We believe our data is secure.

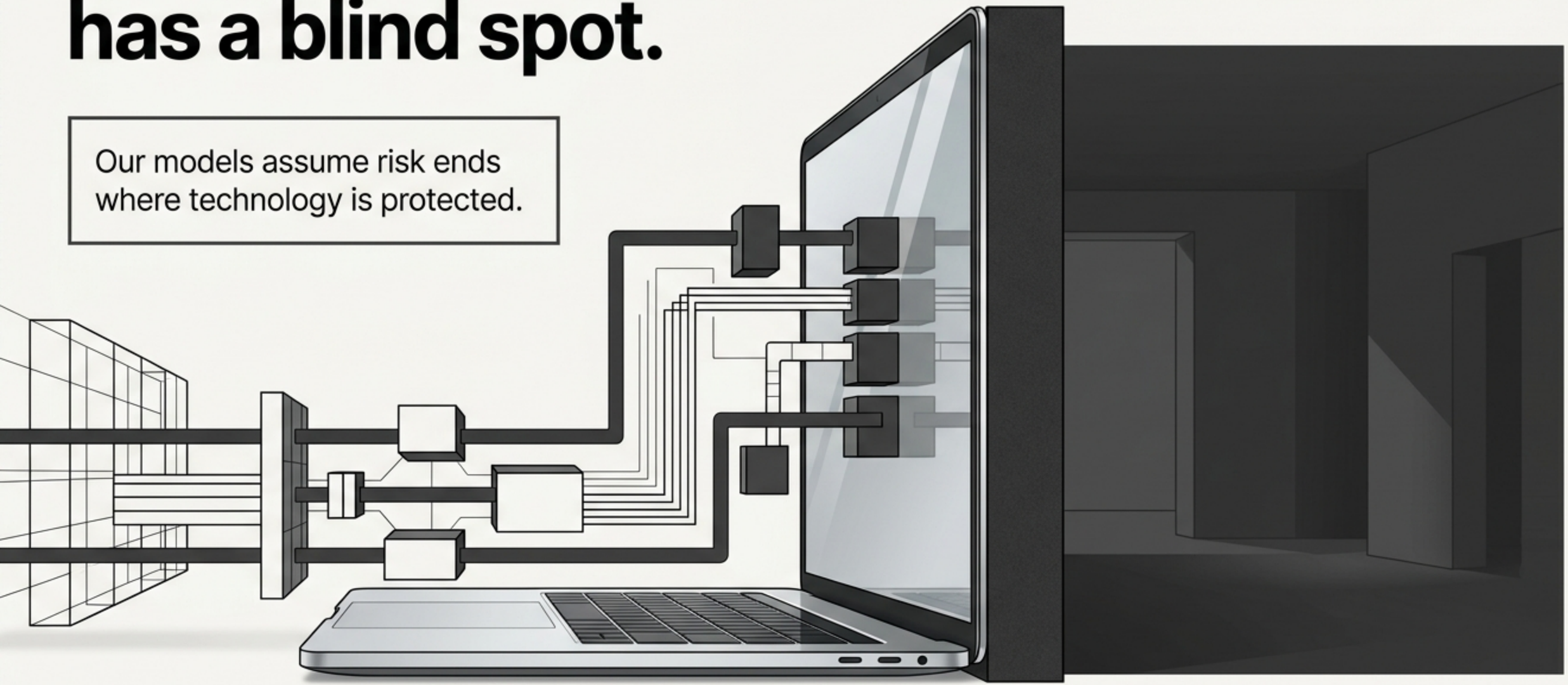
Systems are hardened.

Controls are deployed.

