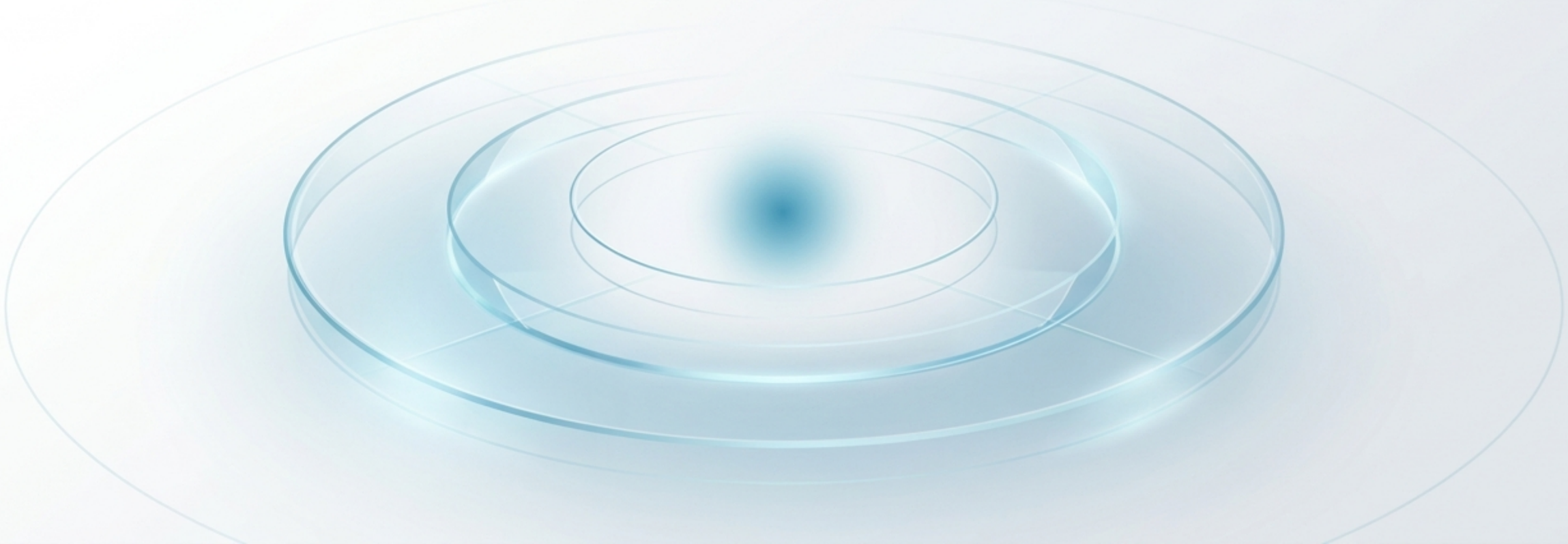
Solution-EDLP

Exposure Data Loss Prevention (EDLP)

Extending DLP beyond the file transfer to control visible data at the human edge.



The Blind Spot in Traditional DLP

Data loss does not require a file to leave the system. It often occurs the moment sensitive information becomes visible on a screen.

Traditional DLP

Trigger:	File transfers and repository movement.
Focus:	Network boundaries and system perimeters.
Blind Spot:	Ignores visible data and human workflow.

Exposure DLP

Trigger:	Visibility and workflow actions.
Focus:	User behavior, application activity, location, and timing.
Advantage:	Controls exposure even when no file leaves the system.

