Market Share Analysis of Antivirus & Compromised Devices

January 2015

OPSWAT®

Contents

Introduction

OPSWAT periodically releases market share reports for several sectors of the security industry. This report includes market share for antivirus applications, as well as compromised device data. The data used in this report was collected on January 2, 2015, using OPSWAT GEARS, a free device security and management tool. OPSWAT GEARS has the ability to collect information regarding the applications installed on endpoint computers and certain settings applied to these applications. Please note that OPSWAT is not a research institution and makes no claims on the accuracy of this data in the real world marketplace; this report aims to distribute the unique data collected to inspire public discussion, not to make any claims as to why changes have occurred. For a description of the data collection method and its limitations, see the data collection section of this report.

About OPSWAT

OPSWAT is a San Francisco based software company that provides solutions to secure and manage IT infrastructure. Founded in 2002, OPSWAT delivers solutions that provide manageability of endpoints and networks, and that help organizations protect against zero-day attacks by using multiple antivirus engine scanning and document sanitization. OPSWAT's intuitive applications and comprehensive development kits are deployed by SMB, enterprise and OEM customers to more than 100 million endpoints worldwide. To learn more about OPSWAT's innovative and unique solutions, please visit www.opswat.com.

Report Highlights

21.4%

Avast leads the antivirus vendor market with 21.4%, followed by Microsoft.

17.8%

Microsoft Security Essentials leads the antivirus product market with 17.8%, followed closely by avast! Free Antivirus.

91.3%

More than 90% of devices in the data had not run a full system scan via their installed antivirus product within the last seven days.

15.1%

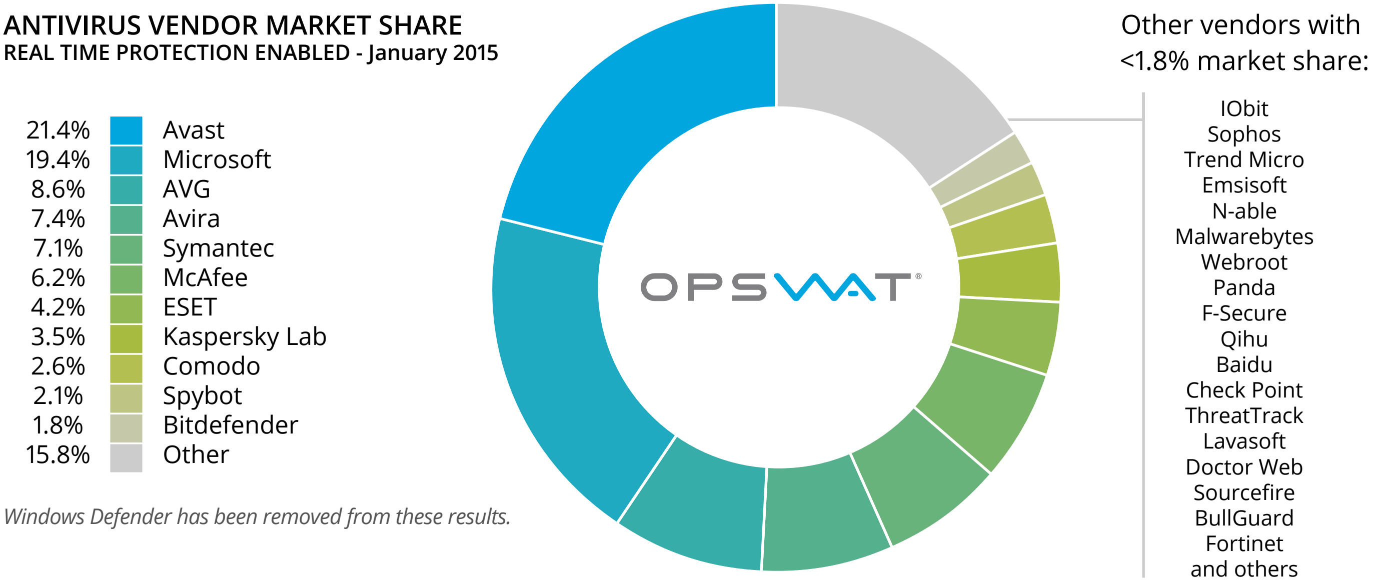
Antivirus definitions were out of date in more than 15% of devices.

