2025 State of Shadow AI Report

Table of Contents

Executive Summary: The Shadow AI Era Is Here

Security leaders face an unprecedented reality: Shadow AI has infiltrated nearly every corner of the enterprise, creating massive blind spots that traditional security approaches cannot address.
Our in-depth analysis of shadow AI usage across our customer base reveals five critical findings that demand immediate action.

1. **The threat is real and it's massive.** We identified the 10 riskiest AI applications currently proliferating across our customer base, with security scores so low they should alarm any CISO. **Three applications (Jivrus Technologies, Happytalk, and Stability AI) received failing grades meaning that they lack fundamental security controls like RBAC, MFA, and audit logging.** These aren't just any tools, they're processing corporate data daily.

2. **Mass adoption doesn't equal enterprise readiness.** The most widely adopted AI tools aren't the most secure. CreativeX and Otter.ai boast thousands of users despite security scores that should disqualify them from enterprise use. **Organizations are choosing AI tools like they choose consumer apps: based on features and convenience, not security.**

3. **The OpenAI monopoly.** OpenAI commands 53% of all shadow AI usage across the organizations we assessed, processing data from over 10,000 enterprise users in our study. **This unprecedented concentration means half of all AI-related risk flows through a single platform.** Any security incident, policy change, or service disruption at OpenAI could simultaneously impact the majority of enterprise AI workflows.

4. **Shadow AI runs deeper than most realize.** These tools do not disappear after the testing and experimentation ends. **For example, some apps run unsanctioned for over 400 days on average.** In our study, we found CreativeX and System.com to have the longest standing access on average. Once embedded in workflows for months, these applications become nearly impossible to remove without disrupting business operations and upsetting its users. Every day they persist, the security debt compounds.

5. **Smaller organizations face disproportionate risk.** The smaller the organization, the bigger the shadow AI problem. Companies with 11-50 employees show the highest risk concentration: **27% of their workforce uses unsanctioned AI tools.** These organizations face the perfect storm: maximum AI adoption with minimum security resources to manage it.

The bottom line:

Shadow AI is here, running loose across enterprises and invisible to traditional security tools. Smart security teams are implementing shadow AI discovery and governance solutions to turn this challenge into competitive advantage. The path forward is clear: AI adoption won't slow down because of security concerns. Security teams must get ahead of shadow AI now or face mounting risks and compliance challenges later.

Methodology

Reco identified high-risk shadow AI applications through detailed analysis of anonymized, real-world usage data collected across its customer base. This comprehensive assessment included:

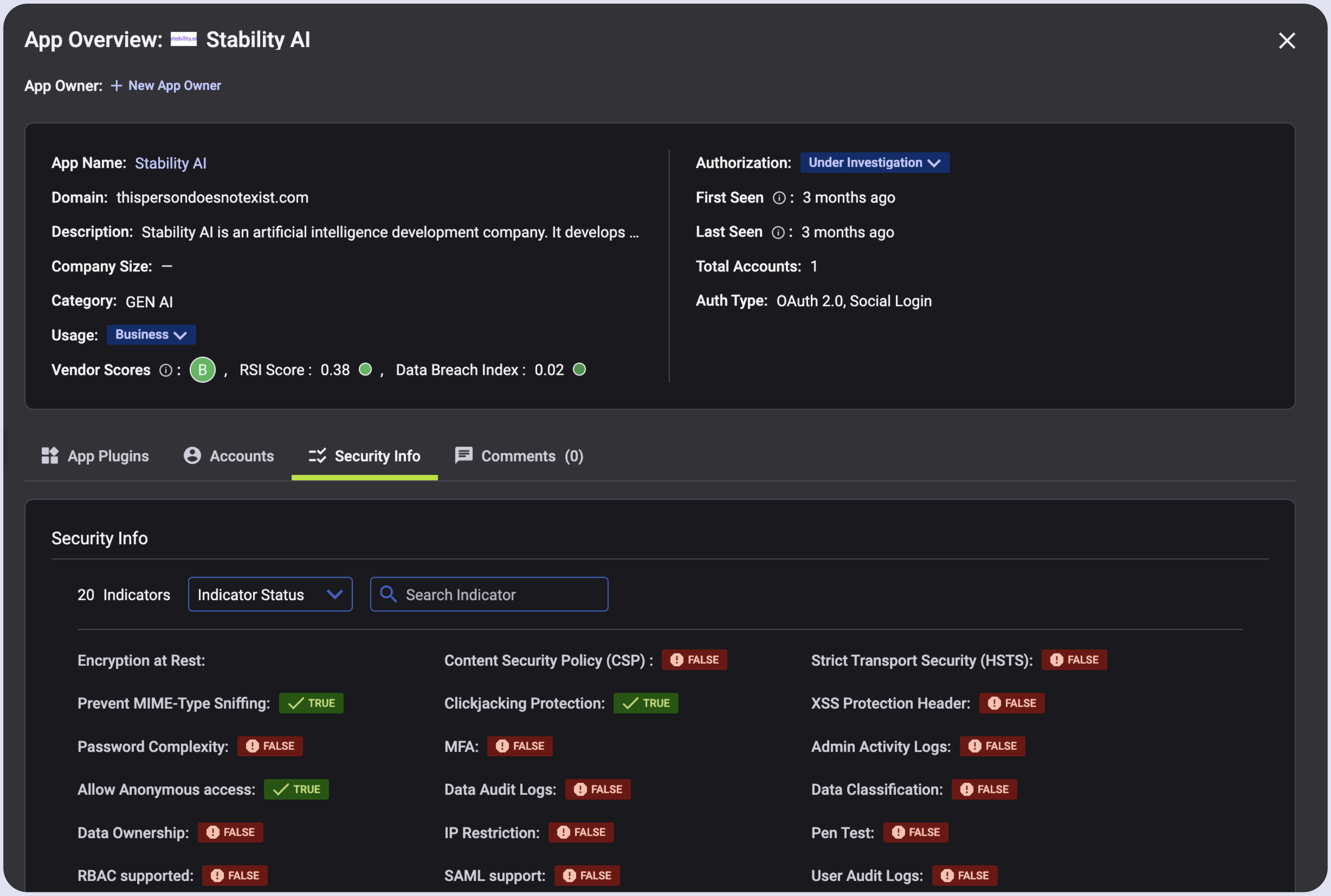
1. **Internal telemetry and SaaS audit logs:** Identifying unsanctioned AI apps actively used by employees.

2. **Evaluation across multiple security-relevant factors:**
   - **Total user count:** Number of employees actively using each AI app.
   - **Usage duration and frequency:** Level and pattern of employee engagement with the app.
   - **Registration type:** Whether employees registered using corporate credentials or personal email accounts.
   - **Authorization visibility:** Assessment of whether apps integrated transparently via standard corporate channels or operated covertly.
   - **Security policy compliance:** Alignment with essential enterprise security controls, such as SSO, data retention policies, and encryption standards.

3. **Correlation of policy violations and risk signals:**
   - Data Loss Prevention (DLP) and shadow AI discovery alerts
   - Abnormal data flows or other suspicious activities linked to shadow AI app usage.

