

Secure AI use. Enable innovation.

Empower your teams to use AI tools without fear.

CultureAI detects unsafe use, coaches users on the fly,
and enforces smart guardrails to keep your business secure and compliant.

Trusted by security leaders at:



THE CHALLENGE

Your workforce is using AI - **with** or **without** your approval.

78%

of employees access
AI at work via personal
tools (BYOAI).

Microsoft

96%

of executives expect
AI-related breach risk
within three years.

IBM

47%

of orgs are using AI with no
specific practices in place
to protect them.

DSIT & NCSC

*"We can now show regulators exactly how we're controlling AI risk, with
anonymised data, and full audit trails."*

Data Privacy Lead, HealthTech Provider

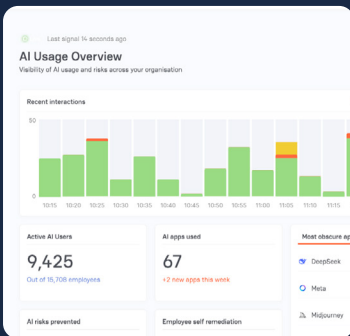
Get visibility across tools with AI & prompt functionality:



& 10,000+ more!

CultureAI, an AI Usage Control Platform

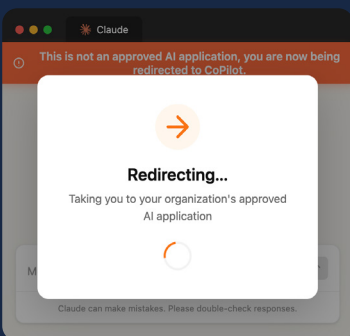
CultureAI combines visibility, risk detection, adaptive controls, and real-time coaching — so you can enable AI safely without slowing your teams down.



AI Usage Visibility

See exactly how AI is being used — across sanctioned platforms, embedded SaaS features, and shadow tools.

- ✓ Tracks prompts, files, and account types.
- ✓ Detects shadow and BYOAI use.
- ✓ Integrates with SIEM, IAM, and device data for unified visibility.



Real-Time Coaching

Educate users in the moment, not after the fact.

- ✓ Inline prompts before risky actions.
- ✓ Role- and risk-aware nudges to guide safe behaviour.
- ✓ Post-incident feedback and behaviour change tracking.

Type	Risks	Outcome
File upload	PII	Warned
Prompt	None	Allowed
App view	None	Allowed
Prompt	PII	Blocked
App view	None	Allowed

Behaviour-Based Risk Detection

Catch risky behaviour before it causes damage — and understand why it's happening.

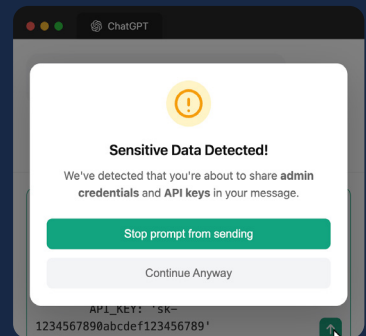
- ✓ Prompt-level inspection with NLP.
- ✓ Behavioural baselining and anomaly detection.
- ✓ Risk scoring by user, tool, and content type.

Type	Risks	Outcome
1 APPLICATIONS	Allow Microsoft CoPilot	Allow
3 APPLICATIONS	Block inappropriate apps	Block
4 APPLICATIONS	Block apps with data hosted in high risk regions	Block
4 INTERACTIONS	Block file uploads in Deepseek and Qwen	Block
4 INTERACTIONS	Block sensitive data in all apps except CoPilot	Block

Privacy-First by Design

Control risk without compromising trust.

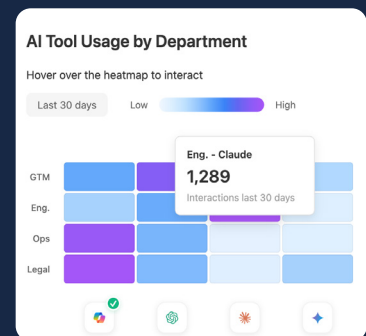
- ✓ No keylogging.
- ✓ Encryption at rest, role-based access, configurable logging.
- ✓ Built for regulated industries (GDPR, HIPAA, ISO 42001, EU AI Act, and more).



Adaptive Policy Enforcement

Go beyond “block or allow” with flexible, context-aware guardrails.

- ✓ Role-aware enforcement (e.g. Finance vs Engineering).
- ✓ Options for soft nudges, hard blocks, or exceptions.
- ✓ Geo- and data-residency aware controls.
- ✓ Map policies to frameworks like EU AI Act & NIST AI RMF.



Reports & Compliance

Give CISOs, DPOs, and execs the proof they need.

- ✓ Security and compliance dashboards.
- ✓ AI usage audit logs and evidence trails.
- ✓ Role-based access controls for reports.
- ✓ ROI and behaviour improvement metrics.