3.3%

After running a multi-scan, previously undetected threats and PUAs were found on 3.3% of devices. Detected but unremediated threats were found on 0.7% of devices.

Antivirus Vendor Market Share
January 2015

Among devices using OPSWAT GEARS for endpoint security management, Avast leads the market for antivirus and anti-malware vendors. The company's anti-malware products make up 21.4% of those detected, while Microsoft comes in second in with a 19.4% market share. Microsoft and Avast are consistently the dominant vendors in our reports, although Microsoft's Windows Defender, which was included in previous reports, has been removed from this data because it is a feature of Windows 8 and 8.1 and not actively acquired by the user. All other vendors show a single-digit market share, with AVG, Avira, Symantec, McAfee, ESET, Kaspersky Lab, Comodo, and Spybot following in the rankings. Spybot appears in the report for the first time due to added detection by GEARS. These results only include devices with real-time protection enabled, indicating that the user's machine is actively being protected.



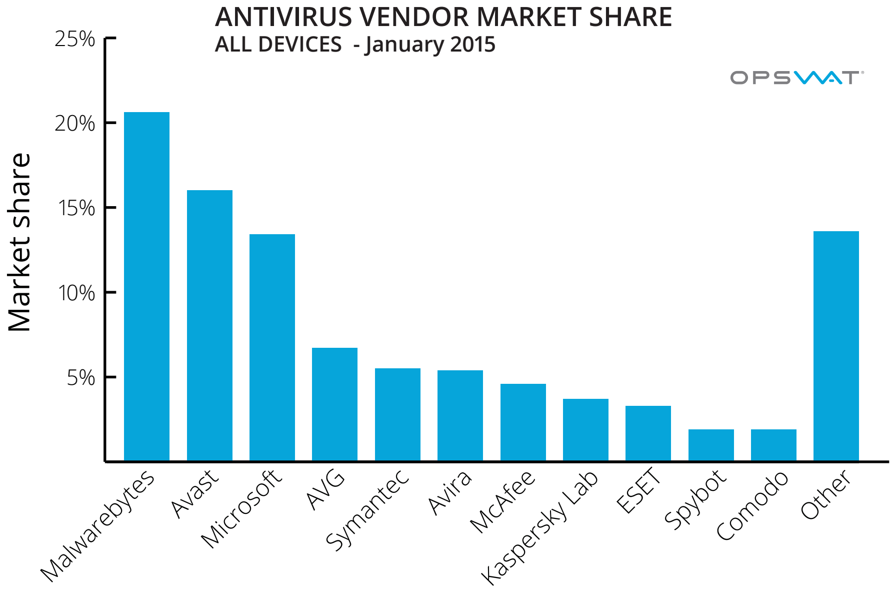
ANTIVIRUS VENDOR MARKET SHARE
REAL TIME PROTECTION ENABLED - January 2015

Other vendors with <1.8% market share:

IObit
Sophos
Trend Micro
Emsisoft
N-able
Malwarebytes
Webroot
Panda
F-Secure
Qihu
Baidu
Check Point
ThreatTrack
Lavasoft
Doctor Web
Sourcefire
BullGuard
Fortinet
and others

Windows Defender has been removed from these results.

While the above comparison only includes data from products with real time protection (RTP) enabled, we also analyzed data for all installed security products, including those that may have expired or been disabled. In this additional data set, Malwarebytes is the leading antivirus provider, with more than a 20% share. Because its free antivirus product is on-demand, without real-time protection, Malwarebytes doesn't rank within the RTP protection data set. Avast and Microsoft follow, with 16.0 and 13.4 percent respectively.



ANTIVIRUS VENDOR MARKET SHARE
ALL DEVICES - January 2015

Windows Defender has been removed from these results.

