Security summary.

How program data is protected from intake to certified destruction

---

The architecture, the controls in eleven areas, the data lifecycle, the incident-response timeline, what clients must do on their side, and how to obtain the independent assessment under agreement.

Brushworks

brwrks.com/reports
research@brwrks.com
Cite as: Brushworks (2026), *Security summary*, Public overview · September 2026.

Contents

Section 1 Scope and assurance

Section 2 Architecture

Section 3 Controls by area

Section 4 Incident response

Section 5 What clients must do

Section 6 Requesting the full report

Section 1

Scope and assurance

This summary describes how program data is protected from intake to certified destruction: the architecture, the controls in each area, the timelines the firm commits to, and what clients must do on their side. It is the public overview. The independent assessment report, penetration-test summary, residency and replication attestations, restoration-test records and the incident-response runbook are available to clients and prospective clients under non-disclosure agreement.

72h
client notification after a confirmed incident affecting their data

90d
certified destruction of program data after close

1 year
immutable access and change logs retained and reviewed monthly

1.1 What is protected

Client files under data-use agreement; licensed behavioral data under provider terms; derived data (scores, cohorts, models, holdout assignments); activation data (hashed audiences in delivery seats); the firm's own records. The classification and handling rules are in the data use policy, Section 3; this summary describes the controls that enforce them.

1.2 Assurance

ASSURANCE	BY WHOM	CADENCE	AVAILABLE
Independent security assessment against a recognized control framework	External assessor	Annual	Summary under NDA
Penetration test of internet-facing and internal systems	External tester	Annual, and after material change	Summary and remediation status under NDA
Practice-wall certification	Counsel with the assessor	Each cycle	Certification to clients
Restoration tests	The desk	Quarterly	Records under NDA
Residency and replication attestations	The firm, with the hosting provider	Per mandate	To the client

Section 2

Architecture

Each practice — candidate, independent-expenditure, international — runs in its own environment with its own identities, storage, keys and delivery seats; no environment can read another's data. Within a practice, each client's program is a separate project with its own access list. Data moves through six stages, and the controls follow it.

1	2	3	4	5	6
Intake	**Resolution**	**Scoring**	**Activation**	**Measurement**	**Close**
Client file received over an authenticated, encrypted channel; hashed on receipt	Matched to the graph inside the practice environment; raw identifiers not retained beyond the match	Models run on derived data; holdout drawn and sealed; assignment delivered to the client	Hashed audiences pushed to the accounts of record; hold list and holdout as suppression	Outcomes joined to assignment in the measurement project only	Program data destroyed within ninety days; certificate issued; holdout retained per the client

The measurement project is the only place assignment and outcome meet; the delivery team cannot read it. The studio receives cohort descriptions and masters, never records. The desk's seven offices access the same environments through the same identities; nothing is stored locally.

Section 3

Controls by area

3.1 Identity and access

- Named accounts only; no shared credentials; single sign-on with phishing-resistant multi-factor authentication for every person and every administrative action.
- Least privilege scoped to a program: access is granted per project, expires with the program, and is recertified quarterly by the program lead.
- Same-day revocation on role change or departure, executed by the desk from the roster.
- Administrative access is separated from analytical access and logged with session recording.

3.2 Encryption and key management

- TLS 1.2 or higher for every connection; AES-256 at rest for storage, backups and exports.
- Keys held in a dedicated key-management service, one key hierarchy per practice, rotated on a schedule and on any suspected compromise; separation of duties between key administrators and data administrators.
- Client files are hashed with a keyed function on receipt; the key is per program and destroyed at close.

3.3 Segregation

- Separate environments per practice; separate projects per program; separate delivery seats per practice.
- No commingling of client files; licensed data is joined to a client's file only inside that program's project.
- The measurement project is isolated from delivery; the studio has no access to records.

3.4 Network and endpoints

- No inbound access to data environments except through the identity provider; private connectivity between components; egress restricted to approved destinations (delivery platforms, licensors, the

hosting provider).

