Anti-Malware Vendor Market Share & Device Security Report

August 2015

Table of Contents

Introduction

OPSWAT® periodically releases market share reports for several sectors of the security industry. This report includes market share data for anti-malware vendors, a comparison of encryption usage between Mac and Windows users, and threat data for devices with persisting or potentially undetected threats and at-risk devices. The data used in this report was collected on August 6, 2015, using OPSWAT Gears, a free device security and compliance platform. OPSWAT Gears has the ability to collect information regarding applications installed on endpoint computers as well as the 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 enterprise data and devices. Founded in 2002, OPSWAT delivers solutions that provide manageability of endpoints and networks, and help organizations protect against zero-day attacks by using multiple antivirus engines for 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.

OPSWAT®

Report Highlights

16.3%

Avast takes top vendor spot among anti-malware providers with a 16.3% market share

4.4%

4.4% of represented devices have persisting threats

31.33%

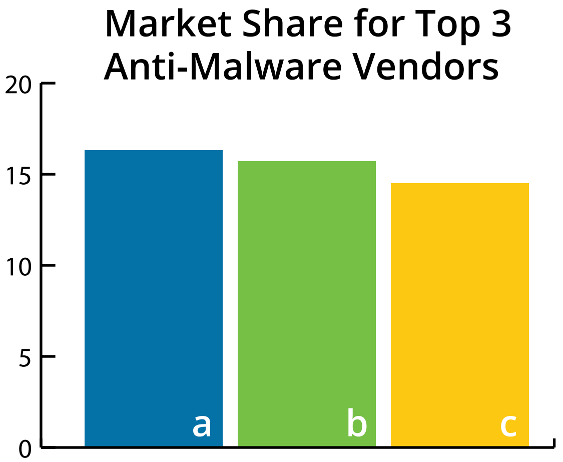
31.33% of Mac devices are encrypted compared to only 2.02% of Windows devices

3.29%

3.29% of included devices have threats or PUAs that may not be detected by their installed anti-malware

Anti-Malware Vendor Market Share

Antivirus products dominated the security market for many years, but with the introduction of new malware types, the industry has shifted toward developing products that protect users from more than just traditional computer viruses. In the 1990's and early 2000's, computer viruses such as the ILoveYou bug were extremely popular, and thus many companies started developing products that were geared toward the detection of these viruses. Since then, malware has evolved, and other threats are now wreaking havoc on users' devices. Anti-malware products differ from the standard antivirus* products in their ability to detect threats including PUAs, ransomware, spyware, keyloggers and botnets that cannot be detected by antivirus products alone.



a.	Avast	16.3%
b.	Microsoft	15.7%
c.	Malwarebytes	14.5%

**Windows Defender is excluded from these results*

In the past, our market share reports focused solely on antivirus products and vendors, but in response to the changes in the marketplace (which our technology has already shifted to recognize) we are re-focusing our reports to reflect the anti-malware market as a whole. This means that, moving forward, antivirus vendor and product data will no longer be exclusively displayed; instead we will examine market share within the larger anti-malware market. This may lead to some changes in the vendor and product names you will see included in future reports and may also cause shifts in the percentages seen for the vendors who have been in the reports all along, but it presents the opportunity for us to explore new data points. We believe that this shift towards anti-malware accurately reflects the trends in the current marketplace, as well as the improved product and vendor detection capabilities of our software. As we are making these changes, the report only highlights the top three anti-malware vendors, but this will be expanded in the future.

The top three anti-malware vendors in our August 2015 data are Avast at 16.3% market share, Microsoft at 15.7% and Malwarebytes at 14.5%. These numbers reflect only those installations where RTP (Real Time Protection) is enabled. It is important to note that Windows Defender has been excluded from the Microsoft vendor data. Although Windows Defender is heavily saturated in the anti-malware product market, we exclude it because we feel that it does not accurately represent the user's product of choice as it comes pre-installed on many Windows systems and cannot be removed. In future reports, other anti-malware vendors such as the ones seen below will be included.