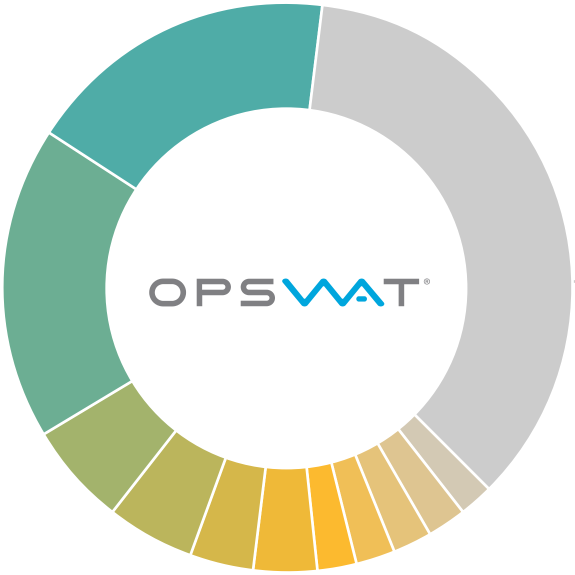
Antivirus Product Market Share
January 2015

When analyzing the market share of specific antivirus and anti-malware products rather than the vendors themselves, Microsoft and Avast continue to lead the market, despite the exclusion of Windows Defender detailed above. At 17.8%, the leading antivirus product detected on devices using OPSWAT GEARS is Microsoft Security Essentials, followed closely by avast! Free Antivirus at 17.6%. In past reports, these two products have alternately led the field, with avast! Free Antivirus claiming the top spot in our previous report. The remaining products all show single-digit market shares, including Avira Free Antivirus, AVG Anti-Virus Free Edition, McAfee VirusScan, and Symantec Endpoint Protection. When combined, products that did not make the top ten in the rankings still make up a sizable 35% share of the market.

ANTIVIRUS PRODUCT MARKET SHARE
REAL TIME PROTECTION ENABLED - JANUARY 2015

17.8%	■	Microsoft Security Essentials
17.6%	■	avast! Free Antivirus
5.9%	■	Avira Free Antivirus
5.0%	■	AVG Anti-Virus Free Edition
3.6%	■	McAfee VirusScan
3.6%	■	Symantec Endpoint Protection
2.4%	■	Norton 360
2.2%	■	Kaspersky Internet Security
2.2%	■	McAfee VirusScan Enterprise
2.1%	■	Spybot - Search & Destroy
1.9%	■	COMODO Antivirus
35.8%	■	Other

Windows Defender has been removed from these results.

