TRUST & COMPLIANCE

BlackFog ADX
Shared Responsibility Matrix

Security for BlackFog ADX is shared across three parties: BlackFog, Amazon Web Services (AWS) and the customer. **This matrix sets out who owns what.**

SOC 2 TYPE 2 | NO DEVIATIONS NOTED | LAST UPDATED NOV 9, 2026

Executive Summary

Security for BlackFog ADX is shared across three parties: BlackFog secures the ADX platform, Amazon Web Services (AWS) secures the underlying cloud infrastructure, and the customer secures its own users, endpoints and configuration.
This matrix sets out who owns what.

BlackFog
Secures the ADX platform.

AWS
Secures the underlying cloud infrastructure.

Customer
Secures its own users, endpoints and configuration.

BlackFog ADX is a hybrid SaaS and agent-based anti data exfiltration platform. A lightweight agent on each endpoint stops unauthorized data from leaving the device, and the BlackFog Console, hosted on AWS, provides policy management and reporting.

For organizations aligning with SOC 2, CMMC or similar frameworks, BlackFog ADX is best understood as a Security Protection Asset (SPA) that generates and stores Security Protection Data (SPD): security event telemetry, device metadata and policy configuration.

BlackFog's controls were independently examined in a SOC 2 Type 2 report covering October 1, 2025 to September 30, 2026, with no deviations noted.

BlackFog ADX is designed to handle security metadata, not the contents of customer files or communications. FedRAMP Moderate or equivalent requirements apply only when a cloud service processes, stores or transmits Controlled Unclassified Information (CUI).

What is BlackFog ADX

- **BlackFog Agent:** installed locally on each endpoint (Windows, macOS, Android and iOS); detects and blocks unauthorized data exfiltration and reports events to the Console.
- **BlackFog Console:** a web application hosted on AWS that displays actioned events, device status and insights for the customer's monitored devices.
- **ADX Protect:** ransomware and data exfiltration prevention at the endpoint.
- **ADX Vision:** detection and governance of shadow AI usage across the organization.
- **Data storage:** MongoDB and Amazon S3 on AWS, encrypted at rest; data sent over public networks uses TLS 1.3.

Data BlackFog ADX typically handles

- **Device inventory and metadata:** hostname, operating system and version, agent version, device user and group assignment.
- **Security event telemetry:** processes attempting outbound connections, destination domains, IP addresses and countries, block and allow decisions, and transfer volumes.
- **AI usage telemetry (ADX Vision):** which AI tools and services are in use, by which devices and users.
- **Policy and configuration:** protection settings, rules and groups defined by customer administrators.
- **Administrative activity:** Console user accounts and activity records.

› Note: Customers must not enter CUI or other regulated data into Console free-text fields such as group names, labels or notes.

How BlackFog ADX maps to CMMC Level 2

SPA
Security Protection Asset

BlackFog ADX provides security functions that protect in-scope systems, including exfiltration prevention, ransomware defense and AI usage governance.

SPD
Security Protection Data

The Console stores security-relevant data, such as event telemetry, device inventory and policy configuration, that could aid an attacker if disclosed.

ESP
External Service Provider

Because the Console stores SPD, BlackFog qualifies as an ESP and is assessed within the customer's CMMC scope using this matrix and BlackFog's SOC 2 Type 2 report.

BlackFog Compliance Posture

BlackFog holds an unqualified SOC 2 Type 2 opinion on the Anti Data Exfiltration (ADX) System, with no deviations noted in any control tested.

ITEM	DETAIL
REPORT	SOC 2 Type 2
SYSTEM IN SCOPE	BlackFog Anti Data Exfiltration (ADX) System: Agent and Console
TRUST SERVICES CRITERIA	Security and Privacy (AICPA 2017 TSC, revised points of focus 2022)
EXAMINATION PERIOD	October 1, 2025 to September 30, 2026
INDEPENDENT AUDITOR	Zero Day CPA, PC
REPORT DATE	October 9, 2026
RESULT	**Unqualified opinion; no deviations noted**
SUBSERVICE ORGANIZATION	Amazon Web Services, Inc. (carve-out method)

› BlackFog also operates a Data Processing Agreement (DPA) and published Privacy Policy, and supports GDPR and CCPA data subject requests as a data processor.

PAGE 2 © 2026 BLACKFOG INC.

Shared Responsibility Matrix

Each row names what each party does. Where a cell is blank, that party has no responsibility for the area.

