



Governance at the Edge: Balancing GenAI Innovation with Enterprise Control

Developing a safe adoption strategy for AI

Matt Pour

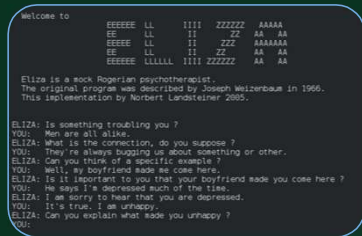
Director, Solutions Engineering

matt@island.io

Backed by :



The Origins of AI (chat)



1966

ELIZA

MIT therapist Joseph Weizenbaum built a conversational patient / psychotherapist program where responses informed the computer-generated replies. (rule-based scripts)

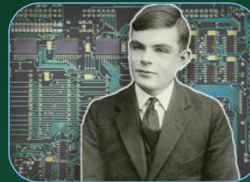
Jabberwacky

British programmer Rollo Carpenter designed a program to "simulate natural human chat in an interesting, entertaining and humorous manner".

A.L.I.C.E

Engages in a conversation with a human by applying some heuristic pattern matching rules to the human's input. (humanoid talking robot)

(Turing Test)



1990's-2000's



2010's



Intelligent personal assistants that use natural language processing designed to answer questions, execute actions through web service requests and offer personalized recommendations.



2020's



The rise of NLU (Natural Language Understanding) enables chatbots to leverage context-aware algorithms to infer intent while deep learning techniques further enhance performance. Large datasets (LLMs) are used to learn nuance, handle ambiguity and adapt to dialects and cultural references.