4. **Detailed Security Indicator Assessment:**
   - Specific security indicators assessed included Encryption at Rest, Password Complexity, Auto-Renewal Subscription status, SSO Support, User Geo-Location Control, Content Security Policy (CSP), Audit Logs, Valid Certificate, Transport Security (HTTPS), 2FA Provisioning, Data Classification, Encryption Key Rotation, User Audit Logs, and Data Retention Policies.
   - Each indicator was classified with clear statuses (Pass, Warn, or Fail), contributing to a composite risk score.

Here’s an example of how Reco assesses the risks of an AI app across 20 indicators:



App Overview: Stability AI

App Owner: + New App Owner

App Name: Stability AI
Domain: thispersondoesnotexist.com
Description: Stability AI is an artificial intelligence development company. It develops ...
Company Size: —
Category: GEN AI
Usage: Business
Vendor Scores ⓘ : B , RSI Score : 0.38 ● , Data Breach Index : 0.02 ●

Authorization: Under Investigation
First Seen ⓘ : 3 months ago
Last Seen ⓘ : 3 months ago
Total Accounts: 1
Auth Type: OAuth 2.0, Social Login

Security Info

20 Indicators

Encryption at Rest:		Content Security Policy (CSP) :	FALSE	Strict Transport Security (HSTS):	FALSE
Prevent MIME-Type Sniffing:	✓ TRUE	Clickjacking Protection:	✓ TRUE	XSS Protection Header:	FALSE
Password Complexity:	FALSE	MFA:	FALSE	Admin Activity Logs:	FALSE
Allow Anonymous access:	✓ TRUE	Data Audit Logs:	FALSE	Data Classification:	FALSE
Data Ownership:	FALSE	IP Restriction:	FALSE	Pen Test:	FALSE
RBAC supported:	FALSE	SAML support:	FALSE	User Audit Logs:	FALSE

By correlating these comprehensive indicators, Reco identified the shadow AI applications posing the greatest real-world risk. All findings reflect aggregated data across multiple Reco customers, ensuring an industry-wide perspective. The rigorous analysis approach ensured objective validation of each AI tool’s security posture, providing a reliable basis for assessing real-world risks rather than relying solely on vendor-provided assurances.

Glossary

Shadow AI

Unsanctioned artificial intelligence applications adopted by employees without explicit IT or security approval.

Generative AI (GenAI)

AI models capable of creating original content—text, images, or code—from minimal prompts.

AI Agent

Autonomous or semi-autonomous AI systems integrated directly into enterprise software platforms, automating tasks with extensive user privileges.

Model Context Protocol (MCP)

An emerging protocol enabling real-time integration between AI models and enterprise data sources or tools.

Prompt Injection

A technique embedding malicious instructions into AI prompts to trigger unintended actions or data disclosures.

OAuth Integrations

Protocol allowing third-party applications secure access to enterprise systems without directly handling login credentials.

Security Score

A numerical rating (typically 0-100) evaluating an application's security posture based on factors like encryption, authentication mechanisms, compliance certifications, and data handling practices.

Attack Surface

The sum of all possible entry points where unauthorized users could access a system or extract data, expanded significantly by unsanctioned AI tool adoption.

AI Sprawl

A security model that requires continuous verification of identity and context for every user and device attempting to access resources, regardless of their location, to minimize risks from both internal and external threats.

Setting the Stage: Why We Should All Be Paying Attention to Shadow AI

Picture this: Your marketing team just connected an AI tool to your CRM to automate campaigns. Your engineers are debugging proprietary code through the latest AI coding assistant. And your HR team? They're processing sensitive employee data through an AI platform with a security score that would fail any basic audit.

Welcome to 2025, where AI transforms how every team works. The productivity gains are real. The innovation is undeniable. But so are the risks. Shadow AI has created a new security landscape where every employee's tool choice can open doors that security teams didn't even know existed (aka unknown unknowns).

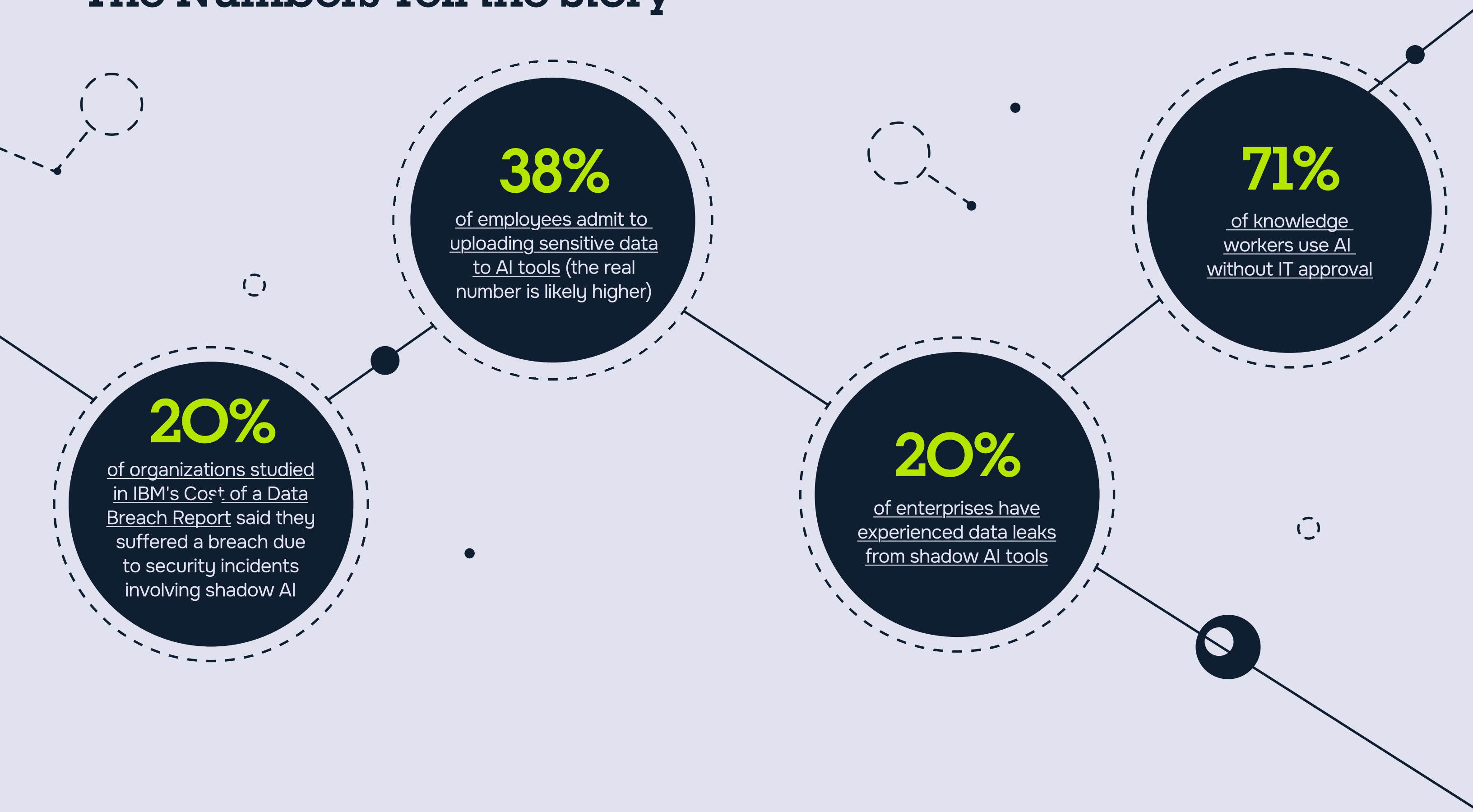
Why This Report Matters Now

This report is landing at the right time for a multitude of reasons. Enterprise AI adoption has introduced a lot of unknowns including shadow AI and how it impacts the traditional security paradigm. Hard data from **IBM's Cost of a Data Breach Report 2025** confirms the financial risk, as breaches among organizations with high levels of shadow AI cost organizations an extra $670,000USD.

