NODRIVE

Security & Zero-Knowledge Overview

Descrizione pubblica del modello di sicurezza della Beta

Versione 1.0 • 23 agosto 2026 • Beta

Indice

1. Cosa significa zero-knowledge in Nodrive
2. Gerarchia delle chiavi
3. Autenticazione
4. Storage locale e “Il tuo storage”
5. Cosa può essere visibile
6. Cosa Nodrive non conserva sul backend nella Beta
7. Limiti dichiarati
8. Stato delle funzioni
9. Segnalazioni di sicurezza

1. Cosa significa zero-knowledge in Nodrive

Nodrive è progettato per cifrare sul dispositivo dell'utente contenuto, nomi e struttura dei file prima che i dati lascino il dispositivo. Nella Beta corrente Fiscalbox non offre storage Hosted dei contenuti: i dati rimangono localmente o vengono inviati cifrati allo storage scelto dall'utente.

2. Gerarchia delle chiavi

- User Key (UK): chiave casuale a 256 bit da cui deriva il materiale usato per proteggere i dischi e i file.
- Chiave derivata dalla password: ricavata localmente con Argon2id; serve a sbloccare la User Key e non cifra direttamente i file.
- La chiave derivata dalla password è effimera e non viene persistita in chiaro.
- La User Key avvolta della Beta corrente è conservata sul dispositivo locale, non sul backend come escrow di recovery.

3. Autenticazione

Secondo il modello tecnico corrente, Nodrive usa OPAQUE per l'autenticazione in modo che la password non venga inviata in chiaro al server. Le comunicazioni con il backend sono protette tramite TLS. Il backend Nodrive è attualmente ospitato su Google Cloud Platform in Europa.

4. Storage locale e "Il tuo storage"

Nel locale, i dati cifrati risiedono sul supporto scelto dall'utente. Con "Il tuo storage", il client invia blocchi cifrati al provider autorizzato. Nel caso Google Drive, Nodrive usa OAuth: non conosce la password Google e conserva il token autorizzativo solo sul PC dell'utente.

5. Cosa può essere visibile

- Al backend Fiscalbox: esistenza dell'account, email/identificativi tecnici, eventi di autenticazione e sicurezza, versione app e dati tecnici necessari al servizio.
- Al provider di storage scelto dall'utente: l'identità del proprio cliente, gli oggetti cifrati e metadati infrastrutturali come quantità, dimensioni e tempistiche.
- A Google Analytics sul sito, dopo consenso: dati di utilizzo del sito, browser/dispositivo, sessioni e localizzazione approssimativa secondo la configurazione GA4.
- A Fiscalbox, solo se l'utente la invia: diagnostica tecnica facoltativa per troubleshooting.

6. Cosa Nodrive non conserva sul backend nella Beta

- Contenuti dei file dell'utente come storage Hosted Nodrive.
- Password Google o password degli altri provider collegati.
- Token OAuth Google Drive, che resta sul PC dell'utente.
- User Key in chiaro o escrow server-side della User Key avvolta nella Beta corrente.

7. Limiti dichiarati

- Un dispositivo compromesso con malware, keylogger o privilegi elevati può aggirare le garanzie applicative.
- Una password debole resta un rischio se un attaccante ottiene il materiale cifrato necessario per tentativi offline.
- Applicazioni esterne e il sistema operativo possono creare file temporanei, autosave, preview, indicizzazione o swap fuori dal controllo diretto di Nodrive.
- La perdita di password e recovery key può rendere i dati irrecuperabili.
- Un provider terzo può essere indisponibile, cambiare condizioni o cancellare oggetti.
- Nessuna dichiarazione di sicurezza deve essere interpretata come garanzia di invulnerabilità assoluta.

8. Stato delle funzioni

Funzioni Beta
Fanno fede la build installata, le note di versione e la documentazione tecnica corrente. Funzioni pianificate - ad esempio storage Hosted o portabilità server-side delle chiavi - non devono essere considerate attive finché non sono effettivamente distribuite e verificate.

9. Segnalazioni di sicurezza

Segnalazioni tecniche o di sicurezza possono essere inviate a info@nodrive.cloud. Non inviare password, recovery key o chiavi crittografiche nei messaggi di supporto.