

Deloitte.



CyberGhost

Independent Limited Assurance Report

September 2022

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 the configuration of IT systems and supporting IT operations used to provide the VPN services to customers, in accordance with the service description in Appendix I and II. Our assurance procedures concluded on 30th of June 2022.

Responsibilities of the Engaging Party

The Management of CyberGhost is responsible for preparing CyberGhost's configuration of IT systems and management of the supporting IT operations and the accompanying statement, including the completeness, accuracy, and method of presentation of the description and the statement and its implementation. This is in accordance with the criteria in respect to the description of the "CyberGhost's configuration of IT systems and management of the supporting IT operations" prepared by the Management of CyberGhost. This responsibility includes the design, implementation and maintenance of the internal control system related to the preparation of CyberGhost's configuration of IT systems and management of the supporting IT operations that are free from material misstatement, whether due to fraud or error. Furthermore, the Management is responsible for the selection and application of the criteria as set out in Appendix I and 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 fulfil our other ethical responsibilities in accordance with the IESBA Code.

Our firm applies 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 the CyberGhost's configuration of IT systems and management of the supporting IT operations and its implementation as set out in Appendix I and II.

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 in respect to the description of CyberGhost's no logging safeguards prepared by the Management of CyberGhost as of 30th of June 2022.

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 Appendix I and II to verify whether the description fulfils 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 an 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 30th of June 2022. 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 30th of June 2022 were not prepared, in all material respects, in accordance with the CyberGhost's description set out in the Appendix II.

Restriction of use and distribution

Our report is solely for the purpose set forth in this report and for the information of CyberGhost and their customers. It is not to be used for any other purpose or to be distributed to any other parties. We do not accept or assume any liability or duty of care for any other purpose or to any other person other than CyberGhost's Management.

Bucharest, 20 September 2022

Alina Mirea

Responsible Practitioner



On behalf of:

Deloitte Audit S.R.L.

Appendix I: CyberGhost Statement No Logs Policy Statement

CyberGhost has prepared the accompanying description hereunder, providing details about how we protect the privacy of our customers through effective policies and controls, which ensure that our IT systems and corresponding infrastructure remain logs free. To the best of our knowledge, we can confirm that:

- a. The accompanying description fairly represents 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:
 1. CyberGhost does not store or share any of the following user information:

§ Incoming and outgoing traffic data, 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 logs and debug information for all services running on our VPN 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 or leak our user activity: If someone were to somehow enable logging within RAM, the production servers are configured to shut down, thus preventing access to the information.

In short, our system architecture is designed so that CyberGhost cannot be compelled to provide any type of information on its users' VPN activity, because that information does not exist. We do not know anything about our users' online activities 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 methods that are not associated with a user account.
3. When error logs or/and debug information are necessary for development or maintenance tasks, a completely new VPN server is created inside an isolated environment. We use this process to ensure that no machine that has or has ever had real users on it will ever be configured to provide logs – all debugging is done on new, test environments or servers.
4. Our no-logs policy and architecture is supported by a set of comprehensive deployment steps, change management, and incident response procedures and policies which enable us to deliver on our promise of complete privacy.

Appendix II: CyberGhost's No-Logging Safeguards

1. To achieve our objective of no logs on our VPN servers, we have implemented several protection measures:

§ Every service is running inside containers which are ephemeral by design – any data that can be found inside the container is destroyed at the end of its lifecycle and no persistent storage is attached to them

§ Containers are isolated at the network level and logging is turned off for them during the deployment process before users can even 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 disabled at the service level for all services by redirecting their output to the null device (/dev/null).

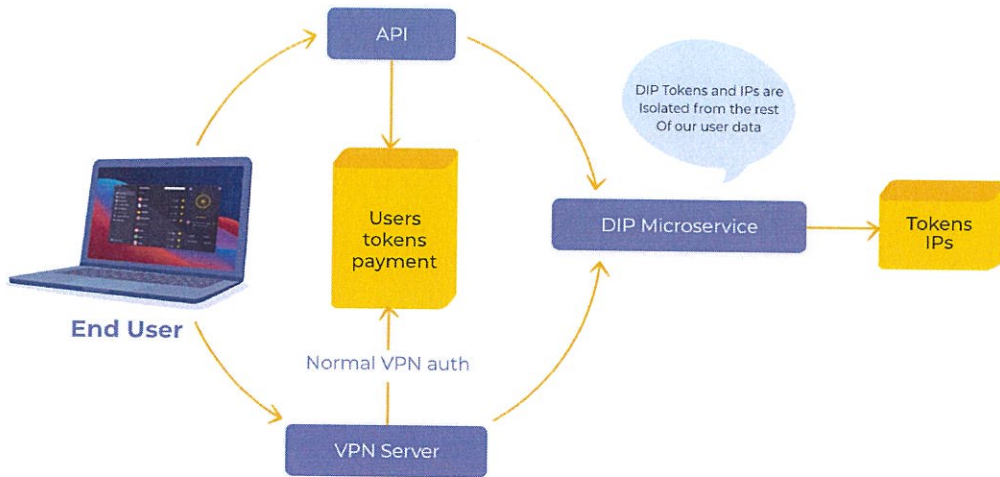
Thanks to the measures detailed above, in the event that one of our servers were to end up in the wrong hands and that our full disk encryption was compromised, the attackers would not be able to find any files containing information regarding our users on it.

