Benedict App — Technical Review

Release reviewed	Benedict App 2.26.4
Date	November 2026
Published by	Benedict Corp.
What this is	A description of how Benedict App is built, how it protects your data, and how it was tested. Not a certification, not a penetration test and not a third-party audit

1. In short

Benedict App records the time your team spends on client projects and turns it into monthly client reports. It is **licensed software that you install in your organization's own Microsoft Azure subscription**. Benedict Corp does not host it, does not operate it and has no access to your data.

- **Your data stays in your Azure.** The database, the app servers and the website all run in your subscription, in the region you choose.
- **Sign-in is your organization's Microsoft sign-in** (Microsoft Entra ID), including your own multi-factor and Conditional Access rules. Only people an administrator has added in the app can use it.
- **Every business rule is enforced by the database itself**, not only by the screens: who may see what, who may change what, and how amounts are calculated.
- **Every change is recorded** in an append-only audit trail: who, when, what changed, and the reason given.
- **Tested** with 786 automated database checks, several hundred application tests, data sets of up to 5 million time entries (local test environment) and up to 75 simultaneous simulated users on Azure.

2. How Benedict App is delivered

Benedict App is not a cloud service run by Benedict Corp. You buy a perpetual license and install the software in your own Azure subscription with the Benedict App installer, a Windows program. After that, the installation belongs to you:

Who	Is responsible for
Your organization	The Azure subscription and its costs; the region where your data lives; who may sign in; backups and their retention; applying updates; your own security policies (multi-factor sign-in, Conditional Access, network rules)
Benedict Corp	The software: its correctness, its security fixes, the installer, the documentation, and support for licensed installations

Because every customer has a separate installation, there is no shared database and no shared platform between customers.

3. What gets installed

All parts run in one resource group in your subscription:

Part	What it does	Azure service
Website	The screens people use, in a browser on a computer or phone	Azure Static Web Apps
App server	Checks every request and passes it to the database	Azure Functions (Node.js 22)

Part	What it does	Azure service
Export server	Builds the Excel files and month archives. It runs separately, so a large export never slows everyone else down	Azure Functions (Node.js 22)
Monthly report job	Prepares each project's report for the previous month, from the 2nd of each month	Part of the app server
Database	Holds all data and all business rules	Azure SQL Database
Monitoring	Technical logs (no business data)	Application Insights

Sign-in uses Microsoft Entra ID in your own tenant. The app servers connect to the database with Azure managed identities: there are no passwords or connection keys to store, rotate or leak.

Sizes. The installer recommends a database size for your team and shows the expected monthly Azure cost before anything is created. You can choose from the free Azure SQL offer up to larger paid tiers, and change later.

Optional extras, chosen in the installer:

- a private network, so the database has no public address;
- Microsoft Defender for SQL;
- backups copied to a second region;
- Azure Front Door with its web application firewall;
- alerts by e-mail for errors and unusual activity.

4. How your data is protected

4.1 Sign-in and identity

- Every request must carry a valid Microsoft sign-in token issued for your installation. The app server checks the signature, the issuer, your tenant, the audience, the expiry and the permission before anything else happens.
- **Who is acting** is taken only from that token. No request can name another person.
- **Signing in is not enough to get in.** Microsoft confirms who someone is; Benedict App then checks its own list of people, which administrators manage in the app. Someone removed from that list loses access at their next request.

4.2 Permissions are decided in the database

- The three roles (member, team lead, administrator) and every rule about who may see or change what are enforced **inside the database**. The screens only show what the database allows.
- The app servers' own identities can do one thing in the database: run its prepared business operations. They cannot read or change tables directly.
- Filters can only narrow what someone may see, never widen it.
- Every request runs as one database transaction: it either completes fully or changes nothing.

4.3 The audit trail

- Every business change is recorded with who made it, when, the values before and after, and the reason the person gave.
- Refused requests are recorded too.
- The audit trail is append-only: entries cannot be edited or deleted through the app. Administrators, team leads and members can each browse the part of it that concerns them on the Audit log page.

4.4 Money and reports

- **Finalized reports are frozen.** Once a monthly report is finalized, its numbers can never change. A correction is made by cancelling it and issuing a new version; the cancelled one stays in the history.
- **Exact arithmetic.** Amounts are calculated with exact decimals, in each currency's own units (0, 2 or 3 decimals). Amounts in different currencies are never added together.
- **No silent double saves.** Saving is one request that either completes or changes nothing. Saving the same entry twice never creates a duplicate, and a changed retry is never mistaken for the earlier save.
- **No false "saved".** If the connection breaks while saving, the app checks whether the save went through before saying anything. It never reports a save that didn't happen, or the reverse.

4.5 Web security

- HTTPS only, TLS 1.2 or newer.
- A strict browser security policy: only the website's own scripts and styles may run, the app cannot be embedded in other sites, and browsers are told to use HTTPS only.
- The app servers accept requests from your own website only.
- Error messages never contain technical details of the server or the database.

