Empower your workforce to adopt AI safely with Nudge Security

Continuously discover all GenAI apps—even the new, obscure ones—and activate guardrails for safe, compliant adoption.

When shown the art of the possible, employees will experiment with AI to make their lives easier—and they don't always tell you about it. There are well-known chatbots like ChatGPT, created by OpenAI, and Claude, by Anthropic. But there are plenty of obscure GenAI apps that simply add an audience-specific UX layer around these providers, with or without any security program in place. In fact, we've observed over 700 unique AI apps across our customer environments. All your workforce needs is an email address and password to start using them.

Furthermore, the 2024 Cisco Data Privacy Benchmark Study found that nearly half of GenAI users admitted to entering non-public company information into GenAI tools, and 62% had entered information about internal processes. How do your employees know what's considered safe, acceptable use of GenAI?

GenAI has entered your employees' workflow. What can you do about it?

You could simply block access to as many GenAI tools as you can list. However, that's a never-ending cycle that drives usage into the shadows, contradicting the critical element you need to actually deal with the risk—visibility. Besides, 2 out of 3 workers would simply find a workaround.

Let's not forget that your SaaS apps want to realize value and revenue from GenAI too. You'll need to know when GenAI gets added to their software supply chain or data subprocessor list so you can ask about how they'll be using your data. Just among our customer environments, 25% of the most popular SaaS apps observed contain a third-party AI service in their supply chain or data subprocessor list, with OpenAI and Anthropic being most common.

When network monitoring solutions and manual cataloging approaches can't keep up with the pace that GenAI tools are created and used by your employees, and analyzing core app integrations only shows a fraction of your GenAI risk, **how do you govern GenAI usage at scale?**

Key Challenges

Incomplete view of what GenAI apps the workforce uses

Missing GenAI risk in the SaaS supply chain

Inflexible controls slowing productivity

Nudge benefits

Discover all GenAI apps used by your workforce, including obscure, newly launched apps

Notice trends like who is most likely to experiment, which departments are adopting GenAI, how many people use specific GenAI tools, and more

Identify GenAI apps used in the supply chain of your third-party SaaS ecosystem

Evaluate risk and make better, quicker decisions with security context like data locality, security program maturity, related data breaches, and risky OAuth scopes

Activate pre-built playbooks to nudge users—at scale—toward safe, compliant GenAI usage

nudgesecurity.com

SOC 2 Compliant

Detect all GenAI and AI-powered apps used by the workforce—in minutes

Our patented discovery method delivers an inventory of all SaaS apps ever used—including GenAI—in minutes from installation. No agents, proxies, or plugins are necessary—all we need is read-only API access to Microsoft 365 or Google Workspace. Then we can continuously monitor for those machine-generated emails sent for account creation, password resets, and invoices.

Know which third-party vendors may share your data with AI

Stay on top of which SaaS vendors are using AI in their software supply chain so you or your team can investigate how they are using your data.

And if any of your third- or fourth-party vendors get breached, quickly view which apps and accounts in your organization could be impacted.

How it works

Connect

to Google Workspaces or Microsoft O365 APIs. That's it.

Discover

all cloud and SaaS accounts, historically and continuously.

