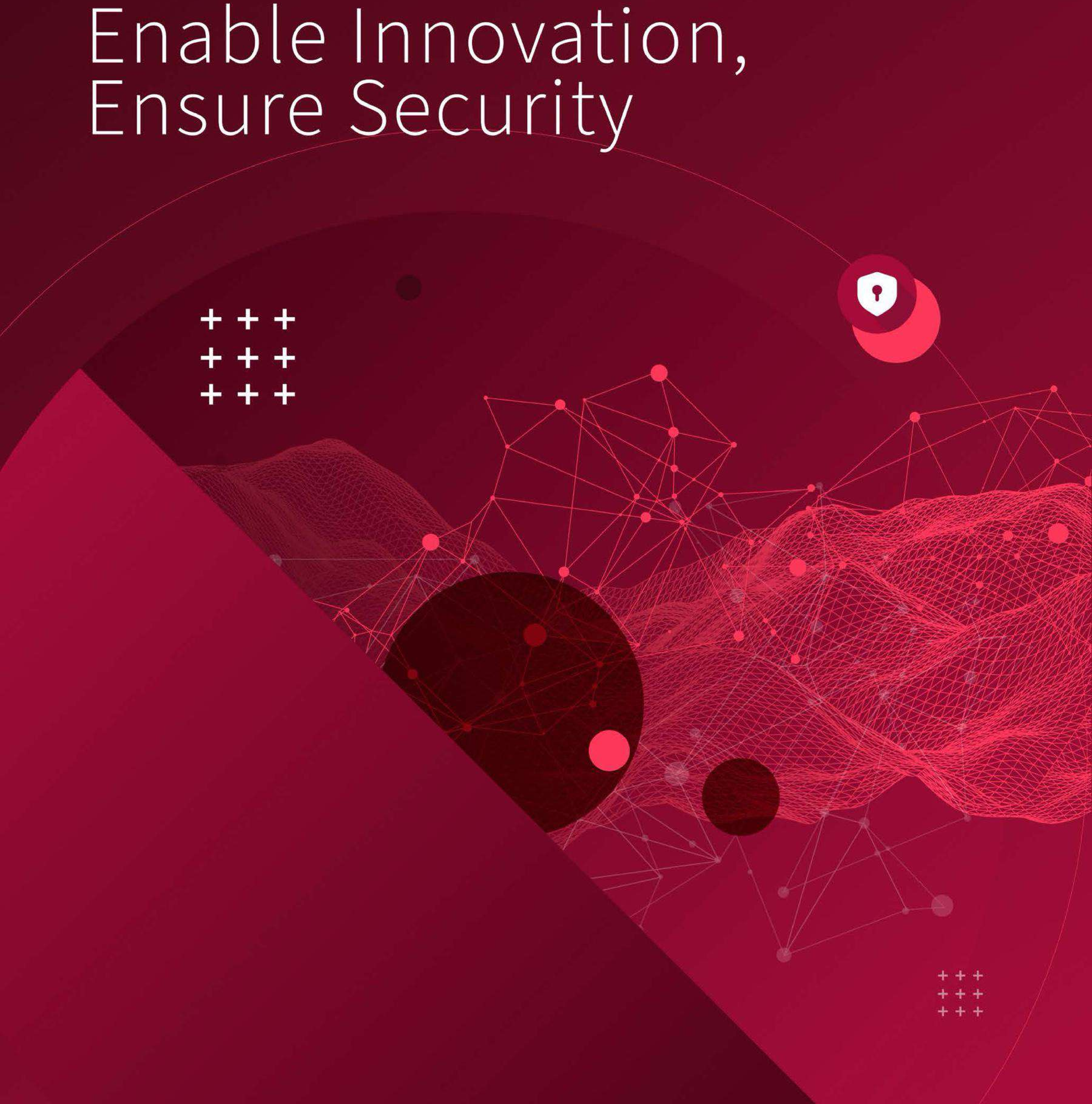
LastPass

The Complete Guide to AI Access Governance: Enable Innovation, Ensure Security



Why banning AI isn't the answer:
AI transformation is a problem of access governance

Someone just dumped 200 customer purchase histories into ChatGPT to get "personalized campaign ideas." **Want to guess where that data is now?**

Here's what most people miss:
Workforce AI isn't a tech problem.
It's an access governance problem.

Right now, your team is using AI tools, but there's no visibility, no oversight, and no foundation to make it sustainable.

