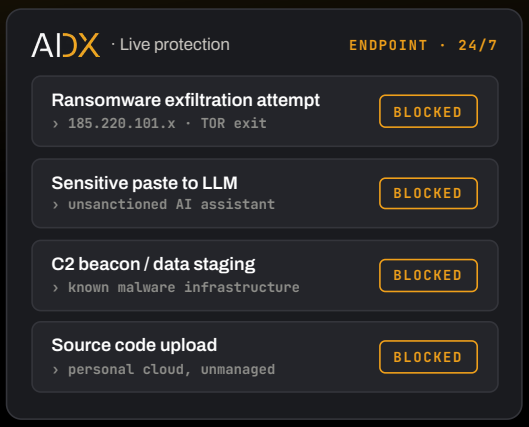
ANTI DATA EXFILTRATION

AI on, exfiltration off.

BlackFog ADX stops sensitive data leaving the device, **whatever sets it in motion.** Ransomware. Shadow AI. Insider threats.

ON-DEVICE · REAL-TIME · PREVENTION-FIRST



One mission. Nothing leaves.

THE PLATFORM

ADX Vision governs AI use and intercepts sensitive data before it's sent. ADX Protect prevents data exfiltration. Together, they protect data at the point of movement, on the device, in real-time.

Powerful alone, complete together.

ONE AGENT · ONE CONSOLE · END TO END

AIDX Vision 2.0

Expose Shadow AI. Control what leaves.

- Seven layers of prompt protection
- Custom policies at company or departmental level
- LLM redirection to sanctioned, licensed services
- Optional prompt auditing and unified token visibility

ADX Vision measures usage across all major vendors from the endpoint.

AIDX Protect

Stop unauthorized data before it leaves.

- Blocks ransomware and double-extortion exfiltration
- Severs C2, TOR and known-bad infrastructure
- Stops insider and accidental data loss

98% of ransomware attacks now end in data exfiltration.
Backups can recover encrypted files. They can't recover stolen data. Stop the exfiltration, and you remove the leverage behind double extortion.

\+

AIDX Instinct
Virtual CISO

› **Two products on one agent. Three if you want us to run it.**
Most vCISOs advise. Ours protect 24/7.

OPTIONAL ADD-ON

Protection across the data lifecycle.

01	02	03	04	05	06
AI interaction	**Policy**	**Infiltration**	**Replication**	**Communication**	**Exfiltration**
Prompts, pastes and uploads are checked against policy first.	Sanctioned and Shadow AI are identified by behavior.	Exploits are stopped; prompt injection is caught in AI tools.	Lateral movement spreads foothold.	C2 beacons call home for orders.	Data attempts to leave the device. ADX blocks it at the source.

AIDX Vision AI GOVERNANCE

AIDX Protect EXFILTRATION DEFENSE

PAGE 1 © 2026 BLACKFOG INC.

Every exit covered.

PROTECTION AT THE POINT OF MOVEMENT



Built to prevent exfiltration.

01 Profile

AI behavioral analytics baseline every process and outbound connection. No signatures required.

02 Detect

Fileless, polymorphic, zero-day, and insider threats surface by behavior, in real-time.

03 Block

Unauthorized data transfer is stopped at the source, before it ever leaves the device.

› **Decisions made on-device, at the process level.** No rules to write, no signatures to update.

The prevention layer you're missing.

HOW IT COMPARES

DLP, CASB, EDR and DSPM each address different aspects of data and threat protection. ADX adds an endpoint-native anti data exfiltration layer, using behavioral analysis to control unauthorized data movement in real-time while complementing your existing stack.

CAPABILITY	ADX	DLP	CASB	EDR	DSPM
AI LAYER · ADX VISION					
Shadow AI detection	✓	✗	◑	✗	◑
Control at the AI interaction	✓	✗	◑	✗	✗
AI data-rights tracking	✓	✗	✗	✗	◑
EXFILTRATION LAYER · ADX PROTECT					
Block exfiltration at the source	✓	◑	◑	◑	✗
Stop ransomware behaviorally	✓	✗	✗	✓	✗
Stop fileless & zero-day	✓	✗	✗	◑	✗
Stop insider data loss	✓	◑	◑	◑	◑
ONE PLATFORM					
Single endpoint agent for both	✓	✗	✗	✗	✗
Unified console	✓	◑	◑	◑	◑
Works off-network	✓	◑	✗	✓	✗
Complements your existing stack	✓	✓	✓	✓	✓

✓ FULL ◑ PARTIAL ✗ NONE

ADX = BLACKFOG ANTI DATA EXFILTRATION

AWARD-WINNING · CUSTOMER-PROVEN

500+ organizations protected worldwide

4.9 / 5 G2 · average across verified reviews

SUPPORTED PLATFORMS

Windows · macOS · iOS · Android · Chrome

SOC 2 · GDPR · HIPAA · CCPA · AWS-HOSTED

Your data doesn't leave. Prove it in 14 days.

Put ADX to work in your own environment with a free 14-day trial. Fast to deploy and built to work alongside your existing security stack.

BOOK A DEMO AT BLACKFOG.COM

PAGE 2 © 2026 BLACKFOG INC.