Analyze

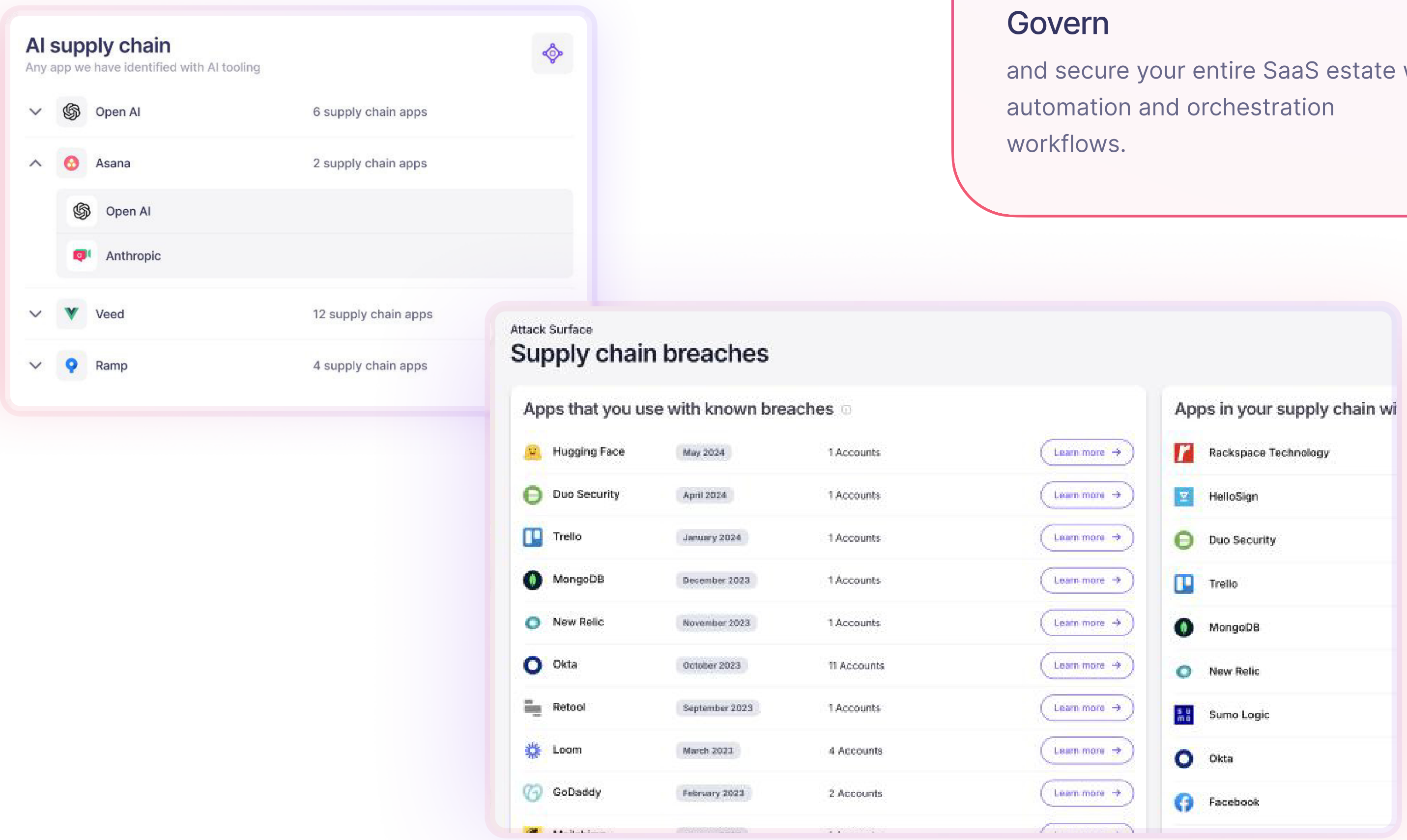
your SaaS attack surface, app-to-app risks, SSO & MFA adoption, and more..

Nudge

your employees towards better security behaviors with automated, real-time engagement.

Govern

and secure your entire SaaS estate with automation and orchestration workflows.



AI supply chain

Any app we have identified with AI tooling

Open AI	6 supply chain apps
Asana	2 supply chain apps
Open AI	
Anthropic	
Veed	12 supply chain apps
Ramp	4 supply chain apps

Attack Surface

Supply chain breaches

Apps that you use with known breaches

Hugging Face	May 2024	1 Accounts	Learn more →
Duo Security	April 2024	1 Accounts	Learn more →
Trello	January 2024	1 Accounts	Learn more →
MongoDB	December 2023	1 Accounts	Learn more →
New Relic	November 2023	1 Accounts	Learn more →
Okta	October 2023	11 Accounts	Learn more →
Retool	September 2023	1 Accounts	Learn more →
Loom	March 2023	4 Accounts	Learn more →
GoDaddy	February 2023	2 Accounts	Learn more →