You're stuck in an impossible position: Ban AI and watch your competitors sprint past you. Or give it free rein and risk a breach that could end your business.

When you ban AI at your company, here's what actually happens: Your employees use it anyway.

Workforce AI bans just drive AI use underground, creating Shadow AI: **40% admit they routinely flout company policy.** [3]

And the dangers are real. Especially when most people don't realize how much AI has expanded the attack surface.

78% of employees already use unapproved AI tools. [1]

Nearly 60% of US workers are using unapproved tools for daily tasks. [2]

Despite these risks, **only 47%** of organizations report having security controls in place for AI use. [4]

> “As we see the traditional technology world adopt certain technologies, the bad guys do too.”
>
> — Alex Cox, *Director, AI Transformation, LastPass*

Take Moltbot (now OpenClaw), for example, an AI agent that can do everything from clearing your inbox to checking you in for flights.

If members of your team set up OpenClaw on unmonitored endpoints, OpenClaw can use whatever passwords, API keys, and OAuth tokens they connect to it. And if endpoints with OpenClaw instances are exposed, so are the corresponding credentials.

Attackers can then use those credentials to access your business systems (CRM, email, payments, SaaS), move laterally, and potentially deploy ransomware.

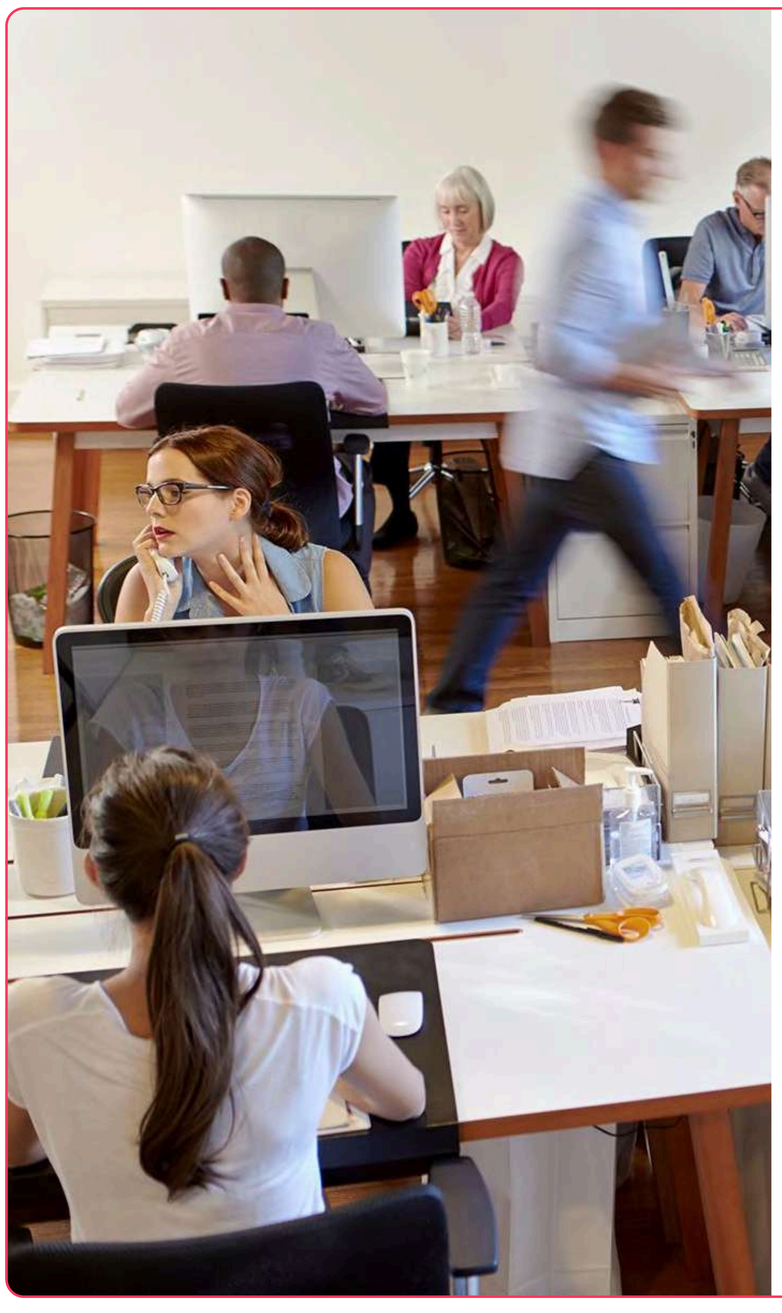
So, what can you do?
Turn your workforce AI from a security risk into a competitive advantage.

