Signify V10 Security FAQs

Service Organisation Control Maturity

Question:

- Is the solution provided part of a valid ISO 27001 certification? If so, please provide a valid ISO/IEC 27001 certificate with the corresponding SOA - Statement of Applicability.

  > Yes. Awaiting certificate from BSI. External Audit completed 4 Dec 2024.
  >
  > Link to SOA: F60_Statement of Applicability.xlsx

- Has the solution provided been audited following SOC 2 standards (e.g., SSAE 16; ISAE 3402) type II within the last year? If so, please provide a valid SOC 2 Type II report covering the solution in scope (following SSAE 16 / ISAE 3402 audit standards).

  > No

Hosting Environment Control Maturity

Question:

- Is the data center hosting environment storing Nestlé data ISO 27001 certified? If so, please provide the ISO 27001 certificate as well as the Statement of Applicability (same version as the one highlighted in the certificate).

  > Yes, we host with Teraco in Isando and their ISO documentation is available on their website: Certifications and Compliance • Teraco

- Has the data center hosting environment storing Nestlé data been audited following SOC 2 standards (e.g., SSAE 16; ISAE 3402) type II within the last year? If so, please provide the SOC 2 type II report.

> Please refer to Certifications and Compliance • Teraco

Penetration Test Report

Question:

- Has an independent third party performed a Penetration Test covering the solution to be provided? If yes, please provide either:
  - The executive summary report created by the third party tester.
  - The full penetration test report created by the third party tester.
- Has the penetration test been performed within the last 12 months? If no, please provide the date when the penetration test was performed.
- Have all services (e.g., Web, Mobile, API, Infrastructure, etc.) part of the solution provided been covered within the Penetration Test scope? If no, please clarify.
- Please refer to and complete the "8.1. PenTest Minimum Scope" sheet.
- Were the penetration tester(s) accredited with industry-recognized security credentials such as: GWAPT, GPEN, OSCP, LPT, ECSA, CPT, or CEH?
- Have the penetration testers found any vulnerabilities? If yes, please provide the severities based on the OWASP Risk Rating Methodology and remediation plan dates for each of them.
- Have the penetration testers followed one of the two following industry standard methodologies: OWASP and OSSTMM? If no, please clarify.

> Penetration tests on app, mobile and network is done once a year. OWASP principles are followed. Reports can be requested from Manco. File location (not open to all): Pen Test Results

Encryption of Data Over Private Networks

Question:

- Is the solution customer data at rest within your or your hosting provider's private network encrypted? If yes, please provide details of the encryption scope and encryption algorithm used.
  - Note: Data at rest refers to all data in computer storage (e.g., hard drives, backup tapes, databases, mobile devices, file systems, etc.).

> Yes, from 2025 we encrypt the data at rest within our SQL Server 2019 databases using SQLs always encrypted configuration with deterministic encryption. The encryption makes use of the **AEAD_AES_256_CBC_HMAC_SHA_256** algorithm.

- Is the solution customer data transmitted within your or your hosting provider's private network encrypted? If yes, please provide details on the encryption scope and encryption algorithm used.

> The system runs within a Kubernetes cluster where the nodes are protected behind an Istio load balancer. Due to the private setup the traffic between the nodes does not move over the private network of the hosting provided but internally within the cluster.
>
> The data transferred from the client to the enclosed server is encrypted using SSL certificate. The client and server is encryption scope include the SSL handshake and secure communication between the client and server. The encryption use is PKCS #1 SHA-256 With RSA Encryption.

Identity, Entitlement, and Access Management

Question:

- Does the solution technically enforce a password length of a minimum of 16 characters for the Privileged (Admin) User Accounts? If no, please provide details on the configuration.

> Yes, it can be configured. The password enforcement can be configured per client for the users accessing the system. One configuration is available that is share for all users administrators and general users

- Does the solution technically enforce a password length of a minimum of 10 characters for the standard End User Accounts? If no, please provide details on the configuration.

> Yes, it can be configured. The password enforcement can be configured per client for the users accessing the system. One configuration is available that is share for all users administrators and general users

- Does the solution technically enforce password change at a minimum of 90 days? If no, please provide details on the configuration.

>

> The password expiry days can be adjusted per client and is 60 days by default.

- Is the solution configured to allow a maximum of 5 failed login attempts before the account gets locked out/wiped? If no, please provide details on the configuration.

> Yes, the maximum failed login attempts is 10 by default and can be customised per client

- Does the solution technically enforce password history control to a minimum of 8 passwords? (e.g., How many unique new passwords a user must use before an old password can be reused?) If no, please provide details on the configuration.

> Yes, the number of password that can be used is customisable and 5 passwords by default

- Does the solution technically enforce idle session timeout of a maximum of 15 minutes? (e.g., After a maximum of 15 minutes of idle time, the user's session will be terminated/required to log back in?) If no, please provide details on the configuration.

> No, the default for the system is an access token lifetime of 100 minutes that is refreshed up to 5 times before the session expires. This is customisable per system.

- Does the solution technically enforce at least three of the following password complexity requirements?
  - Uppercase characters (A to Z)
  - Lowercase characters (a to z)
  - Digits (0 to 9)
  - Special characters (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/etc.)
- If no, please provide details on the configuration.

> Yes.

- Are credentials stored at rest encrypted by using a one-way hashing algorithm (SHA-256, equivalent, or higher security) together with a salt?

> Yes

- Are credentials in transit encrypted? (e.g., not transmitted in clear text)

> Yes

- Does the solution offer audit and reporting capabilities regarding user management and modification of access permissions?

> Yes

- Does the system support Single-Sign-On (SSO) using Identity and Access management standard protocols? (e.g., SAML, OAuth, OpenID Connect) If no, please provide details on the configuration.

> Yes, OpenID Connect

Logging/Tools

Question:

- Do you log any administrative and configuration changes to the Services?

> Yes, as part of the server deployment

- Is physical and logical user access to audit logs restricted to authorized personnel?

> Yes

- Are audit logs centrally stored and retained? If so, please provide details on the retention policy.

>

> Yes, stored actively for up to 6 month, after which it is retained in cold storage accessible on request

- Are the retained logs sufficient to permit forensic analysis on security events?

> Yes, giving insight on who viewed user personal information and changed data

- Are there any tools in place to continuously monitor, detect, and prevent intrusion/attacks to the solution (IDS, IPS, WAF, etc.)? If yes, please share what tools exactly.

> Yes, Fortigate Firewall is used for IPS and AV

Revision #13
Created 2024-12-03 11:09:42 UTC by Nardus van Eyk
Updated 2024-12-04 11:44:49 UTC by Nardus van Eyk