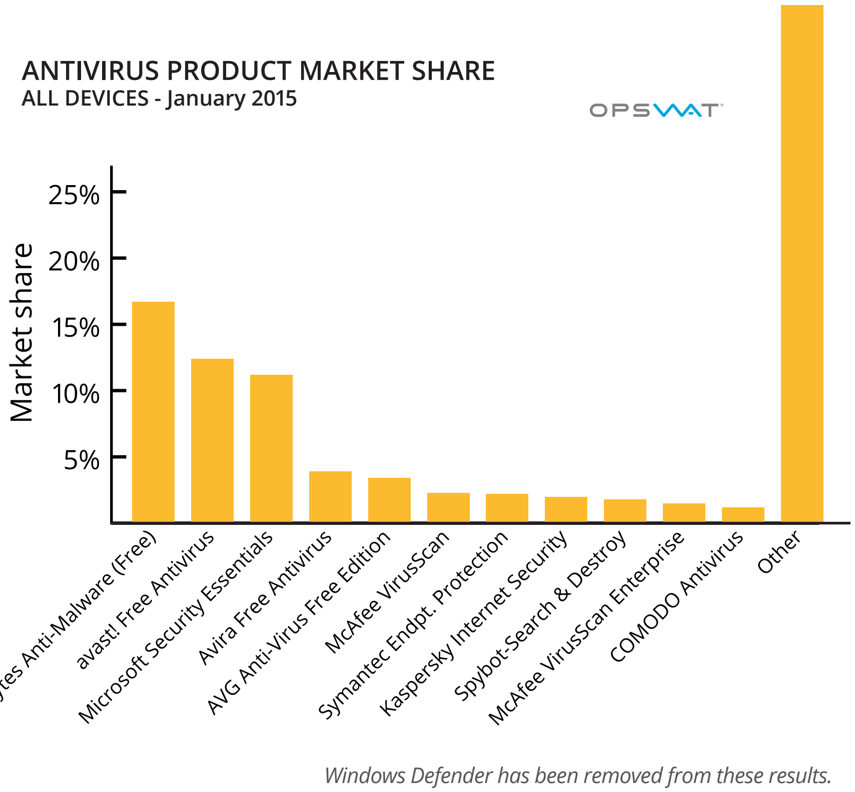


Other products with
<1.8% market share:

AVG Internet Security
ESET NOD32 Antivirus
System Center Endpoint Protection
IObit Malware Fighter
Sophos Anti-Virus
Bitdefender Antivirus Free Edition
ESET Endpoint Antivirus
Malwarebytes Anti-Malware Pro
360 Total Security
Webroot AntiVirus
ESET Endpoint Security
COMODO Internet Security Premium
Emsisoft Anti-Malware
Avira Antivirus Pro
avast! Premier
ESET Smart Security
Norton AntiVirus
Trend Micro OfficeScan Client
Baidu Antivirus
Panda Cloud Antivirus
F-Secure Internet Security
Kaspersky Anti-Virus
and others

While the above comparison only includes data from products with RTP enabled, OPSWAT also analyzed data for all installed security products, including those that may have expired or been disabled. In this comparison, Malwarebytes Anti-Malware (Free Version) is the leading antivirus product with 16.7% of the market. Due to the difference in functionality detailed above, Malwarebytes' free antivirus product did not appear in the comparison of products with RTP enabled. In this expanded pool of product detections, the market share for avast! Free Antivirus and Microsoft Security Essentials decreases to 12.4 and 11.2 percent each.

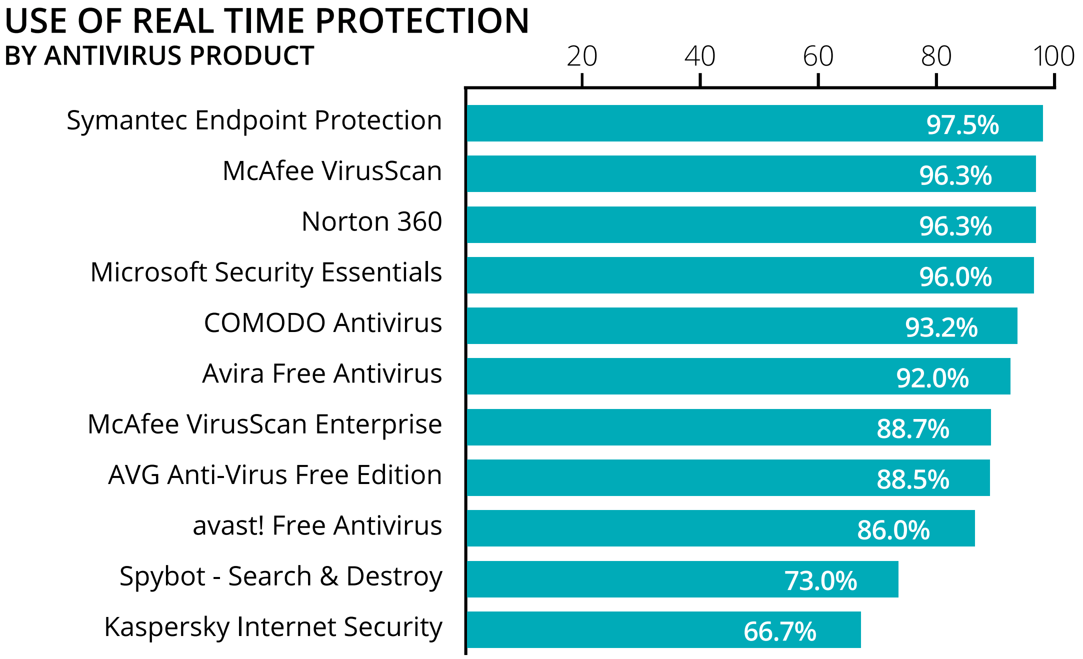
ANTIVIRUS PRODUCT MARKET SHARE
ALL DEVICES - January 2015