“At the end of the day, AI is a major opportunity for everyone. Every company is now having the mandates from their boards to kind of get some of the efficiencies, not only in terms of how they approach their product capabilities, how they go to market, but also internal productivity of employees, right, and those are kind of all of the opportunities that everyone is seeking and those are very valid opportunities.”

— **Mario Platt,** *VP, CISO, LastPass*

The security-first AI framework:
Five ways to empower your team to use AI safely

1 | Get full visibility into your team's SaaS and AI footprint with a SaaS monitoring tool



You can't manage what you can't see.

AI agents like OpenClaw execute locally on employee workstations or personal devices.

Your employees interact with OpenClaw inside messaging apps like Telegram and WhatsApp.

Monitoring logins to OpenClaw-integrated apps (WhatsApp, Telegram, Slack, etc.) alerts IT when employees access these apps with company credentials.

Then, your IT team can manually check for sensitive shares (like company data, credentials, API keys) in these apps, since OpenClaw has broad access to full chat histories, private messages, and shared files.

Why you should do this: If any OpenClaw instance is compromised, it could let attackers see every confidential piece of data in these messaging apps, which increases the potential for data exfiltration.

What you need: Complete visibility into every SaaS tool or messaging app your employees are accessing through their browsers with their corporate emails. And you need these tools automatically detected and continuously monitored.

The average org has
269 shadow AI tools per 1,000 employees. [5]

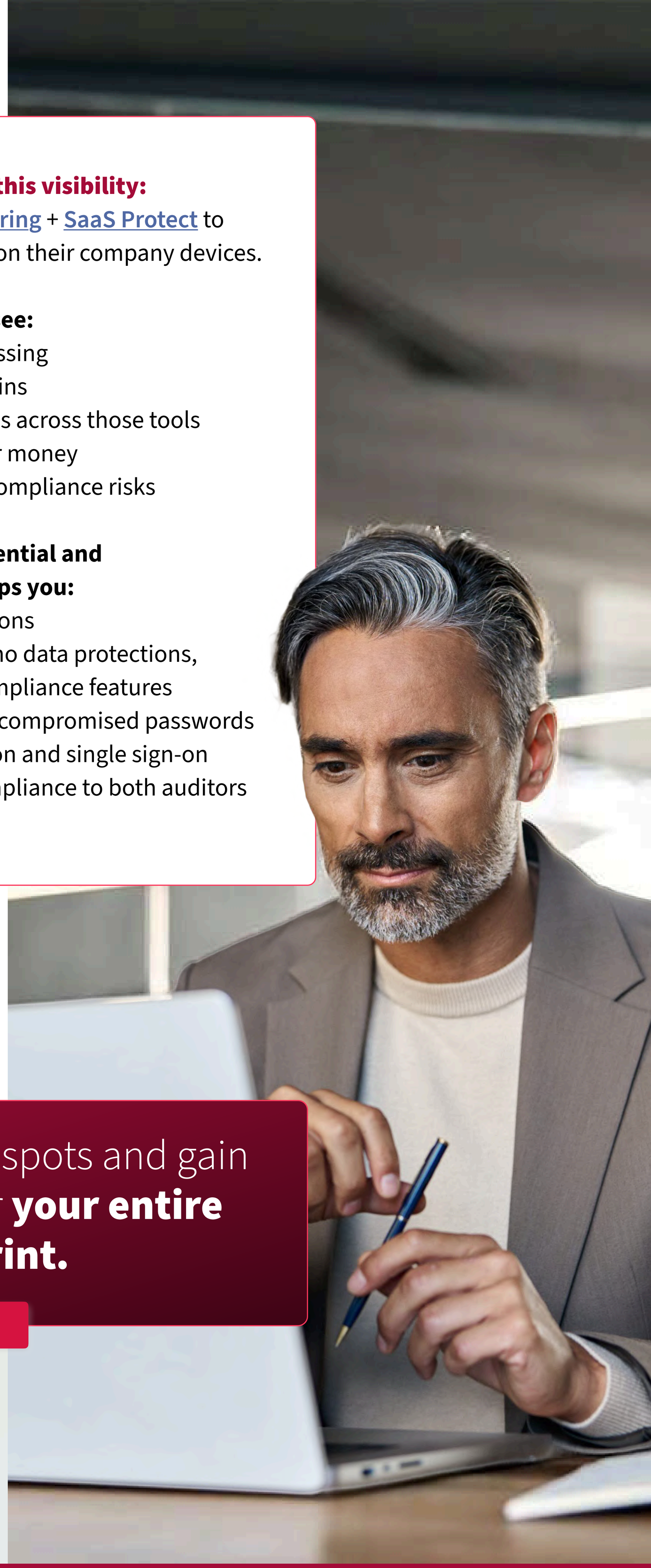
How LastPass Business Max gets you this visibility:
With Business Max, you get SaaS Monitoring + SaaS Protect to discover every app your employees use on their company devices.

