

USING ANTI DATA EXFILTRATION (ADX) TO STOP RANSOMWARE AND OTHER THREATS TO DATA



DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE INC.

TAG





USING ANTI DATA EXFILTRATION (ADX) TO STOP RANSOMWARE AND OTHER THREATS TO DATA

DR. EDWARD AMOROSO
CHIEF EXECUTIVE OFFICER, TAG INFOSPHERE INC.

This series of Book developed by TAG Infosphere, highlights a powerful new cybersecurity solution known as Anti Data Exfiltration (ADX) which provides on-device data security and threat protection. Commercial vendor BlackFog pioneered ADX which is shown to effectively stop cyberattacks such as ransomware, spyware, malware, and phishing.

INTRODUCTION

ANTI DATA EXFILTRATION (ADX)

Page 3

CHAPTER 1

OVERVIEW OF ADX BENEFITS

Page 4

CHAPTER 2

HOW ADX SUPPORTS AND IMPLEMENTS POLICY

Page 5

CHAPTER 3

HOW ADX IS INTEGRATED INTO THE ENTERPRISE

Page 8

CHAPTER 4

HOW ADX IS IMPLEMENTED BY BLACKFOG

Page 10

CHAPTER 5

AN ADX ACTION PLAN FOR ENTERPRISE

Page 12



INTRODUCTION

ANTI DATA EXFILTRATION (ADX)

It is now well-known by organizations of all sizes and across all sectors that ransomware prevention and data exfiltration prevention have emerged as primary objectives for leadership. The problem is that despite such recognition and attention from cybersecurity teams, breach incidents continue to occur. The City of Dallas, for example, recently reported paying millions after a ransomware attack in May 2023.¹

Furthermore, the loss of data in the enterprise continues to be a nagging cybersecurity problem, one that has been subjected to literally decades of attention, mostly with only modest improvement. In 2023, for example, IBM, Deloitte, PwC, and EY were all victims of a data extortion exploit, related to the MOVEit exploit that hit the industry, driven by a Russian-speaking group called Cl0p.²

In this Book we focus on a preventative method known as Anti Data Exfiltration (ADX) that exhibits many important cybersecurity principles for organizations.³ Pioneered by commercial vendor **BlackFog**, ADX involves an on-device means for addressing data security, privacy, and ransomware prevention.⁴ We will show how ADX complements existing controls, while effectively mitigating threats that can lead to high response cost.

The chapters will cover the salient aspects of ADX with the goal of helping security practitioners to understand how the method – and how the BlackFog solution, in particular – can be used to reduce cyber risk. The good news is that in addition to addressing ransomware risk, ADX is also highly effective in reducing the likelihood of successful spyware, malware, phishing, unauthorized data collection, and profiling attacks.

Our hope is that by introducing you to ADX, you will take steps to begin reviewing how this data security method complements or perhaps even replaces your existing endpoint protection. Most of the deployments we've seen utilize ADX to make existing solutions such as endpoint detection and response (EDR) better. As the solution evolves, however, it is possible that ADX will become the preferred security approach for devices that can accept agents.

¹ See <https://www.nbcdfw.com/news/local/dallas-pays-millions-for-ransomware-expenses-after-may-attack/3313643/>.

² See <https://www.cnn.com/news/security/10-major-cyberattacks-and-data-breaches-in-2023?page=5> for example data exfiltration scenarios that have occurred to live production systems.

³ See <https://www.tag-infosphere.com/> for information on TAG Infosphere's Research as a Service (RaaS) and related offerings in cybersecurity, artificial intelligence, and other areas.

⁴ See <https://www.blackfog.com/> for information on how the company implements and support anti data exfiltration (ADX) for enterprise customers requiring data security solutions.



OVERVIEW OF ADX BENEFITS

The types of policies that require attention in the context of any ADX deployment include various practical controls that should be selected based on an understanding of the threat being addressed.

