



CONTROLLING INFORMATION FLOW THROUGH NETWORKS:

EVOLVING FROM THE DATA LOSS PREVENTION MODEL

www.blackfog.com

The ability to protect data flow through networks has changed radically in order to counter today's threats.

CONTENTS

4 The Data Loss Prevention Model Explained

5 Limitations to the Data Loss Prevention Model

1. DLP Is Not User-Centric
2. Traditional DLP Solutions are Expensive to Run and Operate
3. DLP Technology Can Break SSL Functionality

7 Modern Cyberattacks Exploit Weaknesses in the DLP Model

1. Supply Chain Attacks – Accellion
2. Cloud Misconfiguration – LA Times Cryptojacking
3. Remote Employee Access – Shadow IT

10 Data Exfiltration Protection Provides Next-Generation Cyber Defense

How ADX Works

ADX Compared to Other Modern Cybersecurity Solutions

12 Detecting Intent: Behavioral Analysis Ensures Best-in-Class Cybersecurity

13 Face Today's Greatest Threats Using Tomorrow's Technology

The ability to control the way information flows through networks is a critical part of security infrastructure.

There are multiple reasons why this degree of control is so valuable. It represents the most direct way to protect personally identifiable data, secure intellectual properties, and gain visibility into the overall effectiveness of the organization's security approach.

Protecting this data of key importance in today's environment because of the security landscape that most organizations have to navigate when creating value for users.



If your organization collects personally identifiable information (PII), protected health information (PHI), or payment card information (PCI), then you probably have to follow strict rules about how you gather, store, and communicate that data within the enterprise.



If your success depends on trade secrets or other intellectual properties, then controlling the flow of information through your network is vital. At least part of the value that your organization generates is pure information – you have a clear incentive to protect it from unauthorized access.



If you cannot track how data is moving throughout the organization, meaningfully securing that data is near-impossible. In order to identify unauthorized users, you must establish a governance system that indicates who should have access to what data, and why.

Organizations have spent years developing and implementing different solutions for keeping sensitive data secure. For years, the Data Loss Prevention (DLP) model has been one of the most popular approaches for addressing these security pain points.

THE DATA LOSS PREVENTION MODEL EXPLAINED

Traditional DLP approaches combine a variety of data security measures into a unified network edge solution. Individual technologies can vary between vendors, but it's typical for DLP solutions to implement signature matching, structured data fingerprinting, and file tagging alongside other technologies like intrusion detection and firewalls.



**Signature
Matching**



**Structured Data
Fingerprinting**



File Tagging



**Intrusion
Detection**



Firewalls

These solutions typically activate on the edge of the network, giving them a clear line-of-sight towards incoming and outgoing data. This enables the system to analyze content, identify the presence of sensitive data, and put protections in place automatically.

These protections may include blocking the transmission attempt, encrypting the information, or verifying the transfer of information with an administrator. Importantly, these security failsafes trigger automatically whenever protected data is accessed or shared.

This makes DLP a data-centric approach. It does not distinguish between different users, identify user intent, or understand the context behind data transmission and communication. It simply acts in accordance with a strict set of policies designed to limit the ability for unauthorized users to compromise sensitive data.

LIMITATIONS TO THE DATA LOSS PREVENTION MODEL

For years, DLP solutions have helped organizations reduce the risk of transmitting sensitive data through unauthorized channels, but the cybersecurity threat landscape is changing. Cybercriminals leverage different technologies, exploit different attack vectors, and have different incentives than they did only a few short years ago.

As a result, DLP technology now struggles to accommodate some of the challenges that organizations face in today's environment.

1 DLP Is Not User-Centric

Network-based DLP solutions do not discriminate between users who have the same level of access. This makes it difficult for them to detect anomalous behaviors by trusted users. If an attacker compromises a privileged user account, the entire DLP system is then subject to manipulation.

Since DLP does not discriminate between users, it cannot detect the difference between malicious behavior, social manipulation, and unintentional mistakes. Analyzing user actions and identifying suspicious behaviors is outside the scope of a traditional network DLP.

