DEVICE-LEVEL PROTECTION

TECH SPOTLIGHT SERIES

INNOVATION IN GOVERNMENT®

BlackFog ADX prevents unauthorized data exfiltration in real-time by monitoring outbound traffic at the device level.



Anti Data Exfiltration: Next-Generation Protection for Government Data



RESOURCES

BlackFog for State and Local Government
carah.io/blackfog-sled-datasheet

BlackFog FAQ
carah.io/blackfog-faq

Why BlackFog?
carah.io/why-blackfog

BlackFog Case Studies
carah.io/blackfog-case-studies

CONTACT US

BlackFog@carahsoft.com
(703) 673-3608
www.carahsoft.com/blackfog

Product Overview

BlackFog's Anti Data Exfiltration (ADX) technology marks the next generation of cybersecurity, shifting the focus from traditional perimeter defense and endpoint detection to preventing unauthorized data from leaving devices. As ransomware tactics evolve beyond encryption to data theft and extortion, this shift is critical for protecting sensitive Government information such as driver's licenses, tax records and other high-value data targeted by cybercriminals.

Powered by artificial intelligence (AI), BlackFog monitors outbound traffic in real-time, automatically detecting and blocking data exfiltration attempts. This device-level protection is especially valuable for Government agencies operating in mobile work environments, where employees often work remotely outside the reach of network defenses. By safeguarding against both external hackers and insider threats, BlackFog addresses the full spectrum of data theft risks faced by the Public Sector.

How it Works

BlackFog employs sophisticated behavioral and intent analysis to continuously monitor 25-30 packet-layer parameters per device, detecting suspicious outbound data flows in real-time. By analyzing the destination, method and characteristics of each data packet, the solution identifies potential exfiltration attempts and takes immediate action at the endpoint—blocking the transfer instead of generating alerts that require a human response. This automated approach neutralizes threats instantly and reduces the burden on often-overstretched security teams.

Detection accuracy is enhanced through machine learning (ML) algorithms trained on patterns from hundreds of thousands of protected nodes. This data is consolidated in a centralized enterprise console, providing security teams with a comprehensive view of threat activity across the organization. Further processed through BlackFog's proprietary AI engine and Large Language Model (LLM), the system identifies emerging attack patterns and dynamically adapts its defenses to maintain protection against evolving threats.

Designed to work alongside existing Government IT environments, BlackFog integrates easily with solutions like Endpoint Detection and Response (EDR), antivirus and firewalls. The platform is System and Organization Controls 2 (SOC 2) certified and compliant with key security standards, and it is currently working toward National Institute of Standards and Technology (NIST) certification to ensure alignment with Federal requirements.

BLACKFOG™ | carahsoft.

Key Benefits

Dual Protection

BlackFog safeguards Government agencies from both external hackers and insider threats. Its device-level operation detects suspicious activity regardless of origin, whether from unauthorized external actors or internal users with legitimate access attempting to extract sensitive information. This dual-layer protection is particularly valuable for agencies managing classified or high-value citizen data.

Real Time Monitoring

Traditional cybersecurity often focuses on incoming threats, leaving outbound data transfers vulnerable. BlackFog addresses this critical gap by monitoring outbound traffic in real-time, preventing data exfiltration. It is especially effective against browser-based attacks that exploit the vulnerabilities of remote work environments. With a 99.9% success rate in stopping attacks, BlackFog ADX is a trusted defense for safeguarding critical infrastructure and sensitive Public Sector data.



Reduced Workload

Unlike tools that only log suspicious activity, BlackFog takes immediate action at the endpoint to block threats. This automation significantly reduces the workload for resource-constrained Government IT teams, freeing them to focus on strategic initiatives. Operating 24/7 without requiring continuous oversite, BlackFog ensures reliable protection even when agencies cannot maintain around-the-clock monitoring.



Enhanced Performance

In addition to ransomware protection, BlackFog improves network efficiency by blocking background data collection during routine web browsing. Many websites instrument browsers to connect with third-party servers, collecting user and device information without visibility. BlackFog reveals and halts this hidden data exfiltration, enhancing both operational privacy and network performance across Government systems.

Continuous Improvement

BlackFog's effectiveness strengthens over time through continuous learning. It collects data from all protected endpoints, feeding it into training systems to refine detection algorithms. Its domain-specific AI, tailored exclusively for cybersecurity, analyzes threat behaviors and emerging tactics, including those developed with AI, ensuring the system evolves alongside the threat landscape.

CONTACT US BlackFog@carahsoft.com • (703) 673-3608 • www.carahsoft.com/blackfog

© 2025 Carahsoft Technology Corp.

BLACKFOG™ | carahsoft.