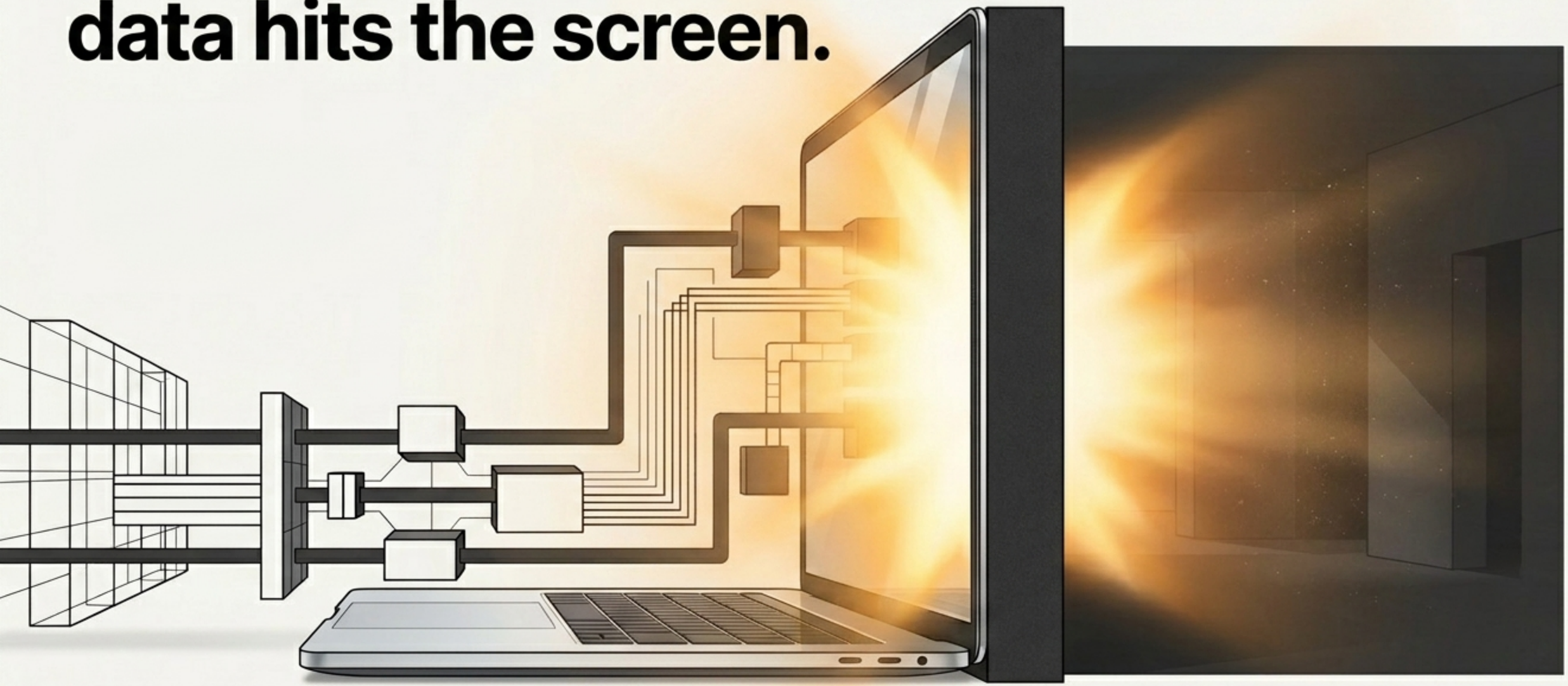
Compliance is met.

But our security has a blind spot.

Our models assume risk ends where technology is protected.



Risk begins the moment data hits the screen.



We rely on a fragile assumption of trust.

People will not make mistakes.

Environments are totally safe.

Behaviors will never deviate.

