

HAYSTACK®



TRACE™ Suite

PROVE WHAT YOUR AI SAW, SAID, AND DID.

ILTACON

August 23-27, 2026

Meet Your Presenter



John Wilson

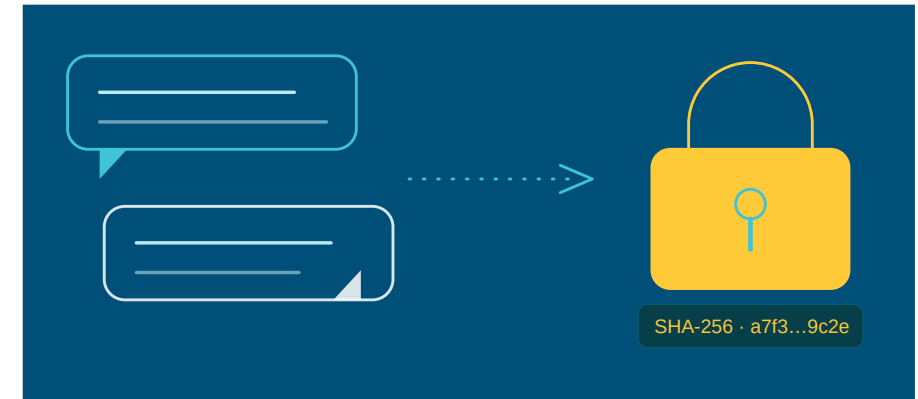
*Chief Information Security Officer and President of Forensics,
HaystackID*

As Chief Information Security Officer and President of Forensics at HaystackID, John Wilson provides consulting and forensic services to help companies address various matters related to electronic discovery and computer forensics, including leading forensic investigations, cryptocurrency investigations, and ensuring proper preservation of evidence items and chain of custody. He regularly develops forensic workflows and processes for clients ranging from major financial institutions to governmental departments, including Fortune 500 companies and Am Law 100 law firms.

Why Now

ENTERPRISES ADOPTED AI FASTER THAN THEIR ABILITY TO PROVE WHAT IT DID.

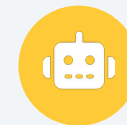
- ✓ Generative AI now drafts, decides, and acts across the business.
- ✓ AI prompts, inputs, outputs, and context are ephemeral by default and preserved with no chain of custody.
- ✓ When a matter or a regulator asks what the AI did, there is often no record that holds up.



Prompts



Inputs



Outputs



Context

The Question Every General Counsel Will Face

PROVE WHAT YOUR AI SAW, SAID, AND DID.

2028

By 2028, general counsel will be asked to account for what their AI produced.

“

Here is the question every general counsel will be asked by 2028: prove what your AI saw, said, and did. TRACE Suite is how you answer it.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

What TRACE Suite Is

FORENSIC PRESERVATION FOR ENTERPRISE AI INTERACTIONS.

1

Preserves the full interaction: identity, timestamps, prompts, inputs, outputs, including images and media, and context.

2

Cryptographic hashing and tamper-evident logging, from the moment of generation.

3

Packaged for chain of custody, ready for authentication, litigation, and regulatory production.

What TRACE Suite Does

CAPTURE. PRESERVE. PACKAGE. ANALYZE.



CAPTURE

The full AI interaction.



PRESERVE

Hashing and tamper-evident logging, from generation forward.



PACKAGE

For chain of custody.



ANALYZE

For matter-specific and compliance review.

The Distinction That Matters

A LOG IS NOT EVIDENCE.

EDITABLE LOG

```
08:42:11 user prompt received
08:42:13 model output logged
08:42:29 entry edited ■
```

It can be edited. It has no chain of custody. No examiner will stand behind it.



FORENSIC PRESERVATION RECORD



SHA-256 · a7f3...9c2e

Sealed · tamper-evident · custody intact

Built on the same discipline behind HaystackID's established forensic work. It is not media authentication, and it is not a logging plugin.