This is a problem in today's threat landscape because modern attacks are predicated on the ability to communicate with third-party servers to steal data. This is how hackers compromised numerous US government databases by funnelling an attack through [networking vendor SolarWinds in 2020](#).

Third-party and supply chain attacks are becoming increasingly frequent, and DLP isn't sufficient to prevent them. This requires a new architectural approach that does not automatically extend trust to third-party partners and privileged users.

2 Traditional DLP Solutions are Expensive to Run and Operate

According to a [ComputerWeekly survey](#), 32% of respondents claim DLP technology is too expensive to implement. This is partly because of the way DLP solutions work. The design of a DLP solution requires it to sit at the edge of the network and decrypt all incoming and outgoing traffic. This is a technically demanding exercise that requires a great deal of computing resources to carry out. Even a small organization will require a DLP solution capable of quickly processing billions of data packets every second.

Deploying DLP in a comprehensive manner requires constant maintenance. Every time the organization undertakes a new project, onboards a new client, or hires a new employee, the security team must update DLP policies to match. DLP software will then generate reams of reports and alerts that require a security response. This puts a strain on security talent, who must spend the majority of their time processing these events.

3 DLP Technology Can Break SSL Functionality

The point of SSL technology is to ensure that web traffic enjoys end-to-end security encryption. Creating a uniquely encrypted channel for private communication over the public Internet is a ground-level foundation for digital privacy and security. Only clients and issuers who have successfully completed the SSL handshake can be sure of message privacy, integrity, and security.

When a DLP solution operates on the edge of a network and verifies all incoming and outgoing traffic for the presence of sensitive data, it necessarily breaks SSL functionality. The DLP software acts as a man-in-the-middle, decrypting traffic, verifying its contents, and re-encrypting it.

This means that your DLP is essentially terminating the HTTPS connection itself, issuing its own certificate to impersonate the domain, and then creating a new HTTPS connection to relay the traffic after it's finished.

The entire process is signature-based, which means the system cannot offer any contextual data about the reason why a specific executable file might be included in an outgoing email, or why a certain .zip file is being downloaded. It merely blocks any files that fit its policy descriptions.

In a worst-case scenario, the process of resigning the browser's [Certificate Authority and Public Key data](#) can confer more trust than it should. The user would never know any better, because users do not see the intended certificate – they only see the internal certificate provided by the DPI.

MODERN CYBERATTACKS EXPLOIT WEAKNESSES IN THE DLP MODEL

Over-reliance on third-party vendors and servers is a hallmark of today's cybersecurity landscape. Over the past few years, outsourcing has gone from a value-protecting tactic to a value-generating business strategy. Yet only [35 percent](#) of organizations contractually enforce data risk and security protocols with third-party vendors.

The increasing complexity of enterprise supply chains, the challenges of configuring cloud-hosted services, and the additional burden of securing remote workers are critical obstacles to the way DLP drives cybersecurity value.

Organizations with comprehensive DLP solutions in place have suffered debilitating cyberattacks due to each of these three obstacles.

1 Supply Chain Attacks - Accellion

Accellion's soon-to-be-retired legacy file transfer appliance service found itself the victim of a debilitating data breach in [December 2020](#). Royal Dutch Shell, the Royal Bank of New Zealand, and multiple US universities all reported massive data theft in the following months. Personal data, including the Social Security numbers of US citizens, were exfiltrated from Accellion's servers.

Accellion has more than 3000 customers, which include large enterprises, government agencies, and public health institutions. All of these organizations now face the risk of data exploitation and ransom.

The attack itself was carried out via SQL injection. This allowed hackers to execute command-line requests through a local web service call, leading to a [server-side request forgery](#) attack allowing for full control of Accellion data through POST requests.

Supply chain attacks like this one bypass DLP solutions because the attack itself is not carried out on the network. The attack leveraged zero-day vulnerabilities in a third-party file transfer service. The attack's victims had given Accellion's software privileged access to their own records.

A DLP system would have flagged the transfer of sensitive data as unusual. But since the data was traveling to a trusted third-party service, it didn't look significantly different from normal network traffic. If a security alert ever showed up, it was probably dismissed as a false positive. Without behavioral analytics, there is no way to tell the difference.