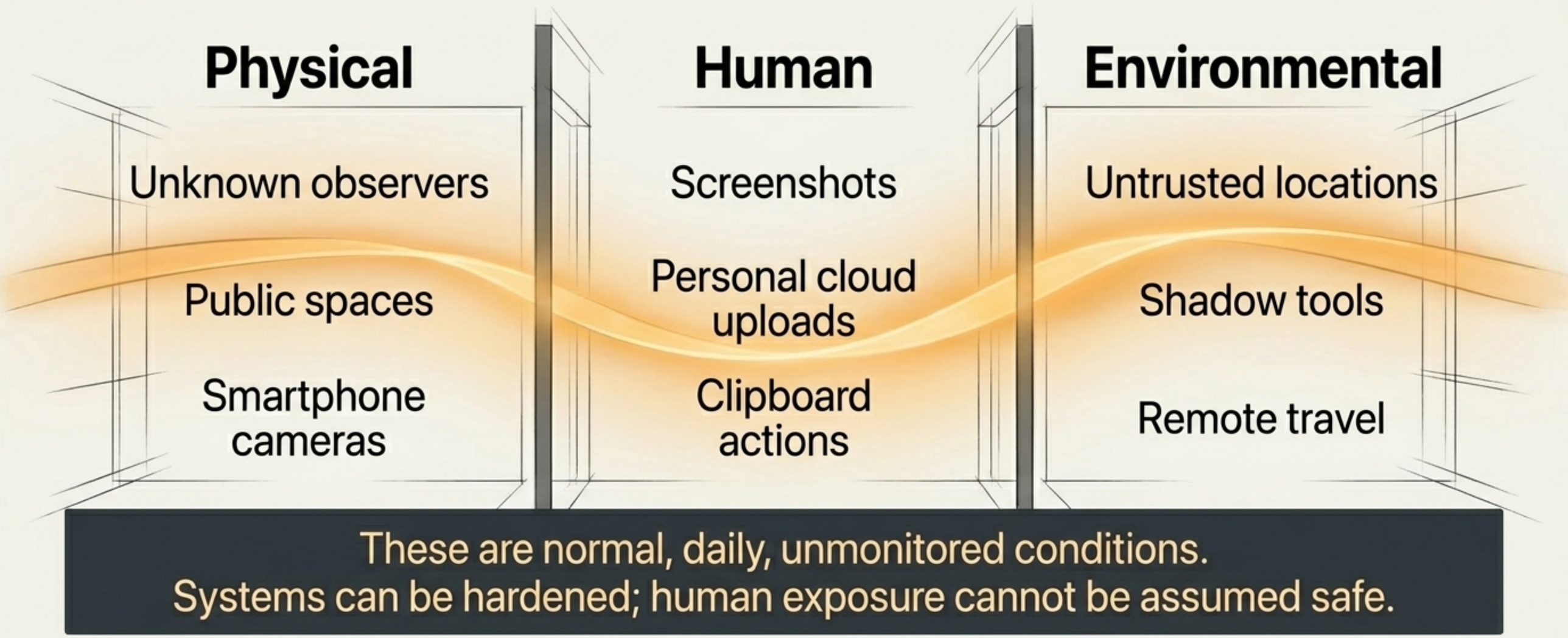
Exposure does not require malice.

A momentary distraction.

An unknown observer.

A single shared screen.

The anatomy of real-world exposure.

