CurrentWare

AI TOOLKIT

Shadow AI Investigation Playbook

A step-by-step process for finding the AI tools your employees use, understanding how they use them, and deciding what to approve, evaluate further, or restrict.

INTRODUCTION

Before you begin

Most organizations have written AI workplace policies to reduce risk and ensure regulatory compliance. Meanwhile, teams tend to build their own practices alongside the official policies and approved tech stack; they try specialized tools, mix company and personal accounts, and paste work product into tools nobody has yet reviewed. With time, the exposure risk increases without visibility into the processes creating this blind spot.

This playbook gives IT, security, and compliance teams a repeatable way to find that gap, understand it, and act on it without shutting down the AI use that is helping people work.



DEFINITION

Shadow AI is any AI tool used at work without IT approval or oversight, including personal accounts on tools the company has approved.

How to use this playbook

01	**Prepare**	Set the scope, define owners, and ground rules.
02	**Discover**	Build an inventory of every AI tool in use.
03	**Investigate**	Find out who uses each tool, why, and what data is used.
04	**Decide**	Approve, further evaluate, or restrict each tool.
05	**Control and Measure**	Enforce the decision and track adoption over time.

PHASE 01

Prepare

Consider the regulatory framework within which you operate, and the problems you are trying to solve with your existing tools. Agree on who is responsible for managing the discoveries and actioning next steps.

1.1 Define the scope of your audit

Choose the departments, locations, and devices to include in your audit. Cover remote and hybrid staff, since they are most likely to work outside managed tools.

1.2 Name the stakeholders

Bring in leads from any department in scope, whether that is IT, security, legal or compliance. Assign specific owners for the final decisions and action items.

1.3 Collect your existing tools and policies

Gather your AI Acceptable Use Policy, the list of approved AI tools, and the licenses you pay for. For **BrowseReporter** clients, you can pull license counts from **Cost Insights.**

1.4 Set a reasonable review window

Collect at least two to four weeks of activity so the results reflect existing workflows rather than a possible outlier, like a single busy day.

1.5 Confirm monitoring requirements

Check with legal and/or HR teams to ensure that employee notice and required consent are confirmed and meet local regulations, before monitoring begins.

BY THE END OF THIS PHASE

You will have a defined scope, a named decision owner, a baseline list of approved tools, and adequate sign-off to begin collecting data.

PHASE 02

Discover

Use **BrowseReporter** to see which AI platforms are being accessed, by whom, on which devices, and for what purpose. Then build a complete inventory of the AI tools in use across the organization and indicate whether they are on the approved list or exist as Shadow AI.

2.1 List every AI tool accessed

Run a web usage report for the review window and highlight every AI platform, including chat assistants, coding tools, research tools, and newly created tools.

2.2 Record usage for each tool

Note how many users, which departments, which devices, and how much time is spent on each tool. In some cases, frequent use by one team often points to a real workflow need.

2.3 Compare against your approved list

Mark each tool as approved or unapproved. Check whether approved tools are being reached through company accounts or personal ones (Example below).

2.4 Flag what is missing

Note any approved, paid tools with little or no usage. Unused licenses provide information on employee preferences, and can help uncover unused investments.

APPROVED, IN USE	UNAPPROVED, IN USE	APPROVED, UNUSED
Healthy user adoption. Measure it in Phase 05.	Shadow AI, in use. Investigate in Phase 03.	Wasted investments. Find out why in Phase 03.

PHASE 03

Investigate

For each tool, find out who uses it, what they use it for, and what information goes into it. If an approved tool is unused, find out why this is the case. Work through the four areas below:

01

Approved tools

Which authorized AI platforms are being accessed? Are they being used in accordance with the AUP or is further evaluation required?

02

Hidden Shadow AI users

Find where Shadow AI is found across employees, departments, or devices. Are compliance requirements or AI AUP breached?

03

Unused investments

Which teams are adopting the approved AI platforms? Are unused licenses adding unnecessary costs?

