Osterman Research

WHITE PAPER

White Paper by Osterman Research
Published **October 2021**
Sponsored by **BlackFog**

Preventing Data Exfiltration: Introducing Anti-Data Exfiltration (ADX)

Executive Summary

Data exfiltration is a significant threat to organizations and is implicated in many types of cybersecurity incidents. For example, ransomware gangs use both encryption that causes operational disruption for the victim and the threat of exposing exfiltrated data if the ransom demand is not paid. Preventing data exfiltration remains a weakness for many organizations, despite having a complex set of cybersecurity tools already, including data loss prevention (DLP) solutions. A new approach is needed to stop the threat and consequential damage of data exfiltration. In this white paper, we report on a survey on data exfiltration and introduce the category of Anti-Data Exfiltration (ADX) cybersecurity solutions.

KEY TAKEAWAYS

The key takeaways from this research are:

- **Data exfiltration is a significant threat**
  Organizations report that preventing data exfiltration is increasingly important and affected by several wider trends, such as high-profile ransomware incidents involving double or triple extortion tactics.
- **Despite having many cybersecurity tools, data exfiltration is still happening**
  Eighty percent of organizations are currently using up to 10 separate cybersecurity solutions, and larger organizations often have more. Despite having these protections in place, organizations are still facing a range of security incidents each year that include data exfiltration.
- **Organizations are not confident they can stop data exfiltration**
  Most organizations do not believe their current protections can stop data exfiltration, prevent insiders from exfiltrating data, or prevent ransomware attacks, among other areas of concern.
- **Data loss prevention (DLP) tools are not working**
  Most respondents indicate that DLP tools are not working at their organization as a means of preventing data exfiltration: DLP is difficult to configure and challenging to maintain, and still does not prevent data exfiltration.
- **Something new is needed to stop data exfiltration**
  Despite the list of current cybersecurity solutions in place today, and since DLP solutions are proving ineffective at stopping data exfiltration, something new is needed to protect organizations from the data exfiltration threat.
- **Introducing Anti-Data Exfiltration (ADX) for on-device protection**
  Anti-Data Exfiltration (ADX) provides a new approach for keeping sensitive data secure. ADX controls the way information flows through networks and offers the most direct way of protecting personal information, securing intellectual property, and disrupting the attack chains used in cyberattacks.

Most organizations do not believe their current protections can stop data exfiltration.

ABOUT THE SURVEY AND WHITE PAPER

Osterman Research conducted a primary market survey of 255 organizations in the United States with a minimum of 250 employees. The 255 respondents were CIOs, IT managers, CISOs, security managers, or cybersecurity professionals. All respondents were familiar with how their organization protected against data exfiltration. The survey and this white paper were sponsored by BlackFog; information about the company is provided at the end of the paper.

The Threat of Data Exfiltration

Data exfiltration is a significant threat to organizations. In this section, we examine the different ways this threat is felt.

DATA EXFILTRATION IS IMPLICATED IN CYBERSECURITY INCIDENTS

The exfiltration of personally identifiable information, intellectual property, classified information, and other sensitive information is widely implicated in several types of cybersecurity, cyber warfare, and cyber espionage incidents. For example:

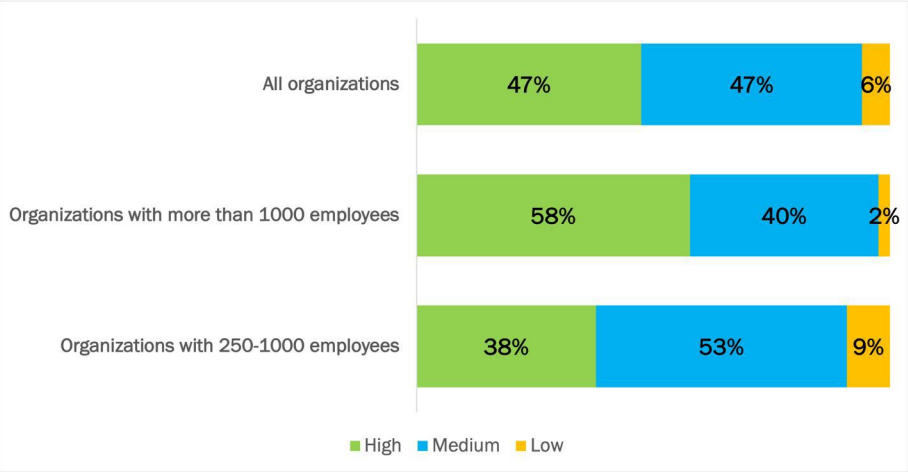
- **Double and triple extortion ransomware attacks rely on data exfiltration** Early ransomware attacks predicated on the assumption that operational disruption would be enough to force the victim to pay the ransom demand proved ineffective. Ransomware gangs now seek to exfiltrate sensitive data to use in multi-level extortion threats against the victim or affected individuals to sell or publish their data. Although backups may restore systems encrypted in a ransomware attack, they offer no ability to recover exfiltrated data.
- **Unintentional insider mistakes and malicious insider threats** Insiders frequently cause data exfiltration incidents. Some incidents are accidental, such as sending a spreadsheet with sensitive data to the wrong recipient. Other incidents are malicious when an insider seeks to steal data.
- **Phishing attacks, credential compromise, keyloggers, financial sabotage** Various flavors of phishing attacks seek to steal account credentials as the first step in data exfiltration, deploy malware for keylogging or crypto mining, and inflict financial sabotage by redirecting payments to malicious bank accounts.

Data exfiltration is the common theme in ransomware attacks, insider incidents, and other types of cyberattack.

PREVENTING DATA EXFILTRATION IS A HIGH PRIORITY

Preventing data exfiltration is ranked as a high or medium priority at most organizations in comparison to all other security priorities. See Figure 1.