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

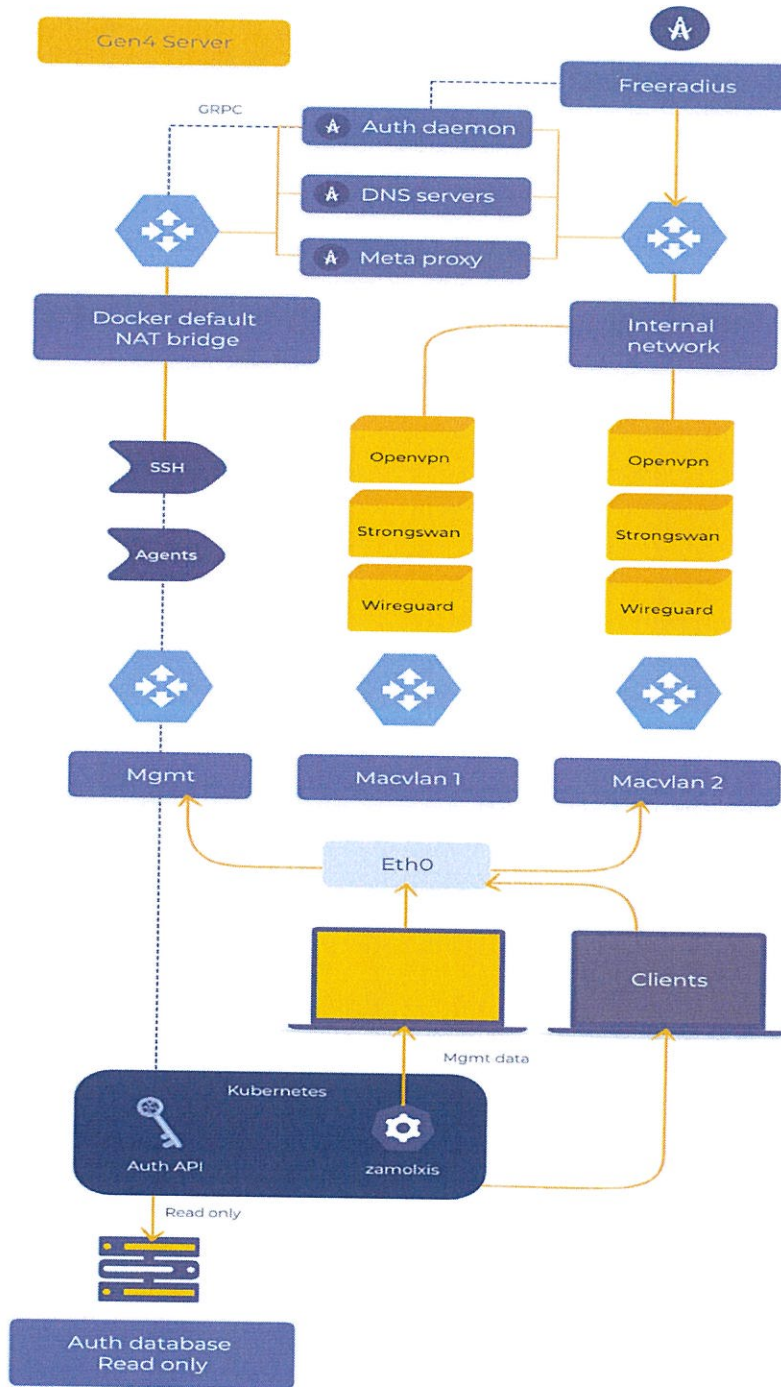
In other words, if a user loses their Dedicated IP token, there is nothing we can do to recover it for them.

Dedicated IP / Authentication Diagram:



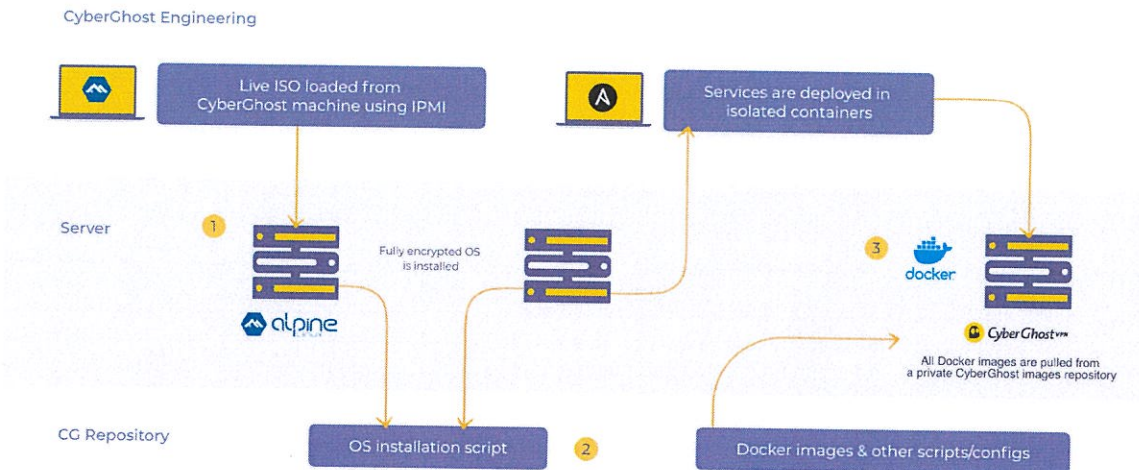
3. CyberGhost has offered to the auditor in-depth information regarding our access, release, deployment, and user management policies. This has been offered alongside access to all the relevant technical information, such as our server configuration.

