VPN Comparative Test

A test commissioned by Kaspersky and performed by AV-TEST.
Date of the report: October 18th, 2025.

Executive Summary

A comparative assessment of Virtual Private Network (VPN) solutions was carried out in February 2025 by AV-TEST GmbH, commissioned by Kaspersky. This evaluation aimed to measure the performance of selected VPN services against unencrypted reference connections, as well as to review their included features, implemented security, IP protection capabilities, and the public transparency of the vendor behind the product. The key performance indicators included download and upload speeds, torrent download performance and measured latency across a range of local and overseas geographical test locations. All tests were conducted over a full week, with multiple runs each day for every product, providing a current overview of their capabilities. The test was done in close alignment with the newly developed AMTSO VPN Guideline, in which development AV-TEST contributed.

The VPN products evaluated for 2025 were: Avast SecureLine VPN, CyberGhost VPN, ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Norton Secure VPN, Proton VPN, Surfshark, and Turbo VPN. The report is prepared with no exclusion of any result reached by any of the products initially requested into the test.

The 2025 tests revealed varied performance across the different VPN services.

For local connections, Kaspersky VPN and Kaspersky Premium demonstrated strong download speeds, with Surfshark also performing well. For local upload, Kaspersky VPN, NordVPN and Kaspersky Premium were among the top performers. In terms of local latency, Avast SecureLine VPN, CyberGhost VPN, Norton Secure VPN, NordVPN, Surfshark, Kaspersky VPN and Kaspersky Premium recorded the lowest values. For local torrent downloading, Kaspersky Premium and Kaspersky VPN significantly outperformed the tested products, with Surfshark coming in third with over 10% less performance. Avast SecureLine VPN and Norton Secure VPN were excluded from torrent performance results, as the tested servers do not support torrenting.

For overseas connections, Kaspersky Premium, Kaspersky VPN and Surfshark led in download performance. ExpressVPN and NordVPN exhibited strong upload speeds, followed by Kaspersky VPN and Kaspersky Premium. Kaspersky VPN and Kaspersky Premium also recorded the lowest latency for overseas connections. For overseas torrent downloading, Kaspersky VPN and Kaspersky Premium once again significantly outperformed the other tested products, only switching positions while outperforming the third-placed product, Proton VPN, by over 10%. Avast SecureLine VPN and Norton Secure VPN were excluded from torrent performance results, as the tested servers do not support torrenting.

The findings indicate that while using a VPN generally leads to some performance reduction compared to an unencrypted connection — due to the overhead of encryption and routing traffic through remote servers — the extent of this impact varies noticeably between different products and connection types.

The graph below reflects the overall efficiency of each solution in user-based scenarios — the higher the score, the more efficient the product. The Combined Score Ranking is calculated using absolute

results across key scenarios (Download, Upload, Latency, and Torrent) for each of the product in both Local and Overseas routes. The calculation method is detailed in Chapter 3.5, which also provides individual rankings for each scenario.

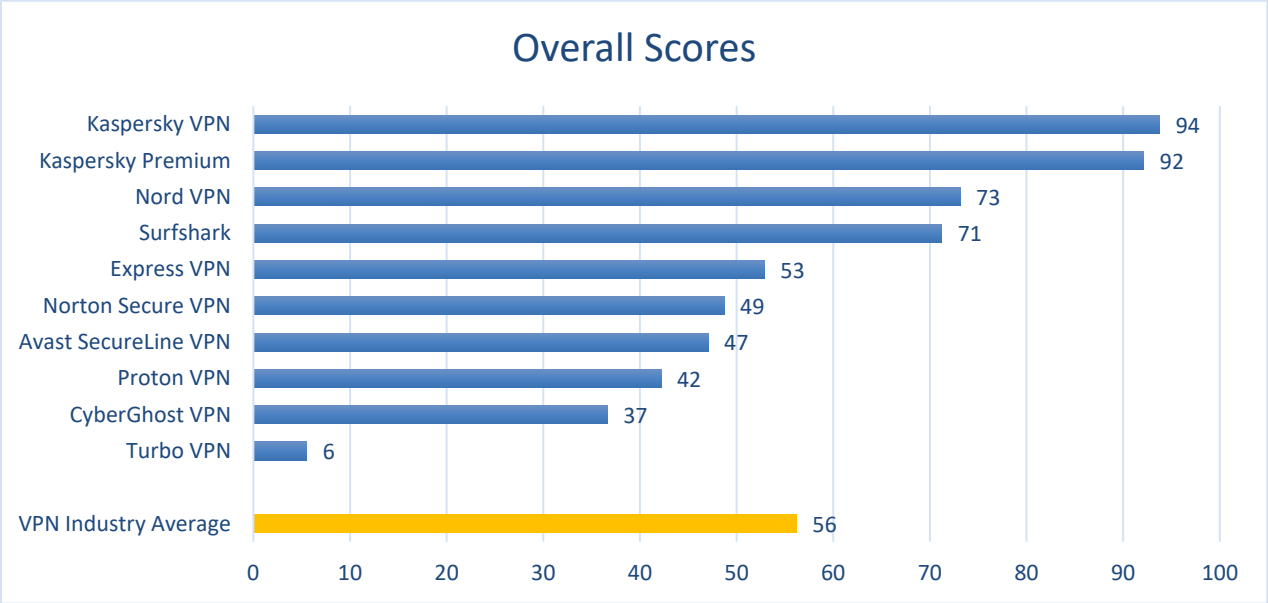

*Figure **1**, the Combined Score Ranking, based on all measured parameters (Download, Upload, Torrent, Latency, both local and Oversea) for each of the tested solution (the more the better).*

Thanks to the outstanding performance of Kaspersky VPN Secure Connection and Kaspersky Premium, as reflected in the test results, both products successfully met all certification criteria and are awarded with the AV-TEST APPROVED VPN certification.

This test report complements the long-standing track record of regular evaluations of Kaspersky's VPN solutions by AV-TEST.[1]

[1]
2020: https://www.av-test.org/en/news/6-vpn-packages-put-to-the-test-under-windows-10/
2021: https://www.av-test.org/en/news/vpn-packages-for-private-users-put-to-the-test-under-windows-10/
2022: https://www.av-test.org/en/news/vpn-packages-put-to-the-test-more-security-and-anonymous-paths/
2022: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_VPN_Test_Report_December_2022.pdf
2023: https://www.av-test.org/en/news/kaspersky-vpn-test-report-2023/
2024: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_VPN_Test_Report_December_2024.pdf
2024: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_Premium_VPN_Test_Report_December_2024.pdf

Contents

1. Test Methodology

The test was carried out as described in the executive summary. No results were omitted — all requested products were tested, and all outcomes reported as measured. The testing process was fully independent.

1.1. Tested Solutions

The tested products are listed below.

- Avast SecureLine VPN(version 24.12.10985) from Gen Digital Inc.
- CyberGhost VPN (version 8.4.10.14516) from CyberGhost
- ExpressVPN (version 12.95.0 (42)) from Express Technologies
- Kaspersky VPN (version 21.19.7.527-1) from Kaspersky
- Kaspersky Premium (version 21.19.7.527 (a)) from Kaspersky
- NordVPN (version 7.31.8.0) from NordVPN
- Norton Secure VPN (version 24.11.9725 (build 24.11.9725.903)) from Gen Digital Inc.
- Proton VPN (version 3.5.1) from Proton
- Surfshark (version 5.12.2) from Surfshark
- Turbo VPN (version 2.26.0.0) from INNOVATIVE CONNECTING

All tests were performed on Windows 11 Pro (English, 64-Bit).

1.2. Performance Test Scenarios

The performance measurement methodology for this evaluation aligns with that used for public VPN certification tests. The test was done in close alignment with the newly developed AMTSO VPN Guideline, in which development AV-TEST contributed.

In the performance test, we run the following measurement scenarios:

1. **Download and Upload Speed, Latency**: These performances were measured using a third-party command-line application provided by speedtest.net. The testing tool was configured to independently select the optimal server test location. For consistency, the server IDs selected during the unencrypted reference tests were reused for testing encrypted VPN connections to the same overseas locations.
2. **Torrent**: Torrent download speed was measured using a third-party torrent client. The final test time was recorded as the duration between the start of the torrent download and the completion of writing the torrent file to the hard drive.

All VPN solutions were tested for both local and overseas traffic. For local traffic tests, both the client and the server were situated in the same geographical location. For overseas traffic tests, performance was measured for connections between different geographical locations. Three geographical locations were utilised for the tests: a US location on the West Coast, a European location in the Netherlands, and an East-Asian location in Japan. Each product was tested across all three VPN locations. Performance tests were conducted multiple times a day for one week to account for variations in network load across different geographical areas and times of day.
When the VPN location matched the geographical test location, the "default connection" was selected; otherwise, the VPN location was manually chosen to connect to the previously mentioned overseas VPN server locations. The selected VPN locations were in geographical proximity to the Virtual Machine (VM) host location. It is noted that not all products permit such specific server selections, often allowing only country-level choices.

Additionally, tests for all described scenarios were performed on a reference system without an active VPN in all three geographical locations, using the same testing tools. These results served as benchmarks for comparing and evaluating the VPN products.

1.3. Qualitative Evaluation Scenarios

The methodology for the qualitative evaluation was designed to assess usability, security, and transparency on the Windows platform. The following scenarios were conducted.

1.3.1. Usability and Feature Assessment

Scenarios were conducted testing the automatic reconnection feature after a system reboot and the practical application of split-tunnelling for excluding specific applications from the VPN tunnel. The client's ability to automatically protect a connection on an unencrypted Wi-Fi network was also evaluated. A review of provider-supplied information was performed to document OS compatibility and server network size. Finally, a practical test was conducted to determine the service's ability to access geo-blocked streaming content from the US, specifically Netflix.

1.3.2. Security and Connection Integrity Tests

A series of tests were performed to measure data protection. This involved conducting DNS, IP address, WebRTC, and email header analyses to identify any potential data leaks. The effectiveness of P2P and torrent protection was measured by checking if the user's location could be determined. The reliability of the kill switch was assessed through simulated network interruptions, including disabling the network adapter and disconnecting the network cable for set durations, to measure its response time and effectiveness in preventing data exposure.

1.3.3. Privacy Specification and Transparency Review

An assessment of the provider's technical specifications and organisational transparency was conducted. This involved a review of the company's documentation on available tunnelling protocols, the stated data encryption standard, and any built-in blocking capabilities for ads or trackers. The review also included an analysis of public transparency reports, the status of any warrant canary, and the scope and findings of relevant third-party security audits. The company's corporate structure, jurisdiction, and privacy policy were examined for compliance with data protection principles like the GDPR.

1.4. Configuration

The tests were performed on Virtual Machines hosted on Microsoft Azure cloud computing service. All test devices had guaranteed identical hardware configurations. All patches available up to February 2025 were installed prior to test.

A few general principles were adhered to:

(1) **Product cloud/Internet connection:** Internet access was available to all tested products.

(2) **Product configuration:** All products were run with their default, out-of-the-box configuration, including the default protocol used.

1.5. Limitations

The performance figures are captured at a specific point in time and may not entirely represent average performance over extended periods. Furthermore, the tests were conducted in parallel across all locations, which implies that the workload may have varied for each location due to different times of the day. Nevertheless, the results offer a good indication of the capabilities and services provided by the different VPN providers.

2. Industry Average

Using a Virtual Private Network (VPN) connection almost always results in a performance reduction when compared to an unencrypted connection. This is an expected characteristic due to the nature of the technology.

2.1. Industry Average: Download and Upload

For local connections, the average download speed for VPNs was approximately 1412 Mb/s, while the average upload speed was around 1610 Mb/s. The unencrypted connection is fast enough that it won't limit the speed of your encrypted VPN connection.

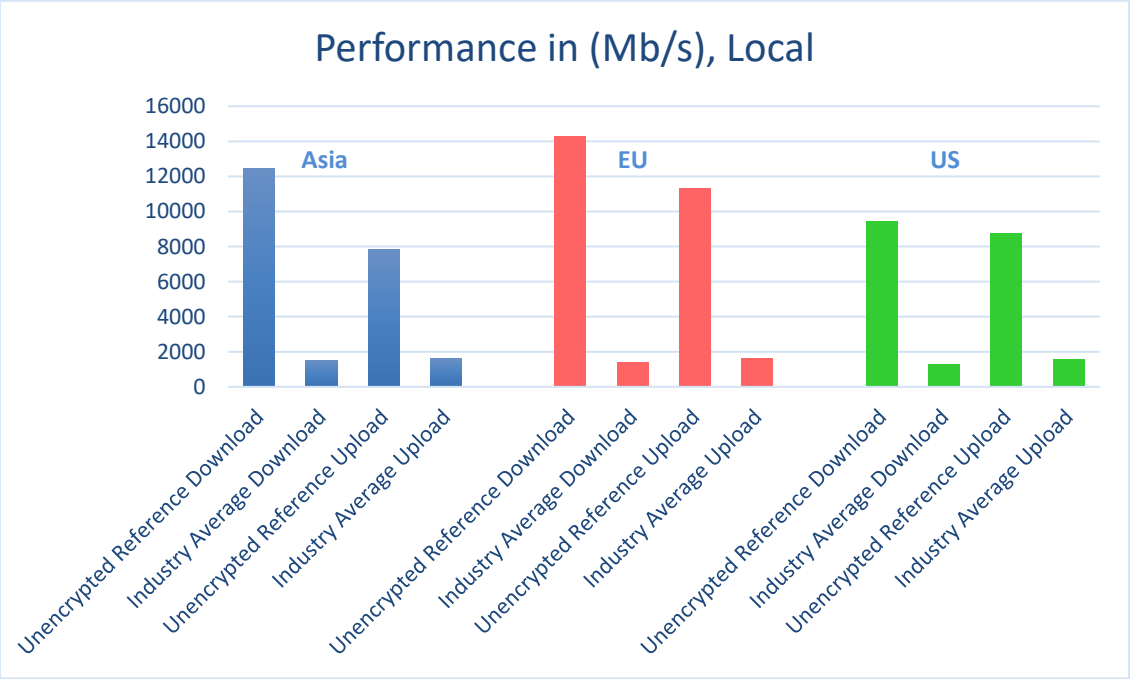

Figure 2, the comparative local results for the unencrypted down- and upload performances and the industry averages for all three tested locations.

For overseas connections, the average VPN download speed was around 800 Mb/s, with an average upload speed of approximately 360 Mb/s. The reduction in performance for overseas VPN connections is less drastic than for local connections, particularly for uploads. The average VPN download and upload speeds for overseas connections were quite similar across the three tested geographical regions.

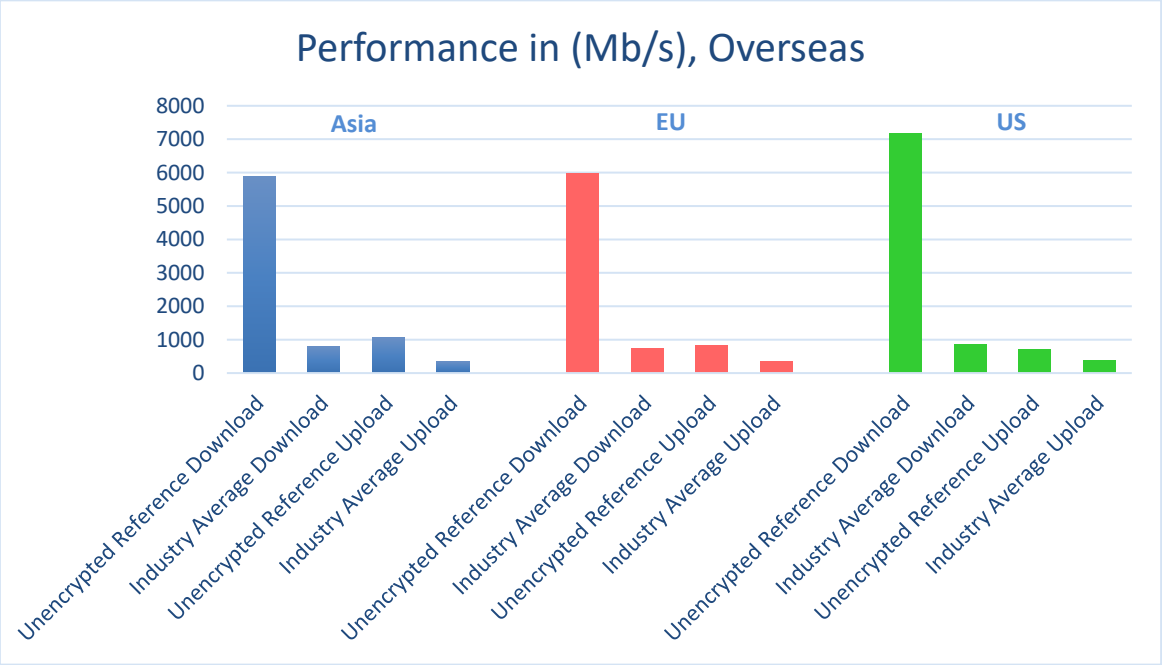

Figure 3, the comparative overseas results for the unencrypted down- and upload performances and the industry averages for all three tested locations.

2.2. Industry average: Latency

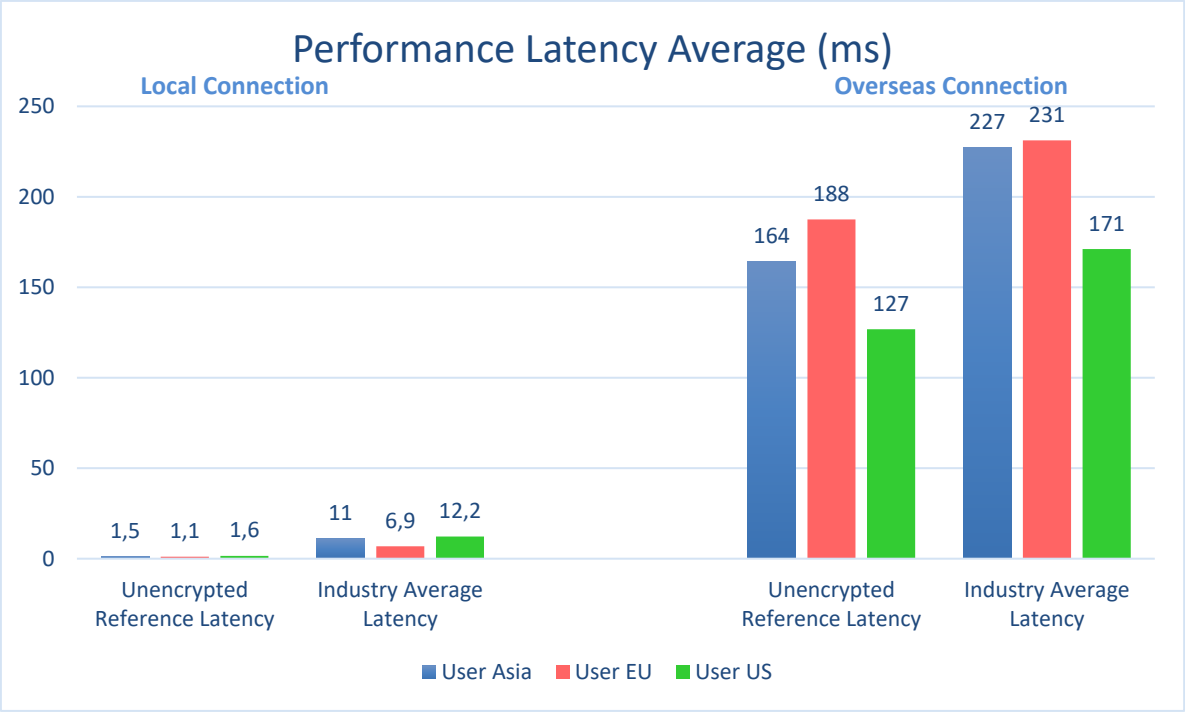

Figure 4, the comparative local and overseas results for the measured latency for the unencrypted reference and industry average for all three tested locations.

For local connections, the average latency when using a VPN was around 10 ms depending on user location. It is important to note that this average was skewed by a few individual products, as the median latency was substantially lower at between 3 ms and 4 ms. A detailed breakdown can be seen in Chapter 3.3, “VPN solutions results: Latency”. This contrasts with unencrypted reference connections, which typically exhibit very low latency, often between 1 ms and 2 ms.

Noticeably, the overseas connection from users to the US was the fastest, whether via an encrypted VPN or an unencrypted reference connection. This connection demonstrated a significant speed advantage compared to other overseas routes, although it was still slightly slower than local connections within the US and even Asia.

As expected, overseas connections showed significantly higher latency for both unencrypted traffic and the one inside VPN tunnels, compared to local connections. The average latency for VPNs connecting overseas was approximately 210 ms. For comparison, unencrypted overseas connections usually have latencies in the range of 200 ms to 300 ms. The difference in latency between encrypted VPN and unencrypted overseas connections was not substantial.

2.3. Industry average: Torrent

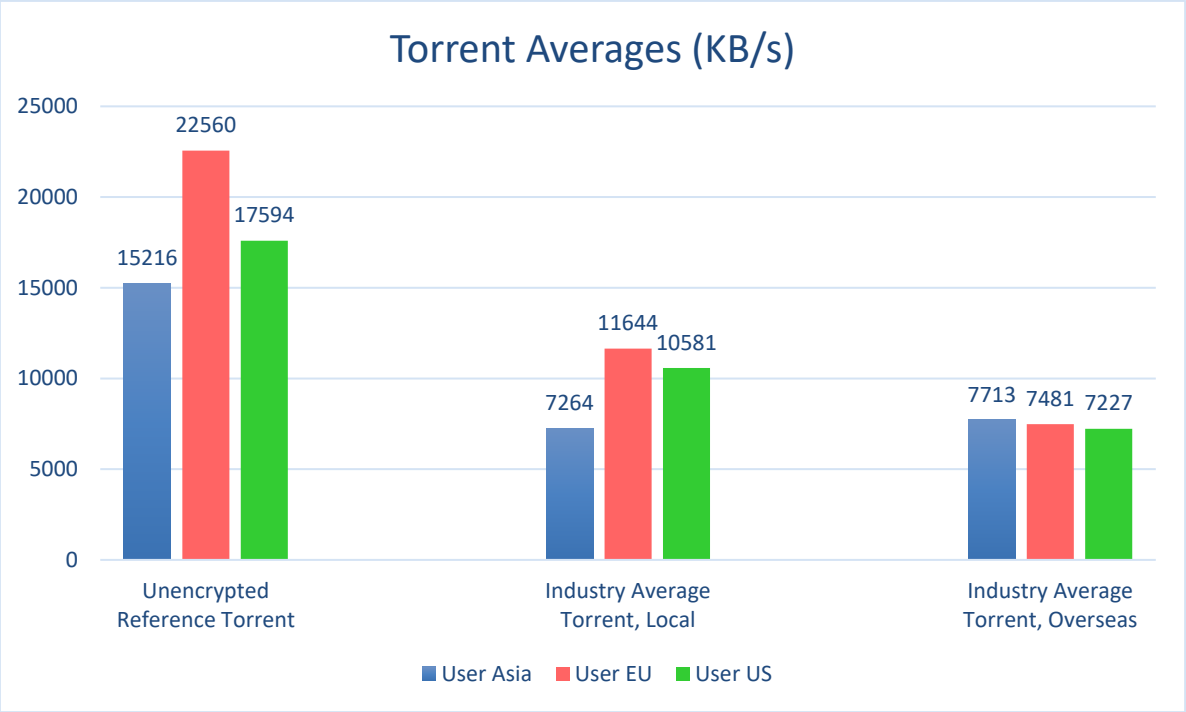

Figure 5, the comparative local and overseas results for torrent downloads for the unencrypted reference and industry average for all three tested locations.

The average torrent download speed for VPNs on local connections was approximately 9830 KB/s. This is in comparison to unencrypted reference connections, which can achieve speeds of around 10,000 KB/s to 15,000 KB/s for torrent downloads.

For overseas connections, the average VPN torrent download speed was about 7474 KB/s. Unencrypted overseas connections typically perform in the range of 8,000 KB/s to 10,000 KB/s. Regional differences were observed, with some variations influencing the measured results. Notably, VPN connections in Asia were generally around 30% slower than comparable connections in the US and EU, which could be related to the distribution of torrent seeders.

3. VPN solutions results

This section presents the measured performance results for each VPN solution across the various test scenarios and geographical regions. As detailed in the methodology, products were tested by connecting to the local server via the "best option" or manual selection for local averages, and to the closest server for overseas averages, such as a user in the US connecting to locations in Europe and Asia for evaluation.

Note: For CyberGhost, the connection location was changed from an "optimal" setting to the closest server for emulated users. This adjustment was made because the service didn't consistently connect to the right server (i.e., those in the immediate vicinity), often opting for geographically distant ones, which worsened performance results. Separately, subsequent independent tests have shown improved download and upload performance for the product. This suggests either product enhancements or the resolution of prolonged technical issues that were present during the initial testing period.

3.1. VPN solutions results: Download

This section details the measured download performance for each VPN solution across the three geo-locations tested for both local and overseas connections. For local averages, each product was connected to a local server, either by selecting the "best option" in the VPN client or through manual server selection. For overseas averages, the closest server to the test locations was selected; for instance, a user in the US connecting to locations in Europe and Asia for evaluation.

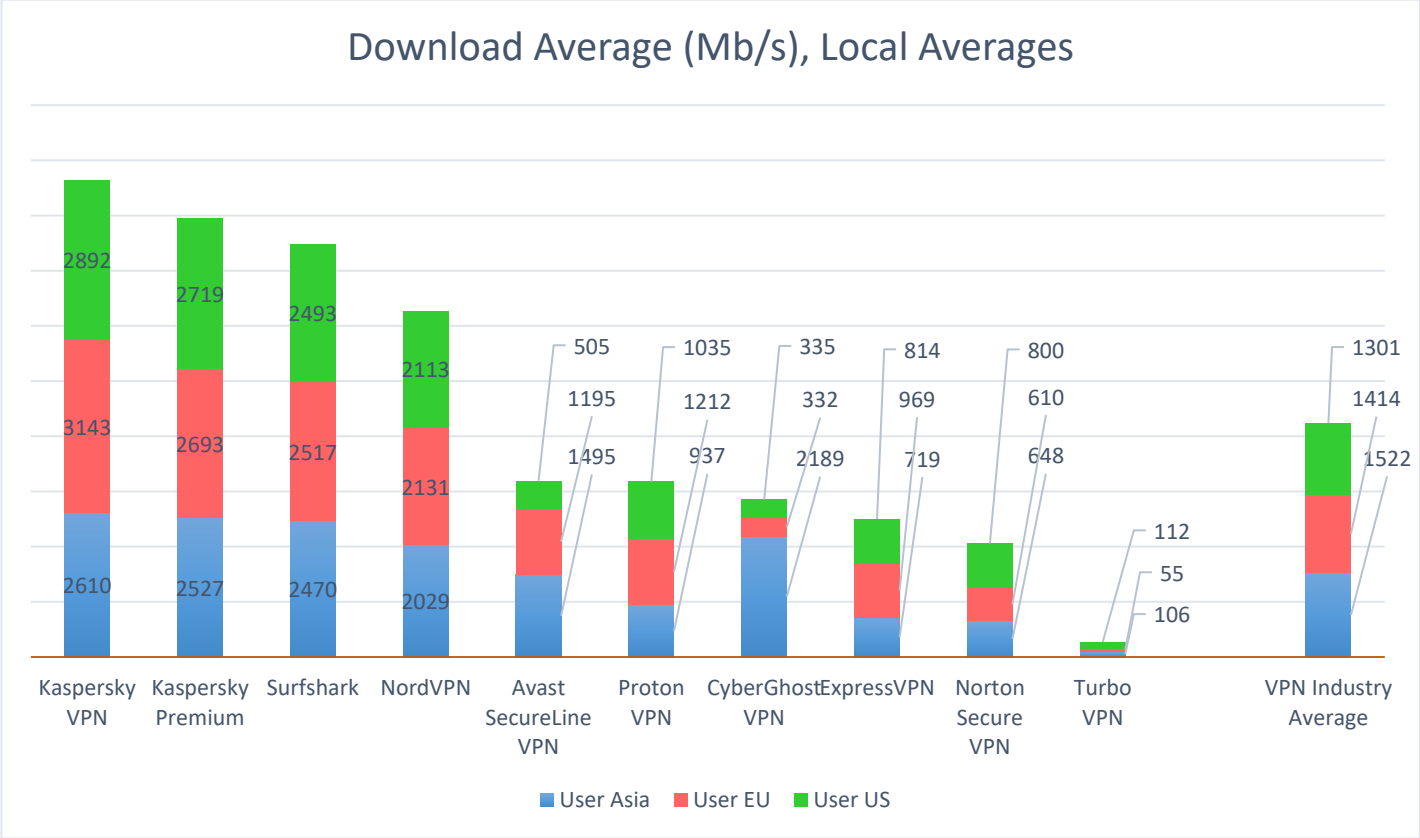

Figure 6, the cumulative local average download speed for all three locations and the industry average.

For local download speeds,

- Kaspersky VPN led the evaluation with an average of approximately 2882 Mb/s.
- Kaspersky Premium followed closely with around 2646 Mb/s, demonstrating strong performance.
- Surfshark also performed notably well, averaging about 2493 Mb/s.
- NordVPN showed consistent results across regions, with an average of approximately 2091 Mb/s.
- Avast SecureLine VPN's performance varied more significantly by region, averaging 1065 Mb/s.
- Proton VPN delivered a solid performance, with an average of about 1061 Mb/s.
- CyberGhost VPN achieved around 952 Mb/s, while Proton VPN recorded about 1061 Mb/s.
- ExpressVPN achieved an average of 834 Mb/s.
- Norton Secure VPN recorded around 686 Mb/s.
- Turbo VPN showed the lowest local download speeds, with an average of about 91 Mb/s.

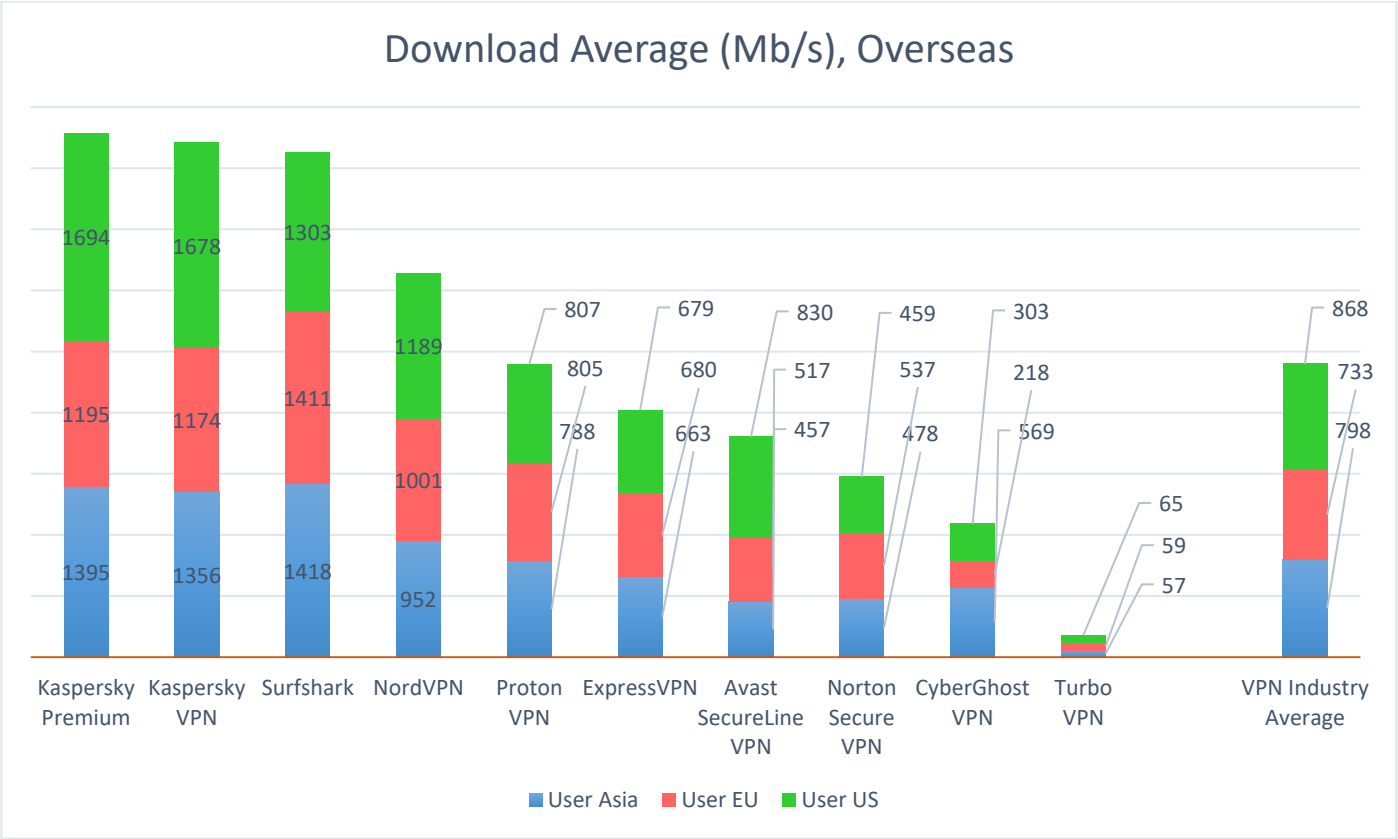

Figure 7, the cumulative overseas average download speed for all three locations and the industry average.

For overseas download speeds,

- Kaspersky Premium maintained a strong position, averaging approximately 1428 Mb/s.
- Kaspersky VPN also performed well, with an average of about 1409 Mb/s.
- Surfshark demonstrated high overseas download performance, averaging around 1377 Mb/s.
- NordVPN achieved an average of approximately 1047 Mb/s, showing consistent performance across different overseas regions.
- Proton VPN recorded around 800 Mb/s.
- ExpressVPN averaged around 839 Mb/s,
- Avast SecureLine VPN averaged about 601 Mb/s.
- Norton Secure VPN averaged around 492 Mb/s.
- CyberGhost VPN recorded lower speeds, with an average of approximately 363 Mb/s.
- Turbo VPN again showed the lowest overseas download speeds, averaging about 60 Mb/s.

3.2. VPN solutions results: Upload

This section details the measured upload performance for each VPN solution across the three geolocations tested for both local and overseas connections. For local averages, each product was connected to a local server, either by selecting the "best option" in the VPN client or through manual server selection. For overseas averages, the closest server to the test locations was selected; for instance, a user in the US connecting to locations in Europe and Asia for evaluation.

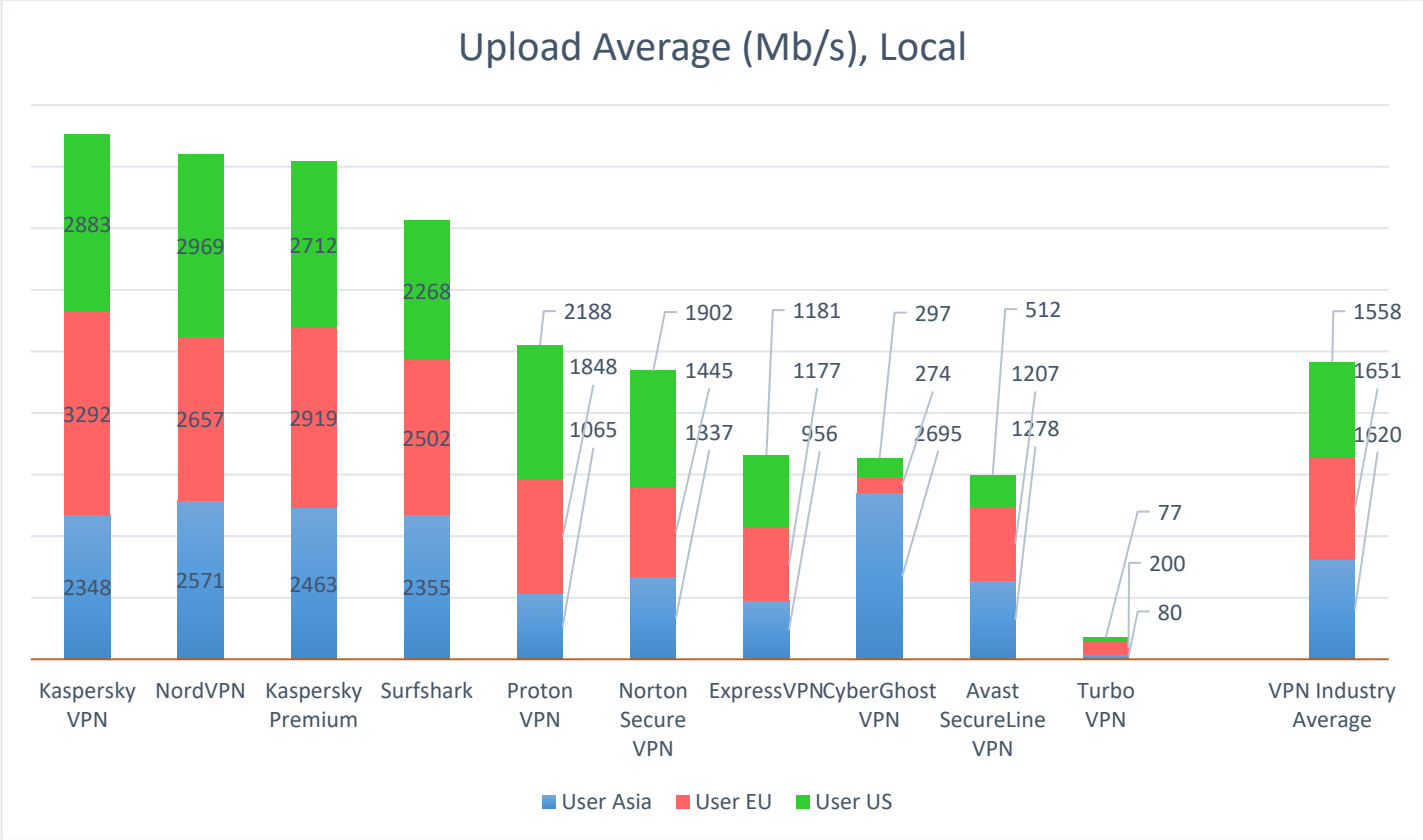

Figure 8, the cumulative local average upload speed for all three locations and the industry average.

For local Upload speeds,

- Kaspersky VPN demonstrated leading local upload performance, averaging approximately 2841 Mb/s.
- NordVPN followed closely, achieving about 2732 Mb/s.
- Kaspersky Premium also followed closely with an average of 2698 Mb/s.
- Surfshark showed robust upload speeds, averaging around 2375 Mb/s.
- Proton VPN achieved about 1700 Mb/s.
- Norton Secure VPN recorded an average of 1561 Mb/s.
- ExpressVPN and CyberGhost VPN averaged about 1105 Mb/s and 1088 Mb/s respectively.
- Avast SecureLine VPN averaged approximately 999 Mb/s.
- Turbo VPN showed the lowest local upload speeds, with an average of about 119 Mb/s.

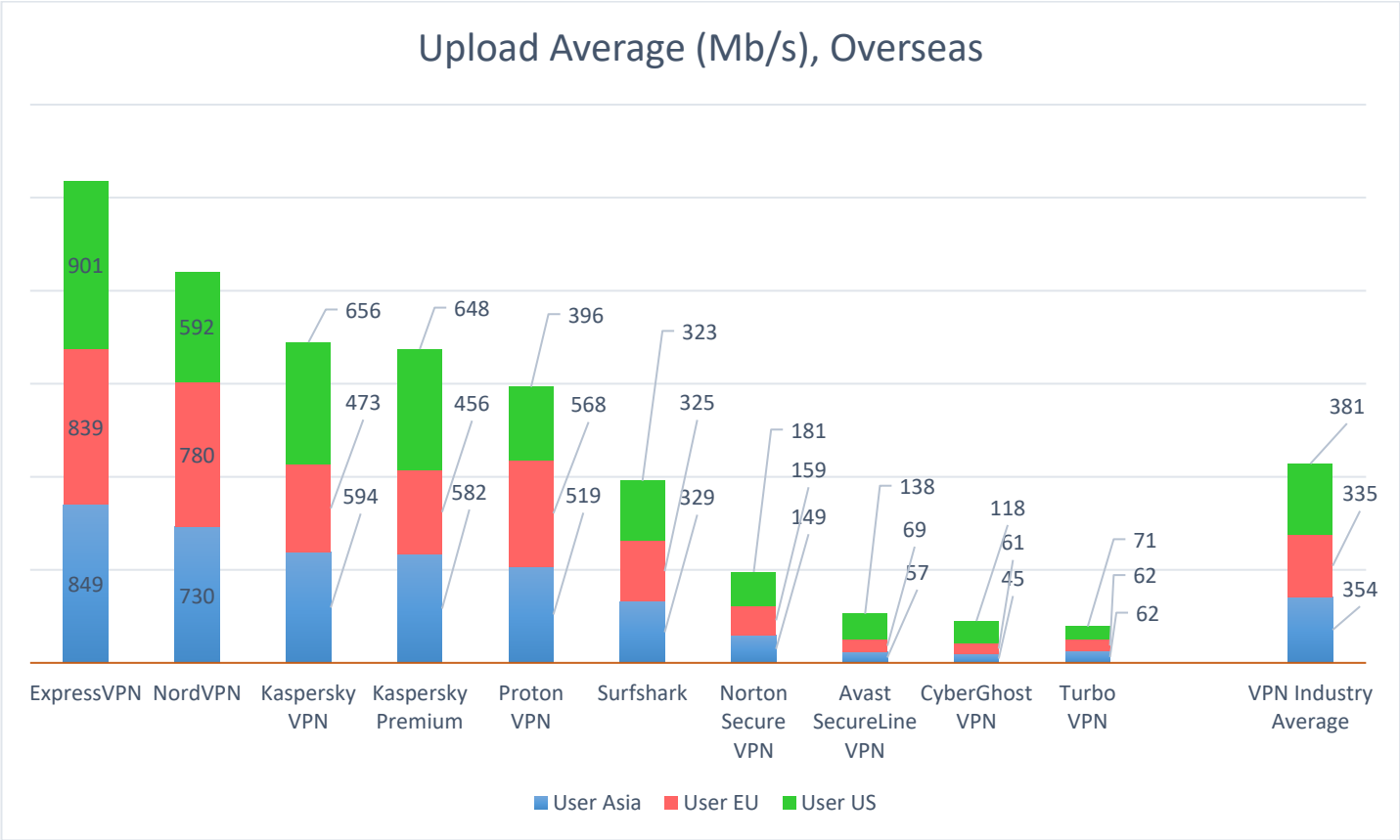

Figure 9, the cumulative overseas average upload speed for all three locations and the industry average.

For overseas upload speeds,

- ExpressVPN led with an average of approximately 863 Mb/s.
- NordVPN achieved a strong second place, averaging about 701 Mb/s.
- Kaspersky VPN averaged about 574 Mb/s, and Kaspersky Premium followed closely with around 562 Mb/s.
- Proton VPN recorded approximately 494 Mb/s.
- Surfshark averaged around 326 Mb/s.
- Norton Secure VPN showed about 163 Mb/s.
- Avast SecureLine VPN recorded 88 Mb/s, and CyberGhost VPN averaged 75 Mb/s.
- Turbo VPN had the lowest overseas upload speeds, with an average of about 65 Mb/s.

3.3. VPN solutions results: Latency

This section details the measured latency performance for each VPN solution across the three world regions tested for both local and overseas connections. For local averages, each product was connected to a local server, either by selecting the "best option" in the VPN client or through manual server selection. For overseas averages, the closest server to the test locations was selected; for instance, a user in the US connecting to locations in Europe and Asia for evaluation.

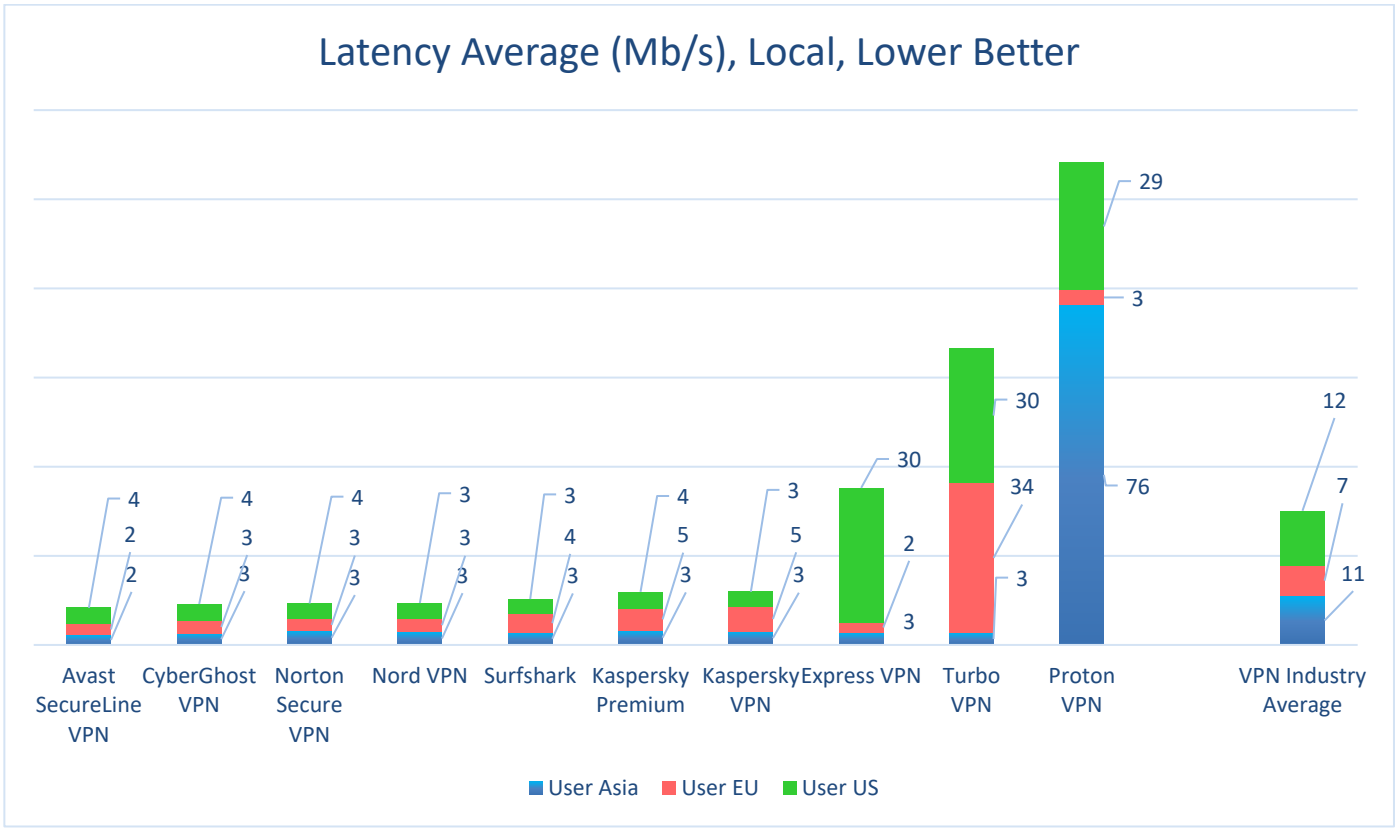

Figure 10, the measured local latency averages for all three locations and the industry averages.

For local latency, lower values indicate better performance. The first 7 solutions showed very close results.

- Avast SecureLine VPN demonstrated the lowest latency, averaging approximately 2.8 ms.
- CyberGhost VPN recorded about 3.1 ms.
- Norton Secure VPN and NordVPN also showed very low latency, both averaging around 3.1 ms.
- Surfshark averaged around 3.4 ms.
- Kaspersky VPN and Kaspersky Premium performed similarly, both averaging approximately 4.0 ms.
- ExpressVPN had a slightly higher average of about 11.8 ms, with some regional variations.
- Turbo VPN averaged around 22.2 ms.
- Proton VPN recorded the highest average local latency at about 36.1 ms.

While the overall averages provide a useful summary, the regional data highlights specific weaknesses. The high averages for ExpressVPN, Turbo VPN, and Proton VPN are driven by very slow connections in the US, all above 30 ms. Additionally, Turbo VPN's EU latency was elevated at 33.7 ms. The highest single measurement in the test came from Proton VPN in Asia (76.4 ms), which disproportionately increased its overall average.

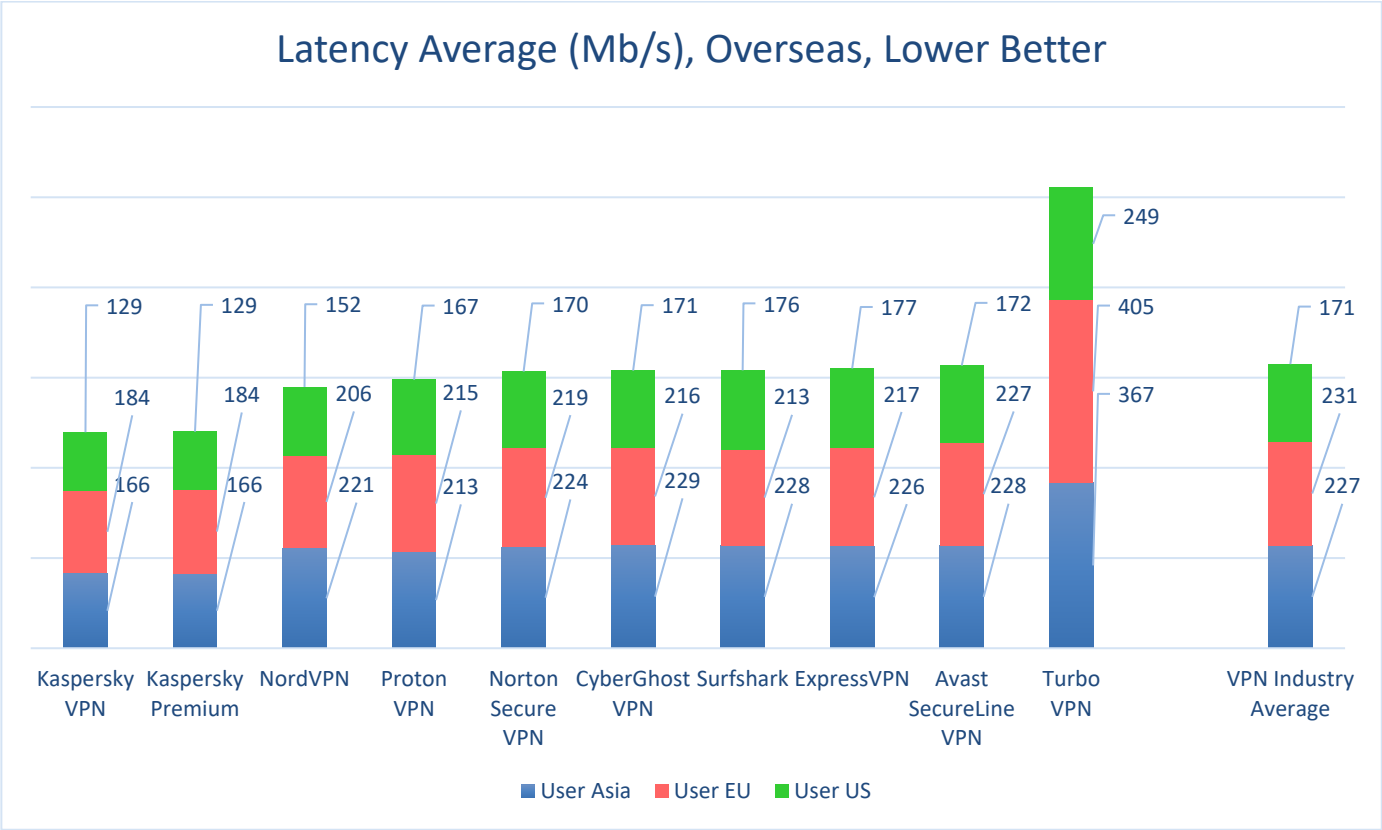

Figure 11, the measured overseas latency averages for all three locations and the industry averages.

For overseas latency, the differences between products for overseas latency were less pronounced than for local latency.

- Kaspersky VPN and Kaspersky Premium demonstrated the lowest values, both averaging approximately 160 ms.
- NordVPN followed with an average of about 193 ms.
- Proton VPN recorded around 199 ms.
- CyberGhost VPN, Norton Secure VPN, and Surfshark showed similar performance, each averaging around 205 ms,
- ExpressVPN averaged approximately 207 ms
- Avast SecureLine VPN averaged about 209 ms.
- Turbo VPN consistently had the highest overseas latency, averaging about 340 ms.

3.4. VPN solutions results: Torrent

This section details the measured torrent download performance for each VPN solution across the three world regions tested. The results are presented for both local and overseas connections. Performance is shown as a percentage relative to the speed of an unencrypted reference connection; a higher percentage indicates better performance.
For local averages, each product was connected to a server within the same region, either by selecting the "best option" in the VPN client or through manual server selection. For overseas averages, servers in distant regions were used; for instance, a user in the US connected to locations in Europe and Asia for evaluation.
It is important to note that Avast SecureLine VPN and Norton Secure VPN did not support torrents so their torrent performance data are absent in these tests

The chart below, illustrates the local torrent performance for each product, with the result being an average of the performance from all three test regions.

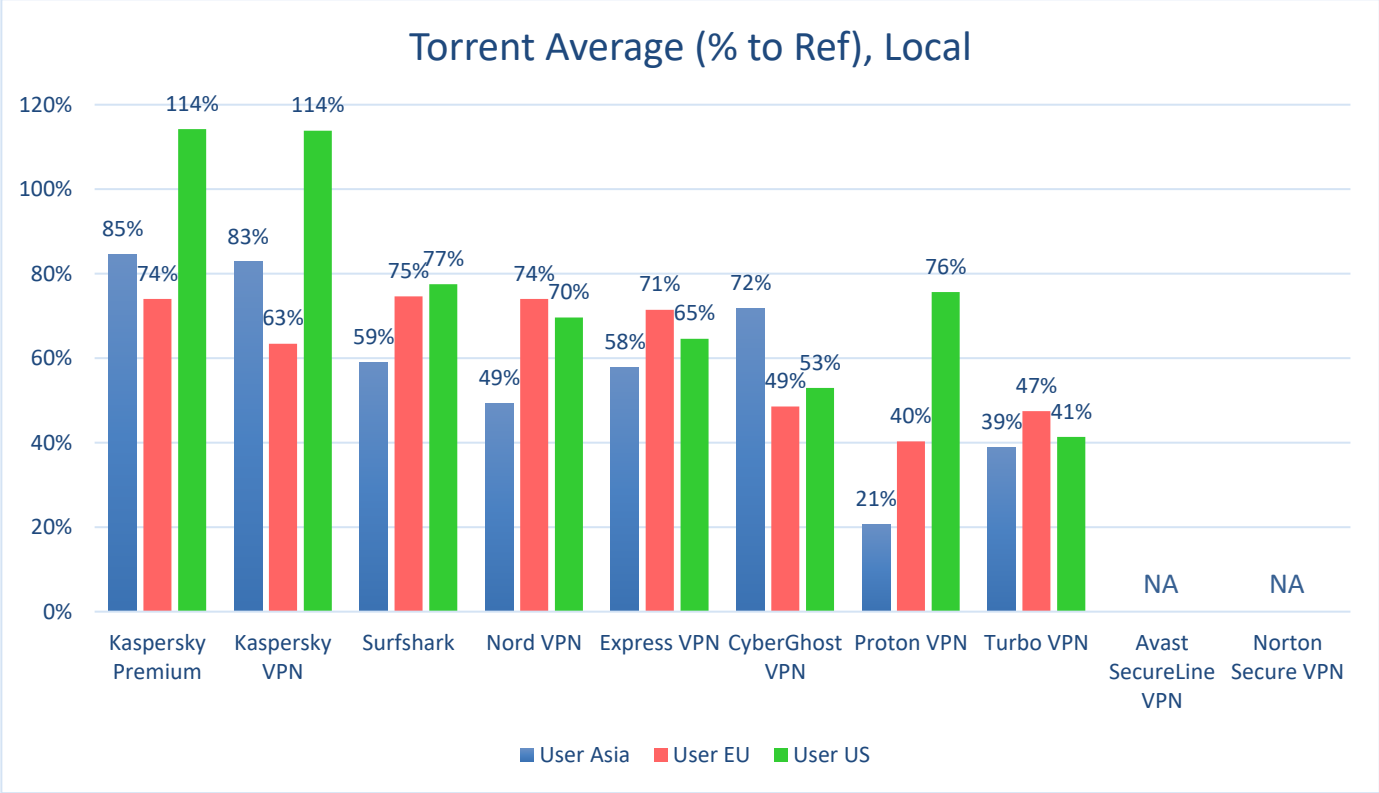

Figure 12, this chart displays the local torrent download performance for each VPN as a percentage of the reference connection speed, with results broken down by the user's geographical location.

For local torrent download performance, relative to the reference system:

- Kaspersky Premium achieved the highest performance, averaging approximately 91% of the reference speed.
- Kaspersky VPN followed with a strong result of about 87%.
- Surfshark achieved an average of around 70%.
- ExpressVPN recorded an average of approximately 65%.
- NordVPN showed a performance of about 64%.
- CyberGhost VPN averaged around 58%.

- Proton VPN recorded an average of about 46%.
- Turbo VPN achieved an average of approximately 42%.

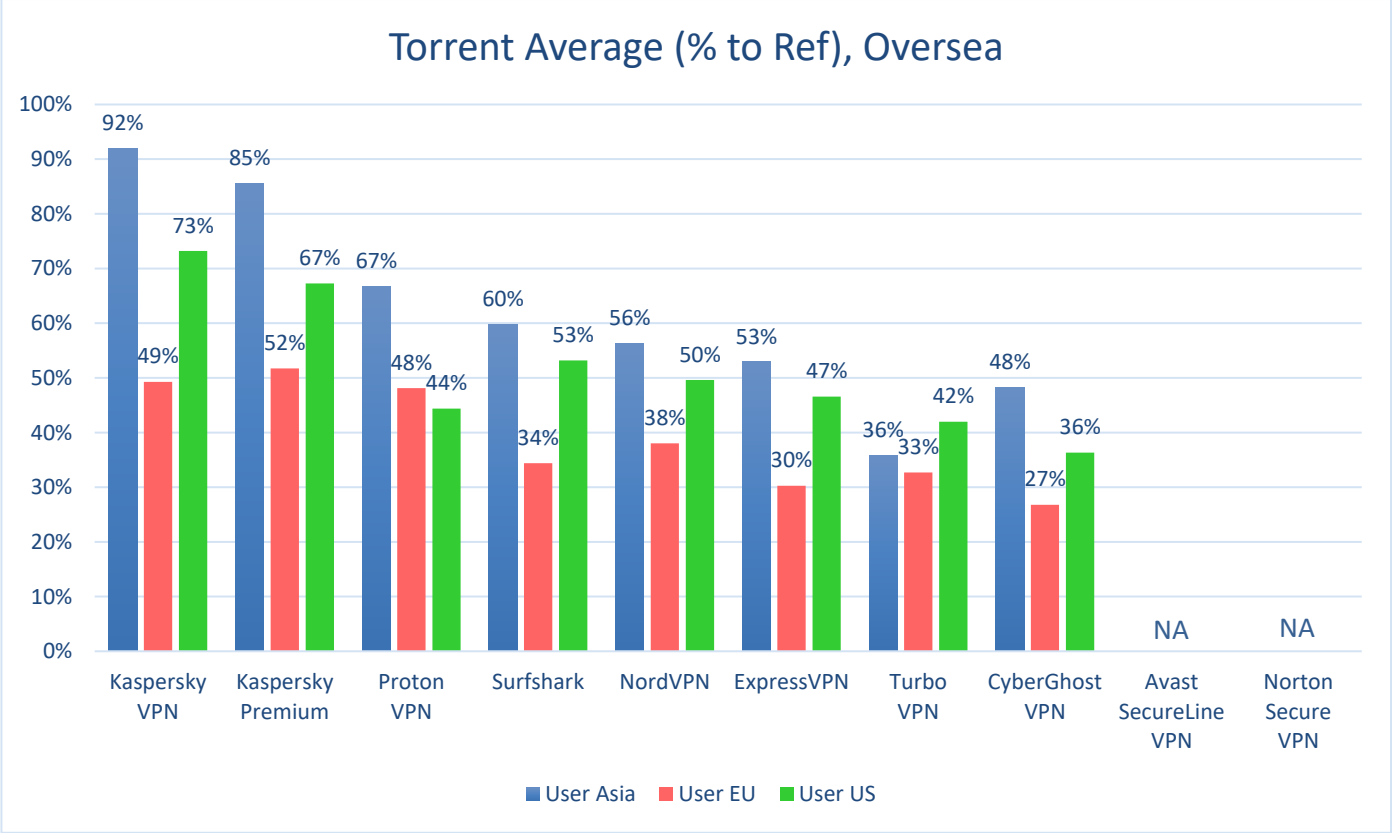

Figure 13, this chart illustrates the overseas torrent download performance for each VPN as a percentage of the reference connection speed, showing individual results from the three tested user regions.

The subsequent chart, shows the overseas torrent performance, also averaged across the three test regions.
For overseas torrent download performance, relative to the reference system:

- Kaspersky VPN led the evaluation with an average performance of approximately 71% of the reference speed.
- Kaspersky Premium followed with a result of about 68%.
- Proton VPN achieved an average of around 53%.
- Surfshark recorded an average of approximately 49%.
- NordVPN showed a performance of about 48%
- ExpressVPN averaged around 43%.
- CyberGhost VPN and Turbo VPN both recorded an average performance of approximately 37%.

Similar to local tests, Avast SecureLine VPN and Norton Secure VPN did not provide torrent performance data in these tests.

3.5. VPN Solutions Results: Combined Score Ranking for Each Tested Solution

3.5.1. Methodology for Performance Scoring and Ranking

The performance evaluation of the products involved numerous tests across various metrics, generating a substantial volume of raw data. To allow a clear and direct comparison between the products, a standardised scoring system is used. This system translates the raw performance measurements into a normalised score for each product, providing easily readable graphs for comparison of their overall efficiency.

The calculation is conducted in two primary stages:

1. Performance Scenario Score Calculation:
   For each of the four key performance categories—Download, Upload, Latency, and Torrent—a single scenario score is produced by aggregating the results from both local and overseas tests. The process involves first normalising the raw results for local and overseas tests to an independent 0–100 scale, where the best-performing product is assigned 100 and the worst-performing is assigned 0. If a product has an overall 0 in a tested category, it means it scored last in all tested locations for that category. Subsequently, the normalised local and overseas scores are averaged with equal weighting to generate the final score for that performance scenario.
2. Combined Score Calculation:
   A final 'Combined Score' is then calculated to represent the total effectiveness of each solution. This score is derived by taking the average of the four individual 'Performance Scenario Scores'.

This scoring methodology offers several distinct advantages for data presentation and analysis:

- A single cumulative graph represents the total efficiency of each solution across all user scenarios. The presentation is limited to four primary graphs—one for each performance scenario—which improves clarity and reduces visual complexity.
- Local and overseas results are combined without distortion through the equal-weight averaging of normalised scores.
- The resulting graphs visually represent the product rankings based on the magnitude of their scores, removing the need for explicit rank labelling.

3.5.2. The result of the calculation:

The graphs show how each VPN performed in four key areas: Latency, Download, Upload, and Torrent, as well as the combined efficiency of the tested solutions.
The results combine both local and overseas tests into a single score, so each bar reflects overall performance in that category. A higher bar means better performance.
The products are listed in order of performance — the top entry in each graph is the best in that category, followed by the next best, and so on.
The length of each bar (horizontal axis) represents the product's overall score on a scale from 0 to 100, where 100 marks the best result among all tested VPNs in that specific category.

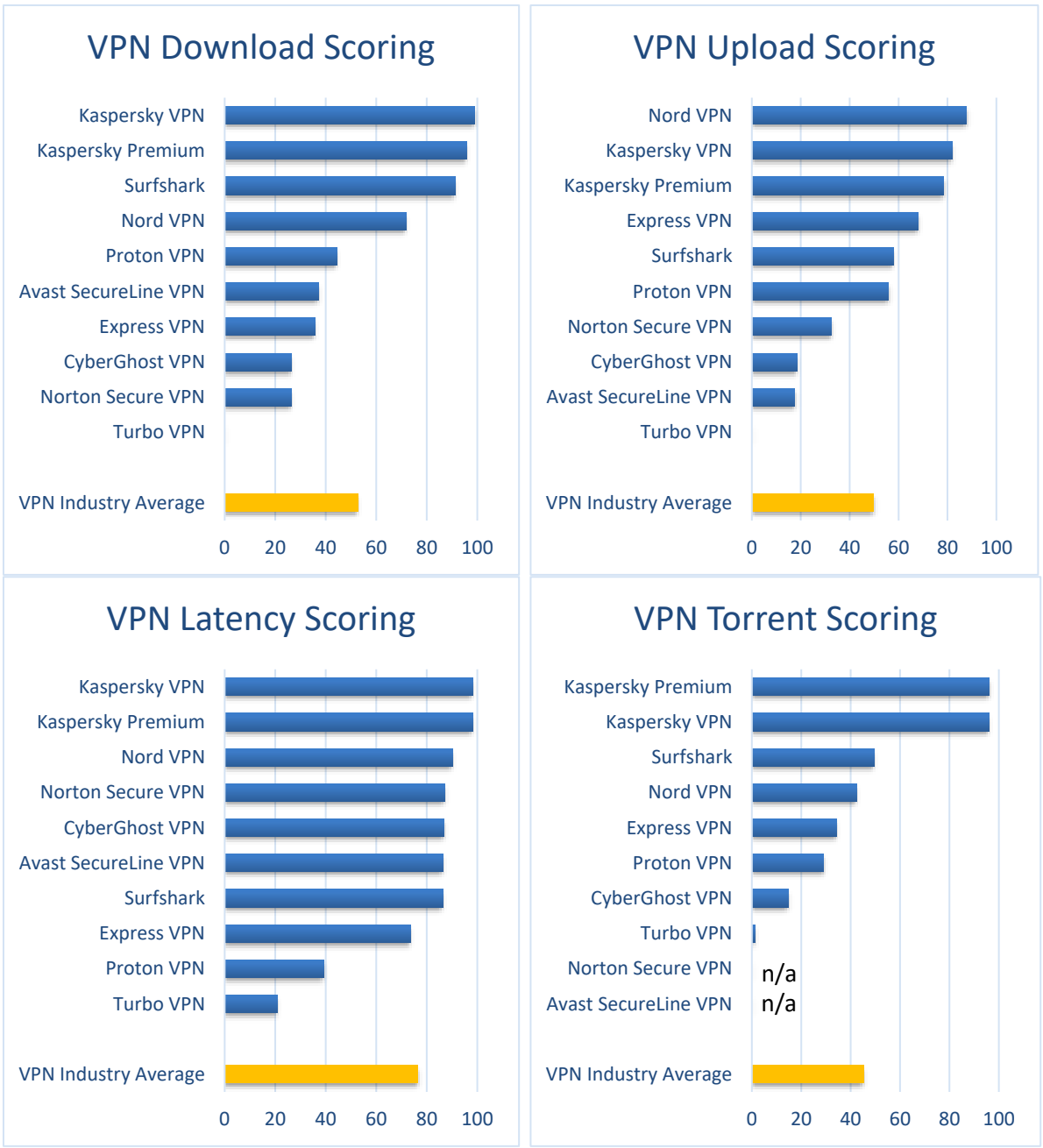

Figure 14, the Score Rankings separately for each of the measured parameters (Download, Upload, Torrent, Latency, both local and Oversea) for each of the tested solution (the more the better).

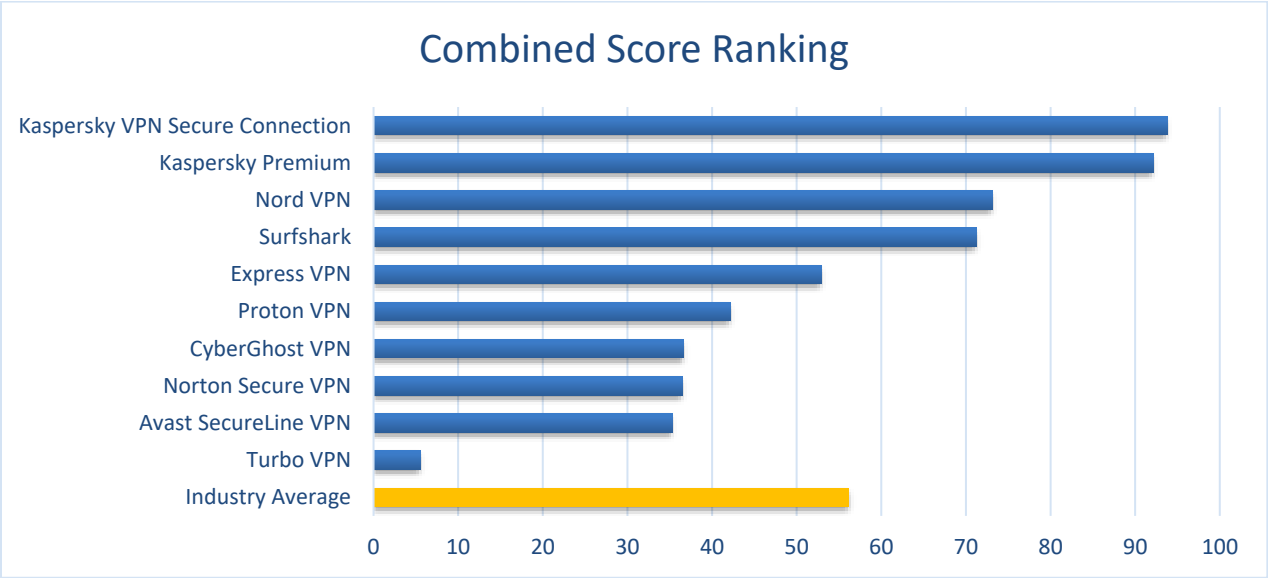

Figure 15, the Combined Score Ranking for each of the tested solution (the more the better).

4. VPN Product Feature Overview

This chapter reviews the functionalities and technical specifications of the Virtual Private Network (VPN) products evaluated in this report, based on the provided feature list. It identifies features commonly available across most products, representing a standard offering in the VPN market, and subsequently highlights distinctive capabilities of individual solutions.

4.1. Standard VPN Capabilities

A foundational set of features is consistently present across most of the tested VPN solutions, establishing a common baseline for VPN service offerings:

- **Data Encryption**: All tested VPNs consistently use AES-256 encryption to secure data transmission. Many products also integrate ChaCha20-poly1305 encryption, particularly when utilising WireGuard or similar modern protocols. Notably, providers such as the Kaspersky products and ExpressVPN have also developed and implemented their own auditable, proprietary protocols as an alternative to standard options.
- **Essential Security and Leak Protection**: A critical aspect of VPN functionality, nearly all products effectively prevent various data leaks. This includes safeguarding against DNS leaks (ensuring the internet provider's identity is not visible), IP address leaks (including local IP for WebRTC), and email address leaks.
  Exclusions: Turbo VPN is not providing protection against browser (local IP) or P2P/Torrent location leaks. It also allows a WebRTC leak – which causes user's real IP address (and possibly physical location) exposing to websites, even when VPN channel is established. Correspondingly, this means that Geo restrictions might not be fully bypassed (i.e. Netflix would see real region and apply its limitation policies), and adversaries/ attackers could use the leak to track of fingerprint the user.
- **Kill Switch Functionality**: All evaluated VPNs incorporate a kill switch, an essential security mechanism that automatically disables the internet connection if the VPN tunnel drops, preventing unencrypted data exposure. For all products tested, the kill switch effectively disconnects the internet with zero delay across various scenarios, such as network card disable-enable or unexpected disconnections.
- **Automatic Reconnection**: The majority of products automatically reconnect after a system reboot and retain previously used connection settings, enhancing user convenience.
  Exclusions: Avast SecureLine VPN is an exception, as it does not offer these automatic reconnection features, which may require users to manually reconfigure their connection after restarting the device.
- **Torrenting Support**: Most products enable P2P and torrent activity while ensuring the user's location remains undisclosed.
  Exclusions: Avast SecureLine VPN and Norton Secure VPN did not support torrenting on the tested servers but have designated torrent servers.
- **Basic Company Transparency:** The majority of VPN providers enhance transparency by disclosing CEO details and official company addresses. All products provide a separate Privacy Statement in addition to their End User Licence Agreement (EULA) and include contact information for data protection officers, aligning with General Data Protection Regulation (GDPR) requirements. Most also participate in a bug bounty program.
  Exclusions: Turbo VPN is an exception, as it does not list a bug bounty program, CEO details, or board/management team details.

- **Broad Operating System Support**: Most VPNs provide native support for Windows (versions 8, 10, and 11) and macOS, alongside mobile platforms like iOS and Android. Some also extend support to Linux, AndroidTV, FireTV and Wifi routers.

4.2. Distinctive Product Capabilities

While core features are widely adopted, certain products differentiate themselves through additional functionalities, broader compatibility, or deeper commitments to transparency.

- **Extensive Server Networks**: All VPN solutions are based on sufficient network of servers, countries and locations. In particular:
  - Avast SecureLine VPN uses VPN servers in 37 countries with 59 server locations,
  - CyberGhost VPN – 100 countries with 139 locations,
  - ExpressVPN – in 100 countries with 166 locations,
  - Kaspersky – in 89 countries with 110 locations,
  - NordVPN - 118 countries with 153 locations,
  - Norton Secure VPN – 29 countries with 29 locations,
  - Proton VPN – 117 countries with 152 locations,
  - Surfshark – in 100 countries with 140 locations,
  - Turbo VPN – 40 countries with 54 locations.

  Exclusions: During the test we faced with an issue of non-support by TurboVPN of some VPN servers and had to change them to another ones.
- **Flexible Setup Options**: ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Proton VPN, and Surfshark provide manual setup options, allowing installation on devices like routers or through OpenVPN applications, offering greater configurability.
  Exclusions: Avast SecureLine VPN, Norton Secure VPN, CyberGhost VPN, and Turbo VPN do not provide this option.
- **Streaming Service Compatibility**: While most products support watching geo-blocked video content, ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Norton Secure VPN, Proton VPN, and Surfshark are notable for their ability to facilitate access to Netflix across different geographical regions, specifically validated for US Netflix.
  Exclusions: Avast SecureLine VPN, CyberGhost VPN and Turbo VPN do not support this.
- **Advanced Network Control:**
  - **Custom DNS Support**: Kaspersky VPN, Kaspersky Premium, NordVPN, Norton Secure VPN, and Surfshark allow users to configure custom DNS settings.
    Exclusions: Avast SecureLine VPN, CyberGhost VPN, ExpressVPN, Proton VPN, Turbo VPN do not offer this option
  - **Multihop / DoubleVPN**: Kaspersky VPN, Kaspersky Premium, NordVPN, Proton VPN, and Surfshark offer Multihop or DoubleVPN features, routing traffic through multiple VPN servers for increased encryption and anonymity. Kaspersky utilizes nested encryption in DoubleVPN implementation.
    Exclusions: Avast SecureLine VPN, CyberGhost VPN, ExpressVPN, Norton Secure VPN, Turbo VPN do not offer this option
  - **Network Automatic Protection (e.g., Wi-Fi unencrypted**): Avast SecureLine VPN, CyberGhost VPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Norton Secure VPN, Surfshark, and Turbo VPN automatically activate protection when connecting to untrusted networks.
    Exclusions: ExpressVPN and CyberGhost do not offer this option.
- **Specific App or Data Protection (Inverse Split Tunneling, Split Exclude) & Split-tunneling**: ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Proton VPN, and Surfshark

provide fine-grained control over which applications or data are routed through the VPN tunnel, including the ability to add exceptions.
Exclusions: Avast SecureLine VPN, CyberGhost VPN, Norton Secure VPN and Turbo VPN do not offer this option.

