Independent Tests of
Anti-Virus Software

IT Security Survey 2025

LAST REVISION: 13TH FEBRUARY 2025

WWW.AV-COMPARATIVES.ORG

Security Survey 2025

We are proud to present our annual Security Survey for 2025. This initiative is part of our ongoing commitment to optimising our service to the end-user community. We want to thank all the respondents who contributed their valuable time and energy to help improve various aspects of anti-virus software and its testing.

Key data

Survey Period: **1st December 2024 – 25th December 2024**
Valid responses of real users: **1,277**

The survey was carefully designed with control questions and checks to ensure the authenticity and validity of responses. The insights gained are invaluable to us and help to shape the future of cybersecurity services.

Overview

In today's digital landscape, where cyber threats loom large, understanding user behaviour, preferences, and concerns is essential for developing effective cybersecurity strategies. This comprehensive survey explores the experiences of users worldwide, offering valuable insights into their digital lives. It highlights the operating systems and applications they rely on, the security measures they adopt, and their concerns about IT security.

The report delves into the factors influencing choices of browsers, operating systems, and security solutions, while also addressing privacy concerns and the need for transparency and independence from organizations that protect our digital world.

Survey findings showcase the diverse ages, expertise levels, and regional backgrounds of participants, all of which shape user decisions and concerns. The data reflects loyalty to specific operating systems, growing preferences for particular browsers, and fears of cyber threats influenced by regional and technical factors.

This report offers a global perspective on current cybersecurity trends, serving as a foundation for further research. Beyond statistics, it aims to provide meaningful insights for users, providers, and testers in the cybersecurity field. We encourage you to reflect on these findings and consider their implications for your own cybersecurity strategies.

The survey, conducted by AV-Comparatives between December 1 and December 25, 2024, gathered responses from about 1,300 participants globally, focusing on IT security. We hope the insights presented here will guide you in strengthening your cybersecurity approach.

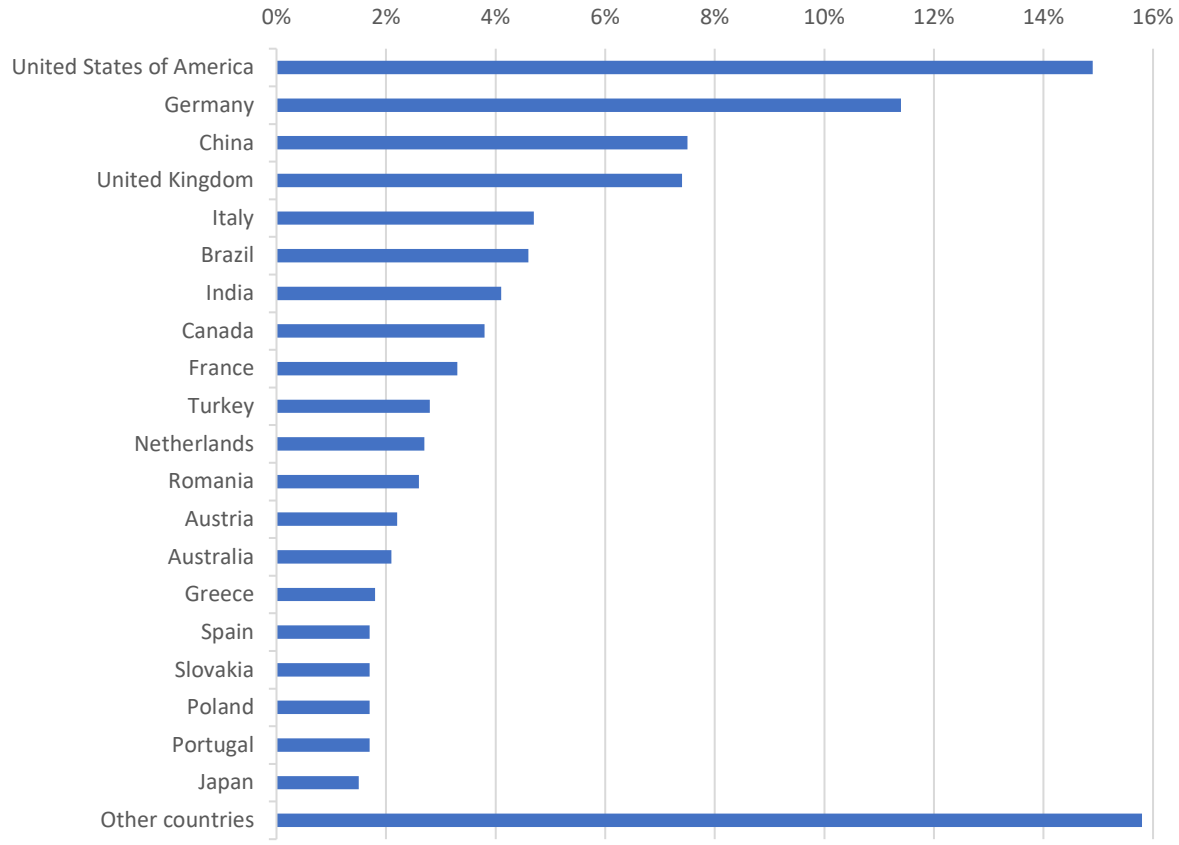
We extend our gratitude to all survey participants. Your input is invaluable in improving the relevance and impact of our tests, helping manufacturers refine their products and benefiting both the industry and its users. We are proud to see our test results frequently cited in security product reviews. For full transparency, all public test results from AV-Comparatives are freely available at www.av-comparatives.org

Key results

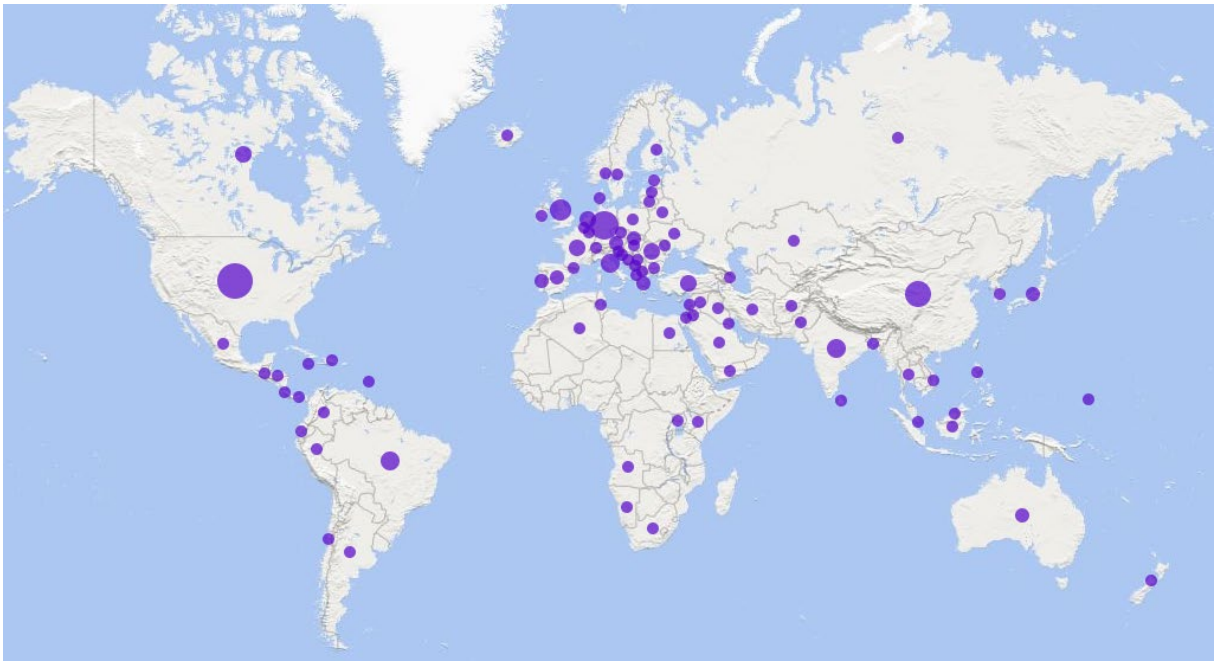
The Key findings or the survey are listed below, by question number. Please note that they all refer only to our survey participants, not the general public.

