Security Information Document

SyncBackPro — On-Premises Backup and Synchronisation Software

2BrightSparks Pte Ltd

Document Classification	Public
Version	1.0
Last Updated	April 2026
Prepared By	2BrightSparks Pte Ltd
Contact	support@2brightsparks.com
Website	https://www.2brightsparks.com

Contents

1. Executive Summary

This document provides security-relevant information about SyncBackPro, a backup, synchronisation, and restore application for Windows developed by 2BrightSparks Pte Ltd. It is intended to assist customers and procurement teams in understanding the product's architecture, built-in security features, and the allocation of data security responsibilities.

> **Key Point:** SyncBackPro is a locally installed Windows desktop application. 2BrightSparks does not operate any cloud services, hosted infrastructure, or data processing facilities. All data handled by SyncBackPro remains entirely within the customer's own environment and under the customer's sole control. 2BrightSparks is a software licensor, not a data processor.

This document is provided as a standard response to vendor security assessment requests. For the majority of procurement scenarios involving on-premises desktop software, the information contained herein should be sufficient to satisfy security review requirements.

2. Company Overview

Company Name	2BrightSparks Pte Ltd
Incorporated	Singapore
Founded	2003
Industry	Software Development (Backup and Synchronisation)
Products	SyncBackPro, SyncBackSE, SyncBackFree, SyncBack Touch, SyncBack Monitor, SBMS
Employees	Small, privately held company
Website	https://www.2brightsparks.com

2BrightSparks has been developing backup and synchronisation software since 2003. SyncBack products are trusted globally by individuals, businesses, and mission-critical organisations including law enforcement agencies, hospitals, and government departments.

3. Product Architecture

3.1 Deployment Model

SyncBackPro is a locally installed Windows desktop application. The software is downloaded from the 2BrightSparks website, installed on the customer's Windows computer, and runs entirely within the customer's environment. There is no cloud component, no hosted service, and no data transmitted to or through 2BrightSparks' infrastructure.

The deployment model means:

- All data handled by SyncBackPro resides within the customer's own infrastructure
- 2BrightSparks has no access to, visibility of, or responsibility for any customer data

- The customer is solely responsible for the security of the environment in which SyncBackPro operates
- 2BrightSparks does not act as a data processor under GDPR, HIPAA, or any other data protection regulation

3.2 Supported Platforms and Destinations

SyncBackPro runs on Windows (x64) and can back up data to a wide range of destinations, all configured and controlled by the customer:

- Local and network drives (internal drives, external USB drives, NAS devices, network shares)
- FTP, FTPS, and SFTP servers
- Cloud storage services including Amazon S3, Google Drive, Google Storage, Microsoft Azure Blob Storage, Microsoft OneDrive, OneDrive for Business, SharePoint (Office 365), Dropbox, Box, Backblaze B2, and others
- SyncBack Touch endpoints (Windows, macOS, Linux, Android)
- Email servers (POP3/IMAP4/Exchange)
- WebDAV servers

3.3 SyncBack Management System (SBMS)

SBMS is a free, on-premises client-server monitoring tool bundled with SyncBackPro. It enables system administrators to centrally monitor and manage multiple SyncBackPro installations across an organisation. SBMS is installed and operated entirely within the customer's own network — no data is sent to 2BrightSparks.

4. Data Handling and Privacy

> **2BrightSparks does not collect, process, store, or transmit any customer data.** The company has no access to customer files, backup configurations, credentials, or any other data handled by SyncBackPro.

4.1 Data Processed by SyncBackPro

SyncBackPro processes data as directed by the customer through locally configured backup profiles. This data never leaves the customer's environment except when the customer explicitly configures a backup destination outside their local network (e.g., a cloud storage service or remote FTP server). In all cases, the data transfer is initiated and controlled by the customer, using the customer's own credentials, to destinations of the customer's choosing.

