

# How MetricsWatch protects your data and your clients' data

MetricsWatch builds marketing reports and sends metric alerts for agencies and businesses. This page answers the questions most vendor security reviews ask. If your questionnaire asks something this page doesn't cover, we're happy to go through it with you.

Last reviewed October 21, 2026. Covers MetricsWatch Reporting (app.metrics.watch) and MetricsWatch Alerts (alerts.metrics.watch).

## ON THIS PAGE

- |                                                             |                                                       |
|-------------------------------------------------------------|-------------------------------------------------------|
| 1. <a href="#">What data we hold</a>                        | 8. <a href="#">Retention and deletion</a>             |
| 2. <a href="#">Access to your ad and analytics accounts</a> | 9. <a href="#">Payments</a>                           |
| 3. <a href="#">Hosting and data location</a>                | 10. <a href="#">AI summaries</a>                      |
| 4. <a href="#">Encryption</a>                               | 11. <a href="#">Service providers</a>                 |
| 5. <a href="#">Sign-in and accounts</a>                     | 12. <a href="#">Monitoring, updates and incidents</a> |
| 6. <a href="#">Who on our side can see your data</a>        | 13. <a href="#">Privacy law</a>                       |
| 7. <a href="#">Backups and recovery</a>                     |                                                       |

## What data we hold

### What do you store?

- Your account details: name, email address, company name, and billing contact.
- Authorization to the platforms you connect, such as Google Analytics, Google Ads, Meta, LinkedIn and Microsoft Ads. This is a token the platform issues, never your password.
- The metrics we pull to build your reports and check your alerts, plus the report settings, branding and recipient lists you set up.
- Delivery records for the reports and alerts we send.

### Do you hold personal data about our clients' customers?

Generally no. We pull aggregated marketing metrics such as sessions, conversions, spend and clicks. We don't pull visitor-level records from analytics platforms. Report recipients' names and email addresses are stored so we can deliver to them.

### Do you look at our metrics?

No, not unless you ask us to or we need to for a support request you've opened. We don't sell, trade or share your metrics with anyone.

## Access to your ad and analytics accounts

---

### How do you connect to our platforms?

Through each platform's own sign-in and consent screen (OAuth). You approve access on Google's, Meta's or Microsoft's own page, and we never see or store the password for those accounts.

---

### What permissions do you ask for?

We ask for the narrowest permission each platform offers for reading reporting data. For Google Analytics, Search Console, YouTube Analytics and Meta Ads, that is read-only access.

A few platforms don't offer a read-only option for the data reports need: Google Ads, Google Business Profile, Microsoft Advertising, LinkedIn Pages and Meta Business. There we have to ask for the standard API permission. MetricsWatch only reads reporting data from these accounts and has no feature that changes campaigns, budgets, ads or listings.

---

### How do we revoke access?

Any time, from the platform itself. For example, a Google account owner can remove MetricsWatch under Google Account, Security, Third-party connections. Once access is revoked, we can no longer read anything from that account. You can also disconnect a source inside MetricsWatch, and we'll stop using it.

## Hosting and data location

---

### Where is our data stored?

In the United States, in the US East region (northern Virginia). Our application servers run on Fly.io. Our databases run on Uvicloud and Fly.io managed PostgreSQL, and files are stored in Tigris object storage. Alert checks run on Microsoft Azure, also in US East.

---

### Is the database exposed to the internet?

No. Our main database only accepts connections from our own application servers' fixed addresses, and every other address is blocked by a firewall. The Alerts database is only reachable over Fly.io's private network.

## Encryption

#### IN TRANSIT

Every page and API uses HTTPS (TLS), and plain HTTP is redirected. Connections from our servers to our databases are encrypted too.

#### AT REST

Our database and storage providers encrypt stored data and backups at rest, with nothing for us to switch on.

---

## How are passwords stored?

Passwords are hashed with bcrypt, a one-way algorithm designed for passwords. We can't see or recover your password; resetting it sends a link that expires.