1. ***Origin of Respondents***: Respondents hailed from 93 countries. The United States had the most respondents from a single country, followed by the Germany and China.
2. ***Age of Respondents***: The youngest and oldest age groups had the fewest respondents, with the 35-44 category providing the most.
3. ***Level of expertise***: 70% of participants identified as advanced or IT/expert users
4. ***Free vs Paid Security Solutions***: over two-thirds of survey participants paid for their chosen desktop security programs. Advanced users overwhelmingly prefer paid tools.
5. ***Operating System Preferences***: A majority now seem to prefer Windows 11 over Windows 10, with older Windows versions generally used more by non-expert users.
6. ***Browser Preferences***: Mozilla Firefox and Google Chrome remain the most preferred browsers.
7. ***Mobile OS Trends***: Android dominates (75%), but iOS is preferred by advanced users.
8. ***Mobile Security:*** 39.3% use no mobile anti-malware, including 43% of IT professionals. Top vendors vary regionally, with Bitdefender, Kaspersky, and ESET consistently prominent.
9. ***Desktop Security:*** Microsoft, Bitdefender, ESET, and Kaspersky dominate globally. Microsoft leads in North America; Kaspersky tops Europe, Asia, and South America.
10. ***VPN solutions***: Over a third of participants did not use a VPN, while those that do had a wide range of preferred products.
11. ***Trusted Test Sources:*** AV-Comparatives and AV-Test are the most trusted. Younger users rely on social media/YouTube.
12. ***Requested Consumer Tests:*** Bitdefender, ESET, Microsoft, and Kaspersky top the list for future evaluations.
13. ***Enterprise Solutions Demand:*** CrowdStrike, Sophos, and Cisco join traditional leaders (Bitdefender, ESET) in business/enterprise requests.
14. **Windows 11 Adoption Plans:** Over 50% plan to switch to Windows 11 in 2024–2025, driven by advanced users.
15. ***Resistance Reasons:*** 32% prefer Windows 10, while hardware/software compatibility (28%) and privacy concerns (18%) delay adoption.
16. ***Top Fears:*** Cyber insecurity, World War, misinformation, inflation, and extreme weather mirror global risk trends.
17. ***Age-Based Differences:*** Younger users fear AI risks and economic issues (e.g., unemployment); older groups prioritize health and migration.
18. ***Most-Feared Actors:*** Russia (53%), China (47%), North Korea (31%), and the USA (30%) are seen as top cyber threats. 15% fear their own country (domestic surveillance).

1. Where are you from[1]?



The graph above displays the top 20 countries[2] from which our survey participants originate. In total, respondents hailed from 93 different countries, which are illustrated on the map below.

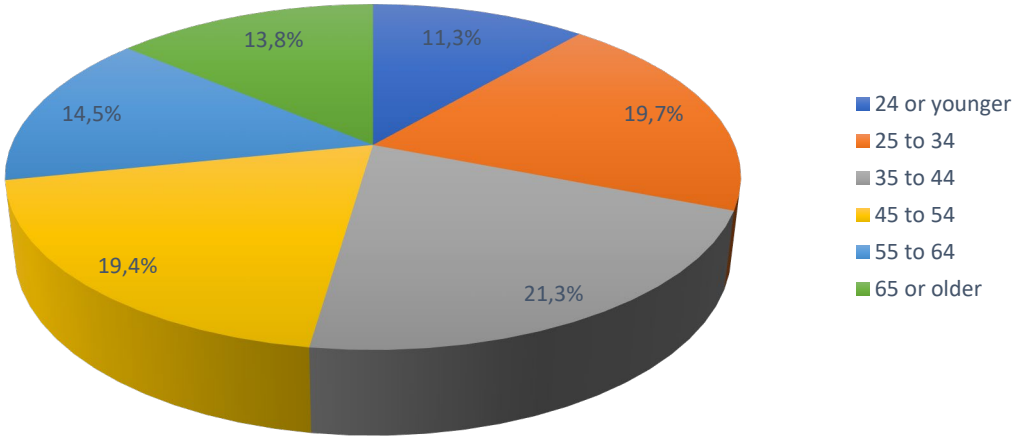


[1] In previous years, we received responses from more countries than this year. However, this year, responses from Russia, Ukraine, Belarus, and other regions could not be collected because SurveyMonkey had restricted access to its site. As a result, we were unable to make certain survey comparisons as in previous years. https://help.surveymonkey.com/en/surveymonkey/policy/export-control-policy/

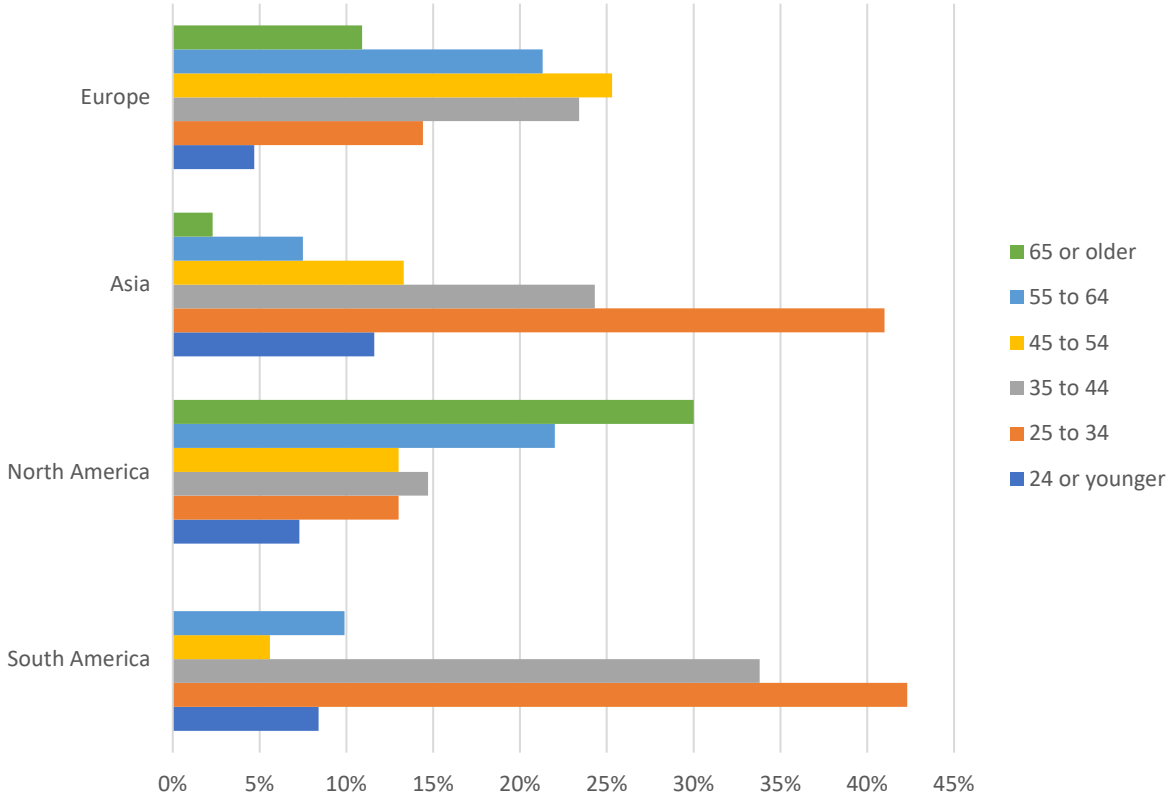
[2] There has been an increase in Chinese survey participants, who have also expressed their desire for Chinese vendors to be evaluated by non-Chinese testing labs.

2. How old are you?

The survey results reveal a wide age range among participants from various continents. The youngest group, aged 24 or younger, makes up a modest 11.3% of the total. The largest share of respondents belongs to the 35-44 age group, representing 21.3%. The 25-34 and 45-54 age groups are nearly equal, contributing 19.7% and 19.4%, respectively, reflecting a balanced distribution among middle-aged participants. Those aged 55-64 constitute 14.5%, while the oldest group, aged 65 or older, represents 13.8% of the total.

