

Ronald Lakin

CIS 130

Nick Romano

November 28 2015

Comparing Antivirus Business Solutions

A small business running 25 work stations and 2 servers require an antivirus solution that will meet all of the needs of the company while offering excellent protection. The console must be centralized, easy to use, well documented, and support all of the platforms used by the business. Cloud based solutions eliminates the need for on-site IT administration. Since many antivirus companies are not in the US, you need to make sure your choice does not conflict with your company's trade policy.

The five small business antivirus solutions compared here are cloud based services that have been tested by independent labs like AV Comparative, AV Test, Dennis Labs, MRG Effitas, and Virus Bulletin. Tests include real world protection, file detection, false alarms, performance, usability and other tests.

Bitdefender is an internet security software company originated in Romania, represented through subsidiaries and partners in over 100 countries. The company has been developing online protection since 2001 (Wikipedia).

Business solutions include GravityZone Business Security, Advanced GravityZone Business Security, and Gravity Zone Enterprise Security. GravityZone Business Security is designed for small businesses and offers both cloud and on premise management consoles. Software supports Windows, Mac and Linux desktop and servers as well as Windows, Solaris,

and Linux virtual desktops and servers. Advanced GravityZone adds Exchange support, mobile support (on premise only) and the ability to offload scanning to central dedicated appliance.

Bitdefender has performed well in comparative testing and received a top award from AV Test in 2014.

Gravity Zone's management console can be either installed locally via a pre-configured virtual machine by an IT administrator, or run on the cloud if you don't have IT support.

Scanning, scheduling, and updating can all be done by the administrator as well as deployment of the client software locally or remotely. The client/server software allows users to run scans and updates but not disable protection. The software comes with plenty of documentation (2 manuals) and a great help section (AV Comparative).

GravityZone Business Security can be purchased and downloaded from the company's website. Cost for 25 work stations and 2 servers is \$748.46. Advanced runs \$1404 and includes 51 mailboxes (Bitdefender).

Kaspersky Lab is headquartered in Moscow, Russia, with its holding company registered in the United Kingdom. The company is specially focused on security systems designed for small business, corporations and large enterprises. The first product, Kaspersky Anti-Virus, was released by Eugene Kaspersky, in the middle of 1997 (Wikipedia).

While Kaspersky offers many Enterprise solutions, their Small Office Security package is designed for up to 25 work stations and 3 file servers. For larger companies they have Endpoint Security for business and Total Security for business. Small Office Security supports Windows Desktops and laptops, Windows Servers, Mac OSX desktops and laptops, and Android phones

and tablets. Comparative testing sites have given Kaspersky high scores and numerous awards for the last 7 years.

Kaspersky's centralized cloud based control requires no installation. While the console is easy to navigate they do not offer a manual or knowledge base for help. The administrator can deploy the client software all at once or send email for users to download themselves. Administrators can run a scan (quick or full) or update on all devices or just one. Scheduling can be configured only on the individual computer/server. Inactive devices (over 4 days) are marked with an x and can be hidden from the screen (AV Comparative). An administrator can enable web management through My Kaspersky portal to manage remotely.

The software can be downloaded from company's website or purchased from a reseller. 25 workstations and up to 3 servers will cost \$599.99 (Kaspersky).

Sophos was founded by Jan Hruska and Peter Lammer and began producing its first antivirus and encryption products in 1985. Sophos primarily developed and sold a range of security technologies in the UK, including encryption tools available for most users (Wikipedia).

Sophos offers a wide range of antivirus software for businesses. Sophos Endpoint Security and Control can support Windows XP-10, Mac IOS 10.6-10.10, Windows Server 2003/2008/2012/R2, Linux, and Android through bundles to fit your needs. Other services include VM support, Amazon Services, Email and more. Sophos received the "best corporate antivirus usability award of 2014" from AV Test.

The management console is cloud based and only requires the administrator to create an account and log in. The administrator can manually download endpoint protection software or send an email link to users. Scans, scheduled scans and updates can be set up in the console. You

can remove a device by simply checking the box on the device page and clicking delete. Users can run updates and scans, but cannot disable protection. A nice feature is automatic reactivation/reinstallation of disabled/removed client software (AV Comparative).