2 Cloud Misconfiguration - LA Times Cryptojacking

The proliferation of cloud services has serious implications for the future of enterprise cybersecurity. [77% of enterprises](#) have at least one application in the cloud, and 60% use cloud technology to store confidential data.

Cloud computing offers significant efficiency, productivity, and security advantages to organizations. But in order to make the most of those advantages, IT leaders need to guarantee their cloud-enabled systems are appropriately configured. [User-level misconfiguration](#) is the biggest cloud security risk in today's business environment, enabling cyberattacks and data breaches in one of three ways:



Misconfiguration of the native cloud environment.



Unequal distribution of security resources among multi-cloud environments.



Mismatched security compared to on-premises computing assets.

Since cloud computing resources are not located inside the network, DLP software solutions cannot effectively secure cloud-hosted data. Instead, they attempt to identify sensitive data in transit to cloud-hosted servers, and flag confidential data according to their configuration policy.

But when cloud-hosted computing resources are misconfigured, it's much easier for sensitive data and login credentials to fall through the cracks. The widespread use of Amazon S3 offers a compelling example.

While Amazon's Simple Storage Service offers robust security protection to users, it must be properly configured. Research shows that as of June 2021, improperly configured AWS permissions expose [42% of organizations'](#) Amazon S3 buckets on average. This allows hackers to mount cross-account attacks that data loss prevention solutions cannot defend against.

One well-known victim of this attack vector is the Los Angeles Times. The newspaper hosted its homicide section on an AWS S3 bucket with public write access. An attacker loaded a [cryptocurrency miner to the website's javascript code](#), exploiting every visitor to the popular news website.

3 Remote Employee Access - Shadow IT

According to [Cisco](#), 80% of employees use software that has not been cleared by the company's IT department. Shadow IT refers to the use of unapproved IT resources to complete daily tasks. It presents a difficult challenge for enterprise security teams that rely on DLP technology to secure sensitive data.

When employees use hardware and software without the IT departments' knowledge, edge network security solutions like DLP no longer produce results. Users are inadvertently exposing themselves and their organizations to security risks by using unapproved devices and software.

At the same time, employees continually demand greater IT agility. When IT departments fail to live up to employee expectations, Shadow IT begins to take form.

Only 8% of all enterprises actually know the extent of shadow IT in their organization. These employee shortcuts are prevalent in every sector and industry, in almost every territory – it's one of the most widespread and underreported security risks in the modern enterprise, and the trend towards remote work has only made it bigger.

DLP solutions are not designed to secure endpoint devices. This makes it near-impossible for them to meaningfully analyze traffic outside of the corporate network. In a remote work environment, the vast majority of privileged user traffic is coming from outside the network, on a wide array of personal user devices without endpoint security protection.

According to an [IBM-sponsored study](#), one out of every five organizations has suffered a cyberattack due to Shadow IT. This is how attackers defrauded Insight Global, an IT management and staffing firm working for the Pennsylvania Department of Health, in April 2021.

Insight Global's official COVID-19 tracking database had robust internal security measures in place. Employees found these systems difficult to use, so they set up alternative Google accounts to share contact-tracing information with one another. The health records of 72,000 Pennsylvania residents' data was exfiltrated, and Global Insights found itself the target of a [multi-million dollar lawsuit](#).

DATA EXFILTRATION PROTECTION PROVIDES NEXT-GENERATION CYBER DEFENSE

Data Exfiltration Protection (ADX) improves on the approach that DLP originally pioneered. An organization's data is its most valuable asset, and all cyberattacks work by exfiltrating unauthorized data in some way.

The problem is not one that a series of data-centric policies can resolve. Instead, organizations have begun to take a more holistic approach to preventing the exfiltration of sensitive data.

Simply infiltrating a network or a device does not make a successful cyberattack. The attack is only successful if sensitive data is stolen from the network. Without data exfiltration, there is no data loss, no data breach, and no data ransom.

How ADX Works

ADX works by investigating outgoing data on endpoint devices. This gives it a markedly smaller footprint than DLP, which examines incoming and outgoing traffic at the network edge. ADX solutions are lightweight enough to run on mobile devices and does not need to work on the corporate network.

Instead of comparing traffic to a dictionary of attack signatures, ADX solutions use behavioral analytics to identify unusual behaviors on a user-centric basis.

Cybercriminal malware applications do not act the same way legitimate users do. They scan for ports, exchange keys with foreign servers, and move laterally through networks in ways that regular users don't. Targeting them through their behaviors makes much more sense than simply locking sensitive data behind a barrier.

The one thing that all cybercriminals do is send sensitive data outside the network. ADX limits the ability for users – including privileged users and administrators – to send sensitive data outside the network. This makes it a next-generation solution that builds on the technology behind Data Loss Prevention while making it relevant to today's security threats.

ADX Compared to Other Modern Cybersecurity Solutions

Most organizations rely on a combination of virtual private networks (VPNs) and antivirus products to secure remote workers against cyberattack. These solutions are not sufficient for preventing some of the most common security threats.



VPNs provide some degree of anonymity to users connecting to corporate networks, but do not prevent malware or mitigate the risk of ransomware. They do not prevent the exfiltration of data to external resources. The [Meow attacks](#) are an excellent example of cyberattacks that specifically target VPN sessions and tokens, destroying valuable databases and leaving only the word "meow" in their place.



Anti-Virus solutions are historically among the first lines of defense against cyberattack. These applications work by comparing local files with known attack signatures. The problem is that more than two-thirds of all cyberattacks use [fileless techniques](#). With a fileless exploit, there is nothing for the anti-virus to inspect.

users, privileged employees, and cyberattackers. Insider threats can be as dangerous as external actors, but they all need to exfiltrate data in order to be effective.

Neither VPNs nor Anti-Virus solutions can effectively prevent malicious actors from compromising Remote Desktop Protocols. Yet RPD compromise has risen to become the most common attack vector in the first quarter of 2021.

