A log is a record. Evidence is a record that *holds up.*

Most audit trails fail the second test. Here's what separates an operational log from defensible evidence — and why it matters before anyone asks.

Swipe to see the difference →

Logs aren't evidence.

A log is a record. Evidence is a record that can *survive scrutiny*. If your logs can be modified, deleted, or "corrected" after the fact — they fail the second test.

- ✕ Editable by admins → not evidence
- ✕ Stored alongside the app → not evidence
- ✕ No integrity verification → not evidence

Three questions your logs *must answer* without ambiguity.

- → Who accessed which file, and when — exactly?
- → Has any record been modified since it was written?
- → Can you prove both — to a third party?

THE UNCOMFORTABLE NUMBER

68%

of breaches involve a human element — and almost every investigation that follows depends on audit data that can hold up to outside review.

VERIZON DBIR · THE AUDIT TRAIL IS THE INVESTIGATION

Three properties. *All required.*

- ✓ Immutable after write — WORM-protected
- ✓ Retention-locked against deletion
- ✓ Cryptographically tamper-evident (hash-chained)

Miss any one — your audit trail is reconstruction, not proof.

Four questions. Answer honestly.

1. Can a privileged admin delete an audit record?
2. Are logs exported to storage outside app control?
3. Is retention enforced by storage, not by policy?
4. Can you cryptographically prove the chain is intact?

If you answered "no" to any — your logs aren't evidence yet.

If your logs can be edited, they're not *evidence.*

By the time someone needs to verify your audit trail, it's too late to rebuild it. Build it before it matters.

See how MnemoShare does it → **mnemoshare.com**