What a SaaS monitoring tool lets you see:

- Which AI service employees are accessing
- Which messaging apps have new logins
- Weak, breached, or reused passwords across those tools
- Duplicate subscriptions wasting your money
- Shadow AI and Shadow IT creating compliance risks

How a SaaS Monitoring tool with credential and authentication-level management helps you:

- See and cancel redundant subscriptions
- Catch logins to risky apps that have no data protections, privacy commitments, or built-in compliance features
- Enforce password resets for weak or compromised passwords along with multi-factor authentication and single sign-on
- Get audit-ready reports to prove compliance to both auditors and customers



Eliminate security blindspots and gain complete control over **your entire SaaS footprint.**

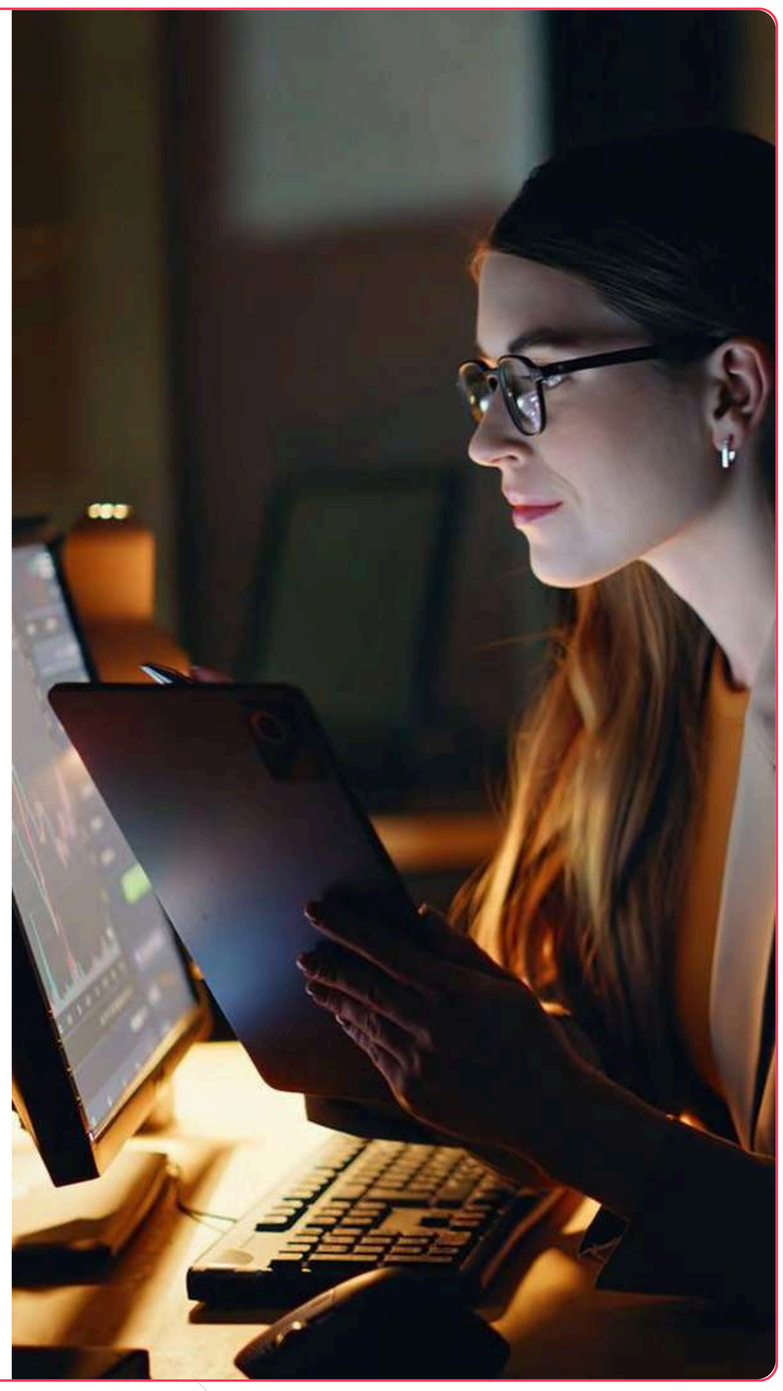
Try for free

2 | Implement an AI corporate policy or acceptable use policy

Every organization needs a foundational AI corporate policy, and the good news is that it doesn't have to be complicated.