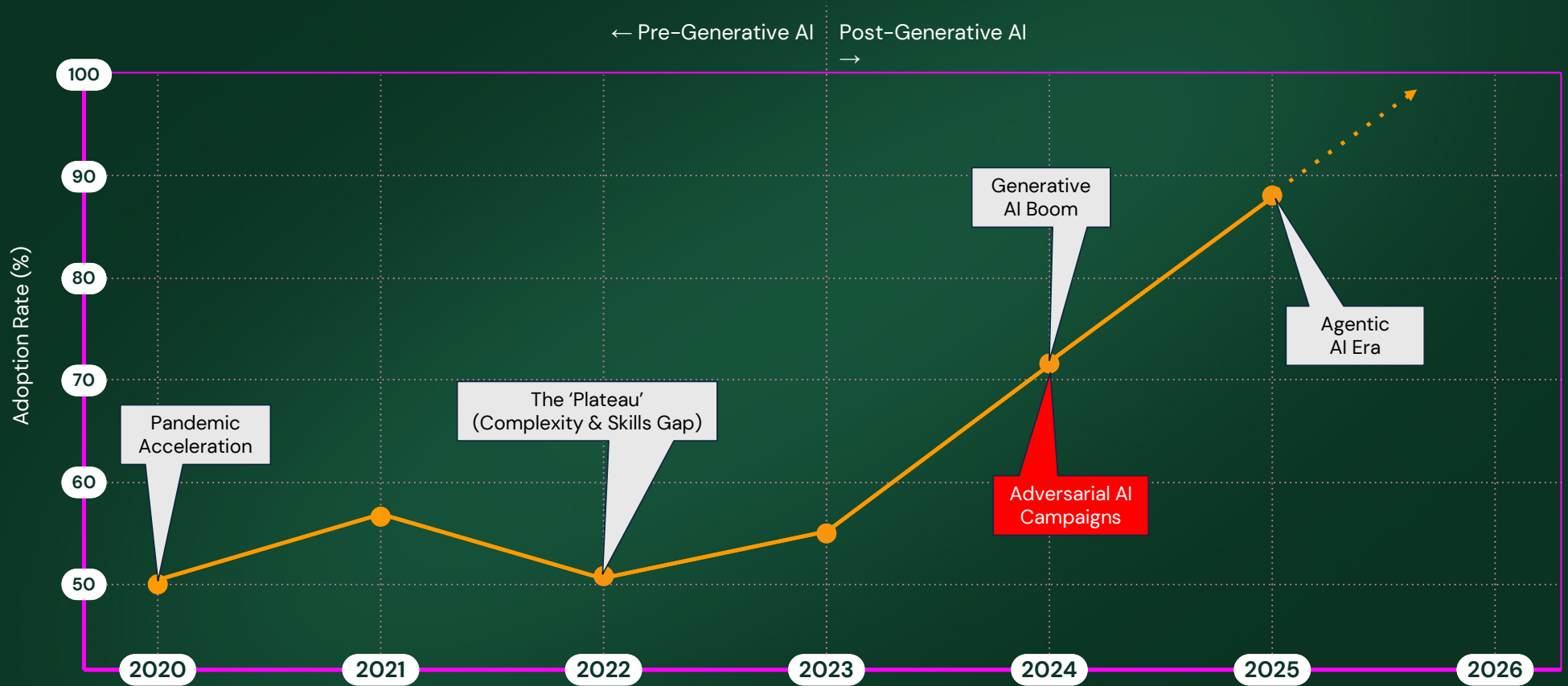


2025+



Highly personalized, deeply integrated, and increasingly autonomous agents that move beyond simple Q&A to handle complex tasks and unified, omnichannel support across platforms. These complex AI assistants can now help non-coders build apps and prototypes, lowering barriers to entry.

Enterprise AI Adoption Hits Unprecedented Levels



AI is Everywhere (*Chaos*)

Sometimes where it shouldn't be!

Chat

 Gemini

 Copilot

 ChatGPT

 Claude

 Grok

 perplexity

Productivity

Coding Tools

 CURSOR

 Claude Code

 PyTorch

 GitHub Copilot

LoB Tools

 Jasper

 Lexis+ AI Harvey

 grammarly

Driving Influences

1. **User Preference**
(BYOAI)
2. **Line of Business Preference**
(Shadow AI)
3. **Executive & Board Pressure**
Innovation, efficiency,
competitive advantage, etc.
4. **Cybersecurity Risk**
Visibility, governance, data
protection, etc.

The Evolution of AI in the Enterprise

The evolving maturity of AI

AI CHAT

- Conversational, natural language **prompt-based** interface.
- Intelligent **virtual assistants** for tasks like customer service & personal help.
- **Learn and improve** from each interaction.



88%

regular AI usage in at least one business function*

AGENTIC AI

- Autonomous, goal-driven AI systems that can **plan, reason, and take actions** independently.
- **Improves accuracy and efficiency** of repetitive tasks by executing multi-step workflows.



62%

experimenting with AI agents*

scaling AI agents in 1+ business function*

23%

AI BROWSER

- **AI-native** environment transforming digital interactions.
- Integrates artificial intelligence **directly into the browsing experience**



too early to tell

The Risks of AI in the Enterprise

Security & Privacy Risks

Data Leakage
Shadow AI
Prompt Injection

Legal & Compliance Risks

Copyright & IP Infringement
Hallucinations & Inaccuracies
Data Residency & Sovereignty

Operational & Reliability Risks

Automation/Confirmation Bias
Measurable ROI
Uncontrolled Cost Escalation

Do Nothing

Continue Saying 'No'
Opportunity Loss
Competitive Disadvantage

AI is too valuable to block, yet your data is too important to risk!

How Customers Solve for this Today

Various approaches to the evolving challenges

BUSINESS

They Don't!

The 'head-in-the-sand' approach blocks all access to AI tools

- Weakens competitive advantage
- Stagnates workforce, hinders recruitment, and increases attrition

Only Sanctioned Providers' Enterprise Plans

Limited optionality delivers a 'generic' AI experience to all users

"AI **Leaders** see a 1.6x improvement in EBIT Margin Impact and 2.5x Revenue Growth compared to AI **Laggards** which remain neutral or negative!"

(Boston Consulting Group & McKinsey)

SECURITY

They Don't!