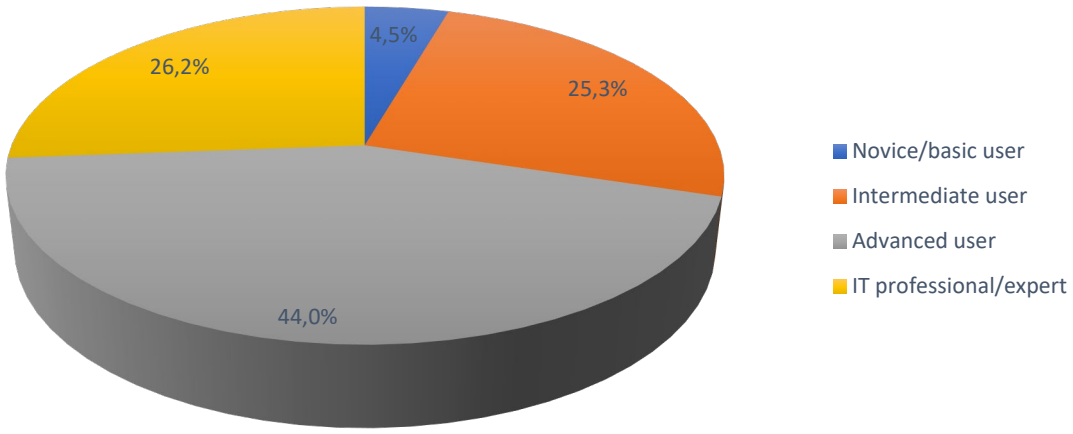


The overall age distribution is displayed above, with a breakdown by continent provided below. Geographically, North America has the oldest age profile, with 50% of participants aged 55 or older. This contrasts sharply with Asia and South America, where more than 75% of respondents are under 44 years old. Europe, on the other hand, shows a strong representation of middle-aged groups, with approximately 47% of participants falling between the ages of 35 and 54.



3. How would you rate your level of expertise in using computers?

The survey also explored the participants' self-assessed level of computer expertise, revealing insights into their technological proficiency. Overall technical expertise is shown in the chart below:

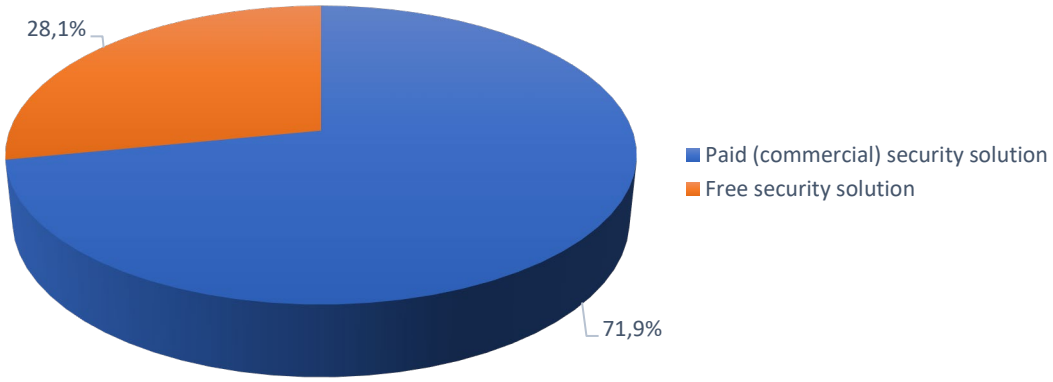


A small portion of participants, 4.5%, identified themselves as novice or basic users, suggesting limited familiarity or comfort with computer technology. This is considerably outweighed by those who described themselves as intermediate users, accounting for 25.3% of respondents. These individuals likely have a solid grasp of standard computer functions and applications.

The largest group, making up 44%, classified themselves as advanced users. These participants are presumably skilled in a wide range of computer functionalities and may have specialized knowledge in software and/or hardware. Finally, 26.2% of respondents identified as IT professionals or experts, reflecting a high level of proficiency and likely a strong involvement in computing as a key part of their career or daily life.

This distribution underscores a strong presence of tech-savvy individuals within the participant pool, with a significant proportion possessing advanced skills or professional expertise. This may explain why survey respondents' preferences, such as their choice of operating system or browser, differ from those of the general public.

4. Which type of desktop security solution do you primarily use?

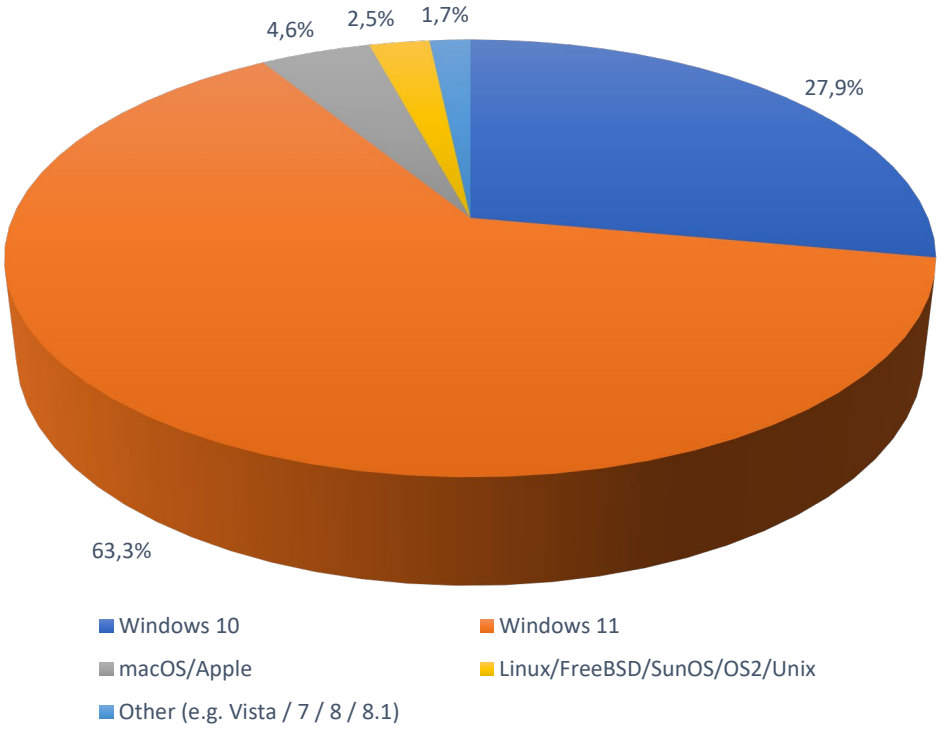


The survey's exploration of desktop security solutions used by participants highlights a clear preference for paid or commercial products over free alternatives, as illustrated in the chart above. Specifically, 71.9% of respondents reported using paid/commercial security solutions, while the remaining 28.1% opted for free versions.

An interesting age-related trend emerges in the choice of security solutions. Younger users, particularly those aged 34 or younger, show a greater inclination toward free security solutions, with approximately 31% using them. In contrast, only 22% to 26% of respondents over the age of 34 rely on free versions. This disparity may stem from factors such as financial priorities, differing perceptions of risk, or the extent of digital assets requiring protection.

Additionally, the survey reveals a correlation between users' self-assessed computer expertise and their choice of security solution. Among novice users, 36% use free solutions, while only 55% opt for commercial products. In contrast, advanced to expert users overwhelmingly prefer paid solutions, with 78% choosing commercial security options. This suggests that as users gain more knowledge and proficiency with computers, they may increasingly recognize the value and necessity of comprehensive, paid security solutions to safeguard against sophisticated threats.

5. Which desktop operating system do you primarily use?



The survey results for desktop operating system preferences among participants – depicted in the chart above – reveal a strong preference for Windows, with 91.2% of respondents using it. Specifically, 27.9% are on Windows 10, while a significant majority – 63.3% – have upgraded to Windows 11, making it the most widely used operating system version.

Only a small portion, 4.6%, use macOS, highlighting its niche presence within the participant pool. Linux, an open-source platform often favoured by tech enthusiasts, is used by 2.5% of respondents. The user base for both macOS and Linux is gradually growing, possibly reflecting broader industry trends or evolving user preferences. Other operating systems, including older versions of Windows such as 7 and 8, make up just 1.7%.