AREA	BLACKFOG	CUSTOMER	AWS (SUBSERVICE)
Physical and environmental security	Secures BlackFog offices; no production servers or physical customer data on BlackFog premises	Secures its own facilities and endpoint devices	Secures data centers, hardware and storage media, including secure decommissioning
Cloud infrastructure	Configures network segmentation, firewalls, high availability and load balancing; blocks unauthenticated public access to resources holding customer data		Operates and secures compute, storage, networking and virtualization
Console application and secure development	Secure Development Policy; changes tested in segregated environments and approved by an independent reviewer; annual third-party penetration test	Reports suspected vulnerabilities to BlackFog	Manages changes to AWS services through its own change process
Agent deployment and updates	Builds, tests and releases agent updates through change management; publishes deployment guidance	Deploys the agent to all in-scope endpoints, keeps it running and current, and investigates devices that stop reporting	
Protection policy configuration	Provides default policies, documentation and support	Configures and maintains policies suited to its risk tolerance; reviews and acts on blocked events	
Customer user access to the Console	Assigns unique user IDs and enforces authentication	Creates, reviews and removes its users; grants least-privilege roles; uses MFA or SSO where available; names an authorized contact for access changes	
BlackFog personnel access	Least-privilege access; MFA on key systems; quarterly access reviews; access removed within 24 hours of termination; background checks, confidentiality agreements and annual security training		Restricts and reviews AWS personnel access to its infrastructure
Encryption	Encrypts customer data at rest; TLS 1.3 in transit; Encryption and Key Management Policy	Encrypts its own endpoint drives and protects local credentials	Provides storage encryption and secures cryptographic key infrastructure
Vulnerability and patch management	Continuous scanning with AWS Inspector and PenTest Tools; critical and high findings remediated by severity	Patches endpoint operating systems and applications	Patches the underlying infrastructure
Logging, monitoring and alerting	Monitors the platform with AWS CloudTrail and CloudWatch; alerts tracked to resolution	Monitors Console alerts and events; forwards them to its SIEM where used	Monitors its infrastructure for incidents
Incident response and notification	Incident Response Plan tested annually; notifies affected customers as agreed in contract	Notifies BlackFog immediately of suspected breaches or compromised accounts; runs incident response for its own environment	Responds to infrastructure incidents
Backup, continuity and availability	Full backups with annual restore tests; Business Continuity and Disaster Recovery Plan tested annually	Maintains continuity plans for its own operations	Provides resilient regional infrastructure
Data retention and deletion	Retains and disposes of data per its Data Retention and Disposal Policy and contract; deletes data on customer request	Defines retention needs and requests deletion at contract end	Decommissions storage media securely
Privacy and personal data	Acts as data processor under a DPA; supports access and deletion requests	Acts as data controller; gives employees any monitoring notices required by local law	
Vendor and third-party risk	Assesses vendors before use and reviews AWS SOC reports annually	Assesses BlackFog as a vendor using this matrix and the SOC 2 report	

PAGE 3 © 2026 BLACKFOG INC.

Customer Responsibilities

BlackFog's SOC 2 controls assume customers operate the following controls. Without them, the controls in BlackFog's report may not achieve their objectives.

CUSTOMER RESPONSIBILITY	SOC 2 CRITERIA
Set up, monitor and remove its users' access to the Console, and ensure that access is appropriate	CC2.2, CC2.3, CC6.1, CC6.2, CC6.3, CC6.6
Assign an appropriate individual to request access changes and removals from BlackFog	CC6.1, CC6.2, CC6.3, CC6.6
Notify BlackFog immediately of any actual or suspected security breach, including compromised user accounts	CC2.2
Supervise, manage and control its personnel's use of BlackFog services	CC4.2, CC5.3

Customers in CMMC programs should also:

- Document BlackFog as an ESP and SPA in the System Security Plan (SSP), and capture shared responsibilities in a Customer Responsibility Matrix using this document.
- Prohibit CUI from entering the Console, including in group names, labels and notes.

Subservice Organization: Amazon Web Services

AWS hosts the BlackFog Console and was carved out of BlackFog's SOC 2 report. BlackFog's controls assume AWS operates these complementary controls, which BlackFog verifies by reviewing AWS's SOC reports annually.

AWS COMPLEMENTARY CONTROL	SOC 2 CRITERIA
Restricts logical and physical access to its infrastructure, reviews access periodically and revokes it on termination	CC6.1, CC6.2, CC6.3, CC6.4, CC6.6
Encrypts customer data at rest and in transit and secures cryptographic keys	CC6.1, CC6.6, CC6.7
Reviews, tests and approves changes to customer-impacting services	CC5.2, CC8.1
Maintains monitoring, incident response and contingency planning	CC7.1, CC7.3, CC7.4, CC7.5
Performs vulnerability assessments and maintains a risk management program	CC3.2, CC9.2
Decommissions storage media securely and keeps customer data out of test environments	CC6.5, CC8.1

REQUESTING FURTHER DOCUMENTATION

The full SOC 2 Type 2 report is available under NDA.

BlackFog's full SOC 2 Type 2 report is confidential and available to customers and prospects under NDA. Contact your BlackFog account representative or visit blackfog.com to request it.

REQUEST THE REPORT AT BLACKFOG.COM

This matrix describes responsibilities in general terms. Specific obligations are governed by each customer's agreement with BlackFog.

AUTHORIZED BY

Dr. Darren W. Williams
Founder and CEO

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.

SUPPORTED PLATFORMS

iOS

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

GET IN TOUCH **blackfog.com/contact →**

LEARN MORE **blackfog.com →**

PAGE 4 © 2026 BLACKFOG INC.