Security Statement

SphinxOnline

Last update: 29/03/2024

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

Summary

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

1 Introduction

Sphinx company publishes and distributes solutions for surveys and data analysis since 1985.
For over 25 years, Sphinx provides hosted services to lead online surveys projects.
SphinxOnline solution is directly accessible on Internet to allow to create questionnaires, distribute surveys, hosting data and share results in interactive reporting.
Since, security and availability has become one of our main concerns.

This statement aims to list and describe all measures to meet this goal.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2 Infrastructure

2.1 Hosting

The servers are hosted in the OVH Datacentre, which provides physical security. The data is stored in Roubaix, Gravelines and Strasbourg, France.
The hosting services and infrastructures (Datacentre, servers, networks) provided by OVH are certified ISO 27001.
Server management is provided by our services. Our provider does not have access to the data stored on the servers.

Datacentres location:

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 intrusion by a network firewall.
The DMZ zone is only accessible on internet over the TCP protocol on ports 80 and 443.
Traffic arriving on port 80 (http) are automatically redirected to port 443 (https).

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

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

SSL is disabled. The minimal usable version of TLS is TLS 1.2.
Certificates are generated from 2048 bits keys and signed with the sha256 algorithm.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.3 System Security

Access to the servers are restricted to IT department employees (<8 persons) and is secured through a VPN connection (IPsec or SSL with two-factor authentication tunnels).

Domain administrator, physical machine administrator and virtual machine administrator access are different. Each access is nominative.

The passwords of these administrators comply with the following policy rules and must:

- be at least 14 characters long
- have at least one number, one lowercase letter, one upper case letter, one special character
- be different from the previous 24 passwords
- be renewed every 6 months

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

Access rights are reviewed quarterly. When an employee leaves the company, access is immediately revoked.

The passwords of the local administrators of each machine are changed to passwords of at least 22 characters with at least one digit, one lowercase, one uppercase and one special character.

2.4 Anti-virus protection

Software antivirus protection is installed on all servers and antivirus administration is centralized. Alerts are reported in real time and protection is checked daily.

The strategies in place include, among others:

- complete analysis every week
- real-time protection
- daily update of the signature database

2.5 Workstations security

Workstations are password protected. Disks are encrypted using BitLocker. Computer is automatically locked after 10 minutes of inactivity.

Only users with privileges (IT department) and technical teams (support, product, development, exploitation) are workstation administrators.

All workstations are protected by antivirus software and local firewall.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.6 Availability

An availability rate of 99.9% for Sphinx servers is guaranteed over 365 days.
This rate does not consider interruptions related to scheduled maintenance.
This one is held once or twice a month between 3:00 am and 4:00 am (Paris time).
If they have to be held outside this time period, the details of the intervention will be communicated to the account owners or their administrative manager at least two weeks before.

2.7 Continuity of service

The service continuity arrangements are described in the service continuity plan.
This document is confidential but covers the following points:

- Background and infrastructure
- Diagnostic assistance and intervention triggers
- Failure scenario
- Network Connectivity Loss: Vrack, VLAN configuration, ...
- Physical server hardware failure: Host, domain controller, backup server
- Failure of the virtual machine acting as a firewall or loss of its configuration

In the event of server failure, the service will be restored to another machine within a maximum of 8 hours after notification of the failure.
The maximum data loss is 24 hours.

The servers are currently hosted by OVH (https://www.ovh.com), so the continuity of SPHINX services is subject to the continuity of Internet access provided by OVH. In the event of interruption of this service, for any reason whatsoever, LE SPHINX DEVELOPPEMENT undertakes to do everything possible to find a new supplier.

The data is stored on disk groups in RAID configuration. A monitoring system alerts our teams in the event of a disk failure.