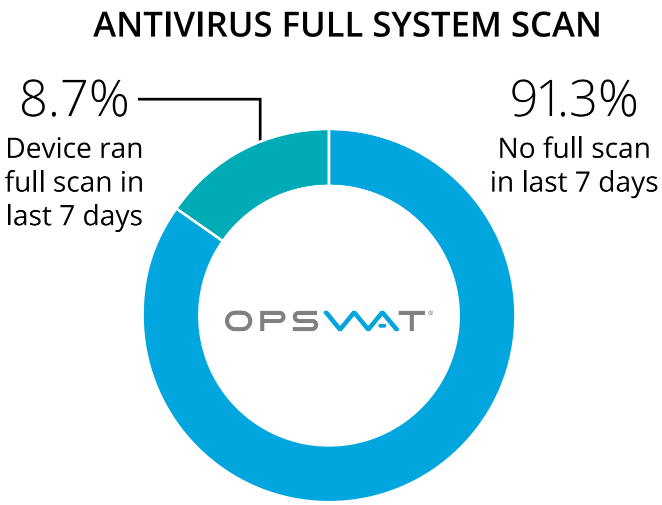
Windows Defender has been removed from these results.

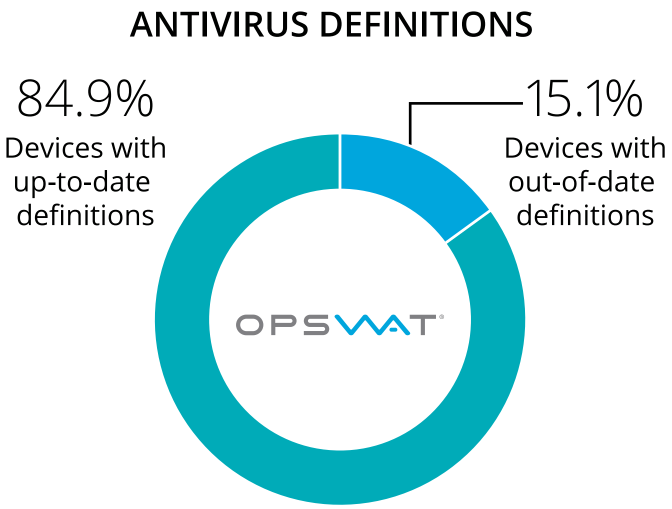
Antivirus Usage
January 2015

In many cases, RTP status provides an indicator of product usability and/or effectiveness. When an anti-malware product is effective and easy to operate, the user is more likely to utilize the product in real time. Among the top anti-malware products found in this data set, RTP use ranges from 66.7% to 97.5%.The product with the highest rate of devices with RTP enabled was Symantec Endpoint Protection, at 97.5%, followed closely by McAfee VirusScan, Norton 360 and Microsoft Security Essentials.



Despite extensive usage of RTP, 15% of devices were found to have out-of-date virus definitions, defined for this report as being at least three days old. Note that this is a rather lenient definition, and by many system administrators' policies the percentage of out-of-date antivirus products would be even higher. Additionally, over 90% of devices had not completed a recent full system scan. A lack of regular updates and full system scanning in sampled devices is especially problematic given today's regulatory environment. Organizations without robust endpoint management and compliance solutions in place to identify and remediate these risks are giving insecure devices access to their networks and could find themselves in violation of HIPAA, PCI and other data security regulations.