04

Sensitive data exposure points

Where could sensitive company data be entering public AI tools? Does screenshot evidence show personal information is handled appropriately?

Gain context on your findings.

CurrentWare's reports will provide you with the facts, and we encourage leaders to conduct conversations with their teams to gather contextual data. Ask each Shadow AI heavy-use team:

- What problem are you solving with this tool that your current tools can not help with?
- What kind of information do you need in order to us it effectively?
- Would an approved alternative do the job? If not, what is missing?

GOOD PRACTICE TIP!

As a first step, treat findings as information about resource deficits. Most Shadow AI use begins with an employee trying to work more efficiently, and the tools they choose can show you where to consider further investments.

PHASE 04

Decide

Give every tool in your inventory one of three outcomes: Approve, Evaluate, Restrict. Remember that decisions on access can differ by team, because a tool that is fine for marketing may not be acceptable for legal or finance teams.

Approve	The tool resolves a real need, meets your security and data-handling requirements, and can be managed through company accounts.
Evaluate	The tool shows clear value but needs further review. Run a proof of concept against a benchmarked workflow before considering wider rollout.
Restrict	The tool creates risk without added value, duplicates an approved tool, or handles data in ways your company policy does not permit.

Moving forward, choose a policy approach for each team

Each approach below trades control for flexibility, and none provide the right fit for every organization. It is important to pick the policy approach that fits your organization's regulatory requirements, data handling practices, or industry, and expect to revisit the policy as your AI tool inventory grows.

MORE CONTROL — MORE FLEXIBILITY

01

HIGHLY RESTRICTIVE

"We are using Copilot. Everything else is blocked."

Clear and easy to enforce, but can push use onto personal devices.

02

APPROVED LIST

"Some AI tools allowed. Others reviewed."

Balances experimentation and control. The list needs ongoing reviews.

03

OPEN WITH MONITORING

"Use whatever AI you want. Just stay within our policies."

Shows what employees prefer, with higher risk and cost.

PHASE 05

Control and Measure

Put your decisions into effect, and then keep assessing for the future.
Use **BrowseControl** and **AccessPatrol** to manage access by team, and **BrowseReporter** to track whether your policies are working.

5.1 Enforce access by team

In **BrowseControl**, allow the AI tools on your approved list and block the rest, with separate policies for each team, department, or schedule. Use **AccessPatrol** to stop sensitive files leaving through USB and other removable devices.

5.2 Set alerts

Configure **BrowseReporter** alerts for anomalies and policy violations, such as a new AI tool appearing in your reports or a restricted tool being accessed, so your team can follow up quickly.

5.3 Measure adoption

Use **BrowseReporter** to track which teams use the approved platforms and how often. Compare active usage with paid licenses, and review trends over time to confirm your AI investment is paying off.

5.4 Report to leadership

Share audit-ready reports showing Shadow AI found, decisions made, and adoption of approved tools. Schedule **BrowseReporter** reports to reach stakeholders automatically each month.

Repeat the cycle

AI tools change rapidly, so an investigation is never finished. Review your inventory monthly and revisit your policy each quarter.

01	02	03	04
Discover	Evaluate	Control	Measure

WORKSHEET

AI tool inventory

This is a sample tool inventory. Copy this page as needed for your investigation.

AI tool	Teams / users	Purpose	Data entered	Approved? Decision	Owner

Every organization's Shadow AI footprint looks different. If your inventory turned up more tools than expected, or you're not sure which to approve, restrict, or monitor, talk to our team. In a short call, we'll review what you've found, show you how BrowseReporter, BrowseControl, and AccessPatrol apply to your environment, and help you build a plan that keeps your teams productive without exposing sensitive data.

Need help with your investigation?

1-888-912-9619

NEW CLIENTS
sales@currentware.com

EXISTING CLIENTS
success@currentware.com

TECHNICAL SUPPORT
support@currentware.com