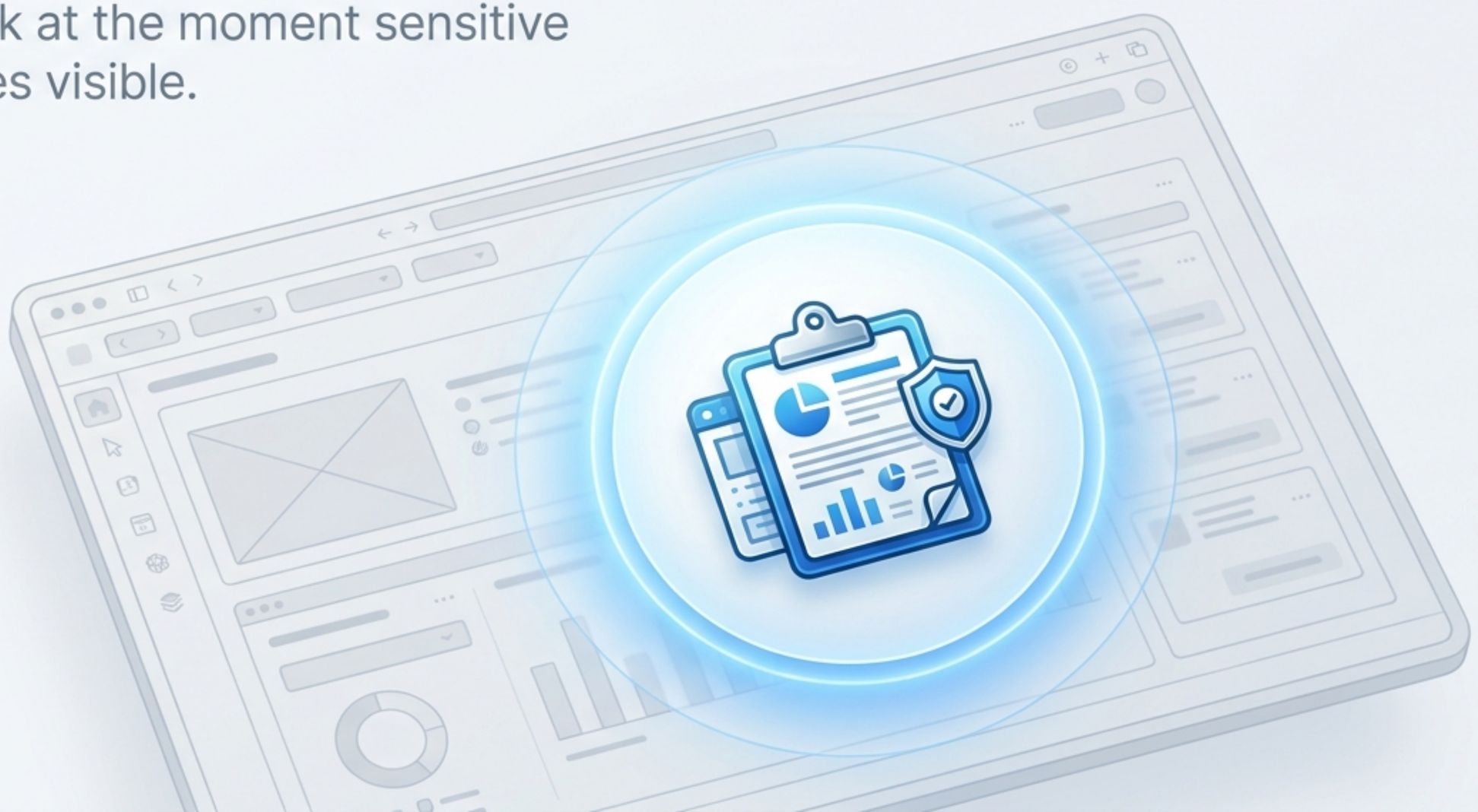
Solution-ITM

Trendzact Insider Threat Management

Detecting risk at the moment sensitive data becomes visible.



The visibility gap in traditional data loss prevention

A file does not have to leave the system for sensitive data to be exposed. Relying **solely on file transfers** creates a **blind spot** during the critical staging phase.