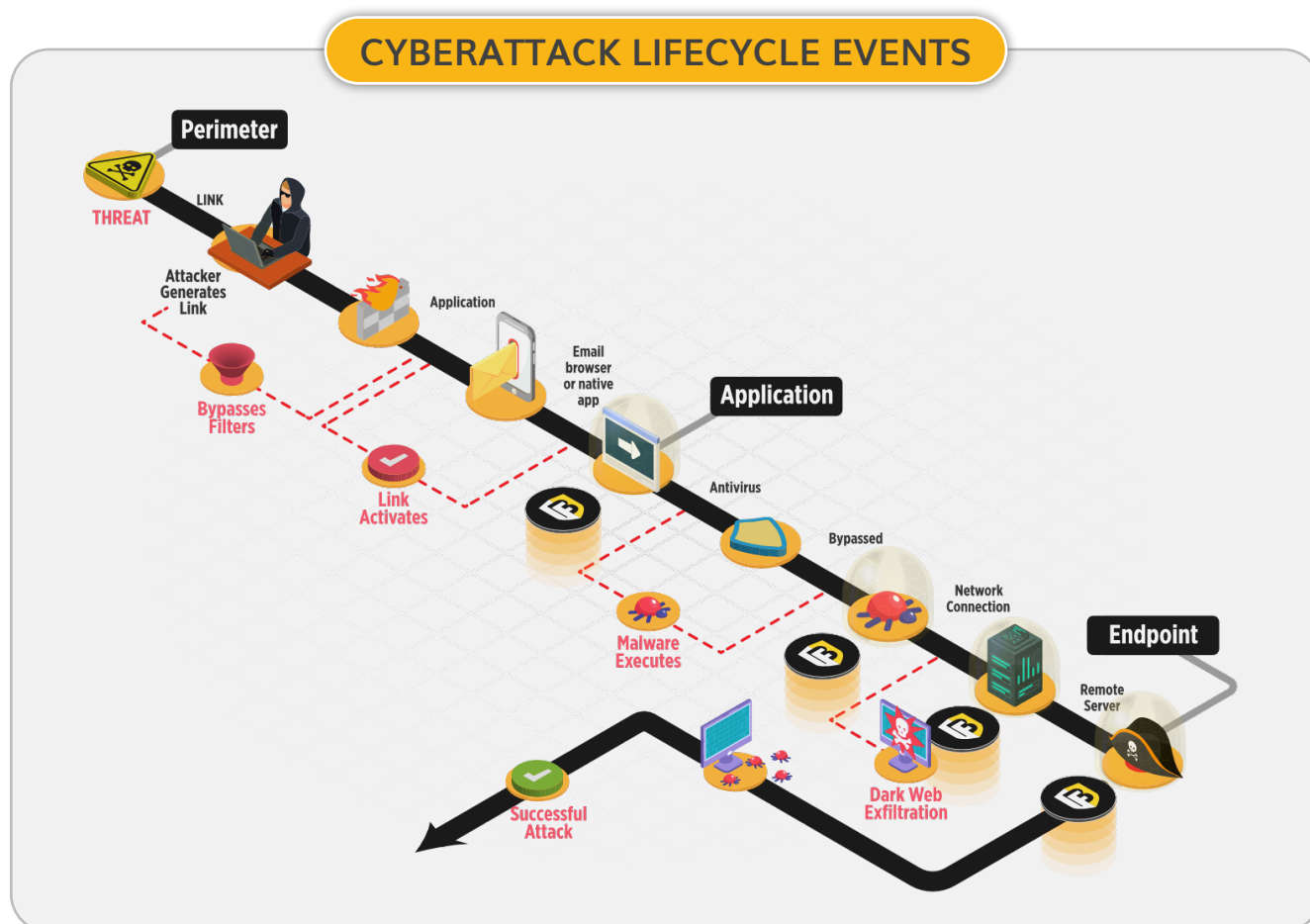


DETECTING INTENT: BEHAVIORAL ANALYSIS ENSURES BEST-IN-CLASS CYBERSECURITY

The ability to monitor and analyze user behaviors is a critical element of the ADX approach. The point of cybercrime and state-sponsored cyberwarfare is to steal information. Hackers who cannot communicate with command and control servers or transmit stolen data outside a network cannot meaningfully execute an attack.

Behavioral analysis is a critical component of data exfiltration protection. It prevents malware from isolating code in the network, preventing the loss of data and mitigating lateral spread to other devices within the network.

By focusing on these tell-tale signs of malicious cybercriminal activity, ADX reduces false positives and allows legitimate users to enjoy unfettered access to corporate data, assets, and applications. There are multiple points in the lifetime of a typical cyberattack where using behavioral data to detect intent can stop the attack by preventing the exfiltration of data.



- Threats at the **Perimeter stage** may use stolen credentials to access privileged user accounts. However, every user account has a unique behavioral profile that aligns with typical usage. Identifying users doing suspicious things in real-time can trigger valuable data exfiltration protection measures automatically.
- Threats at the **Application stage** can bypass antivirus protocols using fileless transfer. However, malware will need to send data to a command and control server in order to begin the fileless transfer process – otherwise, the server does not know where to send its malicious package.
- Threats at the **Endpoint stage** will attempt to exfiltrate sensitive records directly to a hacker-controlled destination. This is the point when an infiltration transforms into a data breach. If the attacker cannot receive sensitive data from a protected endpoint, the attack fails.

FACE TODAY'S GREATEST THREATS USING TOMORROW'S TECHNOLOGY

Data loss prevention gave cybersecurity professionals a critical insight into the nature of cybercrime. Securing sensitive data against misuse is key to preventing devastating cyberattacks in their tracks. This remains true today, but the process of securing that data has changed along with the cybersecurity landscape enterprise IT teams have to navigate.

Data Exfiltration Protection is the next step in cybersecurity technology. It provides organizations with a powerful set of behavioral analytics tools that reliably interrupt cyberattacks, mitigate ransomware attempts, and stop insider threats before they have a chance to succeed. Make ADX part of your enterprise security solution and protect your users' data from exploitation now.



www.blackfog.com