Sophos requires you to fill out a form to get a price quote based on the many services they offer. Trial software can be upgraded and purchased. Online resellers offer licenses and renewals. Estimated basic price for 25 work stations and 2 servers is \$735.00. Sophos is the only service that licenses users as opposed to devices. This means policies follow the user from device to device.

Trend Micro was founded in 1988 in Los Angeles by Steve Chang, his wife, Jenny Chang, and her sister, Eva Chen. Shortly after establishing the company, its founders moved headquarters to Taipei. In 1992, Trend Micro took over a Japanese software firm to form Trend Micro Devices and established headquarters in Japan (Wikipedia).

Trend Micro's Worry Free Services is an excellent choice for small businesses wanting an easy to use cloud service. Worry Free Advanced adds email and phishing protection. For on premise software you can choose from Worry Free Standard and Advanced. Windows, desktops, Laptops, and servers, Mac Desktops and laptops, and both android and Mac mobile devices. Trend Micro was the most inconsistent in comparative testing.

The centralized console is cloud based so it does not require installation or configuration. The administrator just needs to log in to the browser. You can deploy software 3 ways. Send an email, download, or create an exe file to use on a flash drive. Scanning, scheduling, updating, and removal can be easily done on the console. Users can disable the firewall and agent unless the administrator password protects it on the console. While the console is very easy to navigate,

there is no manual or knowledge base available (AV Comparative). For an additional charge you can receive 24 hour tech support.

Trend Micro's Worry Free Services cost \$835.88 for 25 work stations and 2 servers and can be purchased and downloaded from the web site (Trend Micro). The advanced version costs \$1350.00.

F-Secure Corporation, first established under the name Data Fellows by Petri Allas and Risto Siilasmaa in 1988, is an online security and privacy company based in Helsinki, Finland. The company has 20 country offices and a presence in more than 100 countries, with Security Lab operations in Helsinki, Finland and in Kuala Lumpur, Malaysia. F-Secure claims that it was the first antivirus vendor to establish a presence on the World Wide Web, develop the first heuristic scanner for antivirus products and develop the first anti-rootkit technology called BlackLight in 2005 (Wikipedia).

F-Secure Protection has a wide range of solutions. Protection Service for Business is a cloud based service designed for small businesses. Business Suite offers on premise software with VM support designed for large companies. Protection Services for Business supports Windows, Mac OSX, Linux and most mobile platforms as well as file servers, mail servers, and gateways. F-Secure scored well in most testing, and won a "Best Corporate Antivirus Protection" award from AV Test in 2014 (AV Test).

The PBS console is on the cloud so no installation or configuration is needed. F-Secure comes with 2 well laid out manuals, a quick start guide and an administrator's manual. Endpoint software deployment can be done by email link, download or remote push. Scanning can be done by the administrator or user. Users can schedule scans from the client software. Updates have

been pre-configured to run automatically. Manual updates can be run by the user. While the web browser interface may seem strange the GUI is similar to other when open (AV Comparative).

F-Secure requires you to fill out an online form to receive price quotes. Software can be purchased through an online partner. An estimated cost for Protection Services for Business would be \$1000.00 for 25 work stations and 2 servers.

While all of the products compared are very similar and all would be a great antivirus solution, Kaspersky's Small Office Security is the best choice for a small business running 25 work stations and 2 servers. The cloud based console makes it simple for a small business that doesn't have an IT administrator to easily deploy software, scan, and update, remove devices. Software supports Windows, Windows Servers, Macs, and Mobile Devices (Android and Mac). Of course the most important factor is how well it protects your network. Kaspersky has received top awards and high marks from most independent AV comparative testing sites. AV Comparative gave Kaspersky its highest rating (advanced plus) not only for 2015 but for every real world, removal, and anti-phishing test since 2009. They also received highest ratings for performance (10 out of 13) and file detection (22 out of 24) (AV Comparative). AV Tests, Virus bulletin, Dennis Labs and other sites have all given Kaspersky high ratings¹.