Traditional Focus	Trendzact ITM Focus
Evaluates isolated, single events.	Evaluates repeated behavioral patterns.
Triggers only upon file transfers or repository movement.	Triggers on visible on-screen staging and application misuse.
Relies on after-the-fact logs.	Relies on real-time endpoint context.

True exposure risk is a sequence of on-screen behaviors

Visibility

A privileged user opens a highly sensitive application.

Capture

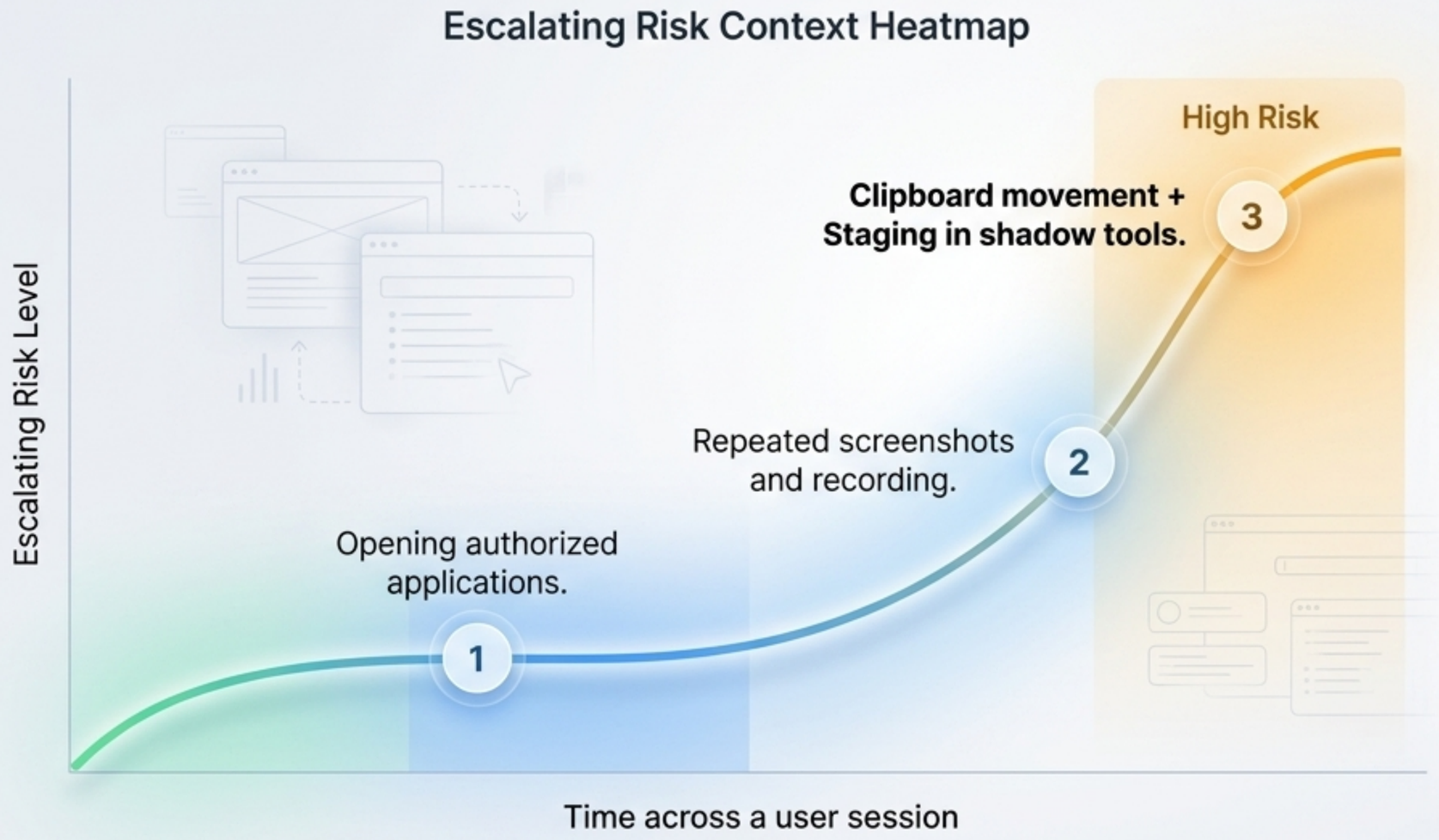
The user repeatedly copies the visible sensitive information to the clipboard.