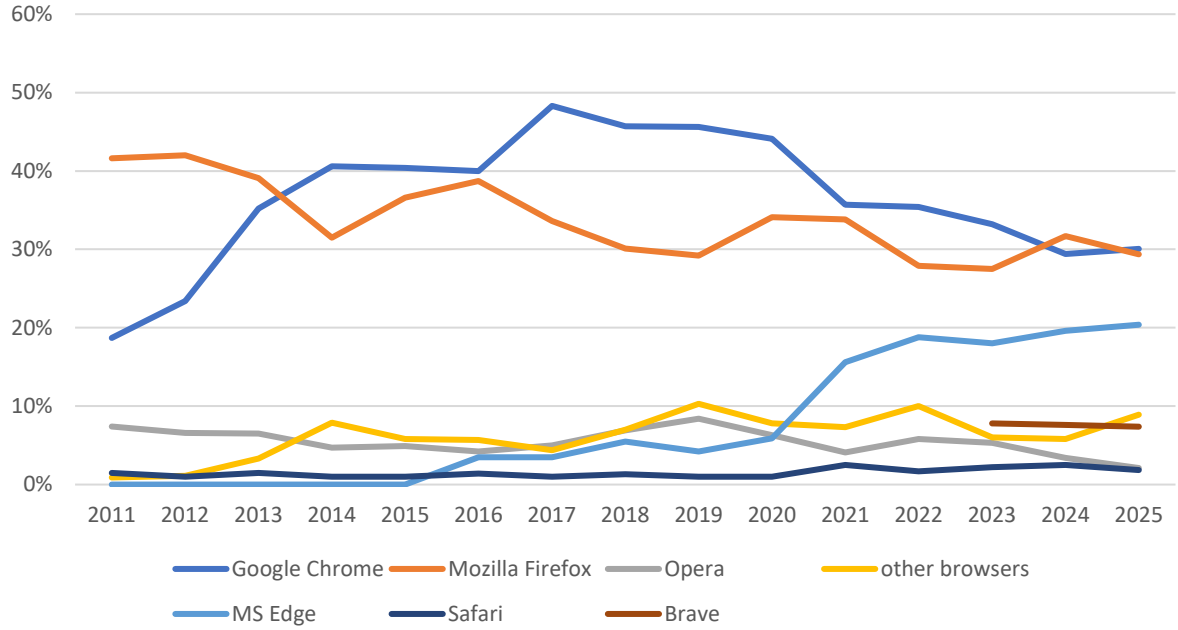
The survey also indicates that IT professionals are more likely to use macOS, suggesting a preference for this system in certain professional environments. Our review and testing of Mac security products[3] can be found at https://www.av-comparatives.org/consumer/testmethod/mac-security-reviews/.

At AV-Comparatives, we plan to adopt Windows 11 as the primary operating system for our 2025 tests. Additionally, it's worth noting that Microsoft will only provide mainstream support for Windows 10 until October 2025, though paid security updates will continue for an additional three years[4].

[3] A list of Mac security products can be found here: https://www.av-comparatives.org/list-of-av-vendors-mac/

[4] https://techcommunity.microsoft.com/t5/windows-it-pro-blog/plan-for-windows-10-eos-with-windows-11-windows-365-and-esu/ba-p/4000414

6. Which browser do you primarily use?



As illustrated in the diagram above, Google Chrome is used by 30.1% of respondents. Mozilla Firefox, which briefly overtook Chrome as the most popular browser last year, now trails slightly behind, with 29.3% of respondents using it as their primary browser. Microsoft Edge continues to solidify its position, with 20.4% of users adopting it.

This shifting browser landscape highlights a diversification of user preferences, likely influenced by factors such as performance, privacy concerns, or specific feature sets. The results also highlight the growing relevance of the Brave browser, which is used by 7.4% of respondents, surpassing other options like Opera, Safari, Vivaldi, Yandex, and DuckDuckGo. This indicates a rising interest in privacy-focused browsing solutions among a segment of users.

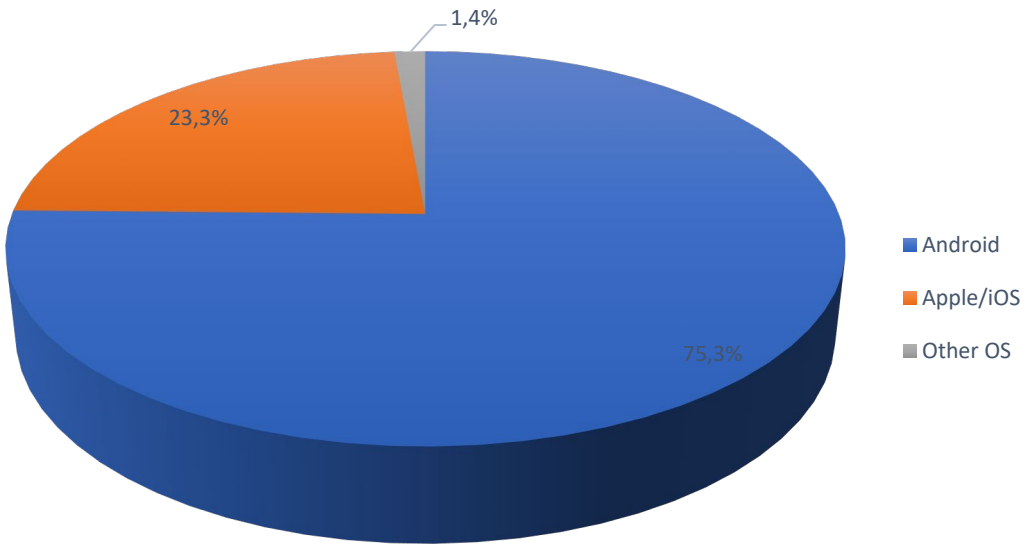
While statistics show that Google Chrome remains the most popular browser among the general public, accounting for nearly two-thirds of all users, we at AV-Comparatives continue to use Chrome in our tests due to its widespread adoption.

The data also reveals differences in browser preferences based on user expertise. Novice and basic users predominantly favor Microsoft Edge, with 38% of this group choosing it. In contrast, more advanced users tend to prefer Mozilla Firefox, aligning with its overall popularity in the survey. Advanced users also show a stronger inclination toward niche browsers like Brave, likely reflecting their preference for customization, privacy, or specialized functionalities.

Among macOS users, Safari usage has declined to 37%, down from over 50% in previous years. Chrome and Firefox are now used by 17% and 25% of macOS users, respectively.

Given the increasing diversity in browser usage, we encourage AV vendors to ensure their browser plug-ins, particularly those for URL-blocking features, are compatible with a wide range of browsers, not just the most popular ones. This will help deliver comprehensive security solutions that cater to the varied preferences of users across different browsers and operating systems.

7. Which mobile operating system do you use?



The survey offers a detailed look at mobile operating system preferences among participants. As shown in the chart above, Android dominates globally, accounting for approximately 75% of users. This widespread adoption highlights Android's accessibility and its diverse ecosystem, which caters to a broad range of devices across various price points.

A notable correlation exists between users' technical expertise and their choice of mobile operating system. Advanced and professional users show a stronger preference for iPhones, with 31% using iOS, compared to just 19% among basic and novice users. This inclination may be driven by factors such as security features, build quality, or specific functionalities that appeal to more tech-savvy individuals.

Our Mobile (Android) security review and test report can be accessed at https://www.av-comparatives.org/consumer/testmethod/mobile-security-reviews/.

8. Which mobile anti-malware security solution do you primarily use on your smartphone?

The survey's findings on the use of mobile anti-malware security solutions highlight a significant divide in cybersecurity practices across different user groups. Overall, 39.3% of respondents do not use any security solution on their mobile devices. This substantial percentage may reflect a combination of trust in built-in security features, limited awareness of mobile threats, or a perceived inconvenience of installing additional security software.

