Security Questionnaire GDPR Compliance

1. What does it do, what is the architecture (cloud, hybrid, on-premise)?

A: The product Access Server is designed to create secure tunnels (VPN) over public or private networks with the goal of securing the data transferred over the secure tunnel from eavesdropping or unauthorized modification.
It is a software solution that can be self-hosted on-premise, in datacenters, or in cloud environments, on physical devices or virtual machines. The choice of deployment is up to the system administrator deploying the solution.

2. How will data be exchanged between our systems?

A: Data exchanged will be either over secure encrypted SSH and/or HTTPS for system administration purposes, and the actual data sent through the secure tunnels is encrypted using our OpenVPN protocol, and details of its operation are available on our website.
Follow Link
https://openvpn.net/community-resources/openvpn-protocol/

3. What security framework/policies is the program based on? (NIST, ISO, etc.)

A: The OpenVPN program is a publicly audited open source project with a track record of many years of excellent security.

4. Do you have a dedicated security team or is security handled as part of regular IT functions?

A: Security operations are assigned to the operations team which is tasked with overseeing deployment, management, penetration testing, and security solutions and practices, for our entire infrastructure.

5. Please describe your incident management process for responding to security events

A: Automated monitoring systems coupled with human monitoring ensure that when an issue occurs, it is noticed quickly. The operations team is spread across multiple countries across the globe (USA, Europe) for 24x7 availability to ensure rapid response in case of an issue.

6. Where is your security team located?

A: The operations team is spread across multiple countries across the globe (USA, Europe) for 24x7 availability to ensure rapid response in case of an issue.

7. Is your support team available 24x7?

A: The operations team is spread across multiple countries across the globe (USA, Europe) for 24x7 availability to ensure rapid response in case of an issue. Our support team is similarly manned for 24x7 support, even in weekends and holidays.

8. What types of advanced security technologies (i.e. DLP, IDS/IPS, SIEM, FIM, etc.) have beendeployed within any environment that stores, transmits or processes data?

A: We use centralized code-based infrastructure and security access management with internal peer-reviewed processes using well-known industry standard solutions. We have our entire infrastructure backed up in multiple ways in both full images and separate file storage, in separate data storage locations, with varying schedules depending on importance of data (weekly, daily, hourly), so disaster recovery is fast and easy, and the chance of data loss is virtually entirely eliminated. Some names of certain software we use: Bacula, CPM, Terraform, Puppet, FreeIPA. We use industry standard and custom solutions to monitoring all our systems and their log output and use anomaly detection to find deviations and act on them. Due to company security policies, we are not willing to release more detailed information as this may be considered a compromise of our internal security.

9. Is you platform protected by a WAF (web application firewall)? How is the technology implemented in terms of protected path scope and protection mode (i.e. monitor, block)?

A: For those platforms that are exposed to the Internet by necessity in order to offer certain online services, multiple layers of online filtering and protection are present before anything can ever reach our servers, both external and internal. They each have automatic rate limiting, signature detection, automated scan and reporting capabilities, and mitigation solutions such as blocking or browser/captcha checking in the event of any type of attack.

10. Which MFA (multi-factor authentication) options are available for users of your platform?

A: By default, capability for certificate-based authentication, credential-based authentication, and time limited token-based authentication is built into the OpenVPN Access Server, but there is capability for extending it to other types. By default, for example the Google Authenticator method is built in, and to name an example, Duo Security can be implemented as well.

11. How are vulnerabilities discovered, managed and mitigated (code scanning, vulnerability scans, penetration testing, bug bounty)?

A: Code scanning, vulnerability scans, and penetration testing, as well as internal code reviews, and reports sent in through our secure security email address. OpenVPN is an open source project and this openness means it can be audited by anyone. It is audited by OpenVPN open source community, the OpenVPN Inc. company, and various projects like OSTIF for example which are aimed at having security companies like FoxIt and Quark Labs audit our code to find any issues. They are then resolved and updates released to address these.

12. How is security included as part of your software development life cycle (SDLC)?

A: Any urgent security issue will be mitigated with hotfixes or emergency update releases. With every release any known security issue is prioritized and resolved.

13. What data will you be storing about us?

A: Email address (required) and optionally any information you provide us like company name, contact name, company address (for invoicing purposes). For OpenVPN Access Server for licensing purposes an irreversible hash is stored of certain hardware specifics of your servers that you run an activated Access Server on. Because the hash is irreversible, its only use is for the purpose of preventing unauthorized duplicate use of a purchase license on multiple servers, and it used only as such

14. How do you ensure that production data is never used a development or test environment?

A: Dedicated software repositories and totally separate infrastructures for quality assurance, development, and production purposes, exist in our infrastructure. Code must be peer-reviewed before it goes to production environment. The flow of information is only in the direction from development, then QA, and then production purposes, and never the other way around. The different environments have no direct contact with each other.