Shadow AI Sprawl creates an invisible, unmanageable data loss reality

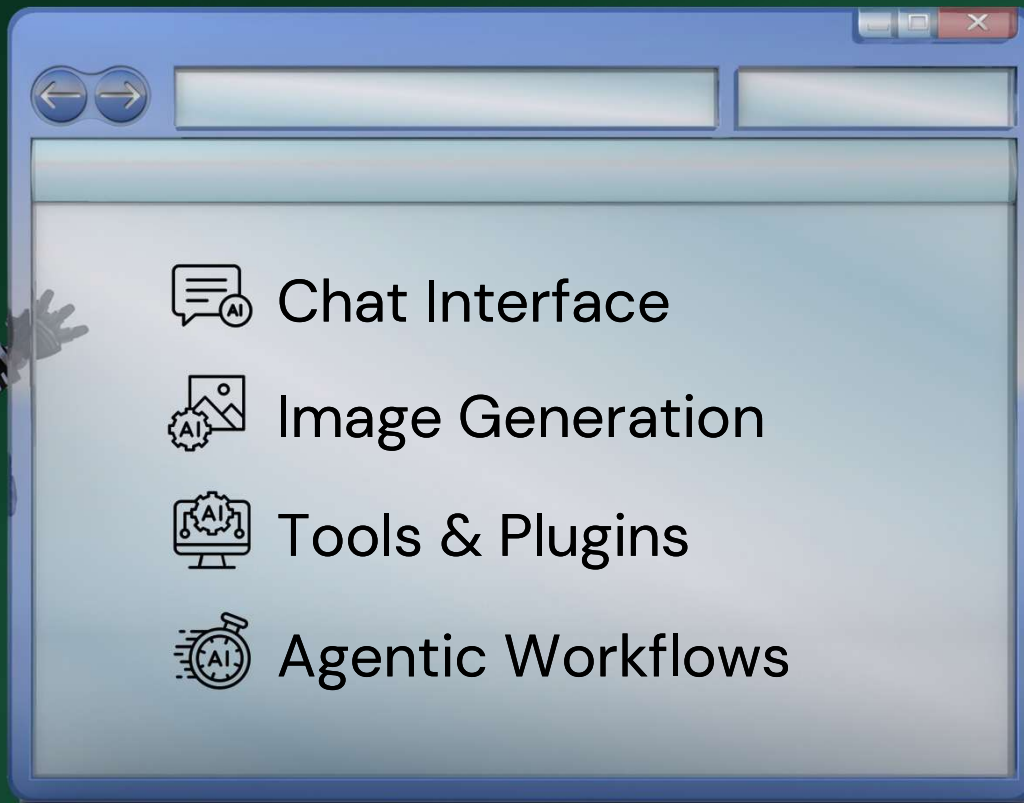
Legacy Security Solutions

Current controls like SASE must mature rapidly to handle complex AI

Patch Together Multiple AI Security Tools

Fragmented AI architectures leave dangerous blind spots and protection gaps

Today's Browser: The Onramp to AI



-  Chat Interface
-  Image Generation
-  Tools & Plugins
-  Agentic Workflows



Identity



Security



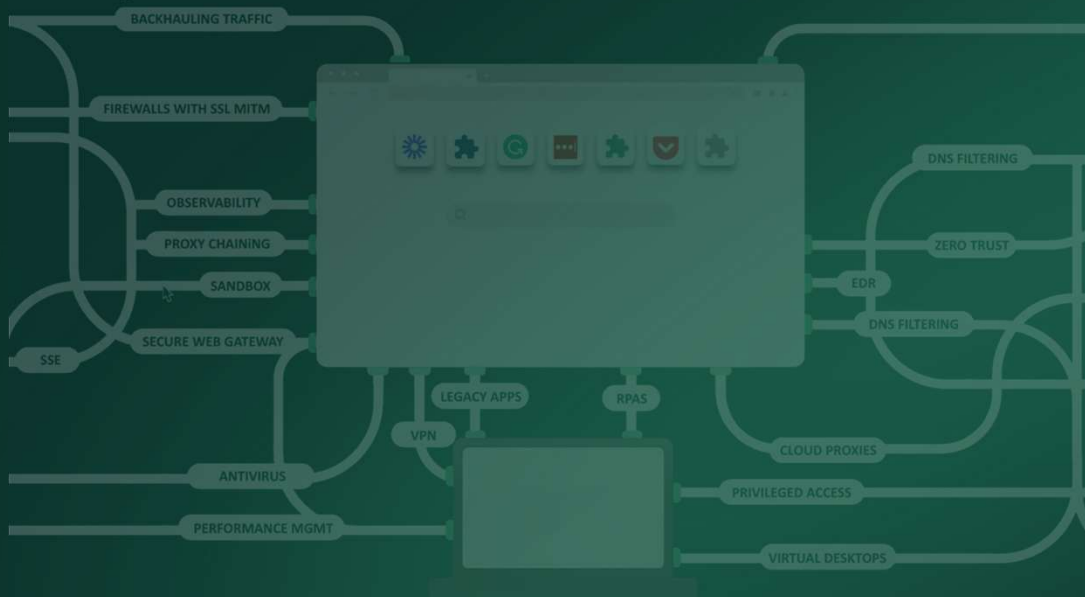
Governance



Visibility

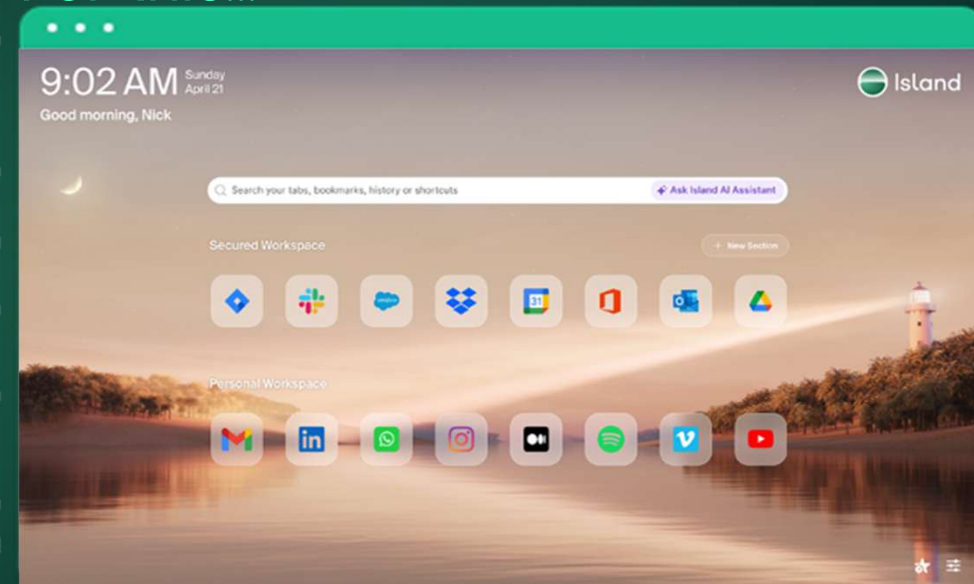
What is an Enterprise Browser Platform?

Swap this...



A complex set of disparate vendors, technologies, infrastructure, and compensating security controls.

For this...



A single, unified, and modern platform that provides secure application delivery, zero trust access, and data protection while reducing cost and complexity.



Identity

IdP Integration

Authentication to existing identity providers drives dynamic policy and AI application entitlements

Zero Trust Principles

Identity, location, and device posture-driven least privilege access



Security & Data Protection

Smart Access Controls

Define who can use AI, in what context, and enforce an acceptable use policy for genAI interactions

Application Boundary

Enforce policy-driven guardrails on data movement using comprehensive last mile controls

Input Protection & Data Masking

Prevent sensitive data (e.g. PHI, PII, IP) from being entered or uploaded into unsanctioned LLMs
Redact sensitive data at the presentation layer



Governance

Tenant Scoping

Restrict access to approved AI tools or enterprise tenants

Data Lineage

Track the movement of data (files and clipboard actions) into and out of AI tools

Compliance Alignment

Map controls and evidence to NIST AI RMF, ISO/IEC 23894, SOC 2, HIPAA/PCI requirements: acceptable use, data handling, access controls, and auditability



Visibility



SIEM & BI Tools

Shadow AI

Monitor all AI usage to steer users from unsanctioned to approved tools

AI Observability

Audit all AI prompt and response content via role-based access control

App & Model Identification

Detects access to genAI sites, extensions, and embedded assistants

User Adoption & Usage

Identify genAI use by identity, role/group, network/location

Island AI Usage Research

99%

Organizations use AI

Technology: 57%
Financial Services: 40%
Business Services: 32%
Pharma/Healthcare: 16%



88%

Employees upload data to AI
52% acknowledge uploading
to personal (non-business)
AI tenants