Figure 1
Priority of Preventing Data Exfiltration Compared with All Other Security Priorities
Percentage of respondents

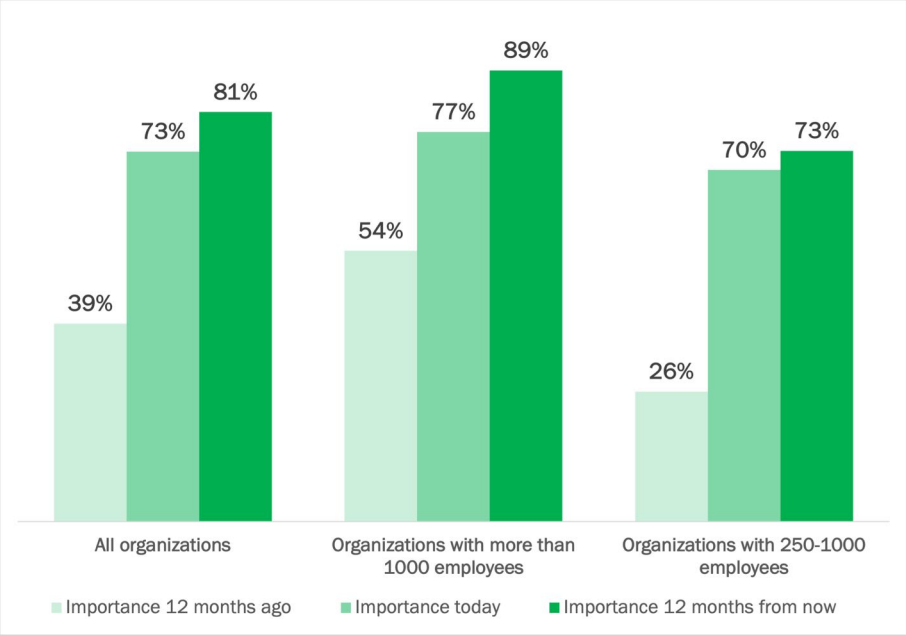


Source: Osterman Research (2021)

PREVENTING DATA EXFILTRATION IS GROWING IN IMPORTANCE

Organizations see preventing data exfiltration as increasingly important year on year. For all organizations on average, the current level of importance (73%) is roughly twice as important compared with 12 months ago (39%). See Figure 2.

Figure 2
Importance of Preventing Data Exfiltration over Three Time Horizons
Percentage of respondents indicating "very important" and "extremely important"



Source: Osterman Research (2021)

Preventing data exfiltration is increasingly important to organizations.

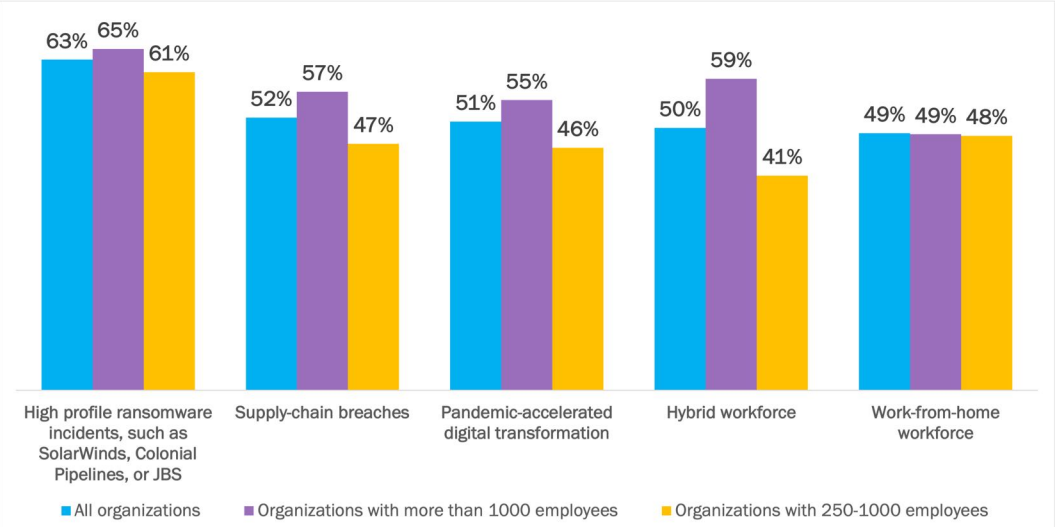
In looking at the data:

- **Large organizations see higher importance**
  Large organizations indicated the highest initial (54%), current (77%), and forecasted (89%) levels of importance for preventing data exfiltration. The task of preventing data exfiltration at larger organizations is difficult due to sheer numbers and the expanded attack surface made up of people, endpoints, applications, and supply chain partners. Large organizations are also likely to face higher costs of data exfiltration under data protection regulations in the form of regulatory penalties, e.g., the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). For example, through early September 2021, there have been 766 fines levied under the GDPR totaling €1.28 billion (US$1.51 billion) in the less than 41 months since the law took effect.
- **Preventing data exfiltration has recently become much more important for smaller organizations**
  Respondents at smaller organizations reported the highest growth rate in the importance of preventing data exfiltration from 12 months ago to today (270%). This growth rate was almost twice as high as the growth rate for larger organizations (142%) and puts organizations in both size groupings within 10% of each other for the rating of current importance.

WIDER TRENDS COMPOUND THE THREAT OF DATA EXFILTRATION

Numerous trends compound the threat of data exfiltration, with high-profile ransomware incidents (63%), supply chain breaches (52%), and pandemic-accelerated digital transformation (51%) the top three trends. See Figure 3.

Figure 3
How Wider Trends Impact Concerns About Ransomware and Data Exfiