Deloitte.

CyberGhost

Independent Limited Assurance Report

December 2025

To the Board of Directors of
CyberGhost S.R.L.
68-72 Polonă Street, Polonă Business Center, District 1, Bucharest, Romania

We have been engaged by CyberGhost S.R.L. (hereinafter "CyberGhost" or "Engaging Party") to perform independent assurance procedures on CyberGhost's configuration of IT systems and management of the supporting IT operations as of October 31st, 2025, in accordance with the service description in Appendix II.

Responsibilities of the Engaging Party

The Management of CyberGhost is responsible for:

    i.   the selection and application of criteria as set out in the statement in Appendix I,
    ii.   the preparation of the description in Appendix II and the accompanying statement in Appendix I, including the completeness, accuracy and method of presentation of the description and the statement,
    iii.   the provision of the services covered by Appendix I and II,
    iv.   the design and implementation of appropriate measures and controls as set out in Appendix II.

Our Independence and Quality Control

We are independent of CyberGhost in accordance with the International Code of Ethics for Professional Accountants (including International Independence Standards) issued by the International Ethics Standards Board for Accountants (IESBA Code) that are relevant to our audit of financial statements and other assurance engagements. We fulfill our other ethical responsibilities in accordance with the IESBA Code.

Our firm applies the International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Responsibilities of the Practitioner

Our responsibility is to perform an independent limited assurance report, and to express a conclusion on the fair presentation of CyberGhost's configuration of IT systems and management of the supporting IT operations and their implementation, described in Appendix II, as of October 31st, 2025.

Our audit has been conducted in accordance with the International Standard on Assurance Engagements 3000 (Revised) applicable to Assurance Engagements Other Than Audits or Reviews of Historical Financial Information (ISAE 3000 (Revised)) established by the International Auditing and Assurance Standards Board ("IAASB"). In accordance with this standard, we have planned and performed our engagement to obtain limited assurance whether CyberGhost's configuration of IT systems and management of the supporting IT operations were prepared, in all material respects, in accordance with the criteria with respect to the description of CyberGhost's no logging safeguards prepared by the Management of CyberGhost as of October 31st, 2025.

Summary of work performed

Based on risk and materiality considerations, we performed our procedures to obtain sufficient and appropriate assurance evidence. The procedures selected depend on the assurance practitioner's judgement.

As part of the procedures to create an independent limited assurance report, we performed the following work:

- Inquiries with responsible CyberGhost employees,
- Review of the statement and description in Appendices I and II to verify whether the description fulfills the required relevant level of details and covers all relevant assertions made in the statement,
- Inspection of relevant IT systems (VPN servers, distribution servers, etc.) and verification of their configuration against the description provided,
- Inspection of the policy and its implementation for user access, change management, configuration management, and incident management against the description, and
- Inspection of the processes for managing, deploying, and configuring the IT systems against the description on a sample basis.

The procedures performed do not constitute a financial audit according to the International Standards on Auditing, nor an examination of compliance with laws, regulations, or other matters. Accordingly, our performance of the procedures does not result in the expression of an opinion or any other form of assurance on CyberGhost's compliance with laws, regulations, or other matters.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our independent limited assurance report conclusion.

Our limited assurance engagement is performed as of October 31st, 2025. The procedures we performed do not provide any assurance about "CyberGhost's No-logs Policy" for any other period.

Conclusion

Based on the procedures and the evidence obtained, nothing has come to our attention that causes us to believe that CyberGhost's configuration of IT systems and management of the supporting IT operations as of October 31st, 2025, were not prepared, in all material respects, in accordance with CyberGhost's description set out in Appendix II.

Restriction of use and distribution

This report is prepared solely for CyberGhost's management for the purpose described in this report. We do not accept or assume any responsibility or liability to any person other than CyberGhost's management in respect of this report or its contents. While CyberGhost may share this report, such sharing does not create any duty of care on our part or extend our responsibility to any third party.

Bucharest, 19 December 2025
Bogdana Buhos
Responsible Practitioner

BOGDANA BUHOS Digitally signed by BOGDANA BUHOS
Date: 2025.12.19 13:37:05 +02'00'

On behalf of:
Deloitte Audit SRL

Or Ifrah   CFO

12/22/2025 | 5:10 PM CST

Signed by:

Or Ifrah

0F2E707D8EEE45F…

3

Appendix I: CyberGhost No-logs Policy Statement

We have prepared an accompanying description of how CyberGhost protects the privacy of our customers by having effective policies and controls in place to ensure that our IT systems and underlying infrastructure are free of activity logs. We confirm, to the best of our knowledge and belief, that:

a. The accompanying description fairly presents how CyberGhost configures the IT systems and manages the supporting IT operations to ascertain that no logs are recorded and stored, related to customers' activity. The accompanying description is:

1. CyberGhost does not store or share any of the following user information:

§ Incoming and outgoing traffic information, including user and destination IP addresses, browsing history / websites visited, amount of data transferred, the VPN servers used, DNS queries, or files downloaded.

§ VPN session information, software used, connection date, and duration.

To prevent any traces of user activity on our systems, CyberGhost has taken the step of disabling all error logs and debug information for all services running on our VPN traffic servers.

Our services run in containers within the RAM, and our systems are designed to prevent human error or malicious intent that would lead to logging of user activity: if someone were to somehow enable logging within the RAM, the production servers are configured to quickly shut down, thus preventing access to the information.

In short, our architecture is designed so that CyberGhost cannot be compelled to provide information on its users' VPN activity because that information does not exist. We do not know anything about our users' browsing activities or identities while they are using our services.

2. The information above also applies to our Dedicated IP (DIP) service, which assigns customers a unique IP address that is not shared with other users. Authentication to the DIP service is achieved using an isolated service based on separate authentication mechanisms that are never associated with a user account.

3. When error logs are necessary for development or maintenance tasks, a completely new traffic server with the required specifications is created in an isolated environment. We use this process to ensure that no machine that has – or has ever had – actual users on it will ever be configured to provide logs. All debugging is done on new, sandboxed servers.

4. Our No-logs architecture is supported by a set of comprehensive deployment, change management, and incident response procedures and policies which enable us to deliver on our promise of complete anonymity and privacy.

Appendix II: CyberGhost's No-Logging Safeguards

1. To achieve our objective of zero logs on our VPN servers, we have implemented several protection measures:

> § All services are running inside containers which are ephemeral by design – any data inside the container is destroyed at the end of its lifecycle and no persistent disk storage is attached to them.

> § The containers are isolated at the network level and logging is turned off for them during the deployment process before users can access the service.

> § All VPN servers run on a RAM disk leveraging full disk encryption. Once a VPN server loses power, all data associated with it is immediately lost.

> § The only real-time system metrics that are exported to other services is hardware usage information (CPU load, memory used, etc.) and the raw number of users currently connected to the server (but not their IPs, identities, or activity). If any server health concerns that require troubleshooting are present, no details about the issue are available, and troubleshooting in an isolated environment is required to understand the root cause.

> § In addition to disabling logging at the container level, logs are also turned off at the service level for all services by redirecting their output to the null device (/dev/null).

Thanks to the measures detailed above, in the event that one of our servers were to end up in the wrong hands – or that our full disk encryption was compromised – the attackers would not be able to find any files containing information regarding our users on it.

2. Authentication to the Dedicated IP (DIP) service is done using a token-based system:

·   The DIP token can never be associated with a user on the server side
·   The DIP token is only saved in the client
·   It is impossible to associate the purchase of a specific DIP token with a user

In other words, if a user loses their Dedicated IP token, there is nothing we can do to recover it for them.

Dedicated IP / Authentication Diagram:
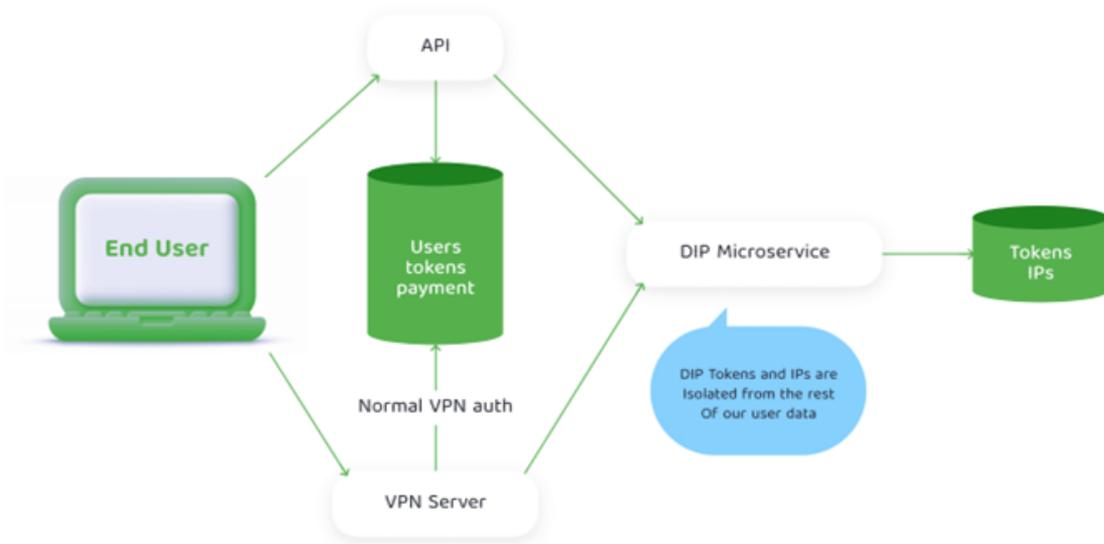
3.   In-depth information regarding our access, release, deployment, and user management policies have been offered to the auditor, together with access to all the relevant technical information (such as our server configuration).

Gen4 Server High Level Architecture
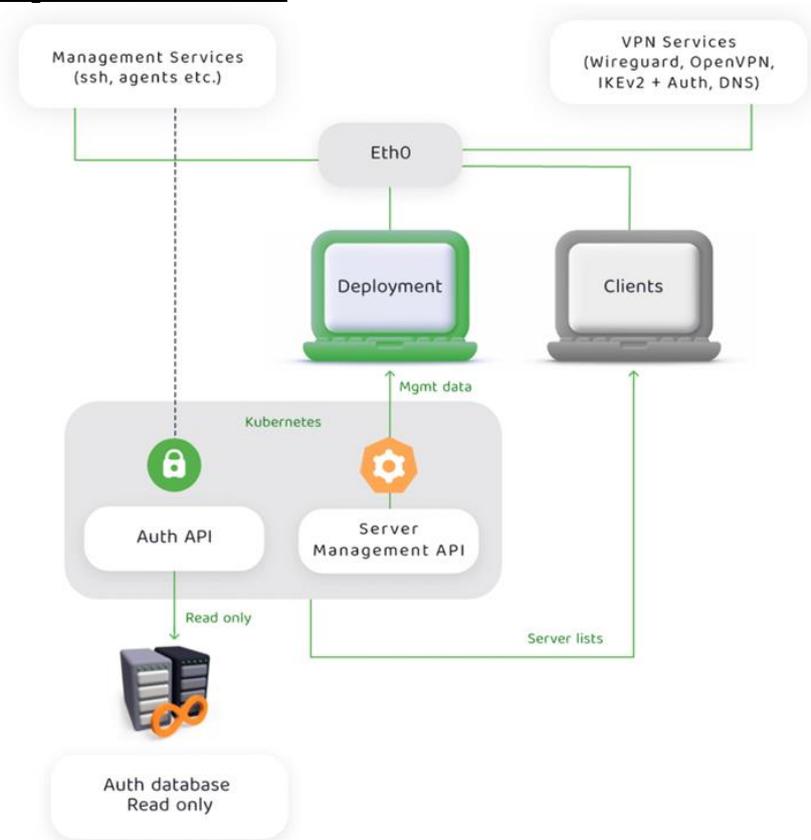
Deployment Process

Our VPN server deployment process ensures the secure deployment of our resources:
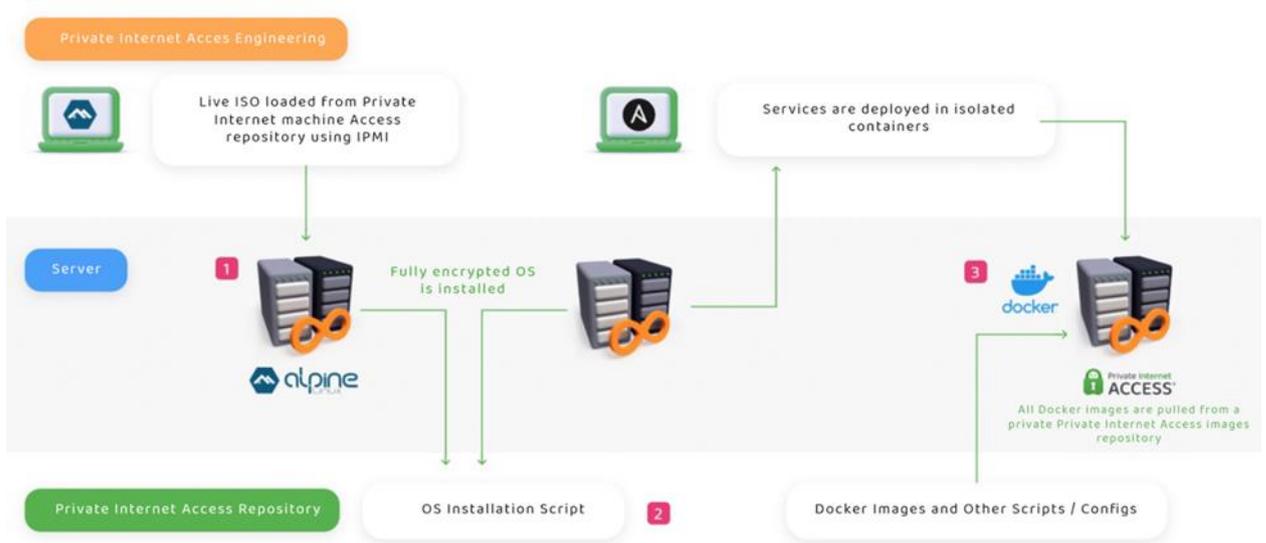
The deployment process follows the following steps:

1.   The server is booted with a standard Linux image and the initial setup begins.

2.   Arch Linux is installed with full disk encryption using a custom installation script.

3.   Additional configuration and deployment of services is done using Ansible. This includes setting up the RAM Disk, disabling logging, adding credentials, firewall rules, certificates, and VPN containers.

4.   After all checks are completed, the server can start accepting user connections.

Upgrades to VPN servers follow a slow rollout schedule. Every update must offer a technical description of all changes, an impact and risk assessment, a list of dependencies and a rollback plan. All updates must be approved by the relevant stakeholders before they can be deployed.

Release Management

The release management process is designed to ensure that no unauthorized changes can be made to our production services.

Our Release Management process covers release control for our production environments on our entire infrastructure. As part of our commitment to the highest level of uninterrupted service quality, we have strict rules to protect against various types of attacks on our infrastructure.

Every change requires an in-depth description, an implementation plan, an impact and risk assessment, a list of technical dependencies, a detailed timeline, a list of stakeholders and several approvals.

<u>Release Management – Simplified Diagram:</u>
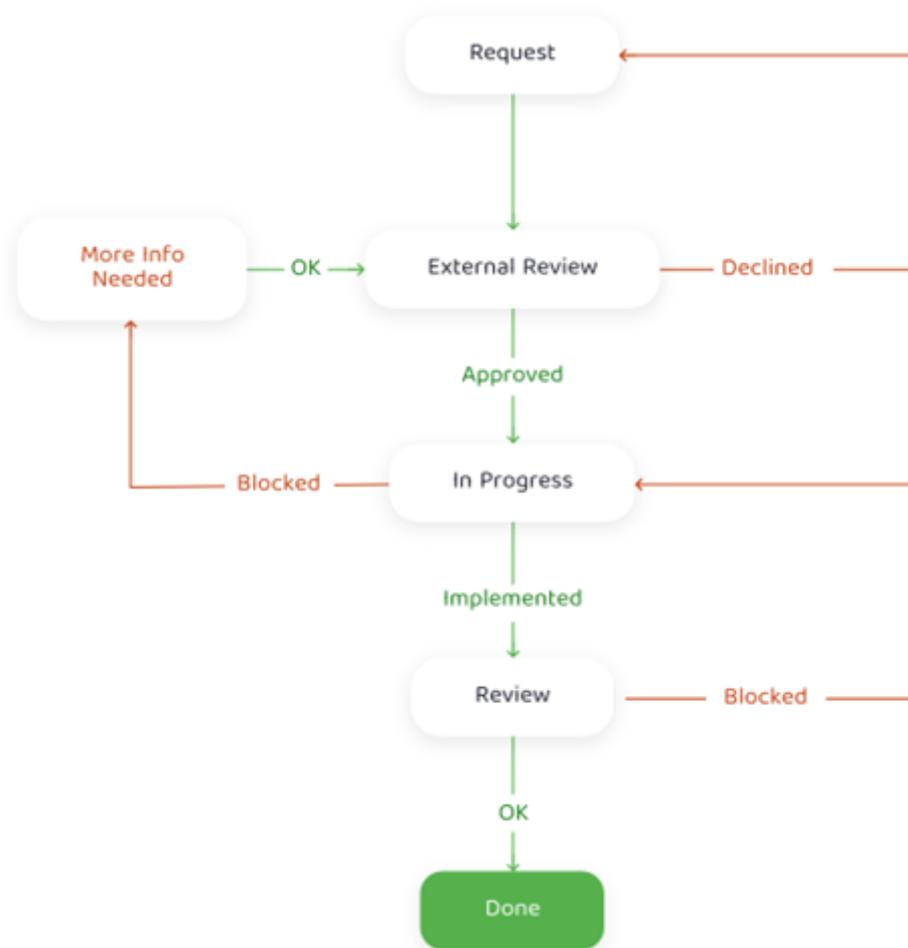
 4. Our Windows, Mac, iOS, Android, and Linux clients do not record any of our users' identifiable connection or traffic information. On certain events – such as connection attempts, connection drops, client start, login successful or settings open – some anonymized data is collected for analytical purposes. This data is not related to the identities or activities of our users, with absolutely no way of tracing it back to them. A full list of all events and recorded data has been provided to the auditor.

Deloitte.