersky Endpoint Security delivers a reliable, enterprise-ready security platform, providing data to automatically enrich your SOC. Endpoint vulnerabilities and protection are managed together through one console, improving efficiency and reducing your TCO. It protects you from ransomware... [Read More]

SAMPLE CUSTOMERS

ACMS, Arqiva, Pakistan International Airlines, RAO UES

TOP COMPARISONS

Symantec Endpoint Protection (SEP) vs. Kaspersky Endpoint Security ... Compared 24% of the time [See comparison]
Cylance vs. Kaspersky Endpoint Security ... Compared 7% of the time [See comparison]
ESET Endpoint Security vs. Kaspersky Endpoint Security ... Compared 7% of the time [See comparison]

VISITORS READING REVIEWS *

TOP INDUSTRIES

Financial Services Firm ... 30%
Construction Company ... 20%
Energy/Utilities Company ... 10%
Security Firm ... 10%

COMPANY SIZE

1-200 Employees ... 60%
201-1000 Employees ... 20%
1001+ Employees ... 20%

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

Kaspersky Endpoint Security

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Ritesh Chandra

* The main thing for us is that we get our reporting. * Deployment and centralized management are essential for us because of the number of loads that we have along with the number of geographic locations where we are based. * If any policy has been breached, it will send you a report. [Full Review]

Samie Ashraf

According to my security engineer, Kaspersky essentially protects the devices. Before Kaspersky, we had other solutions that always had some problems with phishing, malware, and other threats. After using Kaspersky, we never have those issues. Prior to using this solution, we also had performance complaints from users. Now, with Kaspersky, we never have performance issues. I would say it is the protection. Yes, there is the ability to protect against normal malware and the performance of the endpoint. It doesn't degrade any performance while working... [Full Review]

Susan Kamau

* Network Agent * Over the network deployment * Monitoring * Reporting * Manipulation I can easily manage over 300 computers antivirus from my desk. I am able to see detected viruses, run disinfection, and scans remotely. I am able to troubleshoot Kaspersky Antivirus installed on workstations from my desk by uninstalling, starting tasks, communicating with computer users (Network Message), and viewing and deploying to those who are not installed. Updates are also run on a schedule and this saves on bandwidth usage since some updates from the KSC dba... [Full Review]

Antony Muturi

The centralised management console. Ability to discover machines and see their realtime state. Integration with AD also helps in identifying sources of infection and acting appropriately [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Zain-Rehman

Kaspersky Endpoint Security did help us a little but there were still some problems. For example, we had problems in processing payment issues from the gateway country. Overall, we implemented Kaspersky Endpoint Security because it enabled us to reduce costs. [Full Review]

Adnan Adnan

We used to have a lot of phishing attacks and all these kind of things for end users so we decided that we needed endpoint security. We evaluated some solutions and found that Kaspersky is the most appropriate in terms of endpoint security and the speed of the user machine. The encryption is a major factor from our end. [Full Review]

Samie Ashraf

This solution hasn't really been improved any functionality on the organizational level except that there are no complaints related to the endpoint protection. With the new update, they have incorporated some advanced protection and behavior detection. We have gained advanced threat protection without investing more into it. [Full Review]

Kaspersky Endpoint Security

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Zain-Rehman

This solution needs improvement in the reporting section. Reporting in Kaspersky Endpoint is good but it's not that great. The platform needs to centralize reporting control. They should include some BMP features, like a BD board or MP board and some D&B company in the near future. That would be good. [Full Review]

Ritesh Chandra

* I would like to see machine learning and AI as added features. * It would be nice if they had a separate email security solution (instead of only their cloud edition), similar to what Forcepoint and Trend Micro have. * I would rate their encryption as a one out of 10. It needs a lot of improvement. * There are some features built into Kaspersky that do not work at all, so we have to use other products instead. [Full Review]

Adnan Adnan

There should be some AI involved. We already have machine learning involved in recent releases but machine learning should be more enhanced in the upcoming versions. The logs should be more simplified and more interactive for the end user. These are the areas I feel they need to improve on. [Full Review]

Samie Ashraf

I would like to have more forensic features. For example, if we are hit by an attack, I would like to have tools to investigate what kind of attack, who has attacked, how it was attacked, and what we could do to stop this kind of attack in the future. I would like to have more forensics capability built into Kaspersky. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Zain-Rehman

Our license for Kaspersky Endpoint Security is on a yearly basis. We have a yearly subscription. They have multiple options available at no additional costs. [Full Review]

Palo Alto Networks Traps

See 8 reviews >>

Overview

Traps replaces legacy antivirus and secures endpoints with a multi-method prevention approach that blocks malware and exploits, both known and unknown, before they compromise endpoints such as laptops, desktops and servers.

SAMPLE CUSTOMERS

CBI Health Group, University Honda, VakifBank

TOP COMPARISONS

Symantec Endpoint Protection (SEP) vs. Palo Alto Networks Traps ... Compared 15% of the time [See comparison]
Cylance vs. Palo Alto Networks Traps ... Compared 13% of the time [See comparison]
Carbon Black CB Defense vs. Palo Alto Networks Traps ... Compared 9% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 16%
Media Company ... 13%
Legal Firm ... 13%
Comms Service Provider ... 9%

VISITORS READING REVIEWS *

TOP INDUSTRIES

Mining And Metals Company ... 22%
Healthcare Company ... 22%
Government ... 11%
Financial Services Firm ... 11%

COMPANY SIZE

1-200 Employees ... 33%
201-1000 Employees ... 25%
1001+ Employees ... 42%

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

Palo Alto Networks Traps

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Amjad Khan

A majority of its features are very good, well-designed, and programmed. Most of the machine learning has features where we took a deep analysis on kernel level scanning. It has shown that if in case of anything happens, like first-level operation fails or it went to the next level that it will protect the machine. You can see the artificial intelligence working on it. [Full Review]

Netw9886

The most valuable features are the fact that it was running in the background and it would intercept any weird stuff, and the fact that it would send things directly to the cloud for sandboxing. It's quite practical. [Full Review]

Omar Sánchez (Mr.Tech)

If the user leaves our premises or network, Palo Alto Traps will still be on that endpoint and will still apply our policies. For example, if you take that endpoint out of our network, go to a Starbucks with a company laptop, then connect to our our virtualized gateway. That local endpoint will still have our network policies. I'm so used to IPS IDS endpoint security that I don't see anything else that catches my attention other than it's working fine. It's a very good tool. It's the best one that we have. It has Android support. [Full Review]

ManagerO5d72

Wildfire, advanced detection capabilities, and whitelist/blacklist features. These features have provided us an easy way to lock down our systems to prevent execution of unknown code and scripts and to prevent launching of code from end user writable directories. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Luke Teeters

Its multi-layer approach helps my organization with anti-malware, exploit protection, and restrictions. A good analogy would be like peeling back an onion, getting through those layers. It gives you the confidence that it will stop exploits, ransomware, worms, or viruses from compromising endpoints, essentially providing peace of mind. [Full Review]

Amjad Khan

After deploying Traps, we saw the performance of the network improve by 65 to 70 percent. There was a drop in the latency rate over the application, when accessed via our users. We received feedback from users that usually when they were downloading a bunch of things or browsing the Internet, ad popups would spring up which are a gateway to bring viruses and stick in temp files. This improved a lot because Traps occasionally gives an alert to them to be careful, such as don't go on play on this site and download malicious things. The overall perform... [Full Review]

Netw9886

Many people here are surfing the web on Russian sites, Korean sites, Chinese sites, etc., and by definition, they download things that are not very nice. Whenever there was something fishy, most of the anti-virus solutions just wouldn't see it. We needed endpoint protection that would detect as soon as some code started doing funny things. Traps was very good at that. [Full Review]

Palo Alto Networks Traps

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Luke Teeters

With cloud integration, there were several improvements made: * Previously, the endpoint would leave the environment, not being on our VPN, essentially unable to interact with the server to upload files. It was unable to retrieve new file verdicts. It was using a thing called "local analysis" to determine if something was a malicious file or not. There was no dynamic analysis. With the cloud implementation, we now have connectivity to the server at any moment, as long as we have an internet connection. * A new user interface, which is a lot easier t... [Full Review]

Amjad Khan

There are some default policies which sometimes affect our applications and cause them to run around. In the hotel industry, we use a different type of data versus Oracle and SQL. By default, there are some policies which stop us from running properly. Because of this, the support level is also not that strong. We have to wait to get a results. Originally, we wanted to uninstall Traps because we could not run our operations because Traps, by default, had blocked applications and files. This is still a thing, as we still have to give flexibility to c... [Full Review]

Netw9886

There are some false positives. What our guys would have liked is that it would have been easier to manipulate as soon as they found a false positive that they knew was a false positive. How to do so was not obvious. Some people complained about it. The interface, the ESM, was not user-friendly. [Full Review]

Omar Sánchez (Mr.Tech)

There are some limitations on the Traps agents. Traps for Windows has limitations and Traps for Linux too. Traps doesn't work with McAfee. You need to remove McAfee to install Traps. This is very common, and its nothing that should be an issue. Some antivirus engines recognize Traps as an threat component, so maybe they need to shake hands somewhere. With Windows 7 and Windows 8 64-bit, when you want to install Traps, because its Windows, it will crash. They need a little more flexibility with antivirus engines. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Rob Haller

The pricing seems fair, and I do like the licensing model. You use wherever they are, and it is elastic. So, if you have 1100 computers today, you can license that. Therefore, as long as you're below your licensing cap, you're fine. [Full Review]

Saidatta HIndlekar

We did not negotiate the price because the solution did not fulfill our requirements. But the price was fine. I don't know how it would compare with Symantec because I negotiated a lot with Symantec. I don't know what kind of negotiation I could have done with Palo Alto. [Full Review]

Raul Rivera

Our license runs on a monthly basis with a recurring monthly charge. If you want additional options like secure remote access with policies, that requires an additional cost. Palo Alto Networks Traps does not apply secure remote access to devices without policies, which we are implementing. If you want to apply more policies, like an anti-virus program, anti-malware, or configurations for using a VPN on remote connections, that would also be an additional cost. We're not doing that. [Full Review]

Cylance

See 6 reviews >>

Overview

Cylance® is revolutionizing cybersecurity with products and services that proactively prevent, rather than reactively detect the execution of advanced persistent threats and malware. Our technology is deployed on over four million endpoints and protects hundreds of enterprise clients worldwide including Fortune 100 organizations and government institutions.

SAMPLE CUSTOMERS

Panasonic, Noble Energy, Apria Healthcare Group Inc., Charles River Laboratories, Rovi Corporation, Toyota, Kiewit

TOP COMPARISONS

CrowdStrike vs. Cylance ... Compared 17% of the time [See comparison]
SentinelOne vs. Cylance ... Compared 14% of the time [See comparison]
Carbon Black CB Defense vs. Cylance ... Compared 13% of the time [See comparison]

REVIEWERS *

TOP INDUSTRIES

Financial Services Firm ... 18%
Energy/Utilities Company ... 12%
Non Tech Company ... 12%
Media Company ... 7%

VISITORS READING REVIEWS *

COMPANY SIZE

1-200 Employees ... 88%
1001+ Employees ... 13%

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

Cylance

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Andrew S. Baker (ASB)

The CylancePROTECT agent is very low on CPU usage, so it has virtually no adverse impact on my servers, desktops, or workstations. I am also quite impressed with its ability to protect systems against zero-day threats due to the machine learning algorithm, which powers its database. Databases, as old as 2015, are able to accurately detect 2017-era threats, such as WannaCry and other ransomware. [Full Review]

C.J. Oosthuizen

The protection, specifically the wireless protection, has been the most valuable. They've got the optics as well, but most of the clients are more interested in the protection. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Eric Rise

Rather than having to log onto a central server to manage the endpoint protection, I can log onto the dashboard to manage everything. No on-premise server required, chewing up resources needed for other tasks and projects. Endpoints are protected in real-time without the need of a centralized server, whitelist, or the ability to connect to a central host in the cloud. Even if an endpoint loses connection to the Internet, I know that endpoint is protected against 99.99% of the threats in the wild today. [Full Review]

Andrew S. Baker (ASB)

My clients have not had to contend with time-consuming false positives, nor have they had to worry about zero-day attacks, even for systems which have been off the network for months. [Full Review]

Software4704

It streamlines the data and makes it a lot easier to access and sift through. The solution has also helped us a lot in terms of making threats a lot more obvious with our correlation manager. I estimate it has saved us 20 percent of what was our mean time to detect and respond to threats. It has also helped increase staff productivity. We do vulnerability detection for our product's security and Cylance allows us to make our assessments a lot more accurate. [Full Review]

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Eric Rise

Work on the math model. We are catching a lot of false positives, which gets to be a pain at the start of a deployment. It is not hard to decipher and add a global safe list, so you do not have to touch or adjust Clients on all endpoints. After you get passed the initial scan, it is clear sailing and very easy to manage and maintain. [Full Review]