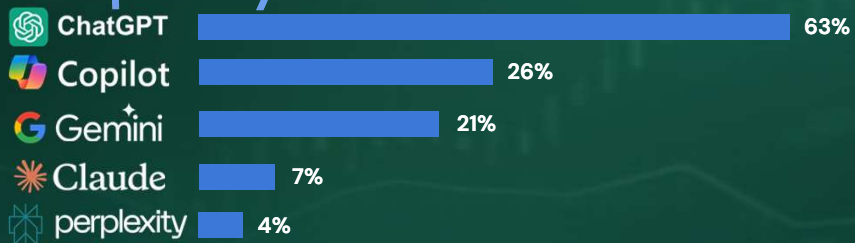


78%

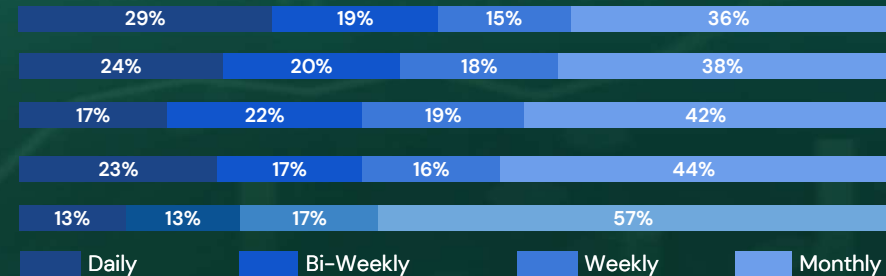
AI browser extensions in
use across enterprise
Up from 52% in 2024



Model Prevalence Frequency



Usage



Built-in Controls and Visibility

Unlock the potential of AI in the enterprise, **safely and securely**

Access

- Govern who can use AI
- Only run AI when access criteria is met
- AI aligned with user permissions

Data protection

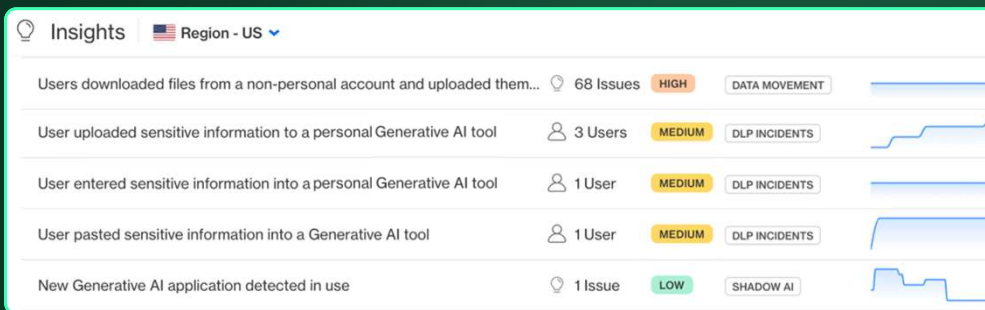
- Keep corporate data where it belongs
- Sanitize PII in prompts & responses
- No training unsanctioned AI models

Visibility

- See data lineage across AI tool usage
- Identify and prevent risky browser extensions

Audit

- Full audit trail including session recordings
- Align AI usage to governance frameworks



AI Visibility					
AI Application Name	Number Of Users	Number Of Navigations	Top Sent Data Types	Total Data Uploaded	
ChatGPT	227	47146	Source Code Credit card number Domain name	450 MB	
Gemini Google	50	1556	Source Code Email Address USA social security number	120 MB	
Claude AI	40	1113	Source Code Domain name	565 MB	
Perplexity AI	25	598	Source Code Domain name	95 MB	

Is Your Enterprise Ready for AI?

A readiness checklist for the safe adoption of genAI



- ☐ Have you **educated users on the risks** associated with genAI (e.g. data loss, prompt injection, hallucinations, etc.)?
- ☐ Do you have **visibility into shadow AI** tool usage across the enterprise?
- ☐ How would you **identify (and prevent) inappropriate data usage** within genAI tools?
- ☐ Is there a browser extension policy that **restricts the use of unapproved extensions** and plugins (e.g. genAI, VPN, password managers)?

Thank you!

For more information or to schedule a demo, visit [Island.io](https://island.io)

