Gap

Plain-English thesis

Cybercrime has become public-scale, but many victims and organizations still face the same basic question: can they show what changed and when?

Why ordinary people should care

Cybercrime is no longer a distant enterprise issue. It touches households, small businesses, hospitals, schools, local governments, and independent professionals.

The FBI reported more than one million IC3 complaints in 2025 and nearly $21 billion in losses. The scale is large, but the after-incident question is personal: what happened to my account, my data, my files, my money, or my system? [S1]

Ordinary people should care because scale does not make evidence easier. It often makes response more crowded, more automated, and more dependent on whatever records survived.

What the real-world problem looks like

Cybercrime creates a gap between event and understanding. A person sees a suspicious transfer. A business sees a login from the wrong place. A vendor reports a breach. A customer record changes. The facts may be real, but the context is not always preserved where people need it.

Verizon reported that its 2025 Data Breach Investigations Report analyzed more than 22,000 incidents and 12,195 confirmed breaches, with third-party involvement doubling to 30 percent of breaches. [S3]

When incidents span vendors, accounts, cloud tools, and internal systems, later reconstruction becomes more expensive and less certain.

What current systems usually leave behind

- Complaint reports, alert records, and ticket histories.
- Security logs and vendor notifications.
- Bank records, email headers, and account activity exports.
- Forensic reports created after outside responders are called.
- Partial timelines built from separate systems.

Why reconstruction is weaker than preserved evidence

Cybercrime response often starts with available fragments. That is understandable, but it leaves responders asking what the fragments mean, whether they are complete, and which system of record should be trusted.

Preserved evidence matters because many decisions must be made quickly: whether to freeze accounts, notify customers, reset credentials, restore backups, contact law enforcement, or change access. Better preserved context makes those decisions less speculative.

Where AuditTrace Labs / Project Aingeal fit

AuditTrace Labs provides the parent public frame: integrity, evidence, observability, accountability, and credible later review.

Project Aingeal is the first formal project in that frame. Its public role is not to replace security operations, law enforcement, fraud teams, or incident responders. Its role is to strengthen the evidence lane around meaningful system change.

The bridge is simple: cybercrime keeps growing, and the evidence needed to understand meaningful change must become more reliable.

What should change going forward

Buyers should demand evidence readiness, not only prevention claims. They should ask what remains after a meaningful change, how long it remains, and whether the context is usable by humans who were not present at the time.

Public discussion should move beyond "more alerts" toward "better preserved context." Both matter, but they are not the same.

Closing

The scale of cybercrime makes the evidence gap harder to ignore. The stronger the preserved context, the less everyone has to rely on incomplete reconstruction later.

Three reusable pull quotes

> **Cybercrime scale makes the evidence gap public, not theoretical.**

> **More alerts do not automatically mean better later understanding.**

> **Evidence readiness should be a buyer expectation.**

Five plain-English FAQs

Does this replace cybersecurity tools?

No. It complements them by focusing on preserved context around meaningful change.

Is the point to catch criminals?

No. The point is to make later review more reliable. Attribution may require separate investigation.

Why does scale matter?

At large scale, people and organizations cannot depend on memory and scattered records alone.

What should buyers ask vendors?

Ask what evidence is preserved when accounts, settings, data, or permissions change in meaningful ways.

Why is this public-facing?

Because the evidence gap affects everyday people, not just technical teams.

LinkedIn-ready excerpt

Cybercrime numbers are large, but the hard question after an incident is often simple: can anyone show what changed and when? AuditTrace Labs and Project Aingeal are focused on the evidence gap that appears after meaningful digital change - not more hype, not all-purpose security claims, just better preserved context for later review.

Website-ready excerpt

Cybercrime scale makes preserved evidence a practical public issue. AuditTrace Labs and Project Aingeal focus on the gap between meaningful change and later understanding, helping frame a future where review starts from preserved context rather than fragments.

Selected public sources

[S1] FBI Internet Crime Complaint Center, 2025 Internet Crime Report / FBI press release

Reported 1,008,597 complaints, nearly $21 billion in losses, and the first IC3 section on artificial intelligence, including 22,364 AI-related complaints and nearly $893 million in losses.

https://www.fbi.gov/news/press-releases/cryptocurrency-and-ai-scams-bilk-americans-of-billions

[S3] Verizon, 2025 Data Breach Investigations Report

Analyzed more than 22,000 security incidents and 12,195 confirmed data breaches; reported third-party involvement in 30 percent of breaches and leading initial vectors including credential abuse and vulnerability exploitation.

https://www.verizon.com/about/news/2025-data-breach-investigations-report

[S4] CISA, Secure by Demand Guide and Secure by Design Pledge

Calls for customer access to evidence of intrusions, including logs around configuration changes, identity events, network flows, and data access or creation.

https://www.cisa.gov/resources-tools/resources/secure-demand-guide

[S5] NIST SP 800-61 Revision 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management

Frames incident response as part of cybersecurity risk management and aims to improve detection, response, and recovery activities.

https://csrc.nist.gov/pubs/sp/800/61/r3/final