Last month's **EchoLeak vulnerability** in Microsoft 365 Copilot (CVE-2025-32711, CVSS 9.3) delivered a wake-up call: even vetted, enterprise-grade AI tools can become attack vectors. Attackers could exfiltrate data from Outlook, SharePoint, and Teams with a single crafted email. Minimal user interaction required.

If that's what happens with AI that went through procurement, security review, and vendor assessments, imagine the vulnerabilities in the 100+ Shadow AI tools your employees are using right now.

The Numbers Tell the Story



20%

of organizations studied in IBM's Cost of a Data Breach Report said they suffered a breach due to security incidents involving shadow AI

38%

of employees admit to uploading sensitive data to AI tools (the real number is likely higher)

20%

of enterprises have experienced data leaks from shadow AI tools

71%

of knowledge workers use AI without IT approval

As you can see, these aren't hypothetical risks. Shadow AI has inherently changed an organization's attack surface and how we should all be approaching security and compliance.

Integration Risks

The risk multiplies with every new integration. ChatGPT's enterprise connectors to Box, HubSpot, and Google Drive are typically activated by individual users, not IT. Each connection expands the attack surface. Each integration creates new data flow paths that security teams can't monitor.

Emerging protocols like MCP allow AI models to interact directly with internal systems. While powerful for productivity, they create sophisticated attack vectors that traditional security tools weren't designed to detect.

A Critical Distinction

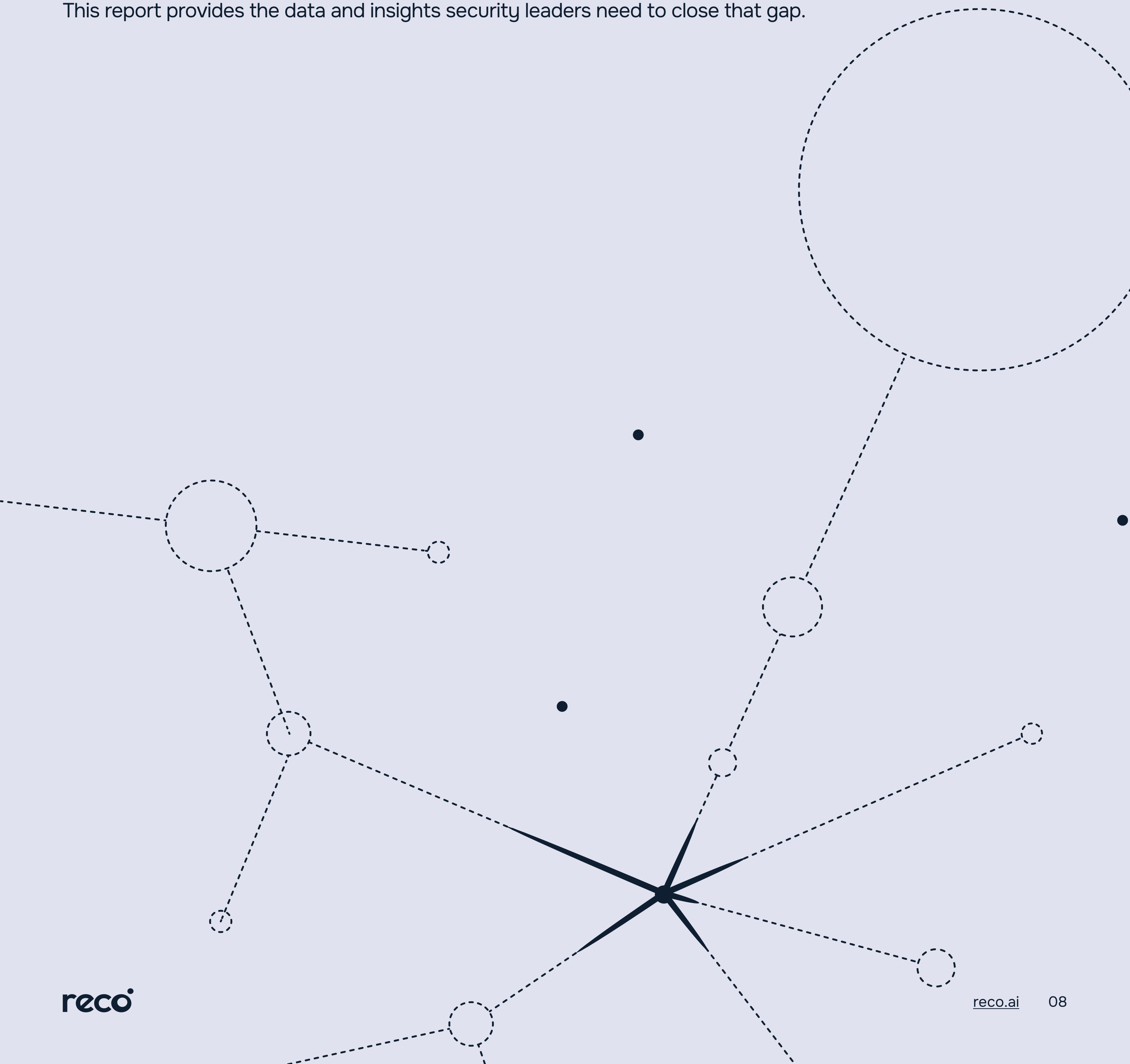
Not all shadow AI is inherently insecure. "Shadow" simply means it's being used without IT or security approval. Some unsanctioned tools may have better security than approved alternatives. The risk comes from the lack of visibility and governance, not the tools themselves.

The Speed of Adoption vs. The Pace of Security

AI tools are adopted in minutes but assessed in months, if they are ever discovered. By the time security teams complete a threat model, employees have already embedded these tools into critical workflows.

