Le Sphinx

Security Declaration

Last update : 2025/02/05

Table des matières

1 Introduction

Sphinx Développement has been publishing and distributing software solutions dedicated to surveys and data analysis for over 30 years. For more than 20 years now, Sphinx Développement has been offering hosted services to enable its clients to carry out online survey projects independently. A set of applications is thus directly accessible via the Internet to configure questionnaires, distribute surveys, host all collected data, and share results in the form of interactive reports. This document aims to list and describe all the measures taken and the systems put in place to meet these objectives of availability, confidentiality, and integrity.

2 Infrastructure

2.1 Hosting

The servers are hosted in the Datacenter of the company OVH, which ensures their physical security. The datas are stored in Roubaix, Strasbourg, and Gravelines in France. The provision and operation of the infrastructures (Datacenter, servers, networks) ensured by OVH are ISO 27001 certified. The server management is handled by our services. Our host does not have access to the data stored on our servers and provides the necessary guarantees regarding the non-intrusion of individuals into their data centers.

Location of the datacenters:
- Route de la ferme Masson, 59820 Gravelines, France
- 2 Rue Kellermann, 59100 Roubaix, France
- 140 Quai du Sartel, 59100 Roubaix, France
- 201 boulevard Beaurepaire, 59100 Roubaix, France
- 9 Rue du Bass. de l'Industrie, 67000 Strasbourg, France

2.2 Network and Communication Protocols

The production servers are isolated in a DMZ and are protected against intrusions by a network firewall. The DMZ zone is accessible from the internet only via the TCP protocol on ports 80 and 443. Traffic arriving on port 80 (http) is automatically redirected to port 443 (https).

OVH integrates a mitigation solution that protects the infrastructure from a massive denial-of-service attack without blocking legitimate traffic.

All data exchanged between client software (web browser or Sphinx IQ2/IQ3) and the server are encrypted via the TLS protocol.

SSL protocols are disabled. The minimum version of the TLS protocol that can be used is TLS 1.2.
Certificates are generated from 2048-bit keys and signed with the sha256 algorithm.

2.3 System access control

Access to the servers is restricted to the operations service personnel (<8 people) and is done through a VPN connection (IPsec or SSL tunnel with two-factor authentication). The domain administrator access, physical machine administrator access, and virtual machine administrator access are distinct. Each of these accesses is nominative.

The passwords for these administrators follow the following policy and must:

- Contain at least 14 characters, including at least one digit, one lowercase letter, one uppercase letter, and one special character
- Be different from the previous 24 passwords
- Be changed every 6 months

After 5 unsuccessful access attempts, account authentication is blocked for 60 minutes.

Access rights are reviewed at least semi-annually based on the principle of least privilege. In case of contract termination, access is revoked immediately.

The local administrator passwords for each machine are changed to distinct passwords of at least 22 characters, including at least one digit, one lowercase letter, one uppercase letter, and one special character.

2.4 Anti-virus Protection

Software antivirus protection is installed on all servers. Its administration is centralized. Alerts are reported in real-time, and the protection is checked daily. The strategies include:

- A full scan every week
- Real-time protection
- An update of the signature database every thirty minutes on average.

Workstation security

Workstations are password-protected, disks are encrypted (BitLocker), and the computer locks automatically after 10 minutes of inactivity. Only privileged users (IT department) and technical teams (support, product, development, operations) are administrators of their workstations. All workstations have antivirus protection and a local firewall.

2.5

Availability

A server availability rate of 99.9% over 365 days is guaranteed for Sphinx servers. This rate does not account for interruptions due to scheduled maintenance. Scheduled maintenance occurs on average
2.6 1 to 2 times per month between 3:00 AM and 4:00 AM (Paris time by default). If maintenance needs to be performed outside this time slot, the details of the intervention are communicated to the account owners or the responsible administrators two weeks in advance.

Service continuity

2.7 Service continuity measures are described in the service continuity plan. This document is confidential but covers the following points:

- Context and infrastructure
- Diagnostic assistance and intervention trigger thresholds
- Failure scenarios
- Loss of network connectivity: Vrack, VLAN configuration, etc.
- Physical server hardware failure: Host, domain controller, backup server
- Failure of the virtual machine acting as a firewall or loss of its configuration

In case of server failure, the service will be restored on another machine within a maximum of 8 hours following the notification of the failure. The maximum data loss, depending on the failure scenario, ranges between 6 and 24 hours.

Since the servers are currently hosted by OVH (https://www.ovh.com), the continuity of SPHINX services is subject to the internet access provided by OVH. In case of interruption of this service, for any reason, LE SPHINX DEVELOPPEMENT commits to doing everything possible to find a new provider.