15. How will the data shared with you be encrypted while at rest and in transit?

A: Standard HTTPS and SSH encryption are applied, as well as encryption of data using AES-256, SHA-256 or brcypt irreversible hash with unique salt.

16. What additional safeguards are in place to protect user credentials beyond the use of basic encryption?

A: All other security measures mentioned earlier, and on top of that, the data is only accessible on our internal production environment, and not outside of it

“We use centralized code-based infrastructure and security access management with internal peer-reviewed processes using well-known industry standard solutions. We have our entire infrastructure backed up in multiple ways in both full images and separate file storage, in separate data storage locations, with varying schedules depending on importance of data (weekly, daily, hourly), so disaster recovery is fast and easy, and the chance of data loss is virtually entirely eliminated. Some names of certain software we use: Bacula, CPM, Terraform, Puppet, FreeIPA. We use industry standard and custom solutions to monitor all our systems and their log output and use anomaly detection to find deviations and act on them. Due to company security policies, we are not willing to release more detailed information as this may be considered a compromise of our internal security.

And on top of that, the data is only accessible on our internal production environment, and not outside of it.”

17. Where in the world will our data be stored?

A: In the United States of America. No data is stored outside of the US

18. For how long will data about our organization be kept following a contact termination?

A: Until a request is put in to delete it, or we migrate to a new system that requires that only active accounts are migrated, and inactive accounts are marked obsolete.

19. Is MFA implemented as an internal access control for critical systems, production systems and remote access (VPN)?

A: MFA and other security measures are implemented for our systems.

20. How do you provision and manage the equipment used by your workforce?

A: Due to company security policies, we are not willing to release information on this as this may be considered a compromise of our internal security.

21. Is staff equipment protected by an anti-malware platform?

A: Yes, anti-malware, anti-virus, etcetera.

22. How is resource access authorized, provisioned and audited?

A: We use centralized code-based infrastructure and security access management with internal peer-reviewed processes using well-known industry standard solutions.

23. What security measures are new hires required to adhere to prior or as part of onboarding? (Acceptable Use Policy acknowledgement, non-disclosure agreement, background check)

A: Backgrounds checks are performed, personal assessment by multiple (management) team members within the company, continuous reassessment in the team, non-disclosure agreements, and standard employment contracts.

24. How frequently do you perform internal security awareness training and what does it cover?

A: Due to company security policies, we are not willing to release information on this as this may be considered a compromise of our internal security.

25. Please describe your approach to disaster recovery (i.e. built-in redundancies across geographical regions, hot/warm/cold sites).

A: For all essential services multiple load-balanced redundancies exist that are stored in physically separate data centers to ensure that any interruption either goes entirely unnoticed to our customers, or can be mitigated within an extremely short period of time, so loss of service is virtually entirely eliminated. In the event of an extremely wide spread disaster, we have our entire infrastructure backed up in multiple ways in both full images and separate file storage, in separate data storage locations, with varying schedules depending on importance of data (weekly, daily, hourly), so disaster recovery is fast and easy, and the chance of data loss is virtually entirely eliminated.

26. What are your expected RTO and RPO times?

A: This is measured in minutes, or at the outside in extreme situation, a few hours, at the most.

27. Which compliance program is your organization certified to? (SOC, ISO, PCI-DSS, Privacy Shield, Cloud Security Alliance, HIPAA)?

A: We are not certified to those programs. We maintain and continuously develop and improve our own security. We are a world leader in security solutions.

28. Is there an individual responsible for ensuring compliance with privacy, security, legal and regulatory requirements?

A: We have a company member that is dedicated to ensuring we are compliant with regulations in terms of law, privacy, regulatory bodies, and so on, and we have legal counsel in those areas as well.

29. Do you have a public privacy policy? If yes please provide a link.

A: Yes, https://openvpn.net/privacy-policy/

30. Please indicate below which of the following you will be providing to our procurement team (via email) in order to help validate your answers. Security assurance, i.e. pentest reports, vulnerability scans, links to public bug bounty programs, external audit reports, i.e. SOC2 Type II, ISO 27001

A: External Audit Reports. You may consult Quarks Labs, and the OSTIF project, for verification of the external audits performed on our OpenVPN code.

OPENVPN®