According to the RAI (Responsible AI) Institute, a good AI acceptable use policy should include these **five elements:**

1. Clearly defined list of approved and unapproved AI tools.
2. Transparent rules for data sharing – what employees can and can't enter into AI.
3. Least privilege permissions for AI – only the minimum access needed to complete tasks.
4. Risk management through continuous monitoring and oversight.
5. Close alignment with trusted frameworks like the NIST AI Risk Management Framework (NIST AI RMF), EU AI Act, and ISO/IEC 42001.



The RAI Institute has provided a **free AI corporate policy template** you can use for usage governance.

Get your free AI security policy template

3 | Create guardrails for security, not roadblocks

Make sure to only deploy enterprise AI tools that come with **data protection agreements.**

Free versions might use your data for training, but enterprise versions come with data retention & residency policies, SOC/GDPR/HIPAA compliance, and Business Associate Agreements that protect you.

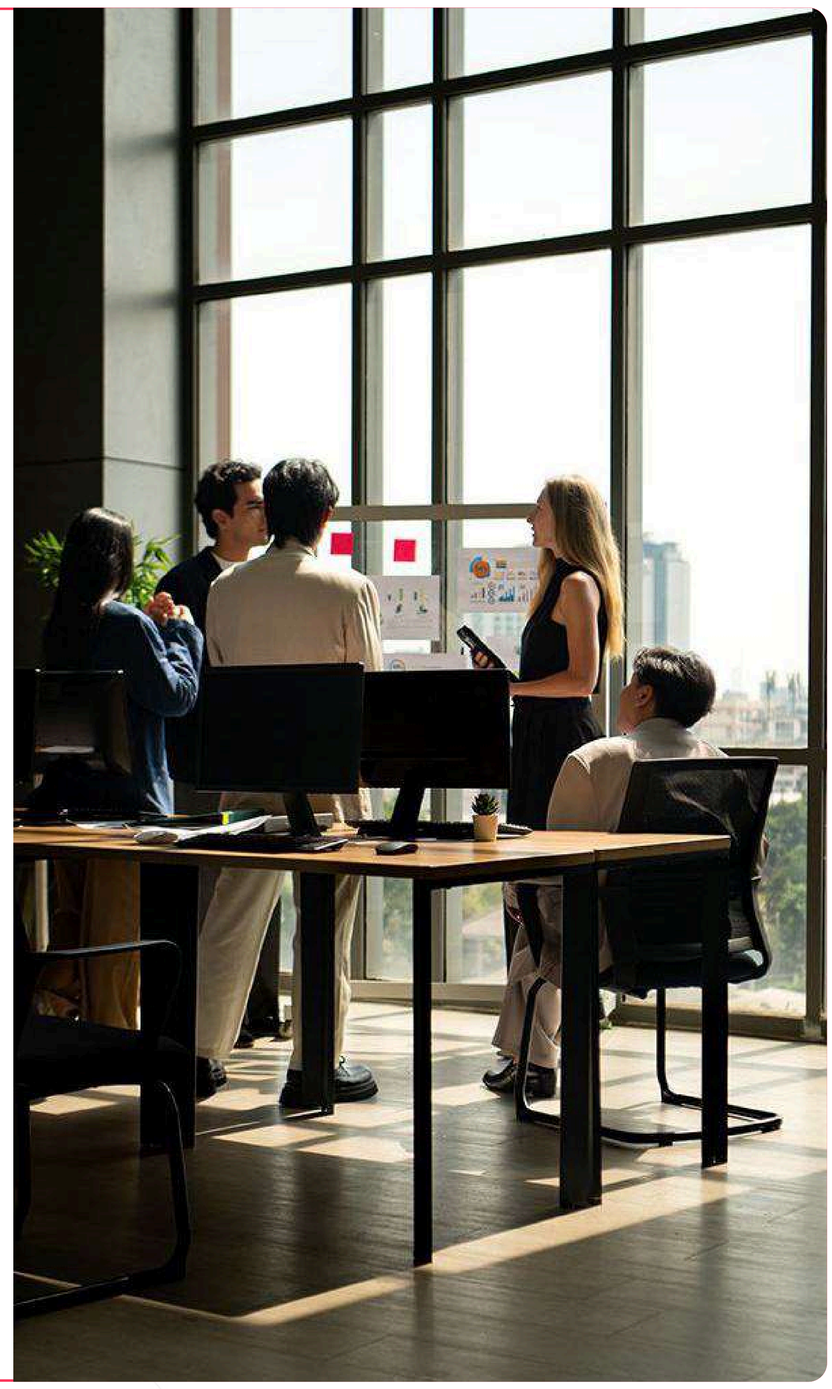
See how free versions of these tools compare with their enterprise versions.