If your business requires VR support Bitdefender GravityZone is the best choice. It scored second in total high marks and awards from AV Comparative. The on premise management console is easy to manage, is well documented and offers 24/7 tech and remote control support.

¹ Stats in charts in executive summary compiled from data at AV Test (AV Test), AV Comparative (AV Comparative), Dennis Labs (Dennis Tech .Labs).

Executive Summary

1. Kaspersky Small Office Security: Best protection with an easy to use management console.
2. Bitdefender GravityZone for Business: Best choice for VR networks and Linux
3. F-Secure: Web based console with good protection but expensive.
4. Sophos: Lots of options, and easy to use but inconsistent protection ratings.
5. Trend Micro: Easy to use console mixed protection ratings.

Company	BitDefender	Kaspersky	Sophos	Trend Micro	F-Secure
Software	Endpoint Gravity Zone	Small Office Security	Endpoint Security and Control	Worry Free Bus. Security Systems	Protection Service for Bus.
Country	Romania	Russia	United Kingdom	Japan	Finland
Console Type	Cloud, On-Premise Virtual Appliance	Cloud	Cloud	Cloud	Cloud, On premise Windows and VM
Client Software deployment	Email Link, Push Install, Exe file for flash drive	Email Link, Push Install	Email Link, Push Install, Exe file for flash drive	Email Link, Exe file for flash drive	Email Link, Exe file for flash drive
OS Support Windows	XP,vista, 7-10	XP,vista, 7-10	XP,vista, 7-10	XP,vista, 7-10	XP,vista, 7-10
OS Support Windows Server	2003, 2009, 2012	2003, 2009, 2012	2003, 2009, 2012	2003, 2009, 2012	2003, 2009, 2012
OS Support Mac	Mac OSX 10.7-10.10	Mac OSX 10.7-10.10	Mac OSX 10.7-10.10	Mac OSX 10.7-10.10	Mac OSX 10.7-10.10
VR Support	VMWare,Oracle,HyperV,Citrix	N/A	Vmware and MS HyperV	N/A	N/A
Linux	Yes	N/A	N/A	N/A	N/A
Android/IOS Support	Yes with advanced	Yes	Yes	Yes	Yes
Tech Support	Email,Phone,Forum, Remote Control by Staff	Email,Phone,Forum	Email,Phone,Forum,Chat, Remote Control by Staff	Email,Phone,Chat, Remote Control by Staff	Email,Phone,Forum,Chat, Remote Control by Staff
Manuals Included	VR Install, Admin Manual	N/A	Admin Manual	N/A	2 manuals Admin,Quick Start
Available download Online	Company Website	Company Website	Reseller	Company Website	Reseller
Trial version available on site	Yes	Yes	Yes	Yes	No
Price 25WorkStns and 2 Servers	\$748.00	\$599.99	\$735.00	\$835.38	Approx \$1000.00

Figure 1 Feature Table (AV Comparative)