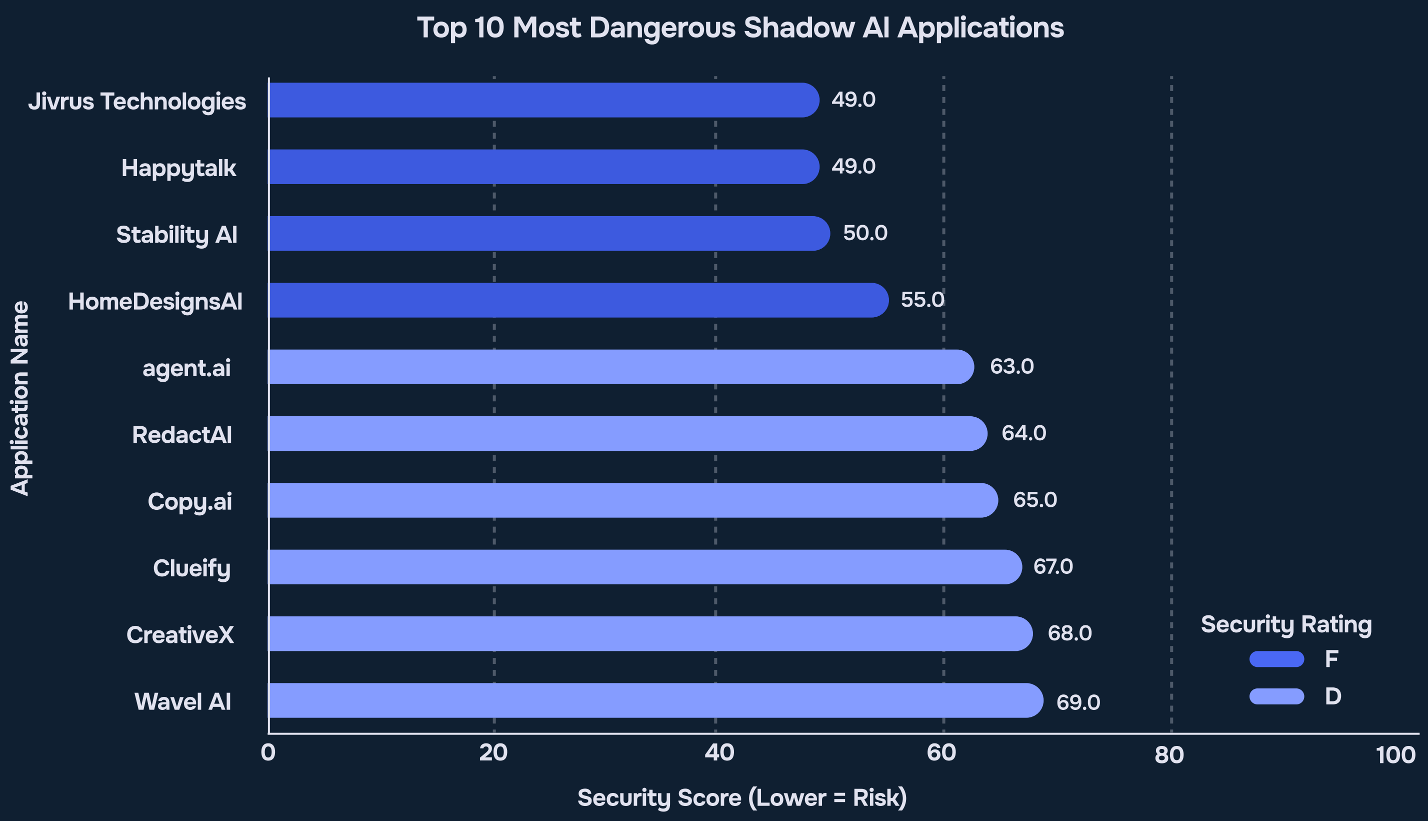
Getting shadow AI under control is not about stifling innovation. It's about preventing your intellectual property from becoming training data for the next public model, or your customer data from appearing in someone else's AI-generated content.

This report provides the data and insights security leaders need to close that gap.



10 Shadow AI Apps Putting Your Data at Risk

Our analysis across our customer base revealed the top ten riskiest shadow AI apps currently proliferating across enterprises. We've ranked these applications by comprehensive security scores, identifying active threats to organizational data and compliance posture. Our scoring methodology incorporates multiple risk indicators including encryption strength, authentication mechanisms, data handling practices, and regulatory compliance.



Severe security failures (F-rated): We identified three applications—Jivrus Technologies, Happytalk, and Stability AI—that received failing grades, exposing organizations to immediate risk. Our assessment found that these applications operate without a combination of these fundamental security controls:

- No encryption for data in transit or at rest
- Absence of multi-factor authentication or SSO integration
- Complete lack of audit logging capabilities
- No compliance certifications or security attestations

High-risk applications (D-rated): We discovered seven additional applications that pose significant threats with a D grade. HomeDesignsAI, agent.ai, RedactAI, Copy.ai, Clueify, CreativeX, and WaveAI each lacked a combination of the following security controls:

- Inconsistent or non-existent data retention policies
- Weak encryption implementations
- Inadequate access controls and user geo-location restrictions
- Limited visibility into data processing and storage locations

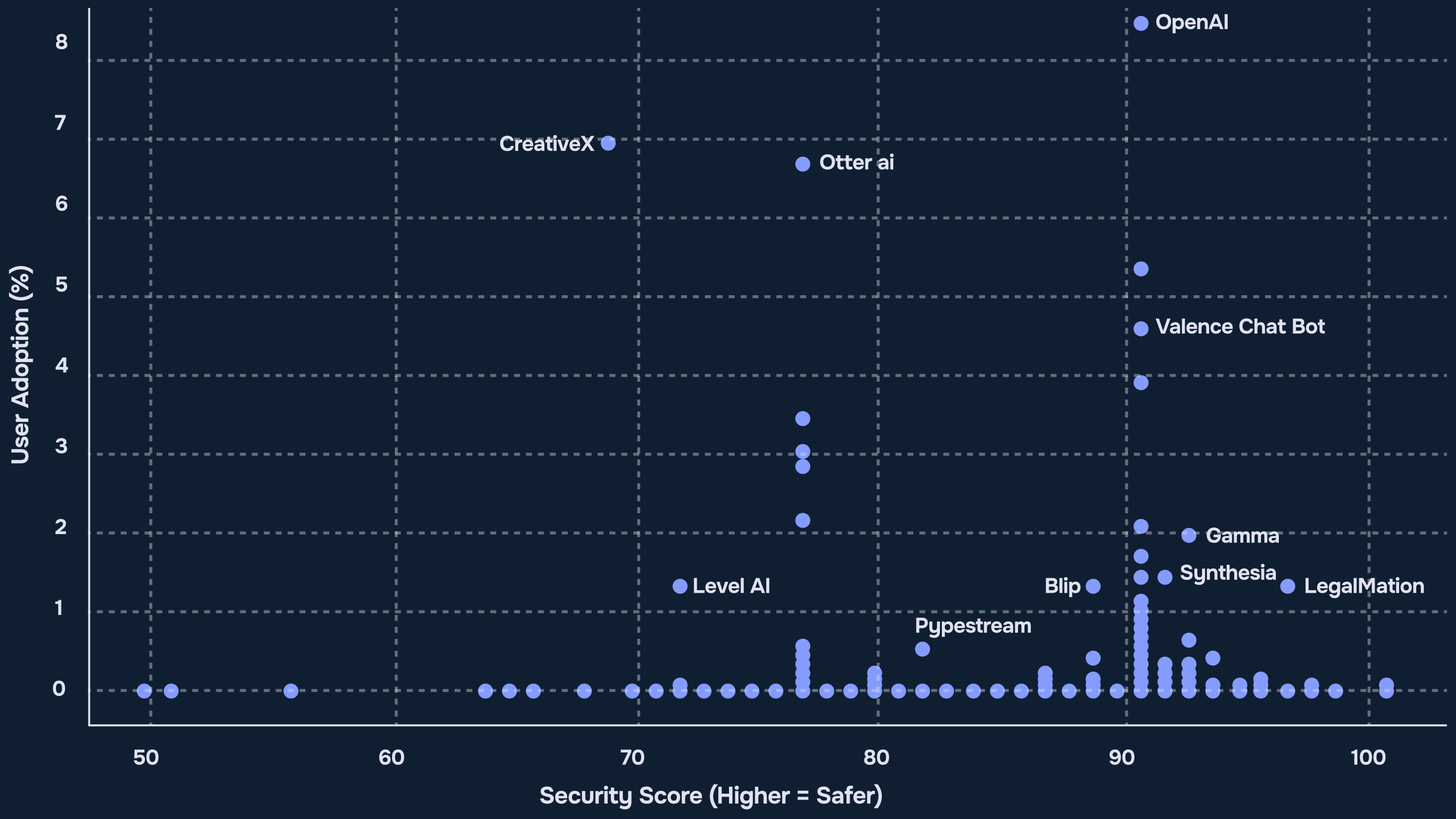
Organizations using these applications are potentially exposing sensitive data, intellectual property, and customer information to unauthorized access or breach.