4.2 Data Collected by 2BrightSparks

2BrightSparks collects only the following limited information:

- Licence registration details (name, email address) for customers who purchase a licence
- Support communications voluntarily submitted by customers
- Anonymous update checks (SyncBackPro can optionally check for new versions; this transmits only the current version number)

No telemetry, usage analytics, backup content, file metadata, credentials, or configuration data is collected.

4.3 Responsibility for Data Security

Security of data handled by SyncBackPro is the sole responsibility of the customer. This includes operating system hardening, network security, access controls, encryption of data at rest and in transit, credential management, and compliance with applicable regulations.

5. Built-in Security Features

5.1 Encryption at Rest

- AES encryption with 128-bit, 192-bit, or 256-bit keys for backup archives (Zip-compatible)
- Filename and metadata encryption to prevent inspection of archive contents without the correct password
- Compatible with PKWare SecureZip and 7-Zip encryption standards
- Profile settings (which may contain embedded passwords and connection credentials) can be encrypted with AES to prevent unauthorised access

5.2 Encryption in Transit

- SFTP (SSH File Transfer Protocol) with host key validation and key-based authentication
- FTPS (FTP over TLS/SSL) with explicit and implicit modes
- HTTPS for cloud storage connections
- TLS 1.2 and TLS 1.3 support
- SyncBack Touch uses a proprietary encrypted communication protocol
- V12 introduces encryption support with Rapid Transfer for secure, high-speed file transfers

5.3 Secrets Management

SyncBackPro can retrieve credentials from external secrets managers rather than storing them locally, supporting:

- AWS Secrets Manager
- Azure Key Vault
- Google Cloud Secret Manager
- HashiCorp Vault
- Infisical (new in V12)
- Windows Credential Manager

5.4 Ransomware Detection

SyncBackPro includes multiple layers of ransomware detection to prevent encrypted or compromised files from overwriting clean backups:

- **Global detection:** Monitors a sentinel file on the local system; if ransomware modifies it, all profiles are blocked from running.

- **Profile-level detection:** Monitors sentinel files on remote sources and destinations (e.g., FTP servers, NAS devices) per profile.
- **SyncBack Touch detection:** Detects ransomware on remote Touch endpoints.
- **Threshold warnings:** Configurable alerts when an abnormal percentage of files are being modified, indicating potential ransomware activity.

5.5 File Integrity and Verification

- File integrity checking to verify that copied files match their source
- S.M.A.R.T. drive health monitoring to detect impending storage device failures
- File versioning to retain multiple previous copies of files, enabling recovery from corruption or accidental changes
- Delta-copy to transfer only changed portions of files, reducing transfer time and bandwidth

5.6 Access Control and Administration

- Profiles can be password-protected to prevent unauthorised modification
- Windows Group Policy templates for enterprise-wide policy enforcement
- SBMS provides centralised management of profiles, history, and reporting across multiple installations
- Administrators can restrict users from creating or altering profiles
- SyncBack Touch supports authentication via password, SBMS credentials, or Windows account impersonation

5.7 Logging and Auditing

- Comprehensive logging of all backup, synchronisation, and restore operations
- Logs available in plain text or HTML format
- Configurable email notifications and alerts for profile run results
- SysLog integration for enterprise SIEM environments
- SBMS provides centralised reporting across all managed installations

6. Software Development Practices

6.1 Development Environment

SyncBackPro is developed entirely in-house by 2BrightSparks using Embarcadero Delphi. No third-party contractors or outsourced development teams are used. The source code is maintained in a secure, access-controlled repository.

6.2 Software Integrity

- **Code signing:** All SyncBackPro installers and executables are digitally signed with a code-signing certificate issued to 2BrightSparks Pte Ltd, enabling customers to verify authenticity and integrity.
- **Hash verification:** SHA-256 hashes are published for all downloadable packages, allowing customers to verify file integrity before installation.
- **Distribution:** Software is distributed exclusively through the official 2BrightSparks website (www.2brightsparks.com) over HTTPS.