The Moment of Exposure

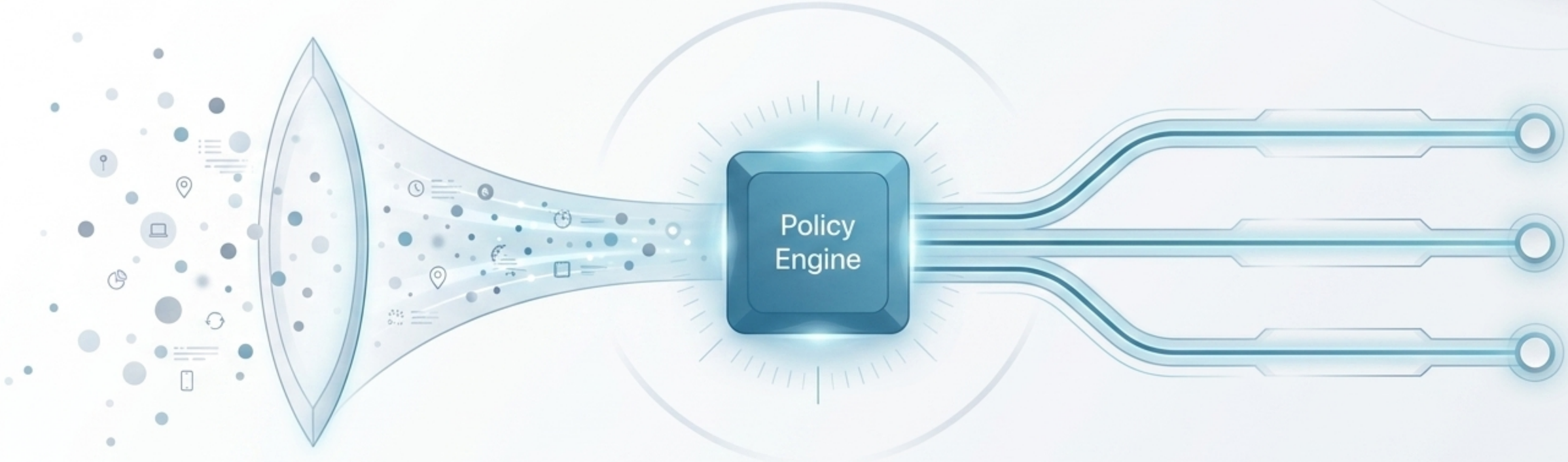
A user views sensitive data on screen while attempting to copy, capture, paste, share, or expose it through a risky workflow.

Context Defines the Risk

Risk escalates when sensitive information is visible, copied, captured, handled, or shown in the wrong context.

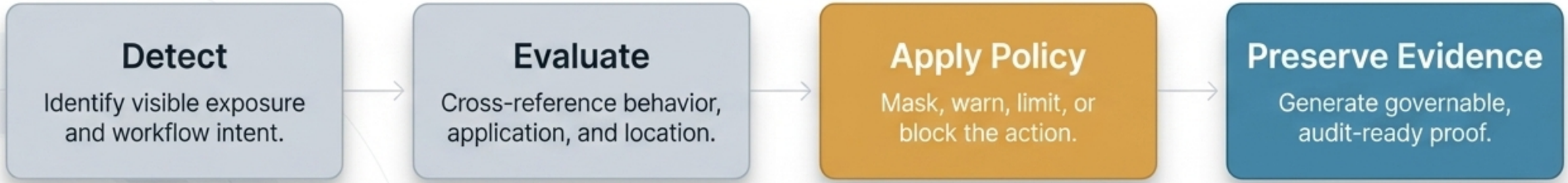
Real-Time Exposure Control

Managing risk as work happens requires a continuous, instantaneous decision flow at the moment of exposure.



Precision Responses, Not Just Blocks

Detect the exposure, evaluate context, and apply the exact policy action or capture audit-ready evidence.



Modernizing Security & Compliance

Closing the critical gap between system perimeter protection and actual human behavior.

Security

Control exposure before data loss occurs, without relying on delayed detection.

Operations

Maintain uninterrupted, secure workflows by targeting only high-risk context.

Compliance

Automatically generate defensible, audit-ready evidence of real-time exposure controls.

Control the View, Control the Risk.

Data loss prevention must control visible data, not only file movement.