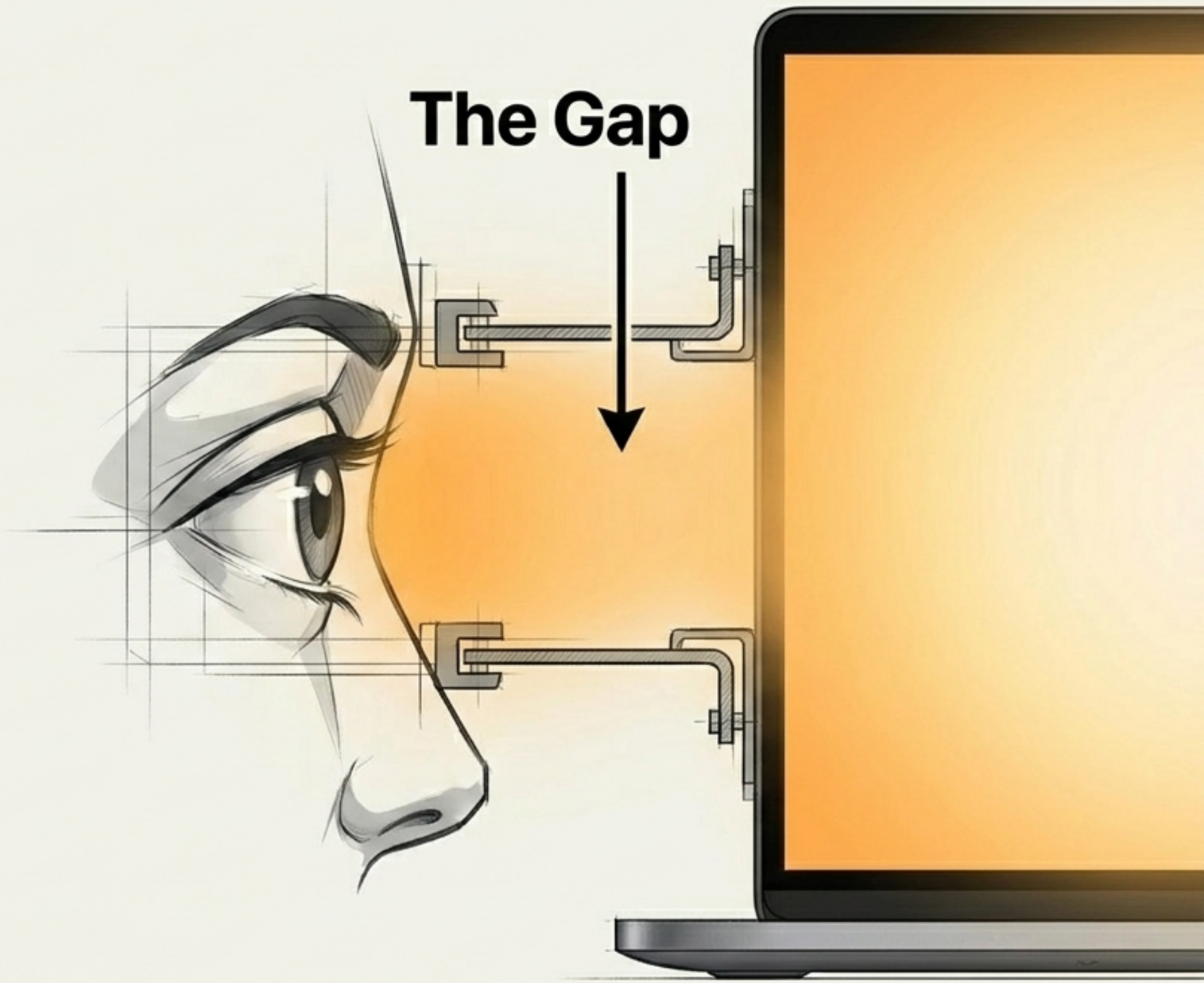


These are normal, daily, unmonitored conditions.
Systems can be hardened; human exposure cannot be assumed safe.

This is the true security gap.

Risk no longer lives inside the system.

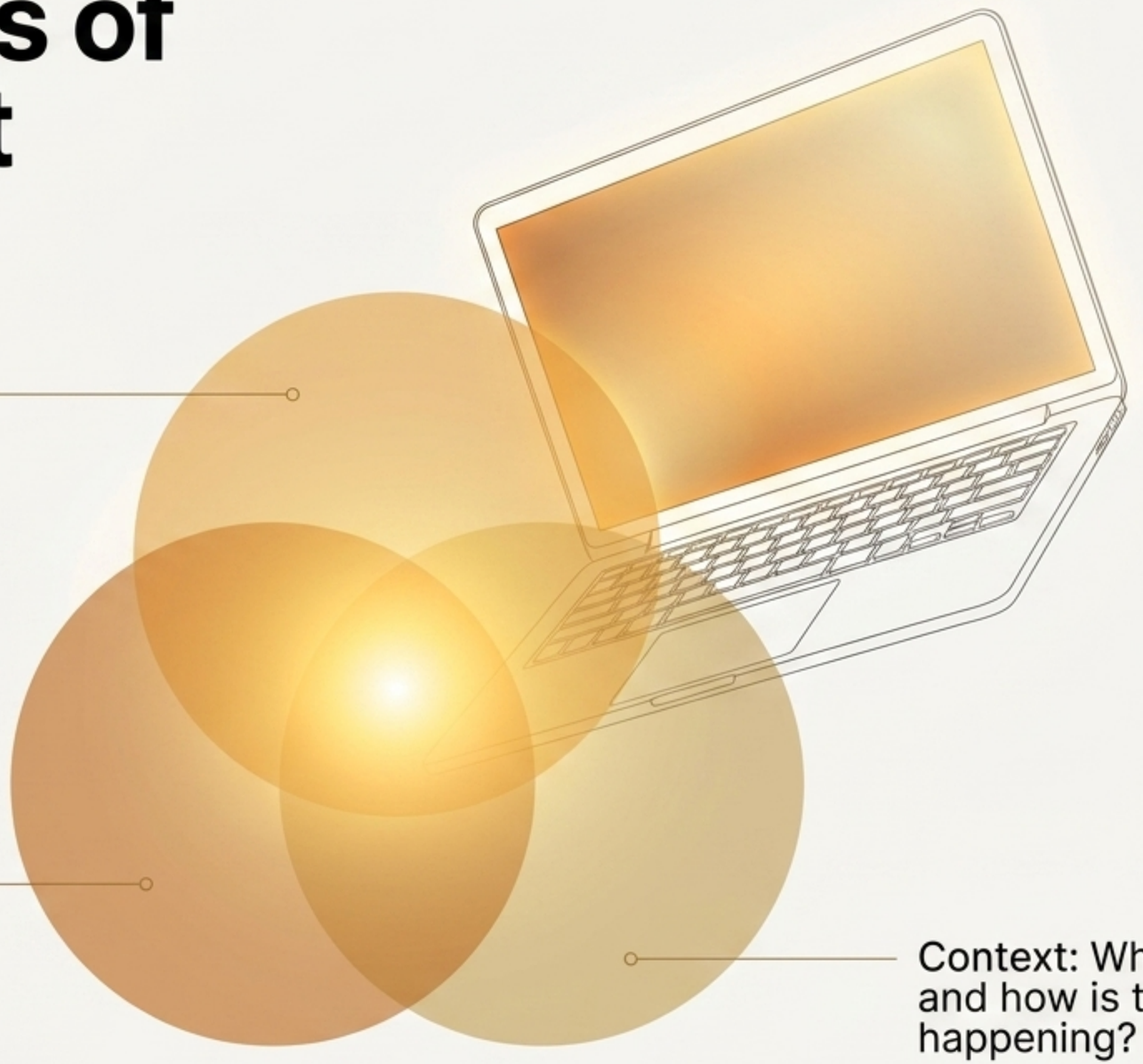
It lives in the unmanaged moments of visibility.