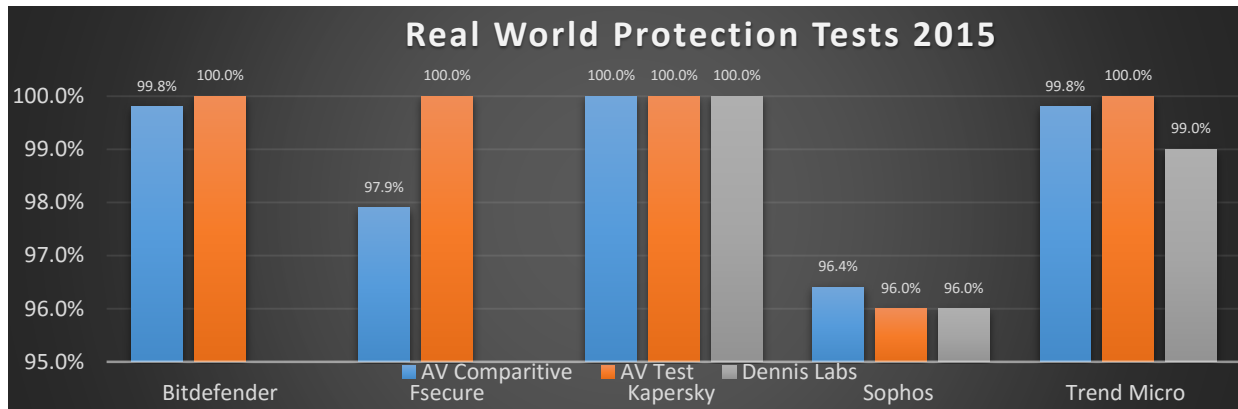


Figure 2 Real World Protection Chart 2015 (AV Test) (AV Comparative) (Dennis Tech .Labs)

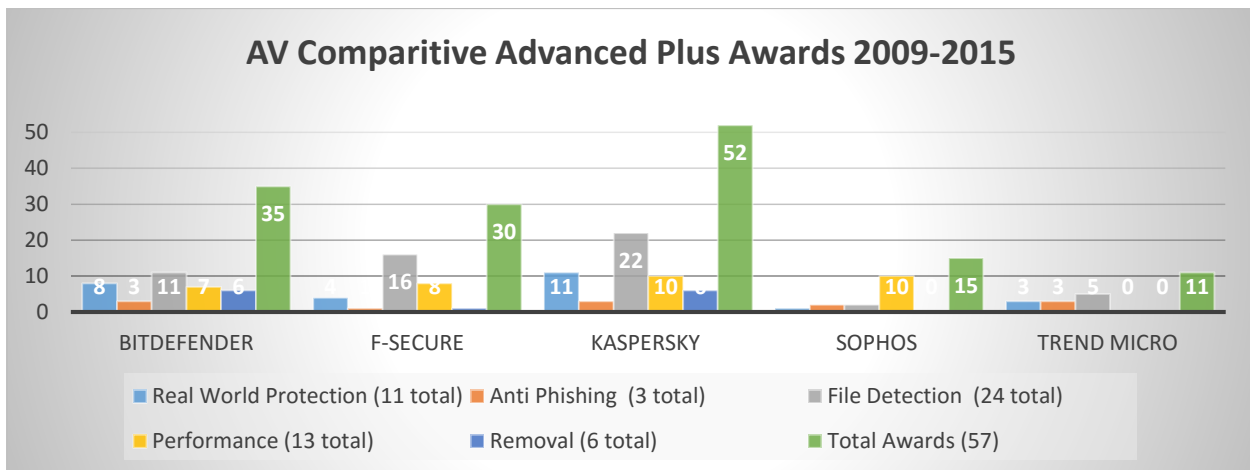


Figure 3 Total Award charts 2009-2015 (AV Comparative)

Works Cited

- AV Comparitive. *Awards Overview - AV-Comparatives*. n.d. Online Charts. 12 November 2015.
- . *Business Review 2015*. 1 October 2015. Online PDF. 8 November 2015.
- AV Test. *AV Test Awards 2014*. 15 February 2015. Website Document. 10 November 2015.
- Bitdefender. *Bitdefender GravityZone Business Security*. n.d. Web Page. 9 November 2015.
- Dennis Tech .Labs. *Dennis Technology Labs*. n.d. Web Page. 12 November 2015.
- Kaspersky. *Business-Grade Security for Small Offices*. n.d. Web Page. 12 November 2015.
- Trend Micro. *WORRY-FREE HOSTED BUSINESS SECURITY*. n.d. Web Page. 12 November 2015.
- Wikipedia. *Bitdefender*. n.d. Web Document. 8 November 2015.
- . *Kaspersky*. n.d. Web Document. 10 November 2015.
- . *Sophos*. n.d. Web Document. 8 November 2015.
- . *Trend Micro*. n.d. Web Document. 9 November 2015.
- . *Trend Micro*. n.d. Web Document. 8 November 2015.