Security teams discovering these applications in their environment should prioritize remediation efforts, beginning with the F-rated tools that pose the greatest risk. Having a shadow AI discovery tool is a great place to start!

The Popularity Trap: High Adoption Doesn't Mean High Security

Our analysis uncovered a dangerous misconception: the most popular AI tools aren't necessarily the most secure. By plotting user adoption rates against comprehensive security scores, we revealed a critical disconnect that puts organizations at risk. Popular doesn't mean protected, and our data proves it.

Correlation Between Security Score and User Adoption



The high-risk favorites: CreativeX and Otter.ai revealed a troubling pattern: sky-high adoption rates paired with security scores that should raise red flags. Our analysis shows that thousands of employees are actively using AI applications that lack fundamental security controls.

Hidden gems: Applications like LegalMation and Gamma demonstrated the opposite phenomenon: excellent security scores coupled with minimal adoption.

The security leaders: We did identify a select group of applications that got it right. OpenAI and Valence Chat Bot achieved the ideal combination: high adoption rates (8% and 4.5% respectively) paired with strong security scores above 85. These tools prove that widespread usage and robust security can coexist. Unfortunately, they represent the exception rather than the rule.

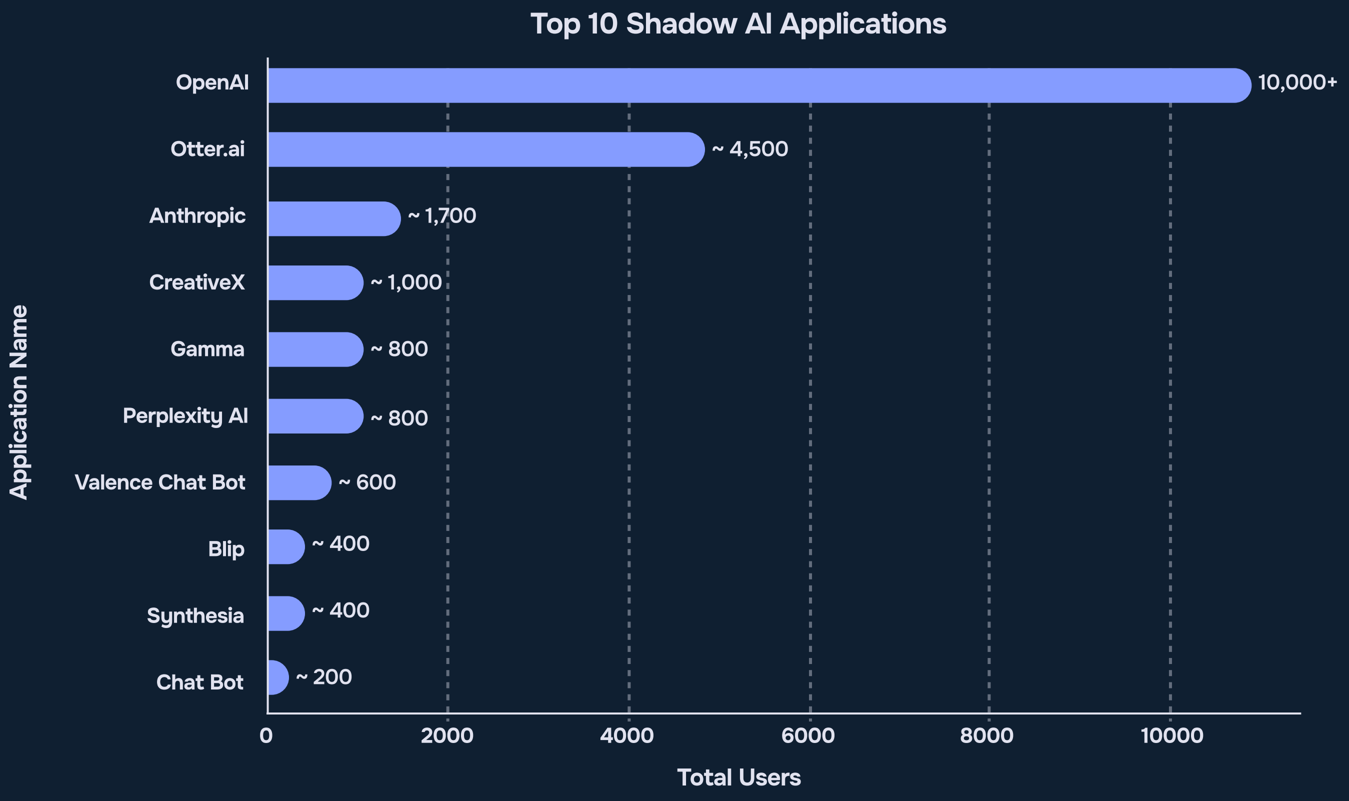
This mismatch between popularity and security reveals a critical blind spot in AI adoption strategies. Organizations are making tool selections based on features, user experience, or peer recommendations without conducting proper security evaluations.

When insecure applications achieve widespread adoption, they don't just create isolated risks; they become enterprise-wide vulnerabilities. Every additional user of a poorly secured AI tool expands the potential attack surface and data exposure risk.

Create and publish a pre-approved AI tools list. Most employees want to do the right thing, but they often choose tools based on features, not security. Guide them to vetted alternatives before they adopt insecure apps.

OpenAI Accounts for 53% of All Shadow AI Usage Across Enterprises

Our analysis reveals an unprecedented concentration of risk: OpenAI alone accounts for 53% of all shadow AI usage across enterprises, with over 10,000 users tracked in our study. This massive consolidation of AI activity into a single platform creates both operational dependencies and security implications that demand immediate attention.