We must extend control into the real world.

Three dimensions of real-time context

Visibility: What data is currently on the screen?



Presence: Who is physically looking at it?

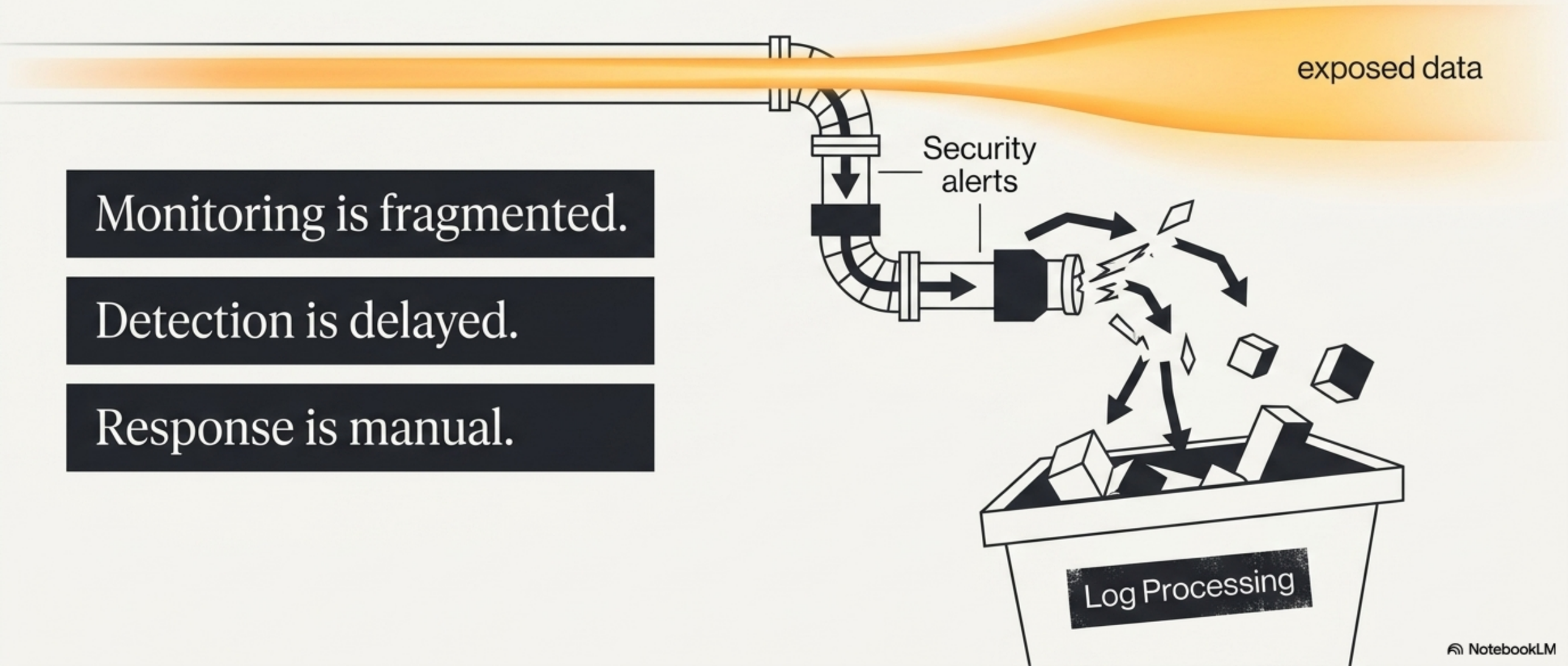
Context: Where and how is this happening?