Cylance

Continued from previous page

Sven Aurich

Improvements could be made on the user interface of the console. Also, right now it's just an antivirus and there's no firewall or anything. So we have to use the Windows firewall. It's a good firewall. But I think other companies have integrated products. The solution needs better dashboards that are easier to use. Also, a better user interface. Maybe even firewall integration of some kind. It would be helpful if you could see which threats have been detected, and have more information about what is going on. What I'm missing is a backup. In Norton... [Full Review]

C.J. Oosthuizen

To be honest, I think the product is, overall, quite good. It's working with AI Technology and machine learning. It picked up files that other platforms don't pick up. I don't really see any improvement. It's actually been great on its own. I would say one thing that they might need to bring in is protection for mobile devices. [Full Review]

Thomas Reisel

Security is an issue because they don't get Powershell. They scan the usual software and they don't scan deeper. The security scripting needs improvement. It needs deeper security for scripting. Also, more speed, less RAM, and less CPU. [Full Review]

PRICING, SETUP COST AND LICENSING

See more Pricing, Setup Cost And Licensing >>

Eric Rise

Shop around for sure and be assured the price you pay will be close to other solutions available, but even at a slight mark-up from the other solutions, you are getting real endpoint protection versus nothing more than a cheap security blanket that might keep you warm at night. However, it is not actually protecting you from anything. [Full Review]

Andrew S. Baker (ASB)

The initial endpoint cost may seem a little high (~$55/device/year), but when you look at the total peace of mind that the solution of Cylance endpoint protection provides, with no reboots for updates, and negligible performance impact, it is well worth it. [Full Review]

McAfee Complete Endpoint Protection

See 14 reviews >>

Overview

McAfee Complete Endpoint Protection allows you to protect all of your devices with intelligent, collaborative security, in one easy-to-manage, integrated solution. Our integrated endpoint security framework helps remove redundancies, enables fast, proven performance and offers an architecture to align both current and future security investments. With a flexible choice of cloud-based or a local management console, security administrators also get true centralized management that simplifies ongoing tasks, deployment and monitoring.

SAMPLE CUSTOMERS

inHouseIT, Seagate Technology

TOP COMPARISONS

Symantec Endpoint Protection (SEP) vs. McAfee Complete Endpoint Protection ... Compared 32% of the time [See comparison]
Cylance vs. McAfee Complete Endpoint Protection ... Compared 10% of the time [See comparison]
Carbon Black CB Defense vs. McAfee Complete Endpoint Protection ... Compared 9% of the time [See comparison]

VISITORS READING REVIEWS *

TOP INDUSTRIES

Healthcare Company ... 19%
Government ... 19%
Financial Services Firm ... 19%
Retailer ... 13%

COMPANY SIZE

1-200 Employees ... 26%
201-1000 Employees ... 34%
1001+ Employees ... 40%

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

McAfee Complete Endpoint Protection

Continued from previous page

Top Reviews by Topic

VALUABLE FEATURES

See more Valuable Features >>

Owais Yousuf

The following are the main features of the McAfee Suite: * Threat/risk protection at the core level: All of the components , including the antivirus and exploit functionalities, all communicate with each other on a real-time basis. * Machine learning: The McAfee Suite consists of sophisticated learning algorithms in order to precisely identify and confirm the presence of any malware, primarily based on their signature profiles. * The containment of applications: With this feature, your IT security staff can mitigate the damaging impacts of malicious... [Full Review]

Reviewer677

The feature I like the most in McAfee Endpoint Protection is when I get reports of unmanaged devices. These are kind of issues that alert me to address a problem. I need to find out how we can eliminate these devices which are connected to our network and not managed by McAfee. [Full Review]

Reviewer7245

You can integrate this endpoint protection with a specific business process that you may want to link to the process of the antivirus. It has the capability to custom define user-defined fields. [Full Review]

IMPROVEMENTS TO MY ORGANIZATION

See more Improvements To My Organization >>

Owais Yousuf

Controlling and Monitoring Change Change control processes are often reactive and require manual responses, an ineffective approach to combating today's threats and handling the growing number of devices in the IT infrastructure. The Security Connected approach from McAfee ensures that every desktop, server, application, network device, and database is in the scope of a change control solution, giving you critical visibility into who is using your systems and what activities are taking place. Enabling Consumerization of the Workforce A flood of iPho... [Full Review]

CompleteEnd677

I need to be able to allow the amount of data used on an authorized user account., i.e. the amount of web data someone uses before a limit. I use other tools for that now. [Full Review]