- AVG
- Avira
- Bitdefender
- Check Point
- COMODO
- ESET
- F-Secure
- Kaspersky Lab
- McAfee
- Panda Security
- Qihoo 360
- Safer-Networking
- Symantec
- Trend Micro
- And Others

If you are an anti-malware vendor that would like to see your product included in our data, you can visit the OPSWAT Certification page to learn how we detect vendor products.

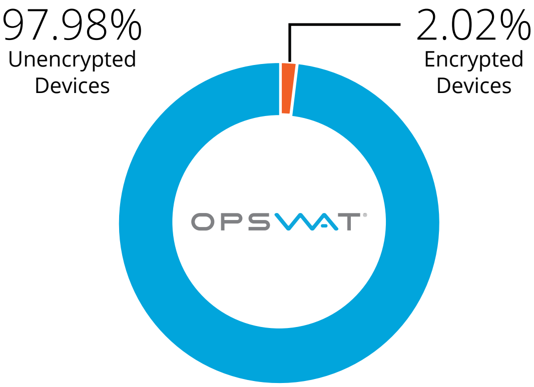
* It is important to note that just because a product has "antivirus" in its name, does not necessarily mean that product only detects viruses. Avast's free antivirus product, for example, detects more than just viruses.

Disk Encryption Usage: Windows and Mac Comparison

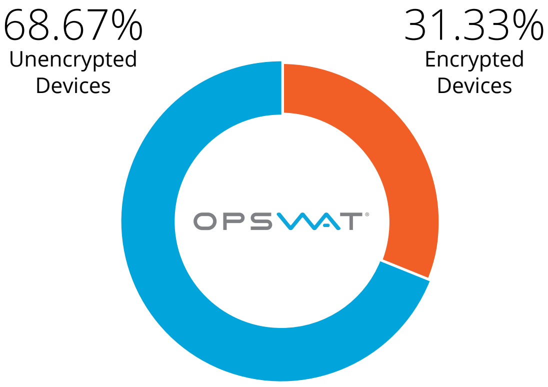
Disk encryption, although often overlooked by most users, is extremely important for the security of a device. The majority of users represented in this report are home users, but that doesn't mean that their device should be left unsecured, as many people do use their personal laptop or desktop computers when working from home or traveling. If a device is left unencrypted, then sensitive company information could be exposed through that vulnerable device, if it is lost or stolen. In Verizon's 2015 Data Breach Investigations Report, they found lost or stolen unencrypted employee devices to be one of the leading causes of compromised data.

Encryption rates for Windows devices included in this report were surprisingly low compared to that of Macs. Only 2.02% of Windows devices were using encryption products compared to 31.33% of Macs. It is important to note that the Mac data included in this section was taken from a much smaller sample size compared to the Windows data.

Windows Device Encryption Usage



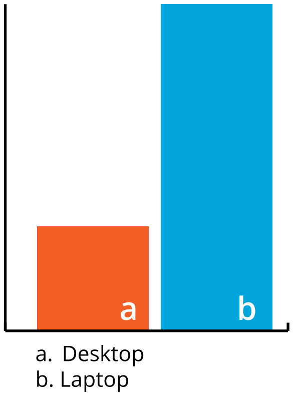
Mac Device Encryption Usage



Both FileVault and BitLocker come pre-installed on Mac and Windows machines, respectively, and have to be enabled by the user. However, since Windows requires both a public and private key, Windows devices are notoriously difficult and take longer to setup than Macs. If encryption of Windows devices were less time-consuming, it is reasonable to assume that they would be encrypted at a higher rate.

We also looked at encryption rates between Windows laptop and desktop users. Without excluding BitLocker, there were three times as many laptops encrypted as desktops. It makes sense for encryption rates to be higher among laptop users as laptop devices are more vulnerable to theft.

