EchoMark

ECHOMARK API

Forensic watermarking inside the applications your organization already runs.

Much of your sensitive content never touches email or a share link. The EchoMark API brings the same individualized watermarking to your custom applications, portals, and document systems.

HOW ECHOMARK API WORKS

- Submit a file and request individually marked copies for each recipient, returned programmatically.
- Create API clients directly in the EchoMark web app. No request form or manual approval.
- Marks documents and images, so any application can watermark content at the point of access.
- If a leak occurs, run an investigation in the EchoMark web app to identify the source recipient with a confidence score.



Watermark at the point of access

Generate a uniquely marked copy every time a document is opened or downloaded, to ensure they are traceable in the event of a leak.

Nothing for recipients to install

Marking happens on the server-side before content is delivered, so recipients do not need any plug-in, agent, or EchoMark account.

BUILT FOR REAL-WORLD ENVIRONMENTS

Document management systems

Mark every file on retrieval so each access produces an individually attributable copy.

Customer and partner portals

Statements, reports, and downloads marked per authenticated user at request time.

High-volume workflows

Batch and on-demand marking at scale, including those conducted as part of applications or automated workflows.

FROM LEAK TO ANSWER IN MINUTES

01

Watermark

Your application calls the API to generate an individually marked copy for each recipient.

02

Detect

You discover a sensitive document, screenshot, printout, or image outside your organization.

03

Identify

Submit the leaked artifact to identify whose copy leaked, with a confidence score and chain of custody.

CONTACT US: info@echomark.com

SCHEDULE A DEMO: echomark.com/schedule-a-demo

Product Videos

Schedule a Demo