Interestingly, IT professionals are the most likely to forgo mobile security solutions, with 43% not using any. This could stem from their advanced expertise and confidence in managing mobile risks manually, or a preference for maintaining optimal device performance without additional software. In contrast, only about 35% of novice or basic users do not use any security solution, though this gap has narrowed compared to previous years' surveys.

Globally, the ten most used mobile security manufacturers, in descending order, are: Bitdefender, Kaspersky, ESET, Avast, Norton, McAfee, Sophos, F-Secure, AVG, Avira, and Malwarebytes.

The list below highlights the ten most popular mobile security manufacturers used by survey participants, broken down by continent. Due to insufficient responses from certain regions, Australia/Oceania and Africa are not included in the breakdown.

Europe	North America	Asia	South/Central America
1. Bitdefender	1. Bitdefender	1. Kaspersky	1. Kaspersky
2. Kaspersky	2. ESET	2. Bitdefender	2. Bitdefender
3. ESET	3. Avast	3. ESET	3. Avast
4. Avast	4. Norton	4. Avast	4. ESET
5. Norton	5. Malwarebytes	5. McAfee	5. McAfee
6. McAfee	6. Sophos	6. Norton	6. Emsisoft
7. F-Secure	7. F-Secure	7. AhnLab	7. Panda
8. Sophos	8. McAfee	8. Sophos	8. AVG
9. Avira	9. Avira	9. Avira	9. Avira
10. AVG	10. Lookout	10. Dr.Web	10. F-Secure

Bitdefender, ESET and Avast were among the most popular mobile security products in all four regions. Since the sale of Kaspersky is prohibited in US since the 20th of July 2024[5], it is not surprising that it is no longer among the top ten security products in North America. Kaspersky is still among the top two most popular security products in the other three regions.

Major security products for mobiles were reviewed by AV-Comparatives in a report[6] in 2024.

[5] https://oicts.bis.gov/kaspersky/
[6] https://www.av-comparatives.org/testmethod/mobile-security-reviews/

9. Which desktop anti-malware security solution do you primarily use?

Globally, the twelve most commonly used manufacturers of anti-malware products for Windows platforms among survey participants are (in order): Microsoft, Kaspersky, Bitdefender, ESET, Avast, Norton, F-Secure, McAfee, Avira, Malwarebytes, AVG, and Trend Micro.

Across all four continents with significant results, the same four vendors consistently appear in the top five positions. These are (in alphabetical order): Avast, Bitdefender, ESET, and Microsoft. Notably, Microsoft has now claimed the top spot in North America.

Meanwhile, Kaspersky has regained first place in Europe after being briefly overtaken by Bitdefender last year. Kaspersky also remains the most popular desktop security solution in Asia and South/Central America. Since the sale of Kaspersky is prohibited in US since the 20th of July 2024, it is not surprising that it is no longer among the top ten security products in North America. Kaspersky is still among the top two most popular security products in the other three regions.

Differences between continents

The table below shows the twelve products most commonly used by survey participants, by continent:

Europe	North America	Asia	South/Central America
1. Kaspersky	1. Microsoft	1. Kaspersky	1. Kaspersky
2. Bitdefender	2. Bitdefender	2. Microsoft	2. Microsoft
3. Microsoft	3. ESET	3. Bitdefender	3. Bitdefender
4. ESET	4. Avast	4. ESET	4. ESET
5. Avast	5. Norton	5. Avast	5. Avast
6. Norton	6. Malwarebytes	6. Norton	6. Malwarebytes
7. F-Secure	7. McAfee	7. Avira	7. F-Secure
8. Avira	8. AVG	8. Qihoo	8. Norton
9. McAfee	9. F-Secure	9. Tencent	9. AVG
10. Sophos	10. Trend Micro	10. Trend Micro	10. Avira
11. AVG	11. Sophos	11. K7	11. McAfee
12. G Data	12. Panda	12. AhnLab	12. Panda

10. Which VPN solution do you primarily use?

The most popular VPN programs are listed below in order of preference:

1. Proton VPN
2. NordVPN
3. Kaspersky VPN
4. SurfShark
5. VPN of my employer/company OR self-hosted VPN
6. Bitdefender VPN
7. Windscribe
8. Avast SecureLine
9. Mullvad VPN
10. Norton VPN
11. Private Internet Access
12. F-Secure Freedome
13. AVG Secure VPN
14. AdGuard VPN
15. ExpressVPN
16. CyberGhost

The survey explored the use of Virtual Private Networks (VPNs) among participants to gauge preferences for these online privacy and security tools. Notably, 35% of respondents do not use a VPN, which may stem from a lack of perceived need, confidence in their existing network security, or limited familiarity with the technology.

Among those who use VPNs, preferences vary widely. Proton VPN emerges as the most popular choice, likely due to its free version. NordVPN and Kaspersky VPN follow closely, both known for their extensive server networks, while SurfShark and Bitdefender VPN also rank among the top choices.

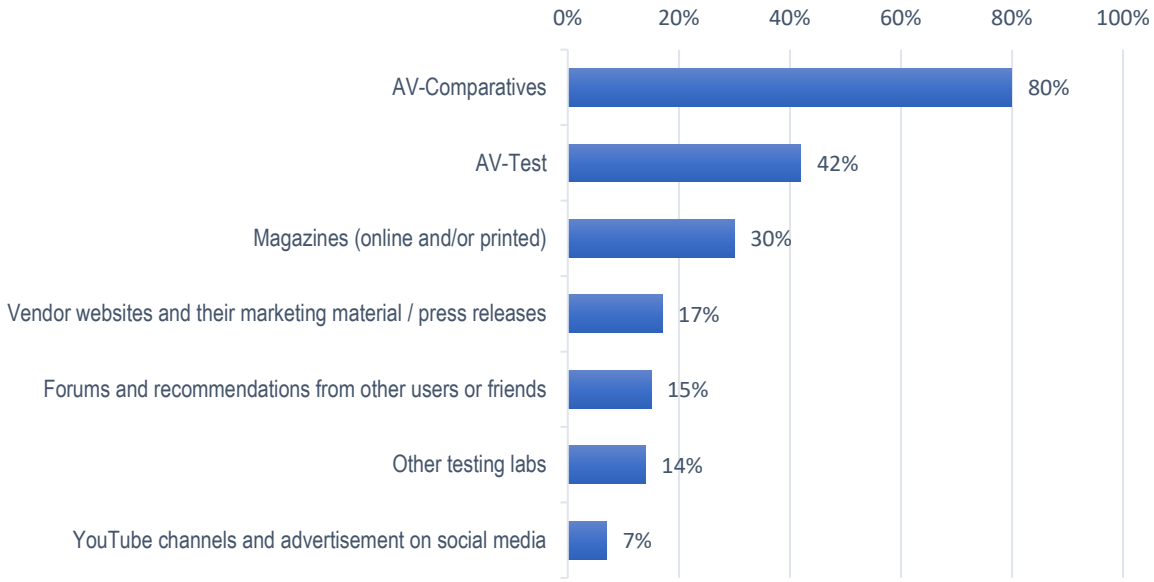
An interesting trend is the use of employer/company-provided VPNs or self-hosted solutions, reflecting the needs of remote workers or those who prefer a more customized and controlled security approach. This category ranks fifth, indicating a significant number of users rely on VPNs for professional or tailored use. It's important to note that employer/company-provided VPNs primarily enable remote users to access their organization's local network resources as if they were on-site. This differs from the typical private user's focus on data privacy and bypassing geolocation restrictions.

The list continues with other reputable VPN services, including F-Secure Freedome, Avast SecureLine, Mullvad, SurfShark, ExpressVPN, CyberGhost, Avira Phantom VPN, Private Internet Access, and Cisco AnyConnect. The diversity of preferred services highlights distinct user preferences, likely influenced by factors such as specific features, pricing, or recommendations. Additionally, some vendors offer security suites that include anti-virus and other functions, making users of these suites more likely to adopt the VPN solution provided by the same vendor.

These findings illustrate the varied landscape of VPN usage and preferences among tech-savvy individuals. They also underscore the growing importance of privacy and security in the digital realm, with users seeking solutions tailored to their specific needs—whether for personal privacy, bypassing geo-restrictions, or ensuring secure remote work connections.