It would be tough to find any business leader, IT practitioner, or cybersecurity expert today who would not identify ransomware as a particularly difficult challenge. Despite many years of industry attempts by vendors and practitioners to reduce the risks of data security and ransomware, organizations around the world continue to experience negative impact, and in particular, the unauthorized loss of data from targeted devices.

In this chapter we address the challenge of data loss in the enterprise, and we explain how a paradigm shift toward the prevention of data exfiltration on the device is an excellent means for taking a positive shift-left step. The commercial solution from BlackFog serves as the practical backdrop to our discussion, illustrating how ADX can be deployed into a live production environment.

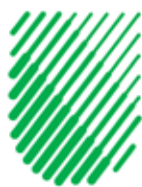
WHAT HAS BEEN THE DATA SECURITY CHALLENGE TO DATE?

Enterprise security teams today generally collect data across their systems and infrastructure to *detect* whether policy violations or data leakage have occurred – a process typically done *after the fact*. Such an approach is the basis of most endpoint detection and response (EDR) programs, as well as extended detection and response (XDR) solutions. This reactive approach is often referred to as a shift-right solution.

Emphasis on detection and response implies that something bad has happened and that the security team must spring into action to contain any potential consequences. Much of this paradigm is driven by the view that adversaries (such as nation-states) are so capable that enterprise security teams are defenseless against these attacks. While breaches continue to occur, our view is that preventive steps can, and should be taken.

Click [here](#) for more information on the specifics and technical details regarding BlackFog's implementation of ADX.

¹ See <https://www.nist.gov/cyberframework> for information on the NIST Cybersecurity Framework (CSF).



HOW ADX SUPPORTS AND IMPLEMENTS POLICY

The implementation of any vendor-provided solution, including Anti Data Exfiltration (ADX) becomes a reality for enterprise teams in the context of establishing policy. When done properly, policy definition incorporates business objectives, perceived threats, and deployed systems and infrastructure into a set of assertions that guide any strategic or tactical security decision-making.

In this chapter we address some of the policy decision options that are available to enterprise teams deploying ADX – and, in particular, the commercial solution from cybersecurity vendor BlackFog. Our objective here is to help practitioners move more closely to deployment of a shift-left preventive solution that addresses the risk of data exfiltration on the device in a proactive manner.

WHAT POLICIES ARE REQUIRED TO PREVENT DATA LOSS?

The types of policies that require attention in the context of any ADX deployment include various practical controls that should be selected based on an understanding of the threat being addressed. For example, organizations with particularly sensitive data such as national security teams will have more urgent need to deploy ADX to their deployed devices than an organization with a much less intense threat.

GEOFENCING

The first policy area in which teams must consider their deployed options involves the technique known as geofencing. This method involves managing data sharing, usage, and security based on the physical location of individuals and groups. Geopolitical concerns often have a direct impact on the policies established by organizations, so legal teams generally work with security teams on establishing appropriate geo-policies.

At the heart of BlackFog Enterprise is its on-device agent, which goes beyond traditional antivirus and Endpoint Detection and Response (EDR) solutions.

UNAUTHORIZED DATA COLLECTION

A second area where policy decisions must be made in the context of ADX involves controls to prevent unauthorized data collection. This is the essence of data security policy in that it demands clear definition of the goals of collecting data and how it is done in a manner that is respectful of data privacy concerns, as well as avoidance of unwanted aggregation for the purpose of data science.

UNAUTHORIZED PROFILING

A related area for policy decision-making in ADX involves avoidance of unauthorized profiling, which could occur in environments that might be particularly eager to identify threat patterns. The policies associated with profiling in the context of data security will also be driven by many different factors. ADX deployments should only occur with vendors (such as BlackFog) that are respectful of security and privacy in all algorithmic implementations.

BEHAVIOR ANONYMIZATION

A fourth policy decision that is required in the context of ADX involves the manner in which user behavior is anonymized. This is important because data security on the device can involve activity that could be commercially, or even personally sensitive. As such, employees and others being protected with ADX need to understand that their activity is properly anonymized to protect their identity.

SUPPORT FOR REMOTE WORK

Finally, a fifth policy decision that is required to support proper ADX security involves how a security team will address the risks of remote work. Everyone knows that the user's endpoint device is now the most important aspect of modern work since it travels with the employee regardless of physical location. As such, ADX is well-suited to protecting remote work in the context of localized networking.

HOW ARE POLICIES IMPLEMENTED AT THE DEVICE LEVEL?

As suggested above, implementing ADX at the device level is especially attractive, because it moves the security controls closer to the asset being protected. This is an important design paradigm that originated in the early days of information security. Additional design heuristics that are important in the design of ADX and in the BlackFog implementation, in particular, include the areas discuss below.

MINIMIZATION OF DATA COLLECTION

Security engineers understand the value of designing systems that minimize the data that must be collected to make cyber prevention decisions. This is especially true for device-resident controls where the logistics of the local computing environment could be constrained and where large volumes of data could cause a problem. Privacy issues can also emerge if the security design is not optimized for the volume of data collected.

SUPPORT FOR EVERY ENDPOINT

Ensuring that a given device control such as ADX covers all types of deployed endpoints is critically important to avoid architectural gaps in coverage. This is particularly important in cybersecurity where malicious actors often target devices or assets where the controls are weakest. This follows the familiar aphorism that a chain is only as strong as its weakest link – hence, the need to provide ADX support for every type of endpoint.

HOW IS ADX POLICY ENFORCEMENT USEFUL FOR COMPLIANCE?

As one might expect, threat mitigation should always be the number one priority in the deployment of any security solution – and that is true for both ADX in general and the BlackFog solution in particular. That said, the practical obligation does emerge for enterprise security teams to provide compliance support for data security requirements. We have found ADX to provide especially useful assistance in meeting the compliance issues listed below.

SUPPORT FOR GLOBAL PRIVACY

The need to create evidentiary data to meet obligations for privacy frameworks such as the General Data Protection Regulation (GDPR) in the European Union (and elsewhere) and PCI DSS, has promoted many enterprise teams to fundamentally rethink their data security approach. We have found ADX to be an effective means for demonstrating a mandatory control that can protect user privacy and to meet stringent compliance requirements.

SUPPORT FOR DATA PROTECTION

Just as with privacy regulations, the need to maintain on-going and continuous support for compliance in the area of data protection comes from a variety of different initiatives. These can include the need to show consistency with frameworks such as the NIST Cybersecurity Framework (CSF) or to meet data security requirements levied on suppliers as part of a buyer's third party risk management (TPRM) program.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.

⁶ See <https://gdpr-info.eu/> for information on the General Data Protection Regulation (GDPR) and <https://www.pcisecuritystandards.org/> for information on the payment card industry data security standard (PCI DSS).



HOW ADX IS INTEGRATED INTO THE ENTERPRISE

No cybersecurity solution can work in isolation, so the integration of any ADX deployment into the enterprise is an important consideration. Since ADX focuses on prevention and the shift-left paradigm, it provides significant synergies with existing technologies that focus on detection and response and makes them more effective. By giving other tools more time to react, the entire solution becomes greater than the sum of its parts.

In this chapter we review how the commercial ADX solution from BlackFog for enterprise customers works in the context of device risk posed in the typical business environment. The ransomware problem that exists for most enterprise is used to illustrate the product in action. We also review how their solution supports the growing needs of the modern managed security service provider.

HOW DOES BLACKFOG ENTERPRISE WORK?

The BlackFog Enterprise product is a comprehensive solution designed to implement ADX for enterprise buyers. At the heart of BlackFog Enterprise is its on-device agent, which goes beyond traditional antivirus and Endpoint Detection and Response (EDR) solutions. As explained above, ADX focuses on preventing unauthorized data from leaving devices, a critical aspect in modern cybersecurity.

This commercial solution works by monitoring data exfiltration from any network to ensure data security and regulatory compliance. The product offers a proactive approach to cybersecurity, using AI based algorithms to identify unusual behavior and the unauthorized removal of data from devices and networks.