Apps in your supply chain wi

- Rackspace Technology
- HelloSign
- Duo Security
- Trello
- MongoDB
- New Relic
- Sumo Logic
- Okta
- Facebook

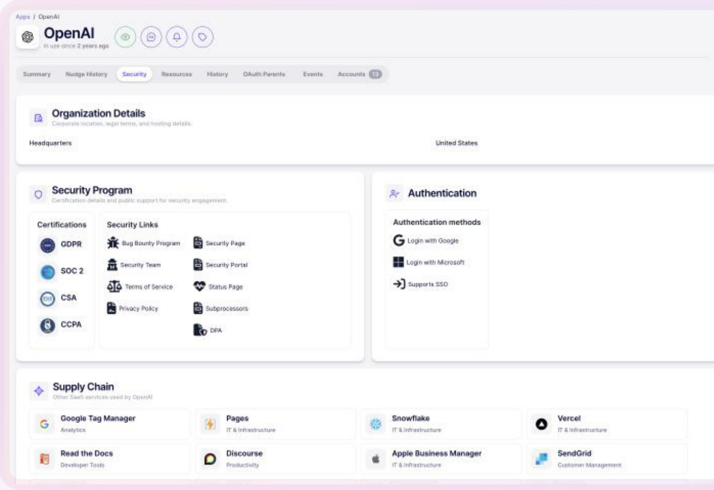
Let context drive controls

Security context at your fingertips

Make risk-based decisions quickly with information like:

- data locality
- security program maturity
- authentication methods
- reported data breaches
- software supply chain

Within these profiles, you can also dig into risky OAuth grants and their scopes, conduct user access reviews, and activate playbooks to nudge human behavior toward safe, compliant use of GenAI.



OpenAI

In use since 2 years ago

Organization Details

Corporate location, legal terms, and hosting details.

Headquarters: United States

Security Program

Certification details and public support for security engagement.

Certifications: GDPR, SOC 2, CSA, CCPA

Security Links: Bug Bounty Program, Security Page, Security Team, Security Portal, Terms of Service, Status Page, Privacy Policy, Subprocessors, DPA

Authentication

Authentication methods: Login with Google, Login with Microsoft, Supports SSO

Supply Chain

Other SaaS services used by OpenAI

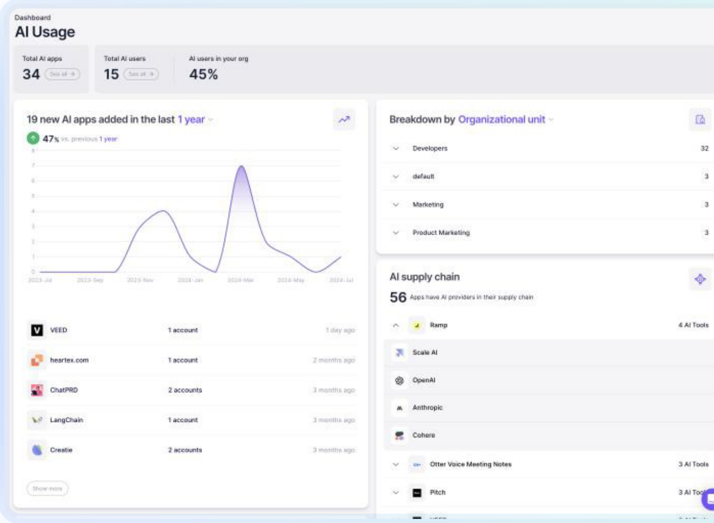
Google Tag Manager	Analytics
Pages	IT & Infrastructure
Snowflake	IT & Infrastructure
Vercel	IT & Infrastructure
Read the Docs	Developer Tools
Discourse	Productivity
Apple Business Manager	IT & Infrastructure
SendGrid	Customer Management

Business context to right-size action

Drill into trends by department, users, and spend, to understand:

- Who is most likely to experiment
- How popular is a GenAI app across your company
- What business outcomes are they trying to achieve

Use these data points to right-size your approach to govern AI instead of jumping to extreme controls.