Data is stored on RAID disk arrays. A monitoring system alerts our teams in case of disk failure.

Monitoring

Applications, systems, and the network are monitored 24/7. Remote access tests to applications, internationally, are regularly conducted by the company INTERNETVISTA (www.internetvista.com). Our teams intervene from 8 AM to 11 PM (Paris time), 7 days a week, in case of alerts raised by the monitoring tools.

2.8

Backup Management

Backups :

- Daily backups are retained for 3 to 4 months
- 2.9 Full monthly backups are retained for 6 months

These backups are encrypted using the AES (256-bit) algorithm.

Backup data is replicated daily between the data centers in Roubaix, Strasbourg, and Gravelines and is stored on a different VLAN from the backed-up machines.

Restoration tests are performed quarterly.

Update Management

2.10

Operating system updates are performed within a maximum of 7 days after the patches are made available. The approval of updates is done manually (WSUS features).

The impact of updates are first evaluated on test and pre-production environments.

2.11

Data encryption at Rest

The hard drives of the servers are encrypted with the BitLocker solution. The encryption keys are
2.12 stored in a password manager. Access to this manager is limited to system administrators.

Logging and Monitoring

All server access logs, a large portion of system logs, and all web server logs are sent in real-time to a
2.13 centralized logging system. Alerts are configured at the SIEM level to escalate events requiring diagnosis or intervention by the teams. The retention period is at least 60 calendar days.

Attack Surface Restriction Policy

Servers are configured to expose or use only the functionalities, protocols, and services strictly necessary for the execution of applications and the services offered.

3 Developpement Security

Environnement Segmentation

Development, pre-production, and production environments are configured on separate virtual machines and databases. Production environments are not accessible by developers. Data used for testing is fictitious or anonymized.

3.1

Training and awareness

The development and operations teams are trained and made aware of best practices and compliance with the OWASP Top 10.

3.2

Design and Specification

3.3 Functionalities are designed to:

- Adhere to the principle of "security by default"
- Warn users in advance of any action impacting data security
- Propose a strong password level

3.4 Best Practices

External inputs (text values, external data, or third-party libraries) are systematically verified and filtered if necessary. Output filtering is performed for applications that serve content to users.

Deep inspection is systematically performed on uploaded files.

Development techniques include several mechanisms to protect against SQL injections:

- Input data validation
- Parametrically constructed SQL queries
- Use of an ORM

Special attention is given to:

- Blocking enumerations
- File recording and reading
- Cross-site scripting (XSS) injections
- Cookie protection

Evolution Management

Source code control is implemented, allowing branch management, new versions, and tracking of deployed fixes. Release notes are maintained at multiple levels.

The source code control server is internalized and administered by the operations team. It is
3.5 accessible only via VPN.

Dependency Monitoring

An alert system for the versions of libraries used in our applications is in place: obsolete versions or those affected by vulnerabilities are monitored. Integration of new versions is carried out as soon as
3.6 possible in accordance with the functional continuity of applications and associated risks.

4 Application

4.1 Authentication and Acces Protection

User account security is ensured by login/password.

Users must set their password upon their first login.

Passwords are stored on servers in a non-reversible encrypted manner (HASH PBKDF2 HMAC-SHA256, 128-bit salt, 256-bit subkey, 10000 iterations).
Passwords must meet certain minimum complexity requirements (12 alphanumeric characters and special characters) and must be changed at least every 6 months.
The last 5 passwords cannot be reused.
After 5 unsuccessful login attempts, account access is blocked for 5 minutes.

Two-factor authentication is available, allowing users to protect account access with a second one-time code generated by a third-party application or a personal key.

Access to surveys and/or additional modules can also be password-protected. This protection is enabled by default.

By default, sessions are time-limited like so:

8 rolling hours for user profiles
45 non-rolling minutes for administrator profiles

Solution administrators can log into a user account. This type of access is only allowed in case of assistance requests or suspicion of data confidentiality or integrity breaches. The validity period for this type of access is set to 20 non-rolling minutes.

Beyond these periods, the tokens used are revoked and cannot be reused.

Session cookies are revoked upon user logout.

Incident Management

The technical support service is accessible at +33 4 50 69 82 98 from Monday to Thursday from 8:30 AM to 12:30 PM and from 2:00 PM to 6:00 PM, and on Friday from 8:30 AM to 12:30 PM and from 2:00 PM to 5:00 PM (Paris time). Correction times are indicative and start from the notification of the problem, depending on the type of anomaly.