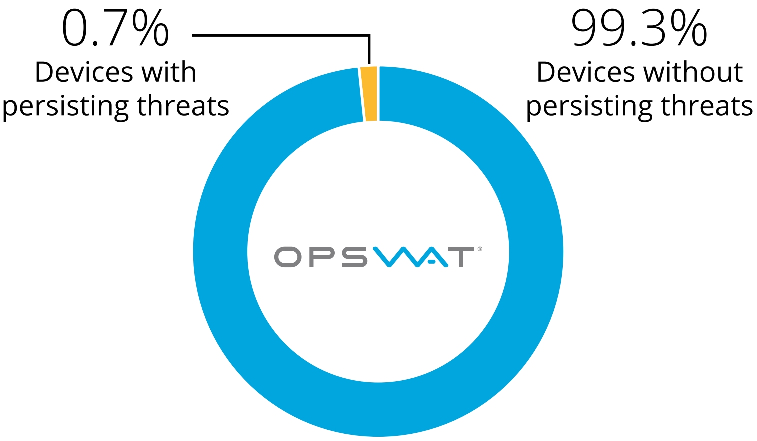




Compromised Devices
January 2015

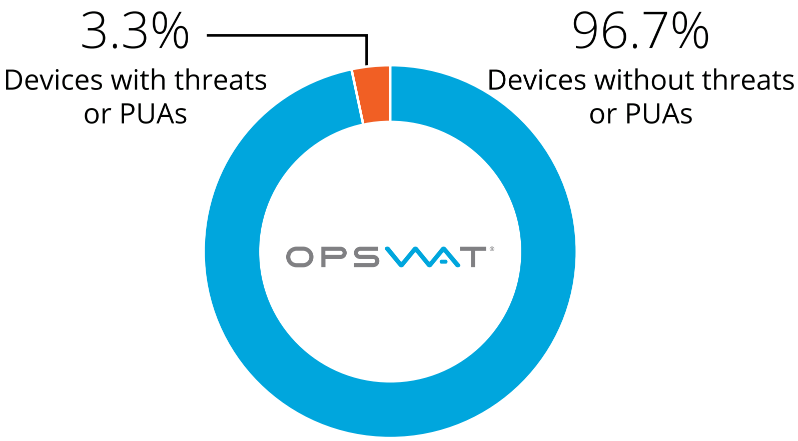
GEARS uses two methods to identify infections that cannot be easily remediated by a device's installed antivirus product. The first method looks for files that are repeatedly detected by the installed antivirus software and persist after efforts to remediate or remove them have been completed. This behavior indicates that even though the antivirus product can detect the threat, further action may be required to secure the system. Alternately, it may indicate suspicious activity on the part of a user who is repeatedly downloading a malicious file. Using a threshold of 5 detections by the installed antivirus, we found this type of infection in 0.7% of devices, most of which contained a single persistent threat.

DEVICES WITH PERSISTING THREATS
AS DETECTED BY THE INSTALLED ANTIVIRUS



The second method GEARS uses to identify compromised devices is a daily cloud-based malware scan of the programs running on a device, using up to 43 anti-malware engines. This helps identify both active threats on the device that may have been missed by the installed antivirus, as well as potentially unwanted applications (PUAs) like adware, that can serve as vectors for an attack. For this report, we looked at malware and PUAs that were detected by at least 4 anti-malware engines in Metascan Online, and discovered that 3.3% of surveyed devices were compromised.

AT-RISK DEVICES
IDENTIFIED BY METASCAN ONLINE



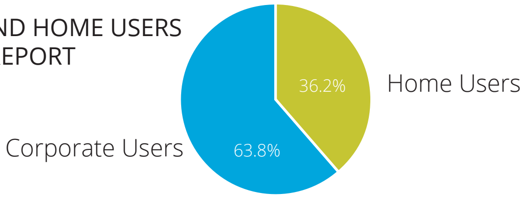
Data Collection

This report shows comparisons for applications on Windows systems from data collected from users of OPSWAT GEARS, a device security and management platform that is free to monitor up to 25 devices, available at www.opswatgears.com. This technology allows OPSWAT to collect information regarding the applications installed on endpoint computers and certain settings applied to these applications. This report includes only free GEARS accounts. This tool is used around the world by home and business users, both by expert and inexperienced users of security software. For the purpose of the report, the sample of about 4000 users is assumed to be representative of the market, based on the wide accessibility of the tool to a large range of users. However, these results are likely to differ from those in the real world (see below for more details). GEARS runs continuously on a user's system as a security tool. This allows for continuous reports over time from each device that is connected, as long as GEARS is installed. The data in this report reflects the state of each user's computer from the most recent data transfer prior to the time of collection on January 2, 2015. The most recent data transfer from each device ranges from October 1, 2014 to January 2, 2015.