Why yesterday's security model fails.

Monitoring is fragmented.

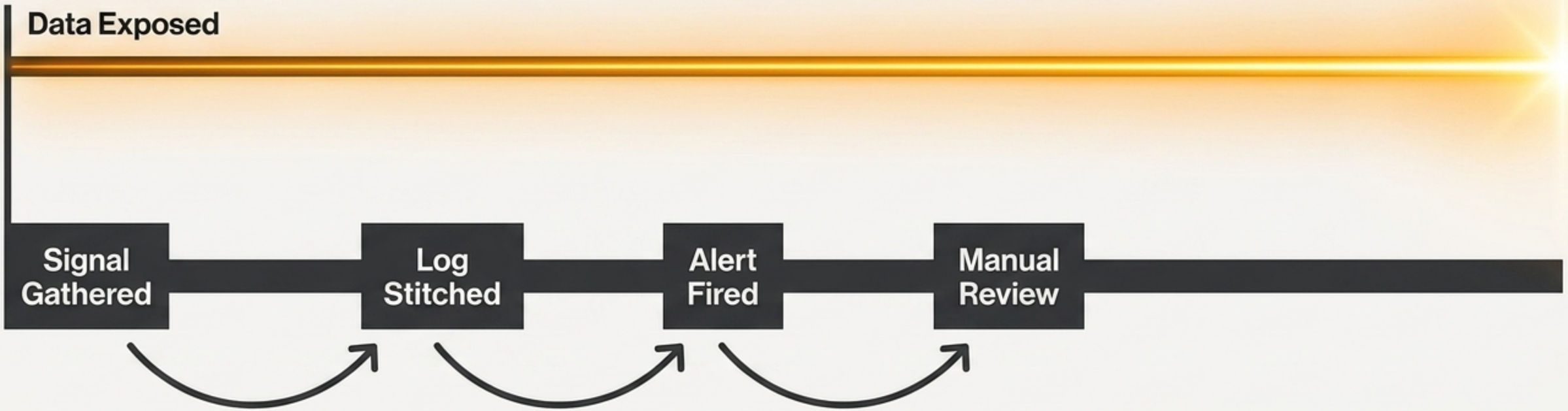
Detection is delayed.

Response is manual.