4.2

FUNCTIONAL ANOMALY		
Type	Definition	Correction Time
Blocking	Any anomaly making the use of a functionality impossible, without a workaround.	Within 8 Working Hours
Major	Any anomaly causing degraded operation of at least one functionality.	Within 72 Working Hours
Minor	Any anomaly with a workaround, without degrading overall functionality.	Provided during minor updates

SECURITY VULNERABILITY			
Risk level	Impact	Exploitability	Correction Time
Critical	Critical	Easy to moderate	Within 8 Working Hours
	Major	Easy	
Major	Critical	High	Within 72 Working Hours
	Major	Moderate to High	
	Important	Easy	
Important	Critical or Major	Hard	Provided no later than the next minor update
	Important	Moderate to Hard	
	Minor	Easy	
Minor	Important	Hard	Provided no later than next minor updates
	Minor	Moderate to Hard	

4.3

Exchange security

When publishing or importing a survey from the Sphinx IQ3 client software, the files exchanged between the server and the software are stored in an encrypted archive (AES 128-bit algorithm). File exchange is only performed after verifying the user's login/password pair (encrypted request using AES 256-bit).

4.4 Datas Reversibility and Portability

It is possible to export survey data, email campaigns, or SMS campaigns in various standard formats such as .csv or .xlsx. Customer accounts and associated data are deleted from the production servers two months after the subscription expires or the service ends. Clients can contact technical support for the return or destruction of data before the end of these two months. A destruction report can be provided upon request.

4.5 Traceability and Logging

Requests and connections are recorded in application event logs. These logs capture all connections, registrations, modifications, navigation actions of respondents, etc. These logs are backed up and retained for a period of one year, after which they are automatically deleted.

4.6 Cookies

The SphinxOnline solution uses only technical cookies necessary for the proper functioning of the applications for the following purposes:

- Security assurance: authentication, access control, etc.
- Preferences: language choice, current working directory, display options, etc.

These cookies are not shared with any third parties and are not used for advertising or targeting purposes.

4.7 Application Filtering

An application firewall (WAF) provides additional filtering upstream of the SaaS solutions. This solution acts as a reverse proxy and provides multiple levels of filtering:

- IP reputation
- Behavioral detection
- Deep request analysis to detect known or generic attacks, cross-site scripting attempts, etc.

5 Administrative and Oragnizational Security

5.1 Security Breach Management

SPHINX DEVELOPPEMENT is committed to ensuring the integrity of the network and systems against any external malicious acts or known cyber-attacks.

In the event of an attempt or suspicion of information security breach or personal data theft, we commit to notifying the account owner within 8 Business Hours from the discovery of the issue.

Our teams monitor alerts issued by CERT-FR daily and, when necessary, take appropriate measures to protect against the vulnerabilities mentioned in these alerts, which may involve applying patches or implementing recommendations.

5.2 Security Incident Management

In the event of a security incident, the DPO (dpo@lesphinx.eu) and the CISO must be informed as soon as the problem is identified. Within two hours of the initial diagnostic phase, a preliminary qualification of the incident is made to take appropriate remedial measures (service interruption, access limitation, etc.). If necessary, DPO and/or CISO will initiate a crisis management situation to mobilize all available resources.

Depending on the origin of the problem, corrective or mitigation solutions must be proposed and decided upon in an appropriate security committee, including at least one member from each affected service. Measures taken may include application modifications, system and network hardening, applying vendor patches, etc.

Impacted clients will be informed as soon as possible, within a maximum of 8 business hours from the discovery of the problem. Partial communication is possible in case of incomplete diagnostics, provided it is mentioned and followed by subsequent communications. Preferred contacts will be those involved in previous exchanges regarding the incident or, failing that, account holders or project managers identified in the ERP.

A "post mortem" report will be drafted and communicated for incidents with strategic or critical impact. In case of an incident, clients will be notified on the Sphinx Online login page. For major incidents, affected account holders may also be notified by email.

Control and Monitoring Measures

A configuration audit and penetration tests on the solution are conducted annually by an external firm specialized in IT security. A summary of the latest counter-audit report is available upon request.

Any critical vulnerabilities identified during these audits are addressed as quickly as possible.

5.3

An internal document lists all known vulnerabilities, potential improvements, and possible security developments.
The information is sourced from:

- Security bulletins (vendors, CERT-FR, ANSSI, etc.)
- Client feedback and needs
- Audit summaries
- Issues related to software and/or hardware developments
- ...

Each item in this document is categorized based on several criteria (exploitability, implementation difficulty, criticality, probability, etc.). This document is reviewed monthly to update elements according to the state of the art in security and to prioritize and define upcoming actions.