ANTI DATA EXFILTRATION

ADX Protect

Stop the breach before your data leaves.

ADX Protect blocks data exfiltration at the source, on every endpoint, in real-time. Ransomware, fileless attacks, and insider threats are neutralized before a single byte leaves the device.

ON-DEVICE · REAL-TIME · PREVENTION-FIRST

THE PROBLEM

Modern attacks don't break in. They quietly move your data out.

AntiVirus and EDR are built to detect threats and respond to attacks. But detection alone doesn't stop sensitive data from leaving the device. By the time an incident is identified, the data may already be gone.

183 days
average time to detect a breach, plus 64 more to contain it.
IBM, 2026

$4.99m
average cost of a single data breach, and climbing.
IBM, 2026

THE SOLUTION

One lightweight agent. Every outbound path covered.

It runs as a lightweight agent across every outbound path. AI behavioral analysis neutralizes threats across the full attack lifecycle, replication, communication, and exfiltration, and blocks unauthorized data before it leaves the device.

Stop ransomware where it actually hurts: data exfiltration.

01 Initial access
Phishing, stolen credentials, or an unpatched vulnerability gives access.

→

02 Data exfiltration
ADX stops the outbound transfer on the device, in real-time.
ADX STOPS IT HERE

03 Encryption
Files are locked, but backups can restore them.
PREVENTED

→

04 Extortion
Pay or the stolen data is leaked or sold.
PREVENTED

PAGE 1 © 2026 BLACKFOG INC.

HOW ADX PROTECTS

01 · Kill the attack at every stage, before data leaves.

Most tools wait for damage. ADX Protect neutralizes threats across the full attack lifecycle, from replication to communication to exfiltration. It blocks lateral movement and stops unauthorized data at the source, before it leaves the device.

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

02 · Catch what signatures never will.

Legacy antimalware depends on signatures of attacks it has already seen. ADX Protect uses AI behavioral analysis to stop zero-day vulnerabilities, fileless attacks, and insider threats the moment behavior turns malicious, no prior knowledge required.

- Decisions made on-device, at the process level
- Trained on every known variant, adapting to new ones
- No rules to write, no signatures to update

03 · Enforcement on-device, not the cloud.

ADX runs as a lightweight agent on every endpoint. It inspects outbound traffic in the data path, evaluates each connection by behavior, and blocks unauthorized data movement in real-time.

- No cloud round-trip
- No content inspection
- Works on or off network

04 · One console. Every threat, scored and mapped.

Lightweight agents report to a centralized cloud console with a unified view of threats across your estate. Optional Threat Hunting adds confidence scoring and MITRE ATT&CK classification, while Dark Web monitoring scans for exposed credentials.

- On-device logging of blocked transfers gives a clear record of what was stopped.
- One agent · One console · End to end

SECURITY & PRIVACY

Built to protect your data without collecting it.

ADX is designed to prevent unauthorized data movement at the endpoint, without sending your sensitive data to BlackFog. Its footprint on the device is deliberately minimal.

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

SUPPORTED PLATFORMS

Every endpoint, one agent.

One ADX agent covers every endpoint your people work on. Desktop, mobile, virtual and cloud, managed from a single enterprise console.



PAGE 2 © 2026 BLACKFOG INC.

HOW IT COMPARES

Detection finds the breach. ADX prevents it.

AntiVirus, EDR, and XDR are built to detect threats after they land. ADX Protect stops the data from ever leaving, and runs alongside the security stack you already have.

CAPABILITY	ADX	AV	EDR	XDR	NDR	SIEM
STOPS DATA EXFILTRATION						
Blocks exfiltration at the source	✓	✗	◑	◑	◑	✗
Prevents in real-time (not just detects)	✓	◑	◑	◑	✗	✗
Stops fileless & polymorphic attacks	✓	✗	◑	◑	◑	✗
Stops insider data loss	✓	✗	◑	◑	◑	◑
DETECTION APPROACH						
Behavioral, signatureless	✓	✗	◑	✓	✓	◑
Zero-day coverage	✓	✗	◑	◑	◑	✗
MITRE ATT&CK classification	✓	✗	✓	✓	◑	✓
DEPLOYMENT & ARCHITECTURE						
On-device, works off-network	✓	◑	✓	◑	✗	✗
Lightweight agent	✓	◑	◑	✗	✓	✗
Complements your existing stack	✓	✓	✓	✓	✓	✓

✓ FULL ◑ PARTIAL ✗ NONE

ADX = BLACKFOG ANTI DATA EXFILTRATION

AWARD-WINNING · CUSTOMER-PROVEN

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

500+ enterprises, agencies and infrastructure operators protected worldwide.

4.9 / 5 G2 · average across verified reviews

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

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-protect →

PAGE 3 © 2026 BLACKFOG INC.