## Sign-in and accounts

### ALERTS

Email and password, with optional two-factor authentication using an authenticator app. You can also sign in with Google, and single sign-on through SAML or Okta is available.

### REPORTING

Email and password, with email confirmation and expiring reset links. Two-factor authentication is not available on Reporting yet.

---

## Can we give team members their own logins?

Yes. Each person gets their own login, so access can be removed for one person without affecting anyone else.

## Who on our side can see your data

---

### Which MetricsWatch staff have access?

MetricsWatch is a small company, and production access is limited to the few named people who run and support the service. Admin tools inside the app are only available to a fixed list of staff accounts.

### Can staff see our account?

To fix a problem you've reported, a staff member can view your account the way you see it. We only do this for support, and we don't browse customer data otherwise.

## Backups and recovery

---

### How is data backed up?

Our main database is backed up continuously by our database provider, so it can be restored to any point within the recent backup window. We also take weekly full copies of the database and keep them in separate, encrypted storage.

## Retention and deletion

---

### How long do you keep our data?

As long as your account is open, so your reports, alerts and history keep working. Some working data expires sooner: in Reporting, working copies of report content are cleared after a few days, and raw metric logs after 90 days.

---

### **What happens when we cancel or ask for deletion?**

Cancelling stops billing and delivery. Your data isn't deleted automatically, so you can come back without rebuilding anything. If you'd like it deleted, email us and we'll delete your account and its data. Where the platform supports it, we also revoke our access to your connected accounts. We keep basic billing records with personal details removed, because tax law requires it. Backups age out on their normal schedule after that.

In Alerts, an account owner can also delete their account from the account settings.

## **Payments**

---

### **Do you store card details?**

No. Payments are handled by Stripe. Card details go straight from your browser to Stripe, so card numbers never reach or are stored on our servers. Stripe is certified PCI DSS Level 1.

## **AI summaries**

---

### **Do you send our data to AI providers?**

Only when AI summaries are turned on for a report. In that case, the report's metric figures and its name and date range are sent to our AI providers to write the summary. We use Anthropic's API, which under Anthropic's commercial terms doesn't train its models on that data, and we use OpenRouter to check a summary's figures against the report. Account passwords and platform authorization are never sent. If AI summaries aren't turned on, no report data goes to an AI provider.

## **Service providers**

These companies process data on our behalf to run the service.

| PROVIDER              | WHAT FOR                                    | LOCATION |
|-----------------------|---------------------------------------------|----------|
| Fly.io                | Application hosting, Alerts database        | US East  |
| Ubicloud              | Main database                               | US East  |
| Tigris                | File storage and database copies            | US       |
| Microsoft Azure       | Alert checks                                | US East  |
| Stripe                | Payments                                    | US       |
| Postmark              | Sending report and alert emails             | US       |
| PostHog               | Product analytics and error tracking        | US       |
| Anthropic, OpenRouter | AI summaries, only when turned on           | US       |
| Twilio                | Text message alerts, only when used         | US       |
| Slack                 | Alert messages, only when you connect Slack | US       |

## Monitoring, updates and incidents

### How do you monitor the service?

We track errors and uptime continuously and are alerted when something fails. Our logs filter out passwords, tokens and other secrets.

### How do you keep software up to date?

Automated tools flag outdated and vulnerable dependencies, and we apply security updates as they're released. Code changes go through automated tests before they're deployed.

### What happens if there's a security incident?

We investigate right away. If we learn that your data was accessed without authorization, we'll tell you without undue delay, explaining what happened, what data was involved and what we're doing about it.

## Privacy law

### GDPR and other privacy laws

We process data only to provide the service, don't sell personal data, and will help you answer access, correction and deletion requests about data we hold. Our data is stored in the United States. If your clients need a data processing agreement, let us know.

Our full privacy policy is at [metricswatch.com/privacy-policy](https://metricswatch.com/privacy-policy). For security questions, email Jon at [jon@metrics.watch](mailto:jon@metrics.watch).

---

MetricsWatch is run by a small team that has been reporting on marketing data since 2015. Support email goes to the people who can fix things.