AI CHAT PLATFORM	FREE	ENTERPRISE
ChatGPT	• Conversations used for training unless disabled • No data protection agreements • No full admin or RBAC controls	• No training on business data • Compliant with SOC 2 Type 2, GDPR, CCPA • Full RBAC and data residency protections
Claude	• Conversations used for training unless disabled • No compliance protections	• Enterprise data not used for training • Compliant with SOC 2 Type 2, ISO 27001, HIPAA, NIST 800-171 • Full RBAC, compliance API, SCIM, and data retention
Microsoft Copilot	• Can opt-out of conversations being used for model training • Conversations saved for 18 months by default • No compliance guarantees	Copilot for Microsoft 365 offers GDPR/ HIPAA/ ISO 27001/ EU Data Boundary compliance, data residency protections, admin controls, no data retention
Perplexity	• No compliance certifications; no data protection agreements • Training on data unless disabled in account settings	SOC 2 Type 2 certified and offers GDPR & HIPAA compliance, no training on enterprise data, PCI compliance for payment security
Gemini	• Gemini Apps activity older than 18 months is auto-deleted • Option to disable Gemini Apps activity entirely	Built-in security & access governance for small teams

4 | Support your AI policy with clear user training

Make it infinitely easier for your team to follow your workforce AI usage policy with a stoplight system:

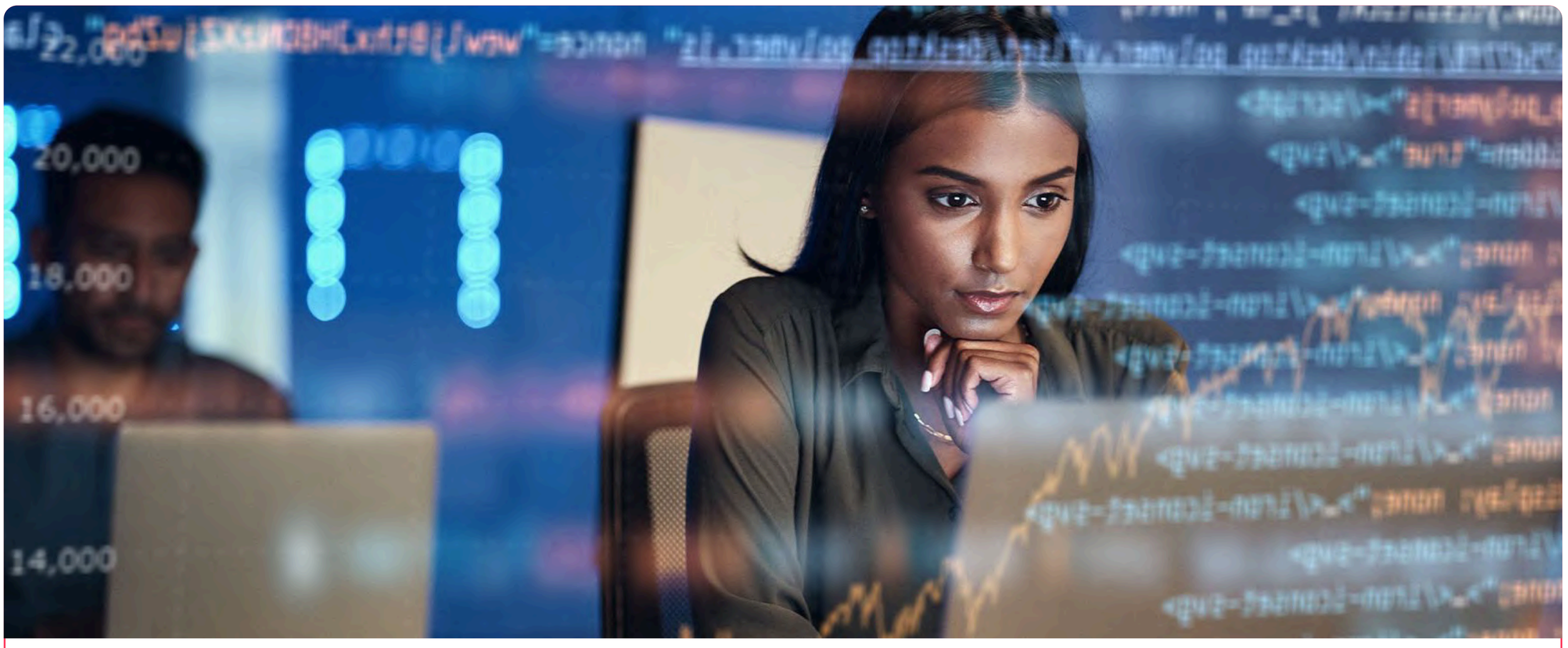
- **Red:** This is data that never enters AI under any circumstances, such as SSNs, API keys, financial info, passwords, legal documents, proprietary formulas, or anything regulated
- **Yellow:** This is data that can only be entered into enterprise-secure workforce AI tools, such as customer names, date of birth, race, gender, customer segments, customer lifetime value
- **Green:** This is data that can be entered into AI without restriction, such as public research and general knowledge queries



