



Which AI uses deserve attention first?

Find each use. Record six fields. Apply three criteria.

01

FIND

Five places AI hides

1 What you built

Internal apps that call a model. Notebooks. Pilots that quietly became production.

3 What people brought

Unapproved tools seen on corporate devices and networks.

5 What is embedded

AI inside security and email tools.

2 What you bought

AI added by update to software you already pay for. Check vendor release notes.

4 What connects

Apps let into mail and files. Check your identity provider's app grants.

First pass: about a week

App grants · outbound traffic · release notes · card spend · then ask, without blame.

THE RULE The routes overlap. Keep one row per use and note where you found it.

02

RECORD

Six fields, one row per use

1 Owner

A named, accountable person.

2 Purpose

The business use.

3 Reads

What comes in. Flag content written outside the organisation.

4 Reaches

The data and systems it can get to, including read-only.

5 Acts

What it can do or send, and whether a person checks first.

6 Runs as

The identity it uses and how long the credential lives.

03

PRIORITISE

Three stated criteria

1 Reads outside content

3 Acts without a person checking first

2 Reaches sensitive data or critical systems

THE RULE Two or more: first review list. Any open finding: review now.

USE	OWNER	PURPOSE	READS	REACHES	ACTS	RUNS AS	CRITERIA
Ticketing assistant Example · found via: bought, connected	Head of customer support	Drafts replies to customer tickets	Customer tickets from outside	Ticket history, order records, customer profiles (read-only)	Drafts; a person sends	Service account; token never expires → finding	1 · 2 · 3 First review
							1 · 2 · 3
							1 · 2 · 3
							1 · 2 · 3
							1 · 2 · 3

MONDAY

Pull app grants and outbound traffic to AI services. Search vendor release notes for "AI".

BY FRIDAY

One row per use, six fields. Apply the three criteria. Name an owner for every first-review row.

WHAT IT IS NOT

Not complete discovery: a first pass covers corporate systems and traffic, not personal devices. Not a NIST template. Reference: NIST AI 100-1, GOVERN 1.6.