TRACE Suite and VALID™

TWO HALVES OF THE AI-EVIDENCE QUESTION.

Prove what your AI did and prove whether the evidence is real. One forensic bench.

PRESERVE · UPSTREAM

TRACE Suite

Preserves the AI interaction, upstream, as it happens.



AUTHENTICATE · DOWNSTREAM

VALID

Authenticates the disputed artifact downstream.

ONE FORENSIC BENCH



Preservation and authentication are two different jobs. TRACE Suite preserves the AI interaction as it happens. VALID authenticates the disputed artifact later. Run both on one forensic bench, and you can prove what the AI did and whether the evidence is real.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

Coverage Today

PRESERVES ACROSS THE PLATFORMS THAT ENTERPRISES RUN.



ChatGPT



Google Gemini



Microsoft 365 Copilot



Claude

OO One forensic chain of custody across all of them.

Additional platforms on the roadmap

Who It Is For

BUILT FOR THE OFFICES THAT OWN AI RISK.



General Counsel

Managing AI exposure and anticipated Rule 707 risk.



Data Protection Officer

Addressing EU AI Act Article 50.



Chief Compliance Officer

Treating AI-interaction preservation as a continuing obligation.

The Regulatory Moment

THE REGULATORS ARE CONVERGING ON ONE QUESTION.

PROPOSED RULE 707

Proposed

Proposed Federal Rule of Evidence 707 addresses how courts treat machine and AI-produced evidence.

Final advisory-committee vote in 2026, earliest effective December 1, 2027.

EU AI ACT ARTICLE 50

Approximate

EU AI Act Article 50 transparency obligations apply from around August 2026.

Together, can you account for what your AI produced?

“

The proposed Rule 707 and the EU AI Act Article 50 are pushing the same question to the front of the room: can you account for what your AI produced? We built TRACE Suite for that question before it turns into a fire drill.

John Wilson, Chief Information Security Officer and President of Forensics, HaystackID

Rule 707 is proposed and not in force. The Article 50 date is to be confirmed.

Built On a Proven Forensic Bench

FORENSIC-GRADE, FROM AN ESTABLISHED BENCH.



Chain of Custody



Cryptographic Hashing



Tamper-Evident Discipline

The same chain of custody, hashing, and tamper-evident discipline behind HaystackID's established forensic offerings.

RECOGNIZED GLOBALLY BY INDUSTRY LEADERS, INCLUDING:

Chambers

Gartner

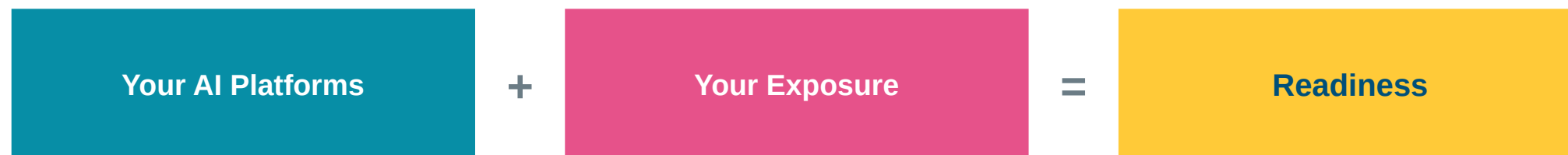
IDC

Legaltech News

Get Ahead Of the Question

For any enterprise deploying AI, a defensible preservation record is the readiness step. Start with a scoping conversation about your AI platforms and your exposure.

HaystackID is introducing TRACE Suite at ILTACON 2026.



Preserve it. Prove it. Defend it.

OPEN FLOOR

TRACE. Preserve it. Prove it. Defend it.

PRESENTER

John Wilson

ROLE

Chief Information Security Officer and
President of Forensics, HaystackID

EMAIL

JWilson@HaystackID.com