2.8 Monitoring

Applications, systems and network are monitored 24 hours a day, 7 days a week.
Remote access tests to applications from different location are carried out on a regular basis by INTERNETVISTA (www.internetvista.com).
Our teams operate from 8am to 11pm, 7 days a week in the event of an alert being sent up by the different monitoring tools.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

2.9 Backup Management

The data are backed up:

- daily are kept for a maximum period of 4 months
- monthly for a maximum period of 6 months (full backup).

They can be retrieved on demand until 2 months after the expiration of the subscription.
These backups are encrypted using the AES algorithm (256 bits).

Backup data is replicated between the Roubaix, Gravelines and Strasbourg datacentres and stored on a different VLAN from the machine saved.

Restore tests are done quarterly.

2.10 Update Management

Operating system updates are performed within a maximum of 7 days after the patches are made available. Updates are approved manually (WSUS features).

Updates impacts are previously monitored on test and pre-production environments.

2.11 Data encryption at rest

Servers hard drives are encrypted with the BitLocker solution.
Encryption keys are saved in a password manager. Only system administrators can access this vault.

2.12 Logs and surveillance

All server accesses, web server logs and part of the system logs are sent in real time to a log centralisation system.
Alerts are configured on the SIEM to notify events requiring team's diagnostics/actions.
Logs are retained for 60 days.

2.13 Attack surface reduction policy

Servers are configured to only use functionalities, protocols and services required for the execution of the applications and services offered.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

3 Development security

3.1 Environments partitioning

Development, pre-production and production environment are set on separated virtual machines and distinct databases.

Production environments are not accessible by developers.

Data used for test activities are fictitious or anonymized.

3.2 Formation and awareness

Development and operational teams are aware about best practices and TOP 10 OWASP respect.

3.3 Design and specification

Functionalities must:

- respect the "security by default" principle
- alert users when their action might affect data security
- suggest strong passwords

3.4 Best practices

External inputs (textual values, external data or third-party libraries) are always verified and filtered when needed. Application data outputs are also filtered when they serve content to users.

Deep inspections are systematically done on uploaded files.

Development techniques include several mechanisms to protect application against SQL injections like input data validation, parametric construction of SQL request, use of an ORM…

A special attention is paid to:

- enumeration locks
- files saving and reading
- cross-site scripting
- cookies protections

3.5 Changes management

A source code control is set. It allows branch, versioning and change tracking.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

The source code control server is internal and administered by the operational team. Server is accessible only by VPN.

3.6 Dependencies monitoring

Libraries version used in our applications are checked. If a version is obsolete or known to be affected by vulnerabilities, our teams will be alerted. In accordance with the functional continuity of applications and risks, new versions of these libraries are integrated as soon as possible.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4 SphinxOnline solution

4.1 Access protection

The security of the user accounts is ensured by login / password.

Users must define their password at the first connection.

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 to a minimum every 6 months.
The last 5 passwords cannot be reused.
After 5 unsuccessful access attempts, the account login is blocked for 5 minutes.

Dual factor authentication is available. This allows the user to protect access to the account with a second one-time code generated by a third-party application or personal key.
Access to surveys and / or add-ons can also be password protected. This protection is active by default.

By default, sessions are limited in time as following:

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

Administrators can connect to user accounts. This kind of access is allowed only on assistance demands or when damages to data confidentiality/integrity are suspected. In this case, the access validity is set to 20 non-sliding minutes.
Beyond these deadlines, tokens are revoked and cannot be reused.

Sessions cookies are also revoked at user logout.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4.2 Incident management

The technical support service is available at 04 50 69 82 98 from Monday to Thursday from 8:30 am to 12:30 pm and from 2 pm to 6 pm and Friday from 8:30 to 12:30 and from 14h to 17h (Paris time).

The response times for performing a corrective update depend on the type of anomaly:

MALFUNCTION		
Type	Definition	Correction time
Blocking	Refers to any anomaly that makes it impossible to use a feature without a workaround.	Within 8 working hours
Major	Refers to any anomaly involving degraded operation of at least one feature	Within 72 working hours
Minor	Refers to any anomaly that has a workaround, without degrading the overall operation.	Available during minor updates

The correction time starts at the discovery of the problem.