Drct0987

It has improved my organization because it helps with visibility, in terms of security. We can see the actual attack and can contain it. The antivirus can detect that. [Full Review]

Enterpri7a3f

Initially, the DLP was very valuable for disabling access to USB drives -- but the need to get a code before granting exceptions made the management cumbersome. [Full Review]

McAfee Complete Endpoint Protection

Continued from previous page

ROOM FOR IMPROVEMENT

See more Room For Improvement >>

Reviewer677

In my experience, the main part of McAfee Complete Endpoint Protection that needs to be improved or simplified to make the platform better is the scanning features. Sometimes when it runs in the background of the endpoint, the devices get slowed down for some software applications. The reporting should be used to enhance our analysis. There are some dashboards for user management. There is still improvement required with them. [Full Review]

Deepti Tewari

The solution is getting better. The new central console is better than the earlier one. Earlier it was too complex to find out which option was there. So, if there was a search menu for certain things and if I wanted to enable or disable something, I couldn't. Now there's a search menu that I can type into and I can navigate through the menu to where I want to go. There are still too many options but it is better now. Sometimes, while installing the ePO we get many errors and I don't know why they happen. So I just want them to work on that part. So... [Full Review]

CompleteEnd677

In our experience, McAfee Endpoint Protection could improve the word control feature. It is absent from the application. I couldn't do that. Everything has been fine with the product. It could use better visuals. The tutorial is very limited. They need better training materials and visuals in reports. [Full Review]

Alvaro Jiménez

We have a lot of problems with the user experience and it's difficult to implement. MacAfee's better than the ancient anti-virus solutions but it's a little slow to resolve. Many files with malware were destroyed through the network, and MacAfee doesn't detect anything. They should improve the time of response, the time of the detection of malware, and the installation of the service. The features we would want a good endpoint solution to contain are: * Multi-operative system * Better performance * Integration with browsers * Firewall control * Vuln... [Full Review]

Answers from the Community

What's the best way to trial endpoint protection solutions?

We all know that it's important to conduct a trial and/or proof-of-concept as part of the buying process.
Do you have any advice for the community about the best way to conduct a trial or POC? How do you conduct a trial effectively?
Are there any mistakes to avoid?

James Carlson

You might want to start out with business cases ... ensuring that your endpoint solution begins to address those. some ideas might include: * antivirus * antivirus updates via automation * antivirus updates via cloud or on premise automation * antivirus reporting to central on premise management server * do you want to rely upon static signatures? * do you want to find the zero days? * what about polymorphic / variants of previously known malware? * will your antivirus mechanism share with other machines / computer their discoveries? * do you want to share your information with the manufacturer (via cloud) or keep your discoveries in house / on premise? * DLP -data loss protection * DLP reporting to central management server * DLP - how easily configurable? * DLP -what type of additional work will this entail for analyses, etc * Host Intrusion Prevention (HIP) * HIP -...

Wim Wilts

Some suggestions: 1. Some products you can test for a restricted period with a trial license. 2. It is possible to test in a virtualized environment (VMware, VirtualBox) 3. Today I have tested myself a new version on a new server (nb: not live). 4. I made a mistake to install SQLEXPRESS 14 on a 2016 domain controller. 5. After trial and error, I solved it with an extra instance on a SQL Server 2017. 6. Kaspersky Support was very fast and helpful with clear tips and tricks.

Eric Rise

Consult with several VARs with any product being looked at. If possible work directly with the vendor of the product to avoid the VAR pressing you in any one direction. The product vendor can then point you to the proper/ best fit VAR offering the best price for the product as this will vary based on VAR choice. Provide the VAR with a list of what things you need and then things you might want in a product. Have a set of hardware and users that will be the test group for your product(s) being tested then have a proper plan in place to document every step all the way through to end result for each and every product being tested. Apples to apples as close as possible for all products to make a decision. It's not always about price either, expensive solutions hurt one time, cheap ones will hurt...

See all 12 answers >>

About this report

This report is comprised of a list of enterprise level Endpoint Protection for Business vendors. We have also included several real user reviews posted on ITCentralStation.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 IT Central Station

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 IT Central Station 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.

IT Central Station helps tech professionals by providing:

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

Use IT Central Station 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

IT Central Station
244 5th Avenue, Suite R-230 • New York, NY 10001
www.ITCentralStation.com
reports@ITCentralStation.com
+1 646.328.1944