6.3 Vulnerability Management

2BrightSparks monitors security advisories and CVE databases relevant to the technologies and third-party components used in SyncBackPro. Security patches and updates are released promptly when vulnerabilities are identified. Customers are notified of updates through the built-in update check mechanism and via the 2BrightSparks website.

6.4 Update Process

SyncBackPro includes a built-in update checker that periodically queries the 2BrightSparks website for new versions. Updates are downloaded manually by the customer and installed locally. There is no forced or automatic update mechanism — the customer retains full control over when and whether to apply updates. All minor version updates (e.g., V12.1 to V12.2) are provided free of charge.

7. Organisational Security

7.1 Policies and Plans

2BrightSparks maintains the following documented security and continuity resources:

- Information Security Policy (reviewed and updated at least annually)
- Incident Response Plan
- Business Continuity and Disaster Recovery Plan (tested at least annually with formally documented results)

7.2 Data Backups

2BrightSparks maintains regular backups of its own business-critical data (source code, build systems, business records) using SyncBackPro. Backups are stored at geographically separate locations, encrypted, and tested regularly for integrity. Multiple generations of backups are retained extending well beyond one year.

7.3 Incident Response

In the event of a security incident that could potentially affect a customer, 2BrightSparks will provide notification within 24 hours. However, given that 2BrightSparks does not process, store, or transmit customer data, the likelihood of such an incident is extremely low. The most plausible scenario would be a compromise of the software distribution channel, which is mitigated by code signing and hash verification.

8. Licensing Model

SyncBackPro is sold under a perpetual licence model. Customers receive a one-time licence that never expires and includes all minor version updates at no additional cost. Major version upgrades and priority technical support are available through an optional Upgrade Assurance subscription.

A single SyncBackPro licence permits installation on up to five computers for personal use. For non-personal (workplace) use, a separate licence is required for each installation. Volume discounts are available for two or more licences, and educational and non-profit discounts are offered.

9. Common Security Assessment Questions

The following addresses questions frequently raised in vendor security assessments. Many standard assessment questions are designed for cloud service providers and data processors and are not applicable to on-premises desktop software.

Question	Response
Does 2BrightSparks process customer data?	No. SyncBackPro runs entirely within the customer's environment. 2BrightSparks has no access to customer data.
Is 2BrightSparks a data processor under GDPR?	No. 2BrightSparks does not process personal data on behalf of customers. A Data Processing Agreement is not applicable.
Does SyncBackPro transmit data to 2BrightSparks?	No. The only optional network communication is an update version check, which transmits only the current version number. No customer data, telemetry, or configuration information is transmitted.
What encryption does SyncBackPro support?	AES-128/192/256 for data at rest; SFTP, FTPS, HTTPS, and TLS 1.2/1.3 for data in transit.
Is SyncBackPro SOC 2 / ISO 27001 certified?	These certifications apply to cloud service providers and data processing organisations. They are not applicable to a locally installed desktop application where the vendor has no access to customer data.
Does 2BrightSparks perform penetration testing?	Penetration testing is performed on an ad hoc basis against the company's development and distribution infrastructure. SyncBackPro itself runs within the customer's own environment, where penetration testing is the customer's responsibility.
Does 2BrightSparks have a SOC 2 report?	No. SOC 2 reports are relevant to service organisations that process, store, or transmit customer data. 2BrightSparks is a software licensor and does not provide hosted services.
How does SyncBackPro protect against ransomware?	SyncBackPro includes multi-layered ransomware detection (global, profile-level, and Touch endpoint), threshold-based anomaly warnings, file versioning, and support for immutable cloud storage destinations.

10. Contact Information

For security-related enquiries or to request additional information, please contact:

Email	support@2brightsparks.com
Website	https://www.2brightsparks.com
Knowledge Base	https://help.2brightsparks.com

This document is reviewed and updated periodically. The version number and date on the cover page indicate the current revision.