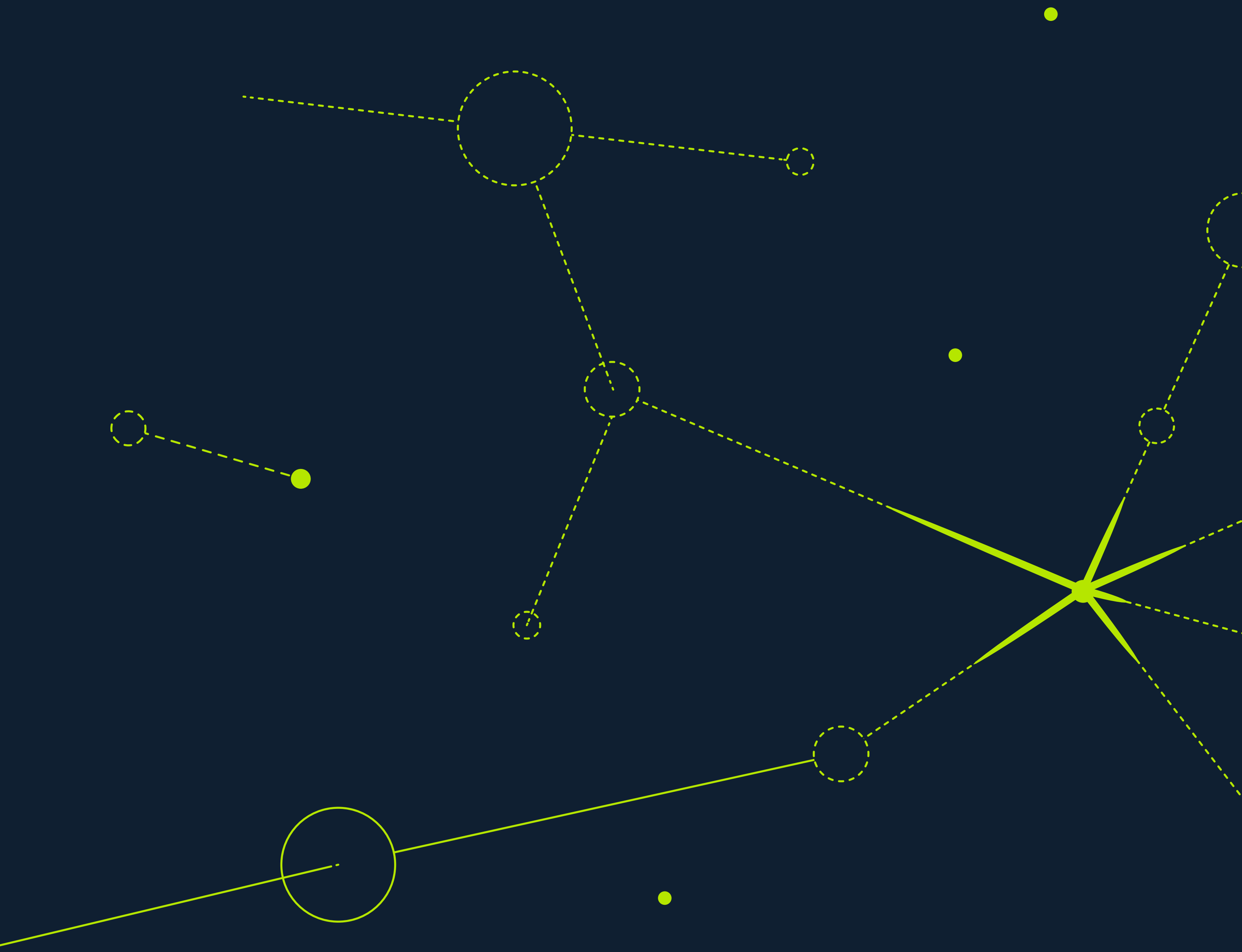


Extreme market concentration: OpenAI's usage dwarfs all competitors combined. With 10,000+ enterprise users, it processes more corporate data than the next nine platforms combined. This dominance means that any security incident, service disruption, or policy change at OpenAI could impact a substantial amount of enterprise AI workflows simultaneously.

Otter.ai (~4,500 users) and Anthropic (~1,700 users) represent the only other platforms with significant adoption. Even these "major" players capture less than 20% of OpenAI's user base, highlighting the extreme imbalance in the shadow AI landscape.

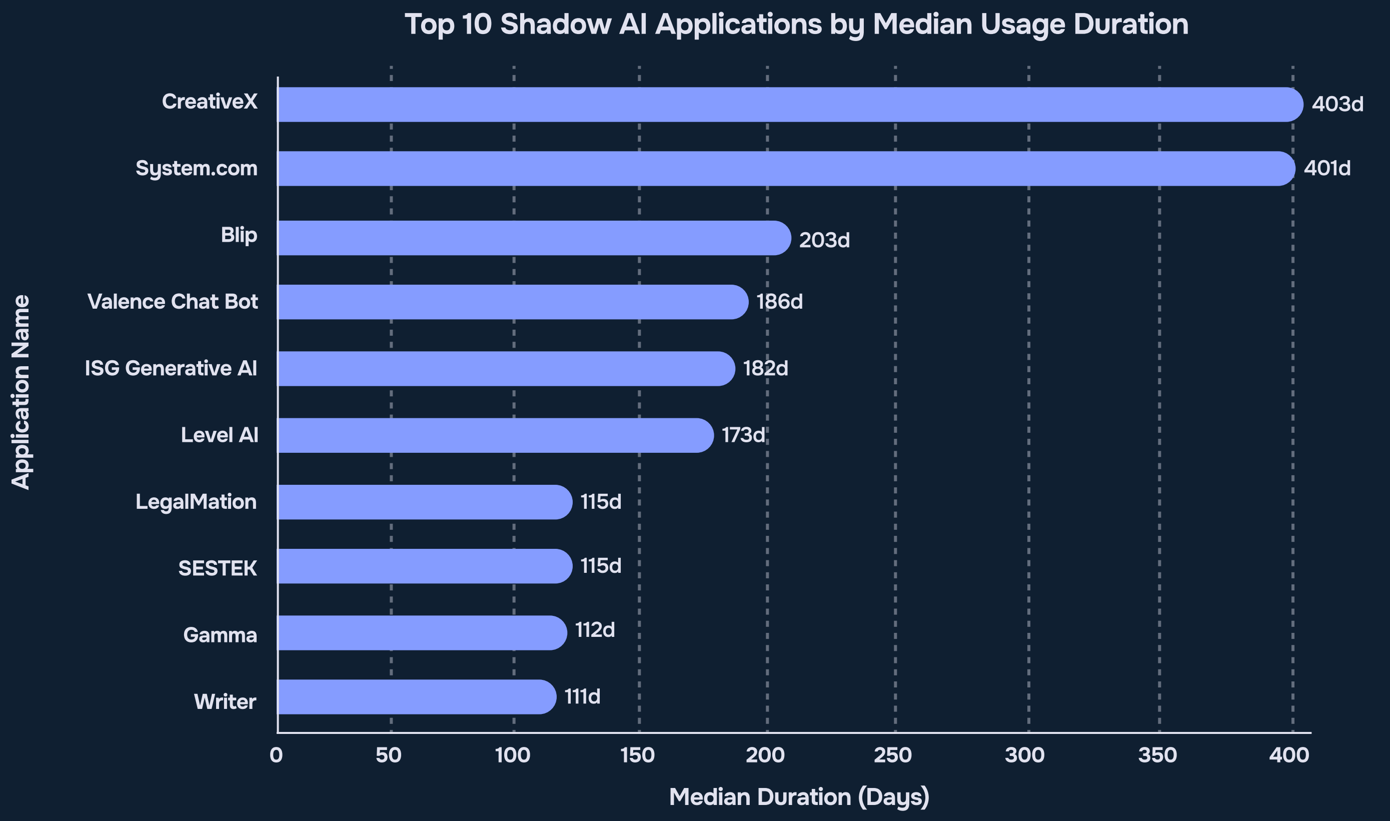
The shadow within the shadow: While security teams scramble to address OpenAI risks, platforms like Perplexity AI, Valence Chat Bot, Blip, and Synthesia quietly expand their footprint. These lesser-known tools often process sensitive data without IT awareness, creating blind spots where data loss and compliance violations can occur undetected.