Several attributes inherent to the data collection methods may cause the results in this report to differ from real-world conditions. OPSWAT makes no claims as to the accuracy of the data in the real world market and, when possible, is continuously working to overcome the following potential anomalies:

- The data that was collected originally contained a high number of German devices, most of which used the same products. 75% of German devices were randomly removed from the sample to offset this anomaly.
- On average, GEARS users are more likely to have high-functioning security on their computers than would be seen in the market as a whole. GEARS allows IT administrators to monitor users who are not security compliant, so the act of gathering OPSWAT's market share data also serves to remind users to increase their security capabilities.
- Though the sample size is large enough to give reliable data, some cross-comparisons and more detailed comparisons result in lower confidence levels. The sample size will continue to increase in each report since the data is collected from every current user of these products. More data in the future will allow for several new in-depth comparisons that have not been included in past reports.
- The data includes both home and corporate users. Because of the nature of the products used to collect the data, the data sample may contain a higher percentage of corporate users than what exists in the real world. The graph below uses the installed Windows version as the criterion to determine which devices are home and which are corporate users.

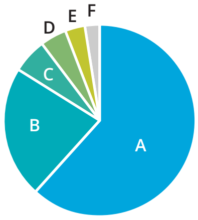
CORPORATE AND HOME USERS
INCLUDED IN REPORT



- These applications are marketed in OPSWAT's own channels. Users sampled may not be representative of the general population. For example, this report may contain a different distribution of Windows operating systems and device types compared to what exists in the real world. While this report contains more than 27% Windows 8 or 8.1 users, Net Applications reports that around 17.5% of all Windows users currently operate under Windows 8 or 8.1.

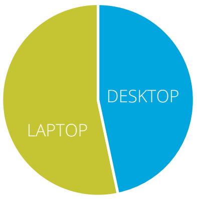
WINDOWS OPERATING SYSTEMS
INCLUDED IN REPORT

A	Windows 7	62.0%
B	Windows 8.1	22.2%
C	Windows 8	5.8%
D	Windows Vista	4.5%
E	Windows XP	3.3%
F	Other	2.3%



DEVICE TYPES
INCLUDED IN REPORT

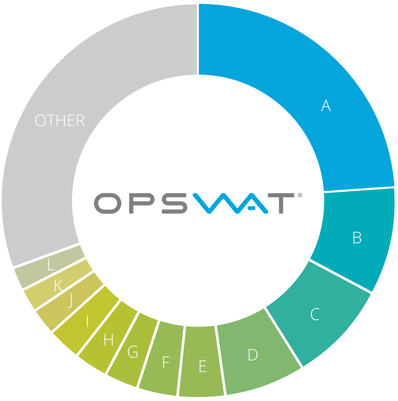
Desktop	46.6%
Laptop	53.4%



Data Collection

- Although GEARS is available for both Windows and Mac, Mac applications are not included in this report, and products that are available for both Mac and Windows would presumably have different market shares in the real world. Market share for Mac users is expected to be added in future reports.
- While GEARS is used on devices around the world, its use is not commensurate with worldwide population distribution. Only English-language versions of this tool are available, so countries with higher numbers of English speakers are expected to use these applications at higher rates, as well as countries that have been exposed to more coverage of these tools by press and partners. For example, the Chinese antivirus vendor Qihu 360 recently reported that it had 440 million users of its internet security products, but it did not make the list of top vendors in this set of data.

WORDWIDE DEVICE DISTRIBUTION



A	United States	23.6%
B	Netherlands	10.1%
C	Brazil	7.9%
D	Germany	5.0%
E	Russian	4.2%
F	Italy	3.9%
G	United Kingdom	3.1%
H	India	3.1%
I	Belgium	2.3%
J	Sri Lanka	2.2%
K	Canada	2.2%
L	Japan	1.8%
M	other	30.7%

Other OPSWAT Market Share Reports

OPSWAT is working to increase global usage of OPSWAT GEARS. Stay tuned for the next market share report in April, which will feature new comparisons and in-depth comparisons of product usage.