Windows Device Encryption Usage

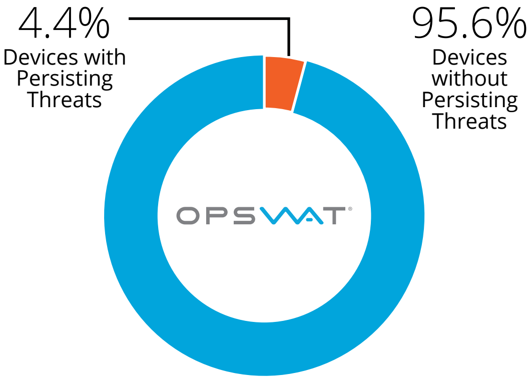


Windows Device Health: Threat Analysis

Gears uses two methods to detect threats to find compromised devices. The first method uses the installed anti-malware product to detect threats. By looking for files that have been repeatedly detected by the installed anti-malware, Gears is able to determine which threats are left unremediated by the anti-malware product on the user's machine. This shows that even though the product may detect a threat, further actions may be required to remediate the threat, which isn't always apparent from the anti-malware product alone. Repeatedly detected threats can also indicate risky behavior on the part of a user who may be repeatedly downloading the same malicious file. We found this type of infection to occur in 4.4% of Windows devices, using a threshold of 4 or more detections of the same threat by the installed anti-malware.

Devices with Persisting Threats

As detected by installed anti-malware

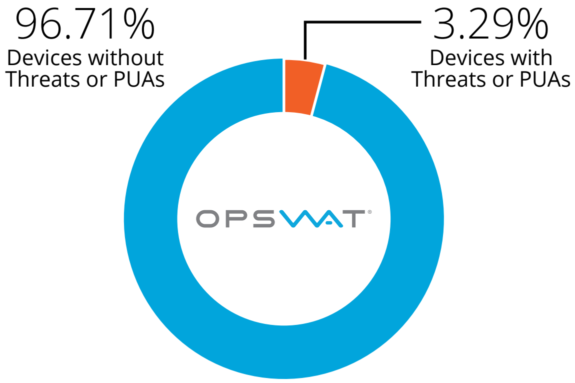


The number of devices with repeatedly detected threats in this report are higher compared to our last report that included this data. The increase in devices with this type of threat is largely due to the improved threat detection capabilities of our technology and shows that this type of threat is more prevalent than previously known.

The second threat detection method used by Gears allows us to identify which devices may be compromised by performing a malware scan of the processes running on a device with many anti-malware engines. For this scan, we use Metascan Online's cloud-based multi-scanning technology, supported by 44 anti-malware engines. This scan looks for threats that could have been missed by the user's installed anti-malware, such as a PUA (Potentially Unwanted Application). As most users may only have 1 or 2 anti-malware programs installed on their device, Metascan's multi-scanning technology may catch threats missed by the installed anti-malware programs. PUAs are not inherently dangerous, but they can come bundled with malware and serve as a vehicle for attack. For example, the malware known as Gunpoder hid behind advertisements and was able to fool many antivirus engines by disguising itself as adware and avoiding classification as a severe threat. For this reason, if a device has PUAs detected on its system, it is considered to be at-risk of infection. Metascan Online uses multiple anti-malware products to check for PUAs, which is important because not all endpoint anti-malware products have strong PUA detection. Multi-scanning also acts as a second-layer of defense to catch threats that may be missed by the users' installed anti-malware. For this report, we looked at malware and PUAs that were detected on machines by at least 4 anti-malware engines and discovered that 3.29% of included devices were considered compromised or at-risk.

At-Risk Devices

Identified by Metascan Online



Data Collection

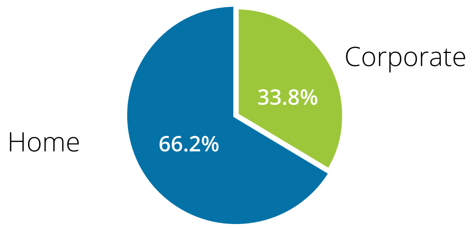
This report shows comparisons for applications on Windows and Mac systems from data collected from free users of OPSWAT Gears, a device security and compliance platform that is free to monitor up to 25 devices, available at opswatgears.com. Free Gears users permit OPSWAT to collect information regarding the applications installed on endpoint computers and certain settings applied to these applications. 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 over 11,000 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 August 6, 2015. The most recent data transfer from each device ranges from May 6, 2015 to August 6, 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:

- 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.