- Managed endpoints with disk encryption, patching and detection; no program data on local storage; personal devices cannot reach data environments.

3.5 Logging and monitoring

- Immutable access and change logs for every environment, retained one year, reviewed monthly by someone other than the administrator whose actions they record.
- Alerts on anomalous access, bulk reads, exports and privilege changes; export of any record-level data is an alert by default.
- Every placement log is matched daily against the holdout hash; a match is an incident.

3.6 Vulnerability and change management

- Continuous dependency and configuration scanning; patch windows by severity — critical within seven days, high within thirty.
- Annual independent penetration test with tracked remediation.
- Code review for every change; secrets kept out of repositories; production changes logged and reversible.

3.7 Data lifecycle

DATA	RETENTION	DESTRUCTION
Client file and derived program data	Life of the program	Within ninety days of close; certificate issued
Holdout assignment	Per the client's instruction (for validated-turnout measurement, until the state's history is published)	On the client's instruction; certificate issued
Activation audiences in seats	Life of the flight	Deleted from seats at close
Licensed behavioral data	Per provider terms; refreshed and superseded	Superseded copies destroyed on refresh
Model cards, kill logs, proof reports	Seven years	Secure deletion
Access and change logs	One year	Secure deletion

3.8 Backups and continuity

- Encrypted backups of every environment, stored separately from production, with restoration tested quarterly and the results recorded.
- Recovery objectives per system: measurement and delivery within four hours; the studio within one business day.
- Operational continuity through the seven-office desk: a program in the field is watched by the office whose business day it is, with a written handoff.

3.9 Residency

- Program data for institutional mandates that require it is held in-country in the provider's regional facilities, with replication disabled or confined as the mandate specifies.
- A residency and replication attestation is delivered to the client at program start and at any change.

3.10 Vendors

- Due diligence before onboarding; written terms binding processors to the same standards; annual review; a maintained processor list available to clients.
- Delivery platforms and licensors are used under their published terms; no processor receives record-level program data except the hosting provider.

3.11 People

- Background screening where lawful; data-protection and political-compliance training before access and annually; written obligations that survive employment.
- Access to a program is limited to the people working on it; the roster is the source of truth for revocation.

Section 4

Incident response

STAGE	COMMITMENT	OWNER
Detection and triage	Alerts triaged around the clock by the desk; an incident declared by the named lead within one hour of confirmation	Head of the desk
Counsel	Engaged from the first hour; privilege preserved	Counsel of record
Containment	Affected identities revoked, keys rotated, environments isolated as required; evidence preserved	Incident lead
Client notification	Within seventy-two hours of confirmation for any client whose data is affected, with what is known, what is being done and what the client should do	Chief executive
Regulatory notification	Where the law requires, within its deadline (seventy-two hours under the GDPR and UK GDPR)	Data protection lead
Recovery	Restoration from backups tested quarterly; measurement integrity re-verified (holdout hash, balance)	Head of research
Review	Post-incident review within thirty days; reported to the board; controls changed and re-tested	Compliance lead

Section 5

What clients must do

- Deliver the file over the authenticated channel the firm provides, never by email or shared drive.
- Name an access owner who approves the program's access list and receives the holdout assignment.
- Keep the holdout assignment sealed from the campaign's other vendors, and supply those vendors' contact records where measurement integrity requires it.
- Tell the firm within one business day of any suspected compromise on the client's side that could affect program data.
- Instruct the firm at close whether the holdout assignment is to be retained for validated-turnout measurement or destroyed.

Section 6

Requesting the full report

Clients and prospective clients may request the independent assessment summary, the penetration-test summary, the processor list, the residency attestation template and the incident-response runbook summary under the firm's mutual non-disclosure agreement through the contact page or through counsel. Requests are fulfilled within five business days.

Security summary, September 2026. Independent assessment: annual; last completed before launch; summary under NDA.