Gen4 Server High Level Architecture



Deployment Process

CyberGhost's VPN Server deployment process ensures the secure deployment of our resources:



Our 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 CyberGhost's VPN servers follow a slow rollout schedule. Every update must include 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

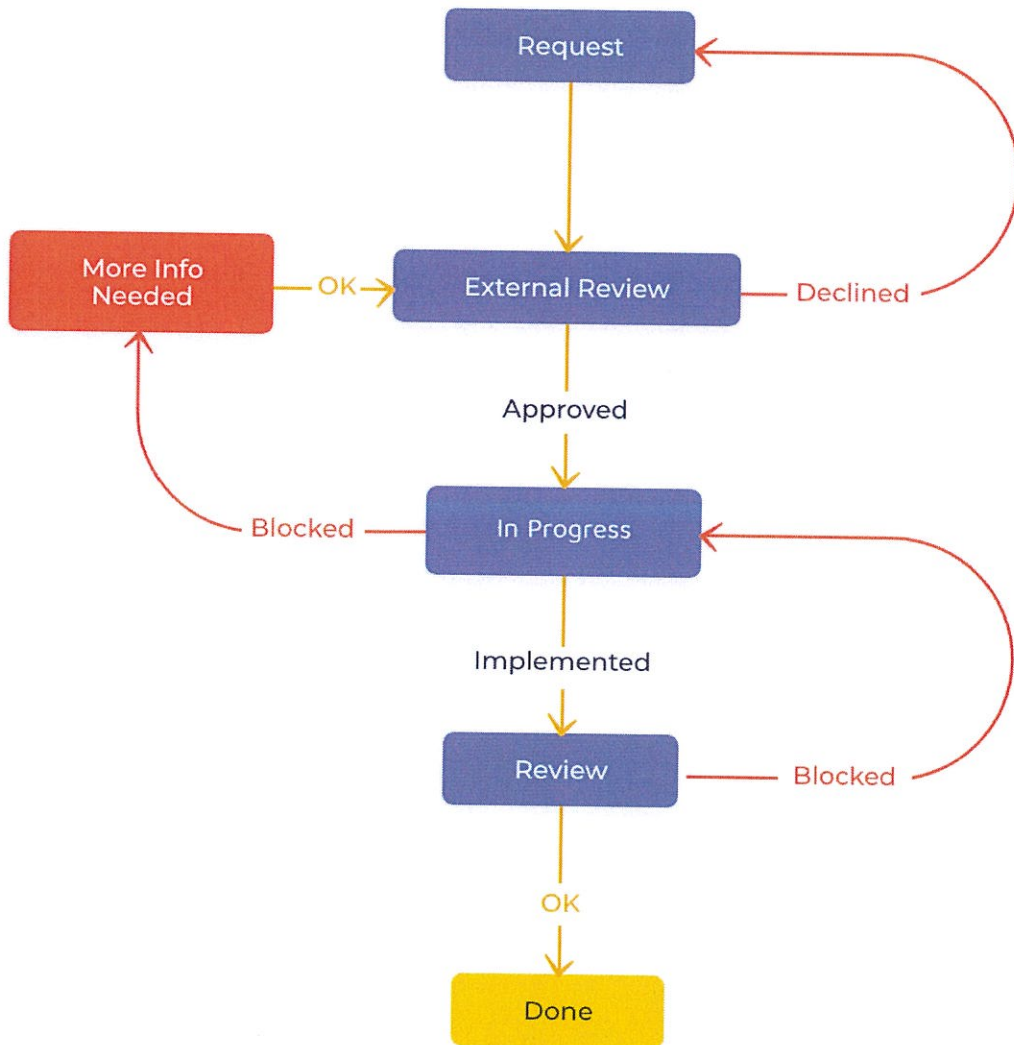
CyberGhost's release management process is designed to ensure that no unauthorized changes can be made to our production services.

Release Management:

The Release Management process covers release control for our production environments on our entire infrastructure. As part of CyberGhost's 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 multiple approvals.

Release Management – Simplified Diagram:



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 client start, login successful, connection attempts, connection drops, 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 refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/ro/about to learn more about our global network of member firms.

Deloitte is a leading global provider of audit and assurance, consulting, legal, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 330,000 professionals make an impact that matters, visit www.deloitte.com.

© 2022. For more information, contact Deloitte.Romania.