AI GOVERNANCE

ADX Vision 2.0

See the AI tools your people use. Govern what goes into them.

ADX Vision 2.0 is an independent control layer for AI. It maps AI usage across your organization from the endpoint and applies your policy to AI interactions rather than trusting the AI system to decide.

ON THE ENDPOINT | LLM REDIRECTION | PROMPT PROTECTION

THE PROBLEM

Your AI risk isn't the tools. It's what goes into them.

Employees paste intellectual property, customer records, and strategy docs into AI tools every day. It leaves through a text box, one prompt at a time, past every control built for files and networks.

47% of security leaders have had sensitive data exposed via AI.

77% of those with an incident said a sanctioned AI tool was involved.

BLACKFOG/SAPIO 2026

THE APPROACH

See first. Then govern.

ADX Vision maps AI tools in use and governs the data flowing in, at the moment of input.
Policy on the data, not the tool, so the employee keeps ChatGPT and the customer record stays behind.

01 Inspect
Inspects data moving to AI tools in real-time, including inside encrypted browser sessions and apps.

→

02 Control
Applies policy independently of the model or service, separating sanctioned AI from Shadow AI by behavior, not a list of domains.

→

03 Block
Blocks sensitive transfers in real-time, before data leaves the device. Sanctioned AI keeps moving.

WHY ADX VISION

01 · On the endpoint
Rules out cloud proxy players.

02 · Not just the browser
Rules out browser & extension tools.

03 · Across major AI tools
Rules out vendor-native admin panels.

04 · Without blocking the tool
Rules out the block-everything approach.

PAGE 1 © 2026 BLACKFOG INC.

HOW ADX VISION PROTECTS

01 · Sensitive prompt interception

Sensitive data stops before it reaches the AI tool.

Intercepts intellectual property, customer records, credentials and financial data at the moment of input, before it's sent to a third-party AI tool.

02 · AI activity monitoring

Shadow AI stops being a guess.
It becomes an inventory.

See the AI tools in use across your organization, on every device, including the ones nobody sanctioned.

03 · Prompt injection protection

7 LAYERS

Data doesn't only leave by mistake.

Compromised pages, poisoned context, and rogue agents can manipulate an AI session into pulling data out. Manipulated prompts are identified before they create risk.

04 · Custom policies

Your definition of sensitive, not ours.

Custom controls apply at company or departmental level, from credit card and Social Security numbers to the terminology that matters to your business.

05 · LLM redirection

Send people to the AI you actually licensed.

AI requests can be redirected to sanctioned, officially licensed LLM services, so employees keep working in the services you approved.

06 · Data rights

Know what each AI tool does with your data.

ADX Vision tracks the license terms behind each model: retention windows, whether your prompts train the model, and whether traffic is encrypted.

07 · Prompt audit trail

An optional record of every prompt,
ready before anyone asks.

Audit prompts sent to frontier LLMs and retain them under the policy you set, for governance, compliance and audits.

08 · Usage & cost analytics

Token spend across all major models, in one view.

A unified view of token consumption across LLMs, showing where tokens are consumed and by whom. It also makes token theft visible.

AGENTIC AI

Don't ask the AI to police itself.

- **On the endpoint** · Policies apply at the endpoint, so AI interactions are governed consistently across different LLMs and services.
- **Visibility and auditability** · One view across endpoints and AI interactions, covering what is used, what is sent and what it costs.
- **Data stays inside** · Whatever an agent is asked to do, sensitive information is held back before it leaves the business.

COVERAGE

Beyond the network.

Reads the data inside encrypted browser sessions, where CASB and SWG see only a trusted domain. Covers AI tools including ChatGPT, Claude, Gemini, and Perplexity, not only sanctioned enterprise deployments. Managed and unmanaged devices, personal machines, offline and air-gapped, even autonomous agents.



PAGE 2 © 2026 BLACKFOG INC.

HOW IT COMPARES

AI created a new security gap. ADX closes it.

ADX prevents exfiltration at the moment of AI interaction. DLP, EDR, DSPM and other security categories were built to solve different problems. ADX adds the control they weren't designed to provide.

CAPABILITY	ADX	DLP	EDR	DSPM	BPE	API
AI-SPECIFIC PROTECTION						
AI exfiltration prevention	✓	◑	✗	✗	◑	◑
Control at AI interaction	✓	✗	✗	✗	◑	✓
Data exposure visibility	✓	✗	✗	✗	◑	✓
Coverage across AI tools	✓	✗	✗	✗	◑	✗
VISIBILITY AND CONTROL						
Shadow AI detection	✓	✗	✗	✗	◑	✗
Control unapproved AI tools	✓	◑	✗	✗	◑	✗
DEPLOYMENT AND ARCHITECTURE						
On-device protection	✓	◑	✓	✗	◑	✗
Works off-network	✓	◑	✓	✗	◑	✗
No browser dependency	✓	✓	✓	✓	✗	✓
Lightweight deployment	✓	✗	◑	◑	✓	◑

✓ FULL ◑ PARTIAL ✗ NONE

ADX = BLACKFOG ANTI DATA EXFILTRATION

AWARD-WINNING · CUSTOMER-PROVEN

MSP Today Product of the Year 2026 · AI in Cybersecurity · AI · teiss Awards 2026 · Winner Cyber Security Excellence Awards · Globee Awards

500+ enterprises, agencies and infrastructure operators protected worldwide.

4.9 / 5 G2 · average across verified reviews

You cannot govern what you cannot see.

Uncover shadow AI, understand where your data is going, and control what leaves, in real-time, from the endpoint.

BOOK A DEMO AT BLACKFOG.COM

ABOUT BLACKFOG

BlackFog is the prevention-first data security platform. Its anti data exfiltration (ADX) technology blocks sensitive data from leaving the endpoint in real-time, on the device, with no classification required, neutralizing ransomware, insider threats and Shadow AI data loss before a byte leaves. BlackFog is SOC 2 certified and supports GDPR, HIPAA and CCPA compliance.

GET IN TOUCH
blackfog.com/contact →

LEARN MORE
blackfog.com/adx-vision →

PAGE 3 © 2026 BLACKFOG INC.