At AV-Comparatives, we have certified a wide range of VPN products, the reports are available here:
https://www.av-comparatives.org/wp-content/uploads/2024/12/kaspersky_vpn_2024.pdf
https://www.av-comparatives.org/wp-content/uploads/2024/12/norton_vpn_2024.pdf

11. What are your main sources for anti-virus/security test results?



The most trusted sources for AV/security test results are listed above in order of preference. It's important to note that respondents were asked to provide their answers in an empty text box, ensuring that the responses reflect the sources they genuinely use rather than being influenced by pre-selected options.

The responses reveal a diverse landscape of preferences and trust, with certain key players standing out in the industry. AV-Comparatives is the most prominent, mentioned by 80% of respondents, indicating a high level of credibility and trustworthiness among users. We believe this reflects our commitment to independence from vendor influence, our comprehensive and meticulously designed testing methodologies, the significant number of samples we use, our transparency, and the detailed, freely available test reports we provide. Additionally, our policy of allowing other publications to cite our results (with proper attribution) further enhances our visibility and reach.

AV-Test ranks as the second most popular source, used by 42% of respondents. The fact that a majority of users rely on both AV-Comparatives and AV-Test highlights a preference for established testing labs with over two decades of experience in the field of AV testing. This underscores the importance of trust, reliability, and a proven track record in shaping user confidence in test results.[7]

International magazines, both online and printed, such as PCmag, ComputerBILD, PC World, Heise c't, CHIP, Security.nl, TechRadar, BleepingComputer, and Comss.ru among others, are also significant sources, mentioned by 30% of respondents.

Other notable sources include vendor websites[8] and their marketing materials, forums (such as MalwareTips, Wilders Security, Rokop Security, etc.), recommendations from peers, YouTube channels[9], social media advertisements, other testing labs like MITRE-Engenuity, Virus Bulletin, SE Labs, MRG-Effitas, AVLab, and as well as analyst-firms such as Gartner, Forrester, and Frost & Sullivan.

[7] https://www.av-comparatives.org/spotlight-on-security-why-independent-testing-of-anti-virus-software-is-important/
[8] https://www.av-comparatives.org/blogs-of-security-vendors-news-sites/
[9] https://www.av-comparatives.org/youtube-security-channels/

When it comes to demographics, IT professionals, experts, and advanced users consistently rank testing labs like AV-Comparatives and AV-Test among their top sources for credible information. We view this as a strong endorsement of professional, independent testing agencies by those with technical expertise.

In contrast, novice and basic users are more likely to rely on vendor websites, potentially placing greater trust in marketing claims. Younger respondents, particularly those under 25, tend to favour forums and peer recommendations, while also showing a strong preference for YouTube channels and social media advertisements when seeking information about anti-virus and security products. This highlights the growing influence of online media on the decision-making processes of younger audiences. Meanwhile, users aged 25-34 are more inclined to turn to forums and recommendations from friends or other users for guidance.

As part of the survey, we gathered feedback from participants about their preferred sources of AV information. Users particularly appreciate AV-Comparatives' reports for their clarity, detailed explanations of methodologies, and comprehensive testing across multiple product aspects. The availability of these reports free of charge, including downloadable PDF versions, is highly valued. Respondents also commend AV-Comparatives for its balanced approach to testing, including the evaluation of false positives, and for not universally awarding top or excellence rankings to all tested products—unlike some other labs in recent years. This approach helps users make meaningful distinctions between products, further solidifying trust in our testing processes.

12. Which CONSUMER/HOME-USER desktop security solutions would you like to see in our yearly public consumer main-test series?

Below are the 15 most-requested consumer/home-user products:

1. Bitdefender
2. ESET
3. Microsoft
4. Kaspersky
5. Avast
6. Norton
7. Avira
8. Malwarebytes
9. F-Secure
10. McAfee
11. Trend Micro
12. AVG
13. Sophos
14. G Data
15. Panda

13. Which BUSINESS/ENTERPRISE desktop security solutions would you like to see in our yearly public enterprise main-test series?

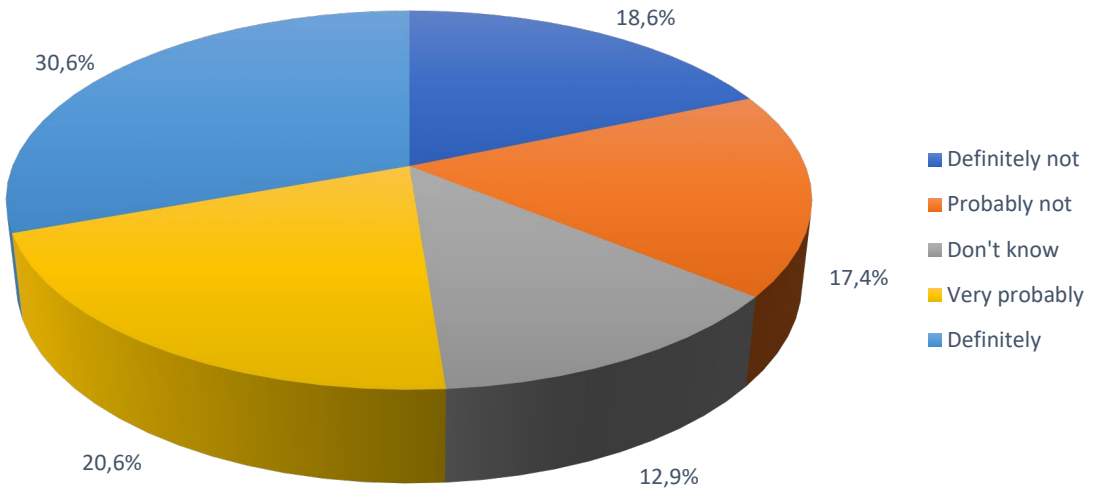
Below are the 20 most-requested business/enterprise products:

1. Bitdefender
2. ESET
3. Microsoft
4. Kaspersky
5. Avast
6. Sophos
7. CrowdStrike
8. Trend Micro
9. Malwarebytes
10. Cisco
11. Check Point
12. Fortinet
13. SentinelOne
14. Palo Alto Networks
15. G Data
16. Broadcom (Symantec)
17. Trellix
18. WithSecure
19. WatchGuard
20. VIPRE

Most of the popular vendors are usually included in at least some of our public tests and reviews of consumer and business software[10], while most of the other vendors commission separate tests and/or participate privately in certain tests.

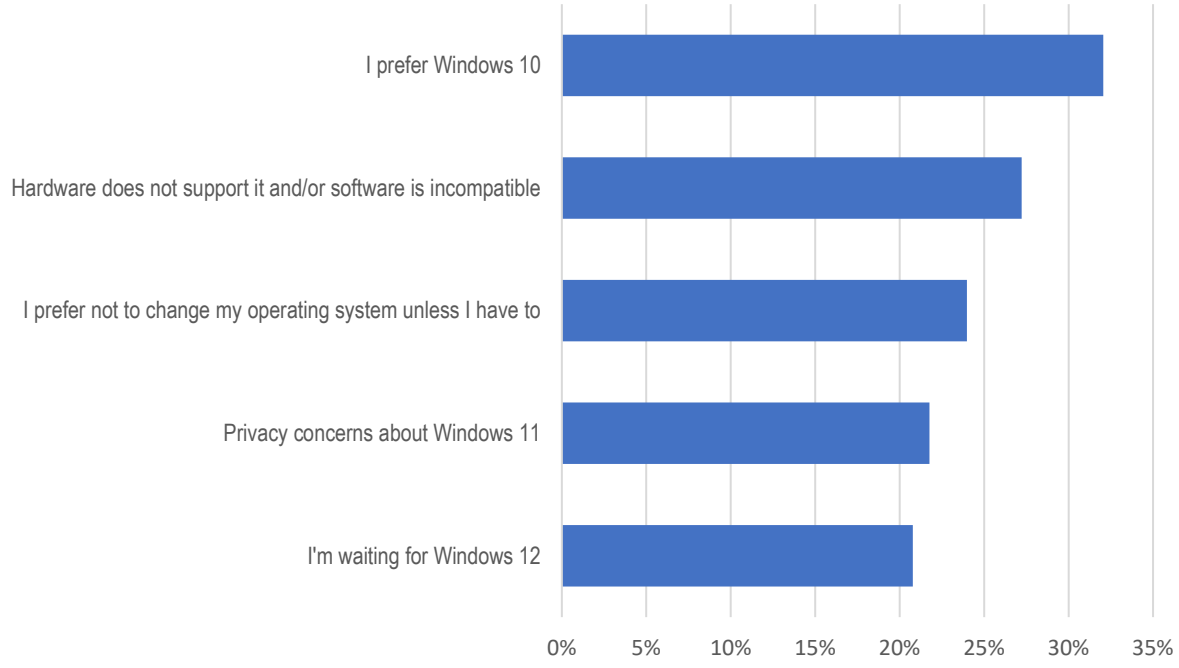
[10] Consumer: https://www.av-comparatives.org/consumer/
Enterprise: https://www.av-comparatives.org/enterprise/