4.6 What leaves your installation

Benedict App and its installer contact Benedict Corp only in three limited cases:

What	When	What is sent
License check	When someone installs or updates with the installer	The license holder's Microsoft sign-in, the organization's name and tenant, and the acceptance of the terms. Installations are identified only by one-way codes
Update notice	When an administrator opens the Admin page, at most every 6 hours	Only the question "which release is newest?". Nothing about you, your installation or your data. It can be switched off
Failure report	Only if the installer fails **and** a person clicks "Send report"	Five fields: what failed, at which step, an error code, the installer version and the release version. Not linked to your organization; kept for 12 months

Your business data — people, clients, projects, time entries, rates, amounts, reports — never leaves your Azure subscription through Benedict App.

5. Installing and updating safely

- **Signed releases.** Every Benedict App release is signed by Benedict Corp. The installer checks the signature and every file's checksum, and refuses anything that doesn't match.
- **Releases are only built from a clean state** and only when no known high or critical security advisory affects the parts Benedict App uses.
- **Updates protect your data:**
  1. The app is closed for a few minutes while the database is updated (people see a maintenance message).
  2. A restore point is noted, so Azure can return the database to that moment if ever needed.
  3. A fingerprint of all data is taken before and after. If anything would change unexpectedly, the update stops before the new version goes live.
  4. The new app servers and website are installed and tested, then the app opens again.
- **Repeatable steps.** If an update stops (a network problem, for example), it can be run again and continues where it stopped.

- **Backups.** Azure SQL keeps automatic backups (7 days on the free tier, 14 days otherwise). Benedict App's installation tools can restore a test copy to prove a restore works, and can restore the real database to an earlier moment.
- **Health check.** The installation tools include a check that reviews an installation's settings and reports anything that needs attention.

6. How it was tested

6.1 Automated tests (every release)

Area	Tests
Database rules and permissions	786 automated checks on a fresh database: roles, scopes, every business rule, audit records, amounts
App server	144 tests: sign-in checks, error handling, transactions, exports
Website	121 tests
Installer	106 tests
Static checks	465 checks that every database call matches what the database expects

Every database change is also rehearsed on copies before release: the updated database must match a fresh installation exactly, and the data must be unchanged.

6.2 Correctness at scale (local test environment)

On a single workstation, with synthetic data of about 100 thousand, 500 thousand, 1 million and 5 million time entries:

- **All 5,835,812 report lines** were recalculated by a separate program in exact decimal arithmetic, across five currencies: **zero differences**.
- **Under load,** with up to 100 simulated users on the largest data set: no errors, and every one of the 6,285 time entries saved during the tests was present exactly once afterwards.
- Everyday screens stayed fast as data grew: a team member's month view took a median of 6 ms at about 100 thousand entries and 10 ms at about 5 million.

Local test environment, synthetic data, not measured on Azure; timings depend on the hardware and are not a commitment.

6.3 Simulated users on Azure

Benedict Corp ran load tests on Azure with synthetic organizations, in temporary databases deleted afterwards. A "simulated user" uses the app continuously, opening a new page every 3 to 8 seconds: much busier than a real person.

Date	Release	Database	Synthetic organization	Simultaneous simulated users	Result
October 2026	2.21	Azure SQL free offer (serverless, up to 2 vCores)	300 people, about 70,000 time entries	up to 75	No errors and no time-outs. Comfortable up to 30 users (95 % of requests within 0.7–0.9 s); slower at 50 (within 1.4–2.5 s); limit reached at 60–75 (within 3.4–5.3 s)
October 2026	2.26	free offer, S0, S1	10 and 20 people	up to 20	No errors. With 20 users, 95 % of screens loaded within 0.2 s on the free offer, 2.0 s on S1 and 4.7 s on S0

Measured in Benedict Corp's own Azure subscription with synthetic data. Your results depend on the tier and region you choose. Not a service-level commitment.

6.4 Real installations

- Installations made with the installer in **a new, empty Microsoft tenant**, on computers that had never had Benedict App, with nothing pre-installed.
- **Updates** from one release to the next with the installer, including an update that was interrupted and then completed.
- **Restores** of the database to an earlier moment, with the app switched to the restored copy.
- **The optional extras** (private network, Defender for SQL, second-region backups, Front Door with its firewall), each on a real test installation.

6.5 Reviews

The code and the tests were examined in several separate review passes by reviewers who had no part in writing the changes they reviewed. Every problem they reported was fixed and re-tested before release. These are Benedict Corp's own reviews, not an external audit.

Internal authorization test (November 2026). 339 checks tried, with every role, to read or change data outside that role's scope, against the product's own code, with synthetic data. Release 2.26.4 passes every check except one, which concerns a documented limit of the design, not a defect. This was Benedict Corp's own test, not an external penetration test.

7. Known limits

- **Very large organizations:** at about 5 million time entries, organization-wide views over a whole year take several seconds, and a full-year text search across everyone can reach the request time limit. Everyday views are not affected.
- **More than 20 simultaneous users on release 2.26** has not been measured on Azure; the 75-user test used release 2.21.
- **The free Azure SQL offer** gives about 40 hours of database activity a month, whatever the number of users. A team that uses the app all day needs a paid tier; the installer explains the choice.
- **Not tested by an outside party.** No external penetration test has been performed. Your organization may test its own installation.

8. More information

A more detailed edition of this review, with the full test results and the status of each security control, is available to customers and prospective customers on request, under a non-disclosure agreement. Ask Benedict Corp.

Benedict App is licensed software installed in the customer's own Microsoft Azure. Statements in this review describe release 2.26.4 as tested in November 2026. Benedict Corp. makes no service-level commitment through this document.