Implement OpenAI-specific monitoring and controls. Given its dominant usage, create dedicated policies for OpenAI that include data classification requirements, approved use cases, and mandatory security training for users.



Shadow AI Isn't Temporary: Uncovering Months of Unsanctioned AI Usage

Our analysis of median usage duration uncovered a critical truth: s**hadow AI is sticky and tough to get rid of once adopted.** We began tracking this metric at the beginning of 2024, labeling an application as "stopped" only after 60 days of no access or activity. These tools embed themselves into daily workflows, with employees relying on them for months or even years. The longer these unsanctioned applications persist, the greater the accumulation of risk inside your business, typically without shadow AI discovery tools.



Long-term exposure: CreativeX and System.com lead with median usage durations exceeding one year (403 and 401 days respectively). This persistent reliance means organizations have been exposed to potential security vulnerabilities for extended periods, likely processing hundreds to thousands of sensitive documents without proper oversight.

When employees use AI tools for 100+ days, they're not experimenting anymore. They've integrated these applications into core business processes, client deliverables, and operational workflows. Removing these tools after months of use can disrupt productivity and face significant user resistance.

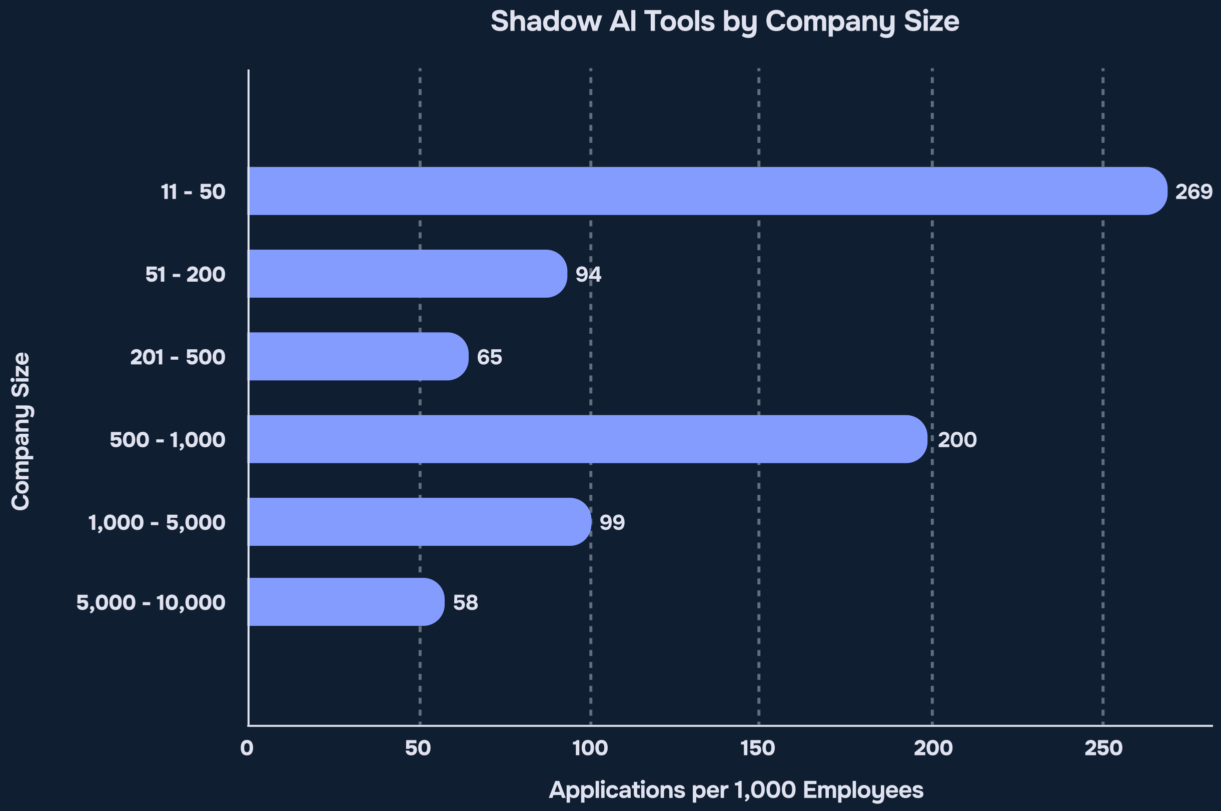
Accumulating risk: Each day of unsanctioned AI use compounds the potential damage. A tool used for 400 days has likely processed exponentially more sensitive data than one used for 40 days. Our data shows that long-term shadow AI users often grant these tools access to email, cloud storage, and internal systems, creating multiple attack vectors.

The persistence paradox: LegalMation, SESTEK, Gamma, and Writer (all showing 100+ days of use) demonstrate how even specialized tools achieve staying power. Once employees find an AI solution that works, they rarely seek alternatives, even if more secure options exist.

Conduct audits of any AI tool showing 60+ days of use in your environment. This duration indicates embedded usage that requires formal security assessment and either official approval with controls or structured migration to secure alternatives.

Understaffed and Overexposed: 27% of Small Company Employees Use Shadow AI

Our analysis uncovered a striking paradox: small-to-medium size businesses (SMBs) face disproportionately higher shadow AI exposure per capita than larger enterprises. With limited IT and security staff, these companies experience a perfect storm of rapid AI adoption without corresponding bandwidth to tame Shadow AI.



David v. Goliath: Organizations with 11-50 employees show the highest concentration of shadow AI usage, averaging 269 tools per 1,000 employees. This means roughly one in four employees (27%) is using unsanctioned AI applications, creating a sprawling attack surface that small security teams cannot effectively monitor or control.

Mid-market challenges: Companies with 501-1,000 employees maintain dangerous exposure levels at 200 shadow AI tools per 1,000 employees. These organizations often lack the sophisticated security infrastructure of larger enterprises while facing similar compliance and data protection requirements.

Smaller organizations typically operate with minimal or no dedicated security staff. When 27% of your workforce uses shadow AI tools, but you lack automated discovery tools, security policies, or governance frameworks, every employee becomes a potential entry point for data breaches.