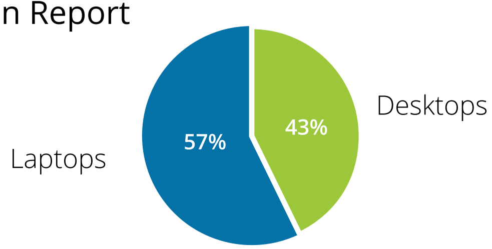
Corporate vs Home Users



- The data includes both home and corporate users. Because this data only includes free Gears accounts, there are a larger number of home users represented. Corporate accounts usually need to manage a large number of devices so they upgrade from the free account as it only supports 25 devices or fewer. The graph to the right shows the distribution of corporate versus home users included in this report.

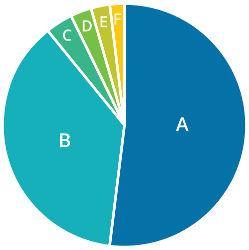
- These applications are marketed in OPSWAT's own channels. Users sampled may not be representative of the general population. For example, this report may contain a different distribution of Windows operating systems and device types compared to what exists in the real world. While this report contains more than 40% Windows 8 or 8.1 users, Net Applications, a web analytics firm, reports that around 15.86% of all Windows users currently operate under Windows 8 or 8.1.

Device Types Included in Report



Distribution of Windows OS

A	Windows 7	52.0%
B	Windows 8.1	37.4%
C	Windows 8	3.5%
D	Other	2.9%
E	Windows XP	2.5%
F	Windows Vista	1.7%



Data Collection

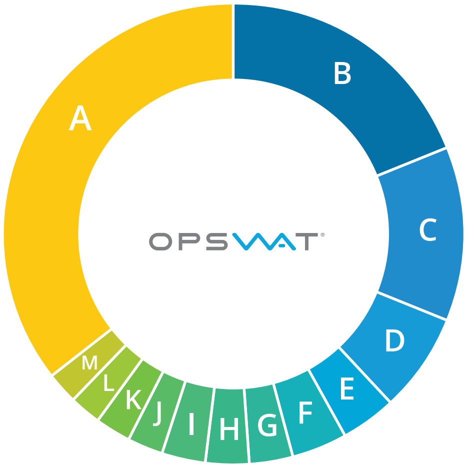
- The purpose of OPSWAT's Market Share Reports is not to make any claims on which anti-malware vendors are the best or to compare these products in terms of quality or performance. The purpose of this report is simply to report on the security practices of our free Gears users.

- We are unable to identify devices that have uninstalled Gears and have later reinstalled the program. For this reason, there is a possibility that a small number of devices in this report may have been represented more than once.

- 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.

Worldwide Device Distribution

A	United States	19.1%
B	Netherlands	12.2%
C	Italy	6.9%
D	India	3.9%
E	United Kingdom	3.8%
F	Hungary	3.2%
G	Spain	3.1%
H	Canada	2.9%
I	Germany	2.6%
J	Indonesia	2.3%
K	Belgium	2.3%
I	Brazil	2.2%
M	Other	35.5%



- The Mac device data included in this report was taken from a small sample as this is only the second report where Mac data has been included. For this reason, Mac data points have a lower confidence level.

Other OPSWAT Market Share Reports

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

Vendors of anti-malware, P2P, patch management, backup, encryption, and other applications interested in inclusion in these reports, Gears, or the 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 an enterprise device security and compliance tool that enables organizations to directly assess and manage the endpoint security posture of their devices through a unified view of mobile and PC endpoints, and their applications/security issues. Administrators can to take rapid action to remediate issues on non-compliant devices and improve endpoint security. Monitor up to 25 devices 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/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 BRONZE CERTIFIED Application Type

OPSWAT SILVER CERTIFIED Application Type

OPSWAT GOLD CERTIFIED Application 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 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 Security for Exchange 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 to 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.