The product emphasizes on-device data privacy and security. It protects endpoint devices by investigating outgoing data on endpoint devices, providing a more streamlined and less intrusive approach than traditional methods like firewalls or Data Loss Prevention (DLP). This makes it effective even for mobile devices and remote work environments, securing data directly on the devices without relying solely on network-based protections.

HOW DOES BLACKFOG ADDRESS RANSOMWARE?

Unlike most enterprise solutions which aim to restore and recover after an attack, BlackFog addresses ransomware by focusing on prevention. Certainly, no organization should ignore the importance of having shift-right controls to deal with the outages and disruptions that come with a ransomware attack, but this should not become the primary goal of a comprehensive security posture.

It is important to understand that ransomware typically has two objectives. The first and most well-known involves essentially freezing the ability of an organization to operate due to encrypted files. While less prevalent than in the early days of ransomware, it still occurs with some ransomware variants, which increasingly resemble nation-state advanced persistent threats. ADX is effective in reducing this risk.

Since ADX focuses on prevention and the shift-left paradigm, it provides significant synergies with existing technologies that focus on detection and response and makes them more effective.

The second objective of many ransomware campaigns involves real data theft. Such data exfiltration occurs in approximately 92% of all attacks. While less well-known by many business leaders, it has become the main challenge in fighting new threats. With most ransomware gangs now utilizing AI to both target and create new threat vectors, the stakes have never been higher. ADX specifically targets these zero-day exploits and data exfiltration directly at the source, and on the device itself.

HOW CAN MANAGED SERVICE PROVIDERS UTILIZE BLACKFOG?

Increasingly, businesses are relying on their managed service providers (MSPs) to deliver an extended range of security services. This is particularly true down-market for smaller companies who might not have a large staff of IT and security support staff to tend to the day-to-day needs of the organization. Managed services are a powerful option here – and BlackFog partners with the best MSPs to provide such coverage.

More recently, we've seen at TAG a shift from just smaller companies using MSPs for cybersecurity toward mid-sized and even much larger companies outsourcing security protection. Since the BlackFog ADX solution is preventive, we believe it is especially well-suited to larger organizations using MSPs for augmented security. Interested readers should contact BlackFog (see [link below](#)) to learn more of its MSP partnerships.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.



HOW ADX IS IMPLEMENTED BY BLACKFOG

It is key for enterprise security teams to understand how ADX differs from traditional data loss prevention (DLP) because most security groups have tended to rely on this method for their data security. Most DLP solutions exhibit many cost, functional, and security-related drawbacks that often prevent successful implementations.

HOW IS ADX IMPLEMENTED ON THE DEVICE?

BlackFog's ADX works by focusing specifically on outbound data packets at level 3 of the OSI stack. As such, the solution works at the packet level to obtain information about the source and destination of the datagrams. Using AI across dozens of parameters, the BlackFog product determines the legitimacy of the packets and therefore whether or not they are permitted to leave the device.

For example, if a packet originates from some system process that does NOT have networking capability, then it has a high confidence level that the process is hijacked and should be stopped. In addition, if a packet is exfiltrating data to the dark web, then it's probably doing something unacceptable. Similarly, the product can geofence data and determine when data is traveling to unauthorized destinations such as Russia or China, telltale signs of many ransomware attacks.

HOW IS ADX DIFFERENT THAN TRADITIONAL DLP?

These rules are applied on every packet using an AI-based algorithms, such as behavioral analysis to stop data exfiltration. It is important to point out here that this is quite different from the way traditional data loss prevention (DLP) works. Recall that most DLP solutions work at the edge of the enterprise network much like a firewall and typically involve a hardware device that must be capable of processing large volumes of data.

Using AI across dozens of parameters, the BlackFog product determines the legitimacy of the packets and therefore whether or not they are permitted to leave the device.

As a result, DLP platforms can be expensive. In addition, all packets must flow through the checkpoint, which means that DLP is only useful behind a corporate firewall and not very useful in today's hybrid workforce environment where everyone works from home, or on the road. Second, many DLP solutions are designed to inspect packets, decrypt them (since most traffic is effectively SSL), which can breach the end-to-end trust of a certificate.