14. If you're not already using it, how likely is it that you will switch to Windows 11 in the next 12 months?



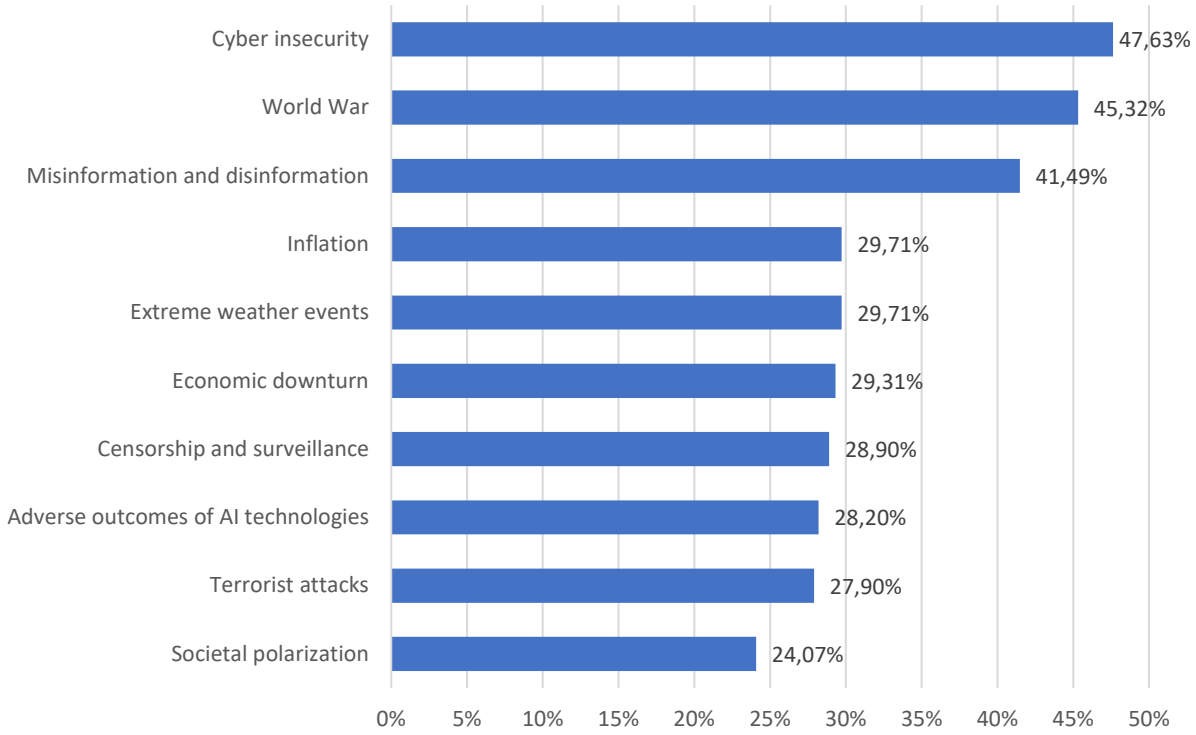
Over half of the respondents say, that they plan on making the switch to Windows 11 in the next year. This further cements our choice to use Windows 11 as the primary operating system for our 2025 tests. More experienced users are more likely to make to the switch, indicating that these users might be more confident in upgrading their operating system and might be more interested in the new features.

15. If not, why not?



The top five reasons for users not wanting to make the switch are shown in the graph above. The most common reason given by 32% of respondents is that users simply prefer Windows 10. This followed closely by hard and software compatibility issues with Windows 11.

16. What are your five greatest concerns for the next two years?



This year we asked survey participants about their fears for the future. The options given are like those given in the WEF's Global Risk Survey of 2024[11]. Four of the top five threats are identical between the respondents of both surveys: Cyber insecurity, World War, Misinformation and disinformation, Inflation, and Extreme weather events. A key difference being that respondents to our survey rank Cyber Insecurity higher. This is likely because our readers are more informed of the continuously developing threat landscape. In general, our readers seem to be more concerned about issues related to technology. Worries about adverse outcomes of AI technologies ranks eighth amongst our respondents but 29th among respondents of the WEF survey. This also applies to censorship and surveillance, ranked 7th amongst our respondents and only 21st among WEF respondents. Since 60% of survey participants rank themselves as advanced or expert users it seems reasonable to assume that those with more contact with technology are more likely to also see the threats that come with them.

Comparing the responses for different age groups reveals certain concerns being more prevalent among younger respondents. For example, those under the age of 25 are more concerned about Adverse outcomes of AI technology and Censorship & surveillance. Similarly, the younger generations are more concerned about economic threats such as inflation, debt, unemployment and lack of economic opportunity. The older generations are significantly less concerned about these issues. The most likely reason for this is that older generations are likely to already be in retirement and therefore less concerned about employment and other more long-term issues as they will not be as affected by these.

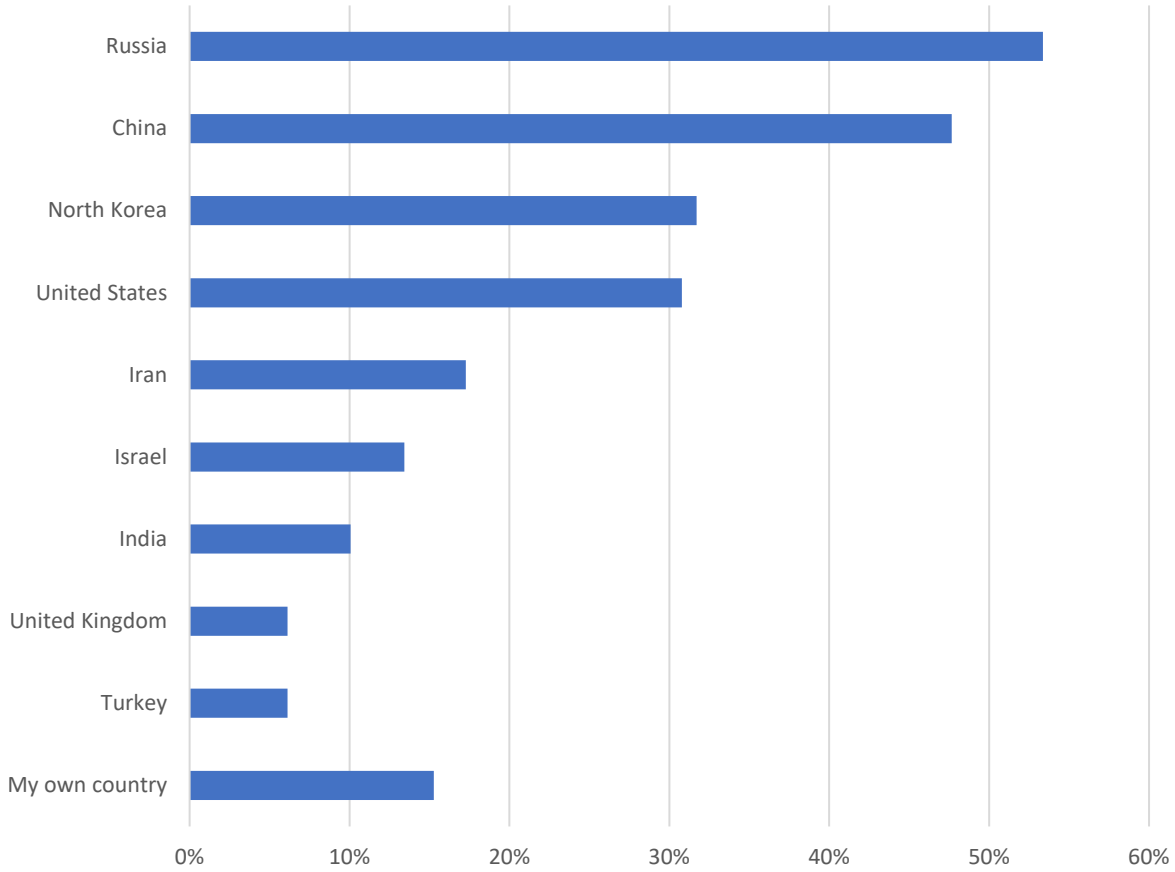
Concerns, which are more common among the older generations are worries about Chronic health conditions and involuntary migration. Similarly, less than 40% of respondents under the age of 55 are concerned about misinformation and disinformation whereas 50% of those 55 and older are concerned about this.