75% share company info with AI.

This includes employee data (35%), customer data (32%), legal, financial, and other internal info (21%), proprietary code (20%). [5]

5 | Make security the easy choice



Remove friction from doing the right thing. Here's how:

- **Provide enterprise-grade tools while deploying smart access policies.** For example, Microsoft Copilot offers standalone add-ons and bundled plans. Pair this with context-aware controls via LastPass SaaS Protect and training on security best practices, instead of outright bans on AI.
- **Create a Slack channel where team members share AI outputs before using them externally.** This sets up peer review to catch hallucinations and prevent sensitive data from being exposed.
- **Create templates and prompts that work within your security boundaries and put them in a shared library.** Pre-built prompts enforce safe practices and limits scope to approved tools only.
- **Celebrate wins when someone uses AI effectively within your security framework.** This encourages everyone else to follow the approved path.

Next steps to take **right now**

Your complete workforce AI security framework might take weeks to perfect, but you can **begin eliminating your biggest risks with three actions:**

1 Pick one enterprise AI tool to approve and fund.

Then send a company-wide message: “We’re embracing AI; here’s the approved tool and here’s why you can’t use free versions anymore.”

2 Download the RAI Institute’s free AI security policy template and fill in your approved tools list.

You’ll go from a “no workforce AI policy” to a concrete policy you’re working on.

3 Set up LastPass Business Max.

Check the SaaS Monitoring dashboard in 48 hours to see which AI platforms, messaging apps, and duplicate subscriptions are draining your budget and creating security holes.

When it comes to workforce AI, make security the easy choice by providing paid tools proactively, creating ready-to-go templates, and celebrating wins publicly.

LastPass can discover every AI app employees are using so admins can block risky apps immediately, identify redundant apps, and enforce access policies to harden security, reduce waste, and stay compliant.

AI isn’t a tech problem. It’s a usage governance problem.

Get started with LastPass Business Max today

Sources

[1] WalkMe: Employees left behind workplace AI boom, new WalkMe survey finds

[2], [5] CyberNews: Shadow AI soaring: 59% of employees hide AI use from their bosses

[3] Fast Company: Why businesses banning AI inevitably lose

[4] Cyber Pulse: An AI Security Report

[5] Reco 2025 State of Shadow AI Report

Silicon Angle: Expanding cyberattack surface from AI agents, models and rogue nations raises new alarms

Endgadget: What is Moltbook, the social network for AI agents?

Infosecurity Magazine: Researchers find 40,000+ exposed OpenClaw instances

AI policy template: Build your foundational organizational AI policy

ESET: Is ChatGPT safe? 2026 guide

NC University: Data management framework