Staging

The data is pasted and staged within an unauthorized shadow tool.

A privileged or high-risk user repeatedly opens, copies, captures, or stages sensitive information across applications.

Context transforms routine actions into high-risk indicators

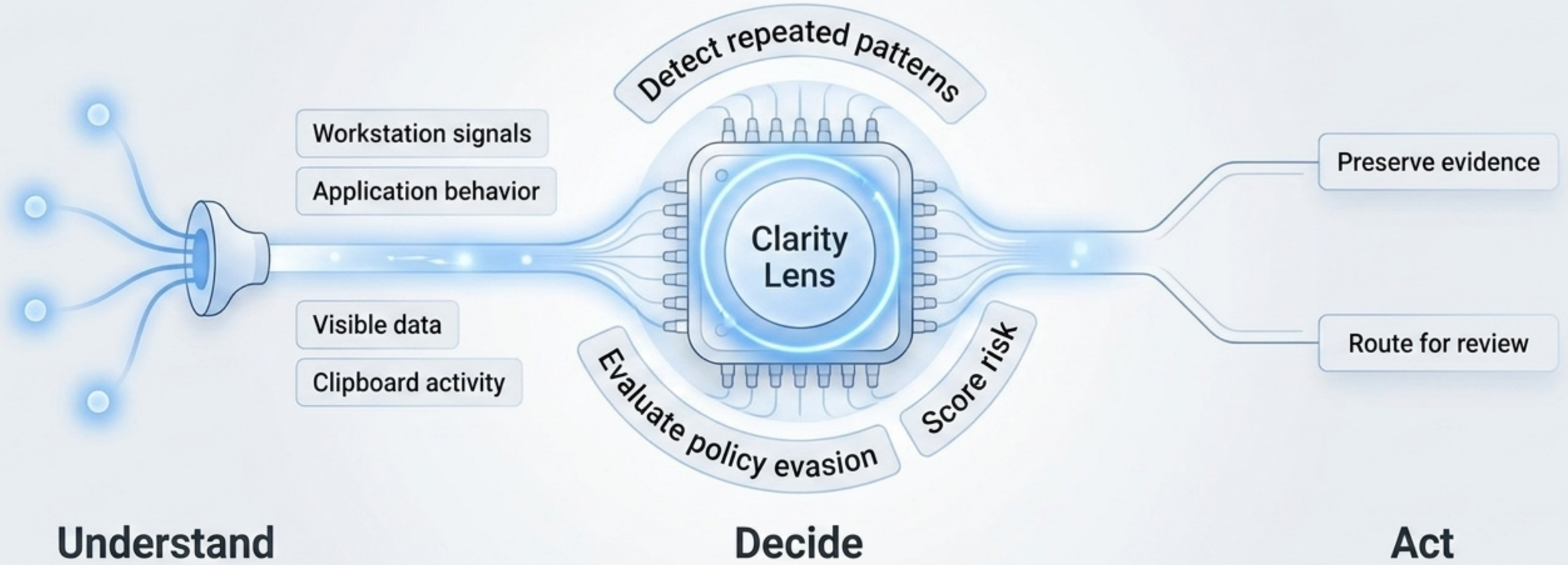


High-Risk Workflow Periods

Risk context is critical during highly sensitive employee periods, including:

- Resignation or layoff preparation
- Active disputes
- Use of highly privileged access

Evaluating exposure context in real time



The engine evaluates stealth, negligent, or malicious behavior before the exposure becomes a permanent loss.

Routing high-confidence events with audit-ready evidence

When escalating exposure behavior occurs, the platform preserves the exact moment of exposure—creating proof, not uncertainty.

Shifting from delayed detection to real-time control

Case in Practice: Global banks utilize this context to identify risky handling of visible data before staging or shadow tools result in data loss.

Leadership Value: CISOs and Chief Compliance Officers gain provable, continuous exposure control aligned with how modern work actually happens.

Insider risk is clearer when exposure behavior is visible.

Access permission does not grant exposure permission.
Control the risk at the moment it occurs.