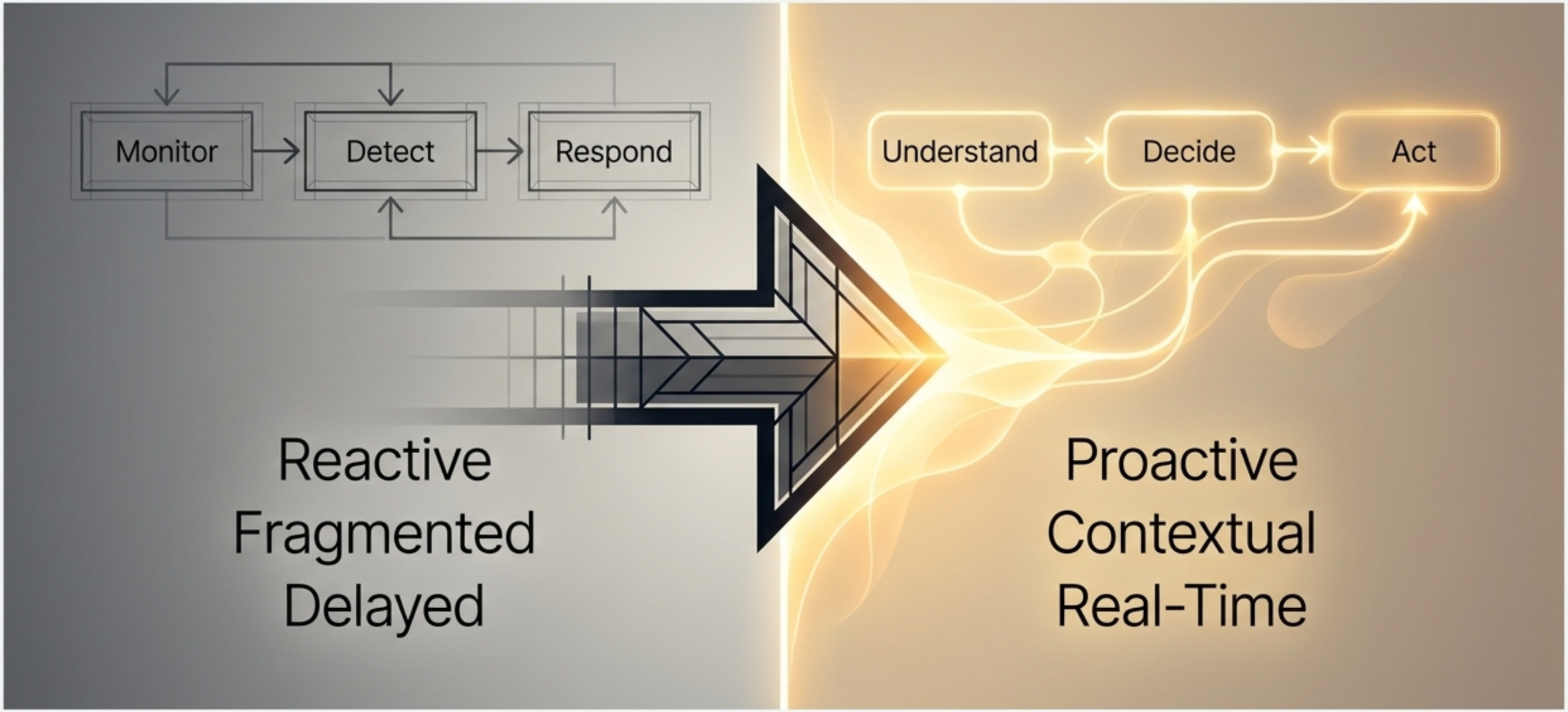


The cost of post-processing.

Controls activate after exposure—not during.



A fundamental shift in methodology.