Vendors of antivirus, P2P, patch management, backup, encryption, and other applications interested in inclusion in these reports, GEARS, and OESIS Framework are encouraged to contact www.opswat.com/certified to learn how to partner with OPSWAT.

Follow OPSWAT

Get updates about the latest reports as well as company and product information by connecting with us online. Sign up to receive OPSWAT's monthly newsletters by visiting www2.opswat.com/connect, or follow OPSWAT:

www.opswat.com/blog

www.twitter.com/opswat

www.facebook.com/opswat

www.linkedin.com/company/opswat

Company and Reproduction Information

Please contact OPSWAT sales for more information on GEARS. For more information about this report, please contact marketing@opswat.com. Parties interested in hosting this report are free to do so as long as credit is given to OPSWAT, Inc., and a link is provided to www.opswat.com/resources/reports.

About OPSWAT

OPSWAT® is a San Francisco based software company that provides solutions to secure and manage IT infrastructure. Founded in 2002, OPSWAT delivers solutions that provide manageability of endpoints and networks, and that help organizations protect against zero day attacks by using multiple antivirus engine scanning and document sanitization. OPSWAT's intuitive applications and comprehensive development kits are deployed by SMB, enterprise and OEM customers to more than 100 million endpoints worldwide. To learn more about OPSWAT's innovative and unique solutions, please visit www.opswat.com.

Products

GEARS

GEARS is the only cloud-based network security and manageability solution for IT professionals that provides visibility and management for many application types from antivirus to hard disk encryption and public file sharing, as well as the ability to remove non-compliant applications. Monitor up to 25 devices for free! Visit www.opswatgears.com to learn more and sign up.

OESIS

OESIS Framework is a cross platform development framework that enables software engineers and technology vendors to develop products that detect, classify, remediate and manage thousands of third-party software applications. OESIS is perfect for SSL VPN, network access control (NAC) and other manageability solutions, and is already deployed on an estimated 100 million endpoints worldwide. Incorporating the AppRemover SDK, OESIS enables quick and thorough removal of potentially unwanted applications to ensure devices remain compliant and secure.

Learn more at www.opswat.com/products/oesis-framework.

OPSWAT Certification

The OPSWAT Certification Program is a free interoperability program designed to enable technology partnerships between independent software vendors and leading network and technology solution vendors, by verifying that their security applications will work seamlessly with solutions employing the OESIS Framework. Additional information is available at www.opswat.com/certified.

OPSWAT GOLD CERTIFIED Product Type

OPSWAT SILVER CERTIFIED Product Type

OPSWAT BRONZE CERTIFIED Product Type

Multi-scanning and Secure Work Flow

OPSWAT offers several solutions to secure the flow of data into and through organizations that need maximum security. Because no single antivirus engine can detect every threat, using signatures and heuristics from multiple engines simultaneously improves the likelihood of detecting malware. Metascan® technology powers each of OPSWAT's multi-scanning solutions, enabling IT professionals and software engineers to enhance network security by scanning with up to 30 built-in antivirus engines from market leaders such as ESET, Avira, Bitdefender, AVG and many others. Metascan also provides document sanitization, file filtering and more to prevent advanced threats, and can be used for rapid malware analysis and to implement secure data upload and transfer systems.

The new Metascan Mail Agent, now in alpha, allows organizations to scan email attachments and files with multiple anti-malware engines, ensuring that all emails and files are free of malware before being uploaded or delivered. Customers also have access to Policy Patrol Mail Security and Secure File Transfer. These products offer additional security features such as anti-spam, antiphishing, email content security and secure transfer of large and confidential files. Metascan also powers Metadefender, a checkpoint designed to process files to detect and prevent known and unknown threats and protect networks from the risks presented by unknown portable media devices.

To learn more about these technologies or to request a free demo please visit opswat.com/products/metascan.

Disclaimer of Warranty

OPSWAT Inc. makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.