Finally, DLP operates on the principle of data classification. That is, once the packet has been decrypted, it looks inside to see if there are tagged documents or elements. Addressing such an issue requires, of course, the ability to constantly tag documents internally. This can be virtually impossible from a resource perspective for most organizations with their high volume of documents and other types of files created on a daily basis.

WHAT IS THE BLACKFOG APPROACH?

BlackFog has taken the view that the traditional approach to DLP is just not feasible for most enterprise teams and designed ADX as a practical solution to all these problems. It uses real time network and process-based AI detection and analysis to provide anti data exfiltration with no human intervention.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.

Click [here](#) for more information on the specifics and technical details of how BlackFog helps enterprise teams implement and enforce security policies using ADX.



AN ADX ACTION PLAN FOR ENTERPRISE

In this book we have emphasized the benefits of ADX and have explained how commercial solution provider BlackFog effectively implements and supports this important on-device protection approach. That said, the only means by which such concepts can be practically useful is through an action plan with the commitment to deploy and support the approach.

In this chapter we make some recommendations for how a team might begin to develop an action plan to move forward with ADX. We understand that every organization will necessarily have a different local approach, but we hope that our general comments below can be applicable to a wide range of different projects plans for organizations of various sizes and business scenarios.

HOW DOES AN ORGANIZATION PREPARE FOR ADX?

The good news for any team considering deployment of ADX into their enterprise, and using BlackFog in particular, is that the options to either overlay, complement, or replace existing solutions is available. Despite limitations of traditional data loss prevention (DLP) solutions, nothing precludes an organization from combining on-device ADX agents with existing approaches.

That said, it is a good idea to address the relevant security control requirements that will exist locally. Our experience at TAG suggests that these can be based on the need to (1) reduce threat, perhaps after an incident, (2) address compliance demands often from major customers with supply chain requirements, or (3) lower the cost of existing solutions as a result of financial and budget challenges. These should be reviewed in advance of any ADX deployment.

Despite limitations of traditional data loss prevention (DLP) solutions, nothing precludes an organization from combining on-device ADX agents with existing approaches.

WHAT PROCESS CAN BE USED TO DEPLOY ADX?

The deployment of ADX to the endpoint devices can make use of any existing processes or tools for pushing agent software to targeted devices. Enterprise customers working with BlackFog can and should discuss any unique requirements that might exist locally to determine the best means for implementation.

Our experience at TAG is that deployments to endpoints do require up-front planning with the commercial vendor. Certainly, once a process has been identified and tested, scaled installation should be the goal. A unique advantage of the BlackFog agent is that it is auto updating. Once the initial deployment has been performed future updates are done automatically and can be controlled directly within the main console. This also includes the ability for MSP's to uniquely apply specific settings based on organization and group as required.

HOW CAN TAG ASSIST WITH ADX PLANNING?

As always, the TAG research and advisory team is always available to help with any projects that include technology such as ADX and products such as BlackFog. While we are not hands-on administrators, we can offer guidance, insight, and recommendations to help ensure that your ADX implementation project is not only successful, but that it future proofs your team from many types of new and emerging threats.

ABOUT BLACKFOG

BlackFog is the leader in on-device data privacy, data security and ransomware prevention. Its behavioral analysis and anti data exfiltration (ADX) technology stops hackers before they even get started. The company's cyberthreat prevention software prevents ransomware, spyware, malware, phishing, unauthorized data collection and profiling and mitigates the risks associated with data breaches and insider threats. BlackFog blocks threats across mobile and desktop endpoints, protecting organizations data and privacy, and strengthening regulatory compliance.

ABOUT TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to provide on demand insights, guidance, and recommendations to enterprise teams, government agencies, and commercial vendors in cybersecurity, artificial intelligence, and climate science.

USING ANTI DATA EXFILTRATION (ADX) TO STOP RANSOMWARE AND OTHER THREATS TO DATA



TAG