- **Ad and Tracker Blocking**: ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN (Ads only), Norton Secure VPN and Surfshark include integrated features to block advertisements and invisible trackers.
  Exclusions: Avast SecureLine VPN, CyberGhost VPN, Proton VPN and Turbo VPN do not offer this option.
- **Enhanced Transparency and Auditing:**
  - **Transparency Centers:** Only Kaspersky provides capability for trusted partners and government stakeholders to review the company's code, software updates and threat detection rules. The company operates Transparency Centers in 13 countries worldwide.
  - **Transparency Reports**: CyberGhost VPN, ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Proton VPN, and Surfshark publish regular transparency reports detailing data requests from authorities.
    Notably, Kaspersky VPN and Kaspersky Premium reported zero data requests and zero data shared during their last reporting period (H2 2024).
    Exclusions: Avast SecureLine VPN, Norton Secure VPN, Turbo VPN do not provide transparency reports.
  - **Warrant Canary**: Proton VPN and Surfshark maintain an up-to-date Warrant Canary, a public statement indicating that the provider has not received certain types of legal requests.
  - **Independent Audits**: Several providers, including CyberGhost VPN, ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Proton VPN, and Surfshark, have undergone independent audits of their security and privacy practices.
  - **Management Team Details**: ExpressVPN, Kaspersky VPN, Kaspersky Premium, NordVPN, Norton Secure VPN, Proton VPN, and Surfshark provide details about their Board of Directors or Management Team, contributing to greater corporate transparency.
    Exclusions: Avast SecureLine VPN, CyberGhost VPN, Turbo VPN.
- **Detailed Data Handling and Privacy Policies**: All products outline data collection and its purpose, adhering to GDPR requirements. Most also provide information on data retention periods. Providers detail their data security measures, often encompassing administrative, technical, and physical safeguards.
  Turbo VPN explicitly states it shares aggregated anonymous data, referral information, and anonymised analytics, and for its free version, works with third-party advertising partners.

Conclusion

The objective of the presented tests was to assess the download, upload, latency, and torrent download performances of several Virtual Private Network (VPN) products. The evaluation provides a comprehensive overview of how these solutions perform in different geographical scenarios, both locally and overseas. Overall, the tests revealed a range of performance levels across the evaluated VPN services. Several products demonstrated strong capabilities in specific areas, while others offered more balanced performance across all metrics.
The following summaries outline the relative strengths and weaknesses of the tested VPN providers, based on their performance across all measured metrics.

Among the tested solutions, **Kaspersky Premium and Kaspersky VPN** demonstrated leadership in the following scenarios:

- Download both local (together with Surfshark) and overseas,
- Upload local (together with NordVPN),
- Latency both local (similar to Avast, CyberGhost, NordVPN, Norton, and Surfshark) and overseas, and
- Torrent both local and overseas. Torrent performance is shown as a percentage relative to the unencrypted reference connection to ensure fair comparison. Kaspersky's tests were conducted in December under lower reference speeds, while others were tested in February. Although Kaspersky VPN and Premium may appear slower in absolute KB/s, their relative performance ranks among the highest across all regions.

Compared to the 2022 comparative research, where Kaspersky showed weaker performance in overseas uploads, the current assessment highlights significant improvements in this area, reflecting the company's ongoing efforts to enhance VPN performance.
It should also be noted that Kaspersky Premium includes comprehensive real-time threat protection, proven in numerous security tests, while maintaining the high VPN performance results confirmed in this study.

Across most performance metrics, **NordVPN** demonstrates lower performance in comparison with Kaspersky Premium and Kaspersky VPN, though there are a few exceptions.

- In download tests, Kaspersky leads both locally and overseas across Asia, EU, and US. NordVPN consistently shows slower performance, with the gap most visible in local EU and US results.
- In upload tests, results are mixed: locally, Kaspersky Premium and VPN are on top in the EU, while NordVPN surpasses them in Asia and the US. For overseas uploads, NordVPN clearly leads in Asia and the EU, but is weaker in the US.
- Local latency is nearly identical for all three solutions (3–5 ms). In overseas connections, Kaspersky shows better latency (166–184 ms vs NordVPN's 206–221 ms).
- For local torrent performance, Kaspersky Premium and VPN dominate in Asia and the US, with NordVPN only comparable in the EU. In overseas torrenting, Kaspersky (especially VPN) is far stronger, reaching up to 92% of reference speed vs NordVPN's 38–56%.

Overall:

- Kaspersky Premium/VPN excel in download speed, latency, and torrenting — both locally and overseas.
- NordVPN stands out only in overseas upload speeds.
- For most use cases, especially streaming, downloads, and P2P, Kaspersky is the stronger choice.

- NordVPN contains AntiVirus protection turned off by default, and in case of turning it on, the performance could be different

Across most metrics, **Surfshark** demonstrates lower performance in comparison with Kaspersky Premium and VPN, though differences are less dramatic than in case with some other vendors.

- In download tests, Kaspersky VPN and Premium consistently delivered higher speeds both locally and overseas, including across Asia, EU, and the US. While Surfshark showed competitive results, particularly in overseas tests for Asia and EU, Kaspersky maintained the lead in the US and achieved the highest combined average across all regions.
- In upload tests, Kaspersky VPN generally leads locally, with Surfshark following Kaspersky Premium. Overseas, Surfshark performs weaker than NordVPN and still below both Kaspersky solutions.
- Latency local is similar for the three solutions, but Kaspersky provides better overseas latency across all test regions.
- Torrent performance favors Kaspersky in Asia and the US, with Surfshark results comparable in the EU. Overseas, Kaspersky dominates with significantly higher relative speeds.

Overall:

- Kaspersky Premium/VPN are faster and more stable in most scenarios.
- Surfshark delivers acceptable performance but falls short in overseas tests and torrenting.

ExpressVPN performs stronger in overseas uploads, but Kaspersky generally outperforms in speed and torrenting.

- Download speeds are consistently higher with Kaspersky, both local and overseas. ExpressVPN is reliable but slower in every region.
- Upload speeds show ExpressVPN closer to Kaspersky Premium, but Kaspersky VPN still leads locally. Overseas, ExpressVPN shows the best results.
- Latency is lower with Kaspersky in overseas regions; locally, all are nearly identical with significant drop for ExpressVPN in the US.
- Torrenting is a clear win for Kaspersky — ExpressVPN lags behind in both local and overseas tests.

Overall:

- Kaspersky Premium/VPN are stronger in downloads, latency, and torrent performance.
- ExpressVPN offers stability but not competitive speeds.

ProtonVPN performed low in comparison with Kaspersky's solutions in all test scenarios.

- Download speeds are notably higher with Kaspersky in all tested regions, both local and overseas. ProtonVPN remains behind across Asia, EU, and US.
- Upload results show ProtonVPN trailing, especially overseas where Kaspersky is significantly faster.
- Latency is consistently better with Kaspersky, especially locally ~~overseas~~ where ProtonVPN has significanly higher delays in Asia and the US.
- Torrent results highlight Kaspersky's advantage, especially overseas where ProtonVPN delivers lower relative speeds.

Overall:

- Kaspersky Premium/VPN provide superior performance in speed, latency, and torrents.
- ProtonVPN cannot compete at the moment in raw performance.

CyberGhost performs low in comparison with Kaspersky's solutions in all test scenarios.

- Downloads: Kaspersky is ahead in every region, with CyberGhost notably slower in overseas scenarios.
- Uploads: in local tests CyberGhost is slower than Kaspersky in EU and US, but performs strongly in Asia. Overseas, it falls short of both Kaspersky products.
- Latency: Kaspersky maintains better latency in overseas tests, while locally the results remain identical.
- Torrents: CyberGhost is weaker both locally and overseas, where Kaspersky Premium/VPN are significantly faster.

Overall:

- Kaspersky Premium/VPN excel in nearly every category.
- CyberGhost is serviceable but clearly behind in torrenting and overseas performance.

Norton Secure VPN offers basic VPN functionality, but Kaspersky Premium and VPN consistently outperform it across most metrics.

- In downloads, Norton lags well behind Kaspersky both locally and overseas, across Asia, EU, and US.
- In uploads, Norton performs weaker than both Kaspersky products locally, and overseas results are also lower.
- Latency is worse for Norton in overseas tests, while locally all providers show similar good latency.
- Norton lacks torrenting support, unlike most competitors.

Overall:

- Kaspersky Premium/VPN are faster and more reliable across all performance metrics.
- Norton Secure VPN remains limited in speed and unsuitable for torrent or performance-sensitive use cases.

Avast SecureLine VPN falls behind Kaspersky Premium and VPN in all performance scenarios.

- Downloads: Kaspersky is consistently faster both locally and overseas across Asia, EU, and US. Avast's performance is comparatively modest.
- Uploads: Avast occasionally comes closer locally but still trails both Kaspersky Premium and VPN. Overseas upload results remain below NordVPN and well behind Kaspersky.
- Latency: Locally similar, but overseas Kaspersky maintains lower latency.
- Avast lacks torrenting support, unlike most competitors.

Overall:

- Kaspersky Premium/VPN offer superior speed, latency, and torrent support.
- Avast SecureLine VPN is functional but falls short for demanding use cases.

TurboVPN struggles to compete; Kaspersky outperforms in all major categories.

- Download speeds: Kaspersky Premium/VPN are consistently higher across all regions, with TurboVPN far behind in both local and overseas results.
- Upload speeds: TurboVPN lags in every test, both local and overseas.
- Latency: Kaspersky demonstrates better results for both local and overseas latency; TurboVPN shows significantly high delays across regions.
- Torrenting: TurboVPN is the weakest performer, with relative speeds far below Kaspersky's.

Overall:

- Kaspersky Premium/VPN are superior across all tested metrics.

- TurboVPN offers noticeably lower performance, unsuitable for demanding use cases like streaming or torrents.
- TurboVPN lacks protection against browser and P2P/Torrent leaks, and its limited transparency is highlighted by the absence of a bug bounty program.

The tests indicate that while VPN usage inevitably introduces some performance overhead compared to unencrypted connections, the extent of this impact varies significantly between different providers. Consumers seeking optimal performance should consider their primary use case, whether it is high-speed downloads, low latency for interactive applications, or efficient torrenting, and compare specific product strengths accordingly.

Thanks to the outstanding performance of Kaspersky VPN Secure Connection and Kaspersky Premium, as reflected in the test results, both products successfully met all certification criteria and are awarded with the AV-TEST APPROVED VPN certification.

This test report complements the long-standing track record of regular evaluations of Kaspersky's VPN solutions by AV-TEST.[2]

2

2020: https://www.av-test.org/en/news/6-vpn-packages-put-to-the-test-under-windows-10/
2021: https://www.av-test.org/en/news/vpn-packages-for-private-users-put-to-the-test-under-windows-10/
2022: https://www.av-test.org/en/news/vpn-packages-put-to-the-test-more-security-and-anonymous-paths/
2022: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_VPN_Test_Report_December_2022.pdf
2023: https://www.av-test.org/en/news/kaspersky-vpn-test-report-2023/
2024: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_VPN_Test_Report_December_2024.pdf
2024: https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_Premium_VPN_Test_Report_December_2024.pdf