VULNERABILITIES			
Impact level	Impact	Ease of exploitation	Correction time
Critical	Critical	Easy to Moderate	Within 8 working hours
	Major	Easy	
Major	Critical	High	Within 72 working hours
	Major	Moderate to high	
	Significant	Easy	
Significant	Critical ou Major	Difficult	Available during next minor updates
	Significant	Moderate to high	
	Minor	Easy	
Minor	Significant	Difficult	Available during minor updates
	Minor	Moderate to difficult	

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

4.3 Transmission security

When publishing or importing a survey from the Sphinx IQ / IQ2 software, the files exchanged between the server and the software are stored in an encrypted archive (128-bit AES algorithm).
The transmission is only done after checking the user's login/password (request encrypted in AES 256 bits).

4.4 Reversibility and data portability

It is possible to export survey, email or SMS data in different standard formats like .csv or .xls.

Client accounts and associated data are deleted from production servers two months after subscription or service end.
The technical support must be contacted for data destruction or restitution within these two months. On demand, a destruction certificate can be provided.

4.5 Traceability

Queries and connections are logged in application event logs. These logs record all the connections, recordings, modifications, navigation actions of the respondents, ... These logs are kept for a period of one year then 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 guarantee: authentication, access control, ...
- Preferences: Choice of language, current working directory, display options, ...

These cookies are not communicated to any third party and are not exploited for advertising or targeting purposes.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

5 Administrative and organizational security

5.1 Vulnerabilities management

SPHINX DEVELOPPEMENT is held to an obligation of means to ensure the integrity of the network and systems against any act of external malicious or known cyber-attack.

In the event of an attempt or suspicion of breach of information security or theft of personal data. We undertake to notify the owner of the account within 8 business hours from the discovery of the problem.

Our teams monitor daily the alerts issued by CERT-FR and, when necessary, take the appropriate measures to guard against the vulnerabilities mentioned in these alerts, which may involve the application of corrective measures or the implementation of recommendations.

5.2 Security incident management

When a security incident is identified, the DPO and CISO must be informed as soon as possible.

Within two hours after the initial diagnosis, a first qualification of the incident is made to decide on appropriate workarounds (service interruption, access limitation, etc.). If needed, we will mobilise all available resources and pass in a crisis management situation.

A security committee, with at least one representative per department concerned, will propose corrections or mitigations. These solutions may imply system and network hardening, changes to system applications, patching, etc.

We undertake to notify impacted clients and competent authorities (CNIL) within 8 business hours from the discovery of the problem. In case of incomplete diagnosis, a partial disclosure can be considered by mentioning it and with subsequent communications. The preferred contacts will be those included in previous exchanges concerning the incident or, failing that, the account holders or project managers identified in the ERP.

A post mortem statement will only be prepared and communicated for incidents with a strategic or critical impact.

In the event of an incident, clients are notified on their SphinxOnline login page. For major incidents, concerned account owners may be notified by e-mail.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34

5.3 Control and monitoring measures

A configuration audit and intrusion tests on the solution are performed each year by an external firm specializing in computer security. The summary of the last audit report is available on request.

Any critical faults reported during these audits are corrected as soon as possible.

An internal document lists all possible improvements in terms of security.
The information comes from:

- security bulletins
- customer feedback
- audit summary
- issues related to software/hardware upgrades

Each element of this document categorized according to several criteria (exploitability, difficulty of implementation, criticality, probability ...). A monthly review of this document is performed to update the elements with regard to the state of the art in terms of safety and to define future actions.

LE SPHINX DEVELOPPEMENT
Parc Altaïs – 27 Rue Cassiopée – 74 650 CHAVANOD - France
Phone : +33 4.50.69.82.98 - Fax : +33 4.50.69.82.78
Email : contact@lesphinx.eu Web : www.lesphinx.eu
SARL au capital de 100 000 € - Code NAF 5829C - Siret : 398 616 342 000 34