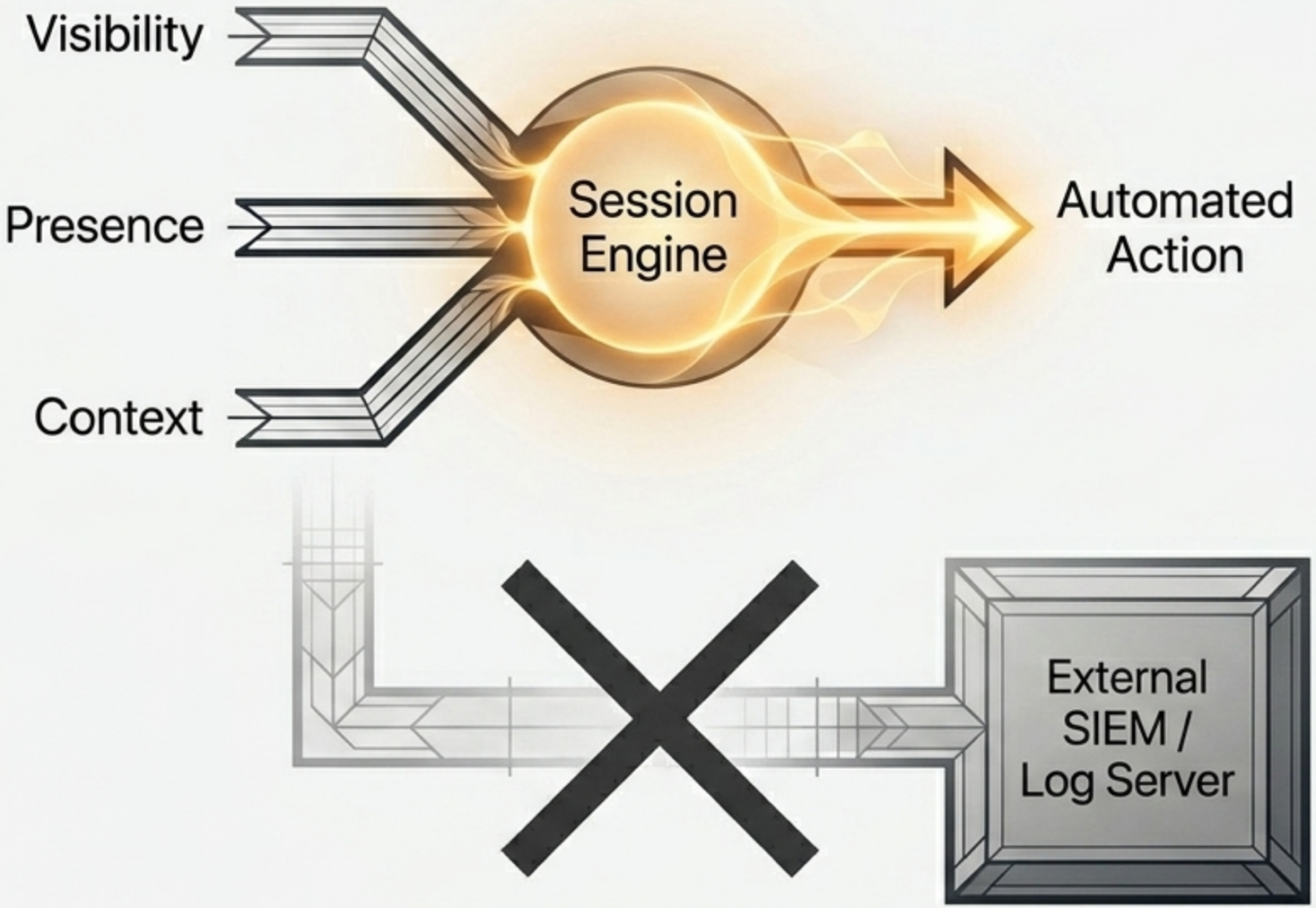


Operating inside the active session.

No reliance on log stitching.

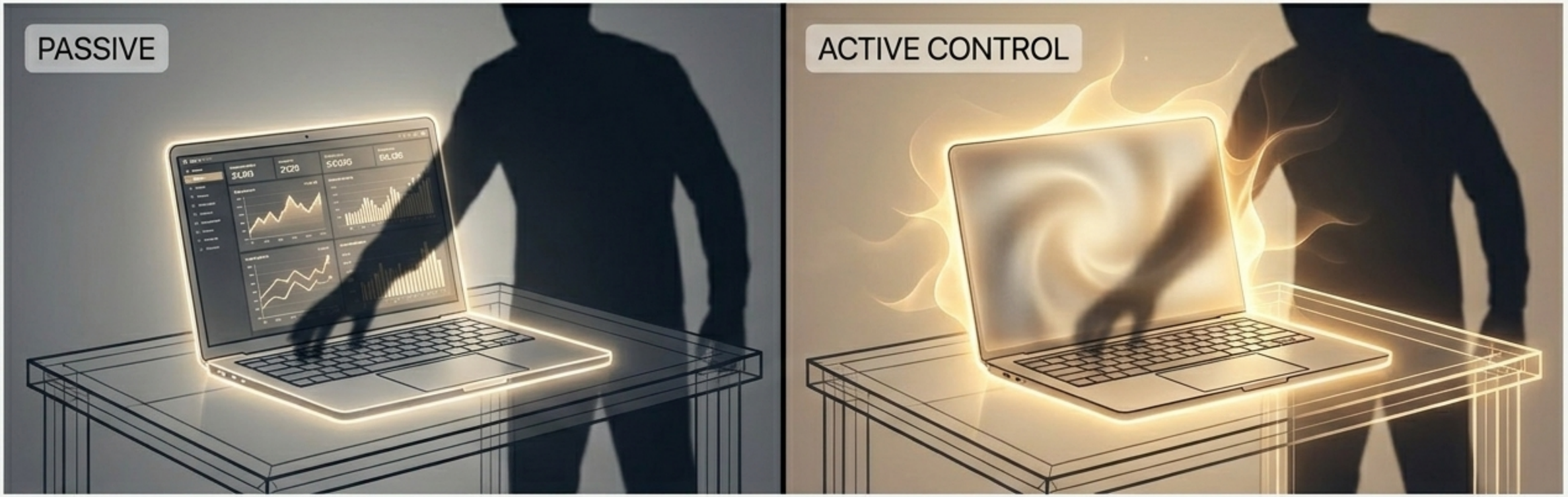
No delayed post-processing.

Evaluated and enforced as it happens.



From passive assumption to active control.

- Real-time exposure awareness.
- Context-driven intervention.
- Zero response delay.



The new standard.

Security is no longer about protecting systems.

It is about controlling exposure the moment data becomes visible.