AI Usage

Total AI apps: 34

Total AI users: 15

AI users in your org: 45%

19 new AI apps added in the last 1 year

47% vs. previous 1 year

VEED	1 account	1 day ago
heartex.com	1 account	2 months ago
ChatPRD	2 accounts	3 months ago
LangChain	1 account	3 months ago
Creatie	2 accounts	3 months ago

Breakdown by Organizational unit

Developers	32
default	3
Marketing	3
Product Marketing	3

AI supply chain

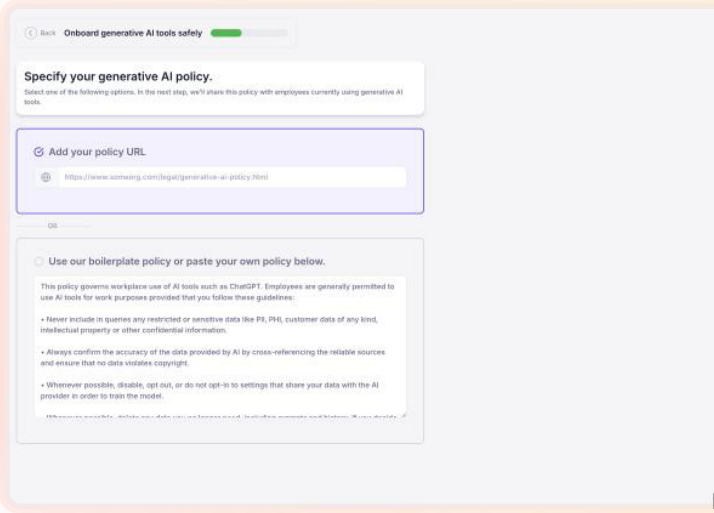
56 Apps have AI providers in their supply chain

Ramp	4 AI Tools
Scale AI	
OpenAI	
Anthropic	
Cohere	
Otter Voice Meeting Notes	3 AI Tools
Pitch	3 AI Too

Use guardrails, not gatekeepers

Nudge Security is built on the belief that employees perform best when given autonomy to deliver business outcomes, supplemented with just-in-time guidance or "nudges." Automatically nudge employees to:

- review the acceptable usage AI policy
- share business context for using the GenAI app
- enable MFA on AI accounts
- remove abandoned or unapproved AI accounts
- onboard AI apps into Okta
- use a different recommended app



Onboard generative AI tools safely

Specify your generative AI policy.

Select one of the following options. In the next step, we'll share this policy with employees currently using generative AI tools.

Add your policy URL

https://www.someorg.com/legal/generative-ai-policy.html

○ Use our boilerplate policy or paste your own policy below.

This policy governs workplace use of AI tools such as ChatGPT. Employees are generally permitted to use AI tools for work purposes provided that you follow these guidelines:

• Never include in queries any restricted or sensitive data like PII, PHI, customer data of any kind, intellectual property or other confidential information.

• Always confirm the accuracy of the data provided by AI by cross-referencing the reliable sources and ensure that no data violates copyright.

• Whenever possible, disable, opt out, or do not opt-in to settings that share your data with the AI provider in order to train the model.

• Whenever possible, delete any data you no longer need, including prompts and history. If you decide

Customers trust Nudge Security to govern GenAI

> “When I see an AI tool that I don't want them to be using, I use Nudge to tell them, ‘hey, we have an alternative, please use it.’ If they're not using it, I just revoke it, and if it's unsafe, I just block it out. Without Nudge, I probably wouldn’t even know about it. There's like 10 new AI services that pop up every single day, so it's almost impossible to keep up.”
>
> Leo Chui, IT Manager at GLAAD

See what GenAI tools are in your SaaS ecosystem today.

Zero commitment. No credit card necessary. Start your 14-day trial now.

nudgesecurity.com