The same flexibility that helps smaller companies innovate quickly also enables ungoverned AI adoption. Without bureaucratic approval processes, employees freely experiment with AI tools to boost productivity, inadvertently exposing customer data, intellectual property, and competitive intelligence to unknown third parties.

Focus your limited resources on the highest-risk AI categories first. Start by blocking or monitoring AI tools that access email, process customer data, or generate code. This targeted approach provides maximum risk reduction while allowing productivity tools that pose minimal security threats.

Recommendations for Security Leaders

To transform shadow AI from risk to opportunity, security leaders should focus on five core practices:

Implement Real-Time Shadow AI Discovery

Deploy continuous discovery tools to identify all AI tools employees are using, including both web applications and browser extensions. By monitoring network traffic, SaaS logs, and OAuth authorizations, security teams can maintain real-time visibility into shadow AI adoption. You cannot secure what you cannot see.

Create and Publish Pre-Approved AI Tool Lists

Based on our findings, employees choose AI tools for features, not security. Get ahead of risky adoption by publishing vetted alternatives for common use cases. Focus on the categories with highest demand like chatbots, writing assistants, coding tools, and productivity applications. Update this list monthly as new tools emerge and security assessments are completed.

Establish OpenAI-Specific Controls

With OpenAI commanding 53% of shadow AI usage, it demands dedicated governance. Implement specific policies covering data classification requirements, approved use cases, and mandatory security training. Monitor OpenAI integrations with enterprise systems like Box, HubSpot, and Google Drive. Consider enterprise licensing to gain better visibility and control over usage.

Prioritize High-Risk Tool Remediation

Focus immediate action on the F-rated tools identified in our analysis (Jivrus Technologies, Happytalk, Stability AI). For tools showing 90+ days of usage, conduct formal security assessments within 30 days. Either approve them with appropriate controls or migrate users to secure alternatives. The longer these tools persist, the harder they become to remove.

Scale Security for Smaller Teams

Organizations with fewer than 500 employees face the highest per capita shadow AI exposure (27% of employees using unsanctioned tools). If you're resource-constrained, start with a "default deny" approach. Whitelist 3-5 essential AI tools that meet security requirements rather than trying to monitor dozens.

Monitor AI Agent and NHI Proliferation

As AI agents become autonomous, they create new categories of non-human identities accessing your systems. Implement controls specifically for AI agents, including credential rotation, access reviews, and activity monitoring. Track which AI tools are creating persistent identities in your environment.

Leveraging Reco to Tackle Shadow AI

At Reco, we've built our dynamic SaaS security platform specifically to address the shadow AI governance challenges outlined in this report. Our AI-based graph technology maps all SaaS applications, identities, and relationships across your enterprise. We currently support **over 200 SaaS applications** and detect major AI tools including ChatGPT, Claude, Gemini, and Microsoft Copilot—with new app support added in days, not quarters.

How We Discover Shadow AI

Our multi-layered detection system provides comprehensive visibility through:

- **Identity Provider Integration:** We sync with Entra ID/Okta to establish your approved application baseline
- **Email Metadata Analysis:** We scan Gmail/Outlook headers to detect unauthorized AI tool communications
- **Advanced NLP Matching:** We consolidate identities and accurately map them to AI applications
- **Real-Time Alerts:** We notify you instantly when new shadow AI tools are deployed

Real Customer Impact

Our customers are seeing measurable results. **BigID** eliminated months of manual work using our hundreds of pre-built threat detections, integrating Reco as a core SOC automation component.

Wellstar Health System discovered over 1,100 SaaS applications in their environment. Their Executive Director shared: "I was expecting to see several hundred apps, but nothing could prepare me for what Reco was to uncover."

Our Solutions for Each Finding

For High-Risk Applications (Finding 1)

- Our **Vendor Risk Score System** prioritizes dangerous applications
- We dynamically score risks as security postures change
- We automatically recommend how to remediate those F-rated tools

For The Popularity Trap (Finding 2)

- Our **Security Scorecard integration** rates every AI application from A-F
- We surface security risks for popular but insecure tools like CreativeX and Otter.ai
- We help you guide employees from risky popular apps to secure alternatives

For OpenAI Coverage (Finding 3)

- We provide **native ChatGPT** detection with plugin identification
- We track data sharing with OpenAI services in real-time
- We enable granular policy enforcement for the platform processing most of your AI activity

For Long-Term Shadow AI Usage (Finding 4)

- Our **behavioral analytics** identify 400+ day usage patterns
- We track historical usage with anomaly detection
- We reveal deeply embedded Shadow AI dependencies

For Small Company Challenges (Finding 5)

- We offer scalable architecture requiring minimal IT overhead
- We deploy rapidly for resource-constrained teams
- We provide flexible options for organizations under 500 employees

Our Latest Innovations

We launched Reco AI Agents to eliminate alert fatigue. Our AI-driven prioritization surfaces only critical issues while empowering your Tier 1 analysts without requiring deep expertise.

Our Agentic AI Security features address autonomous AI agents through non-human identity detection, behavioral monitoring, and proactive threat protection across your SaaS ecosystem.

Why Organizations Choose Reco

- **NPS Score: 82** across all our customers
- **10x faster deployment** than competitors with 80% less effort
- **CRN 2024 Stellar Startup** recognition for security innovation

Conclusion

Shadow AI has fundamentally altered the enterprise security landscape. Our data reveals the reality: while security teams plan their next moves, employees have already deployed hundreds of AI tools, processing sensitive data through applications that would fail basic security audits. This is today's operational reality.

The evidence is overwhelming: F-rated applications handle corporate data daily. OpenAI processes 53% of all AI activity. Small companies see 27% of their workforce using unsanctioned tools. These aren't anomalies. Our findings provide a true depiction of just how messy the shadow AI challenge is.

What makes shadow AI unique: The employees creating these risks are driving unprecedented productivity gains. They're not reckless; they're resourceful. Any security strategy that ignores this reality will fail.

The opportunity is now. Every day these tools become more embedded in workflows. Every integration expands the attack surface. Every new AI tool discovered is another security decision made without visibility. Teams that implement discovery and governance now will outpace and out-innovate those who don’t.

Every organization must decide whether to chase shadow AI incidents after they happen or get ahead with real governance. The tools exist. The data is definitive. Shadow AI isn't going away, but with the right approach, it doesn't have to stay in the shadows.

Take Your Next Steps with Reco

Reco is the leader in **Dynamic SaaS Security**, the only approach that eliminates the SaaS Security Gap: the growing gap between what you can protect and what's outpacing your security. This gap is driven by SaaS Sprawl—the proliferation of apps, AI, and identities—the challenge of keeping their configurations secure amidst constant updates, and the challenge of finding threats hidden within an ever-growing number of events. Dynamic SaaS Security by Reco keeps pace with this sprawl, no matter how fast it evolves. Founded by security and AI experts, Reco protects over 2 million users across Fortune 500 companies worldwide.

Schedule a Demo

This report presents analysis conducted by Reco and authored by The Cybersecurity Pulse, based on comprehensive shadow AI data from Reco's enterprise customer base.

The Cybersecurity Pulse