DEEP WELL LABS

Know what AI can access Keep control.

AI EXPOSURE & CONTROL DIAGNOSTIC

See what selected AI tools can read, share or change.
Leave with a practical plan for safer day-to-day use.

$750

FIXED-PRICE PILOT

One workflow. Clear boundaries.

BUILT FOR Small business owners and operations leads in Lansing and Grand Rapids using off-the-shelf AI tools.

Sound familiar? AI at work. Unclear access. No agreed rules.

A small engagement. Tangible answers.

01 Focused discovery
60-90 minutes with your owner or IT lead. One workflow and up to three AI tools.

02 An AI access map
Review up to two connected systems: what AI can read, share or change.

03 A guided control review
Inspect available settings on your screen: permissions, data use and approvals.

04 A safe scenario walkthrough
Discuss one plausible mistake or misuse: who notices, pauses it and recovers?

05 A two-page action plan
Priority actions, owners and a 30-day plan, plus a separate access worksheet.

06 Three-business-day delivery
After discovery and agreed inputs. Includes a 30-minute results discussion.

HOW IT WORKS

1 Map
See the access.

2 Review
Check the controls.

3 Decide
Assign the next steps.

CLEAR BOUNDARIES

Guided, point-in-time review of agreed tools only. No direct system access, live attack testing, implementation, breach investigation or security/compliance certification.

OPTIONAL NEXT STEP

External exposure audit

Audit: $2,950. Hardening: $1,950.
Fixed pilot scopes. See page 2.

Bring one AI-enabled workflow.

Fixed-price pilot. Scope agreed before work begins.

begin@deepwelllabs.com

DEEP WELL LABS

Could outside AI reach your internal data?

Scan audit details

Scan hardening details

EXTERNAL AI & BOT EXPOSURE AUDIT

Investigate available evidence. Close exposed access paths.
A separately scoped technical service for Lansing and Grand Rapids businesses.

A PLAUSIBLE SCENARIO

A customer-document portal was intended for staff, but one folder or API endpoint was reachable without signing in. An external crawler or AI assistant may have followed a public link and requested confidential material. The owner needs to know what was exposed, what was actually accessed and how to prevent it happening again.

---

01 Map the exposure

Identify the agreed public entry points, sharing settings and paths into internal data. Distinguish intended public content from unintended exposure.

02 Reconstruct the access

Correlate available web, cloud and identity logs. Report attempted requests, supported evidence of access and any unresolved gaps; assess AI/bot attribution separately.

03 Harden and verify

Under a separately approved change scope, restrict access, remove public sharing, reduce permissions and improve logging. Retest the affected path and legitimate workflow.

EXTERNAL EXPOSURE AUDIT

$2,950

Exposure map, access timeline and findings.
Up to 5 hosts, 1 tenant, 5 log sources; 30 days.

INFRASTRUCTURE HARDENING

$1,950

One exposure path; up to 3 configuration fixes.
Change record, retest and 7-day verification.

Fixed pilot scopes after fit review. Both: $4,900. Remote delivery; additional work quoted separately.

Log availability limits historical conclusions. A bot name alone does not prove AI identity; no evidence found does not prove no access. Active incident response, licenses and onsite work are excluded. Written scope confirms evidence-volume limits and approved changes. No security certification.

Start with a scoped evidence review.

deepwelllabs.com/consulting/external-ai-bot-exposure-audit

deepwelllabs.com/consulting/infrastructure-hardening-sprint