[11] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf

Our survey also revealed that respondents with a higher degree of technical proficiency are more concerned about technological threats. For example, 26% of respondents are describing themselves as novice or basic users are concerned about censorship and surveillance. This number rises the more experienced users are, reaching 33% amongst expert users. Similarly, 32% of novice users are concerned about misinformation and disinformation, this number rises to 50% among the most experienced user group. IT professionals and expert users are also almost twice as concerned with technological power concentration.

There are also some key differences regarding concerns, based on the continent of the respondent. Amongst respondents from Australia/Oceania and South/Central America concerns about biodiversity loss are twice as common compared to other continents. Similarly, survey participants from these continents are also more concerned about critical changes to earth systems. One likely explanation for this is that the global south is already more affected by climate change and will likely more affected in the future as well. This is likely also the reason for respondents from Africa being more concerned with extreme weather events, 47%, compared to those from other continents, 30%. Lastly, respondents from Europe and Asia are more concerned about the potential of a third world war compared to those from other countries. With the ongoing conflicts between Russia and Ukraine and surrounding Israel nearby it is of no surprise that these concerns are more present here.

17. Which country or entity, including both governments and individuals within that country, do you fear the most in terms of the potential for a cyberattack on your personal or organisational data?



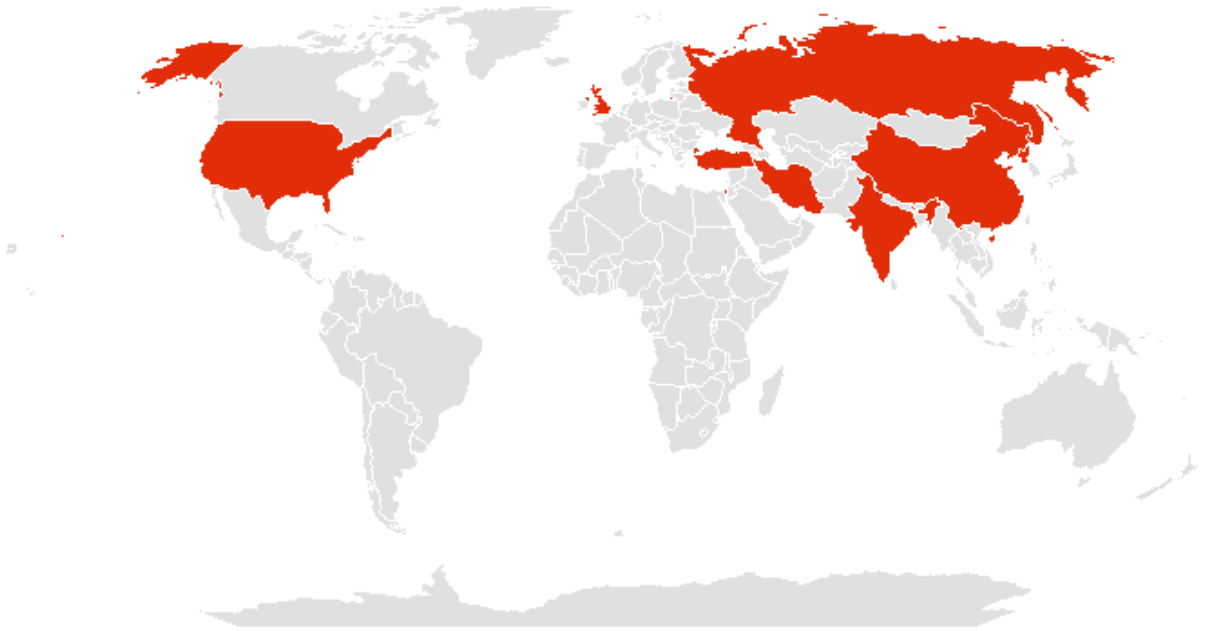
The survey reveals a geopolitical landscape[12] of perceived cyber threats, as shown in the graph above. Russia tops the list, with 53% of participants identifying it as the primary source of concern for cyberattacks. China follows at 47%, while North Korea and the USA are cited by 31% and 30% of respondents, respectively. These results reflect widespread concerns about the cyber capabilities of these nations. [13]

Interestingly, 15% of respondents cited their own country, reflecting concerns about domestic surveillance, data privacy laws, or mistrust in local governments and corporations[14]. This highlights awareness of internal threats and the impact of national policies on privacy and security. The list also includes Iran, Israel, India, the UK, and Turkey, representing diverse geopolitical powers and regions, each seen as contributing to global cyber tensions and uncertainties.

Due to SurveyMonkey restrictions in certain countries (see footnote on page 4), the responses may be influenced by the countries that were able to participate and those that could not (see question number 1).

[12] https://www.av-comparatives.org/spotlight-on-security-politics-and-cyber-security-a-troubled-relationship/
[13] https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/
[14] https://www.av-comparatives.org/av-comparatives-explains-the-implications-of-takeovers-in-the-it-security-industry/

Map of the topmost feared countries



Most feared countries by continent of respondent

Asia	Europe	North America	South America
China	Russia	Russia	China
USA	China	China	Russia
Russia	USA	North Korea	USA
North Korea	North Korea	USA	North Korea
Own country	Iran	Own country	Own country
India	Israel	Iran	Israel
Israel	Ukraine	Israel	Iran
Pakistan	India	India	UK
Iran	Turkey	Ukraine	India

Breaking down fears by continent, the survey reveals regional differences in threat perceptions. China is most feared in Asia and South America, while Russia tops the list in Europe and North America. Respondents' own countries rank fifth in most regions, except in Europe. The four most feared countries - China, North Korea, Russia, and the USA - remain consistent across all regions. Factors like political relations, media coverage, historical cyber incidents, or geographic proximity likely shape these perceptions. For instance, North Americans fear China, while Asians fear their own countries, highlighting the complex and varied nature of cyber-threat perceptions globally.

Most feared countries by country of respondent

Brazil	China	Germany	India	Italy	UK	USA
Russia	China	Russia	China	Russia	Russia	Russia
China	USA	China	USA	China	China	China
USA	Russia	North Korea	Pakistan	USA	North Korea	USA
Brazil	India	USA	India	North Korea	USA	North Korea
North Korea	Israel	Iran	Russia	Israel	Iran	Iran

Among the seven countries with the most respondents, the top four most-feared countries consistently included China, Russia, and the US. Except for Germany, Italy, and the UK, respondents also cited their own country as a source of concern.

The survey underscores a global sense of vulnerability and concern over cyberattacks from various actors, reflecting awareness of the capabilities and historical actions of specific nations in the cyber domain. For governments, organizations, and individuals, understanding these perceptions is vital for shaping cybersecurity strategies, international policies, and cooperative efforts to mitigate threats and reassure the public. It also highlights the need for robust, transparent, and trust-building measures within countries to address domestic concerns about privacy[15] and cyber security.

[15] https://www.av-comparatives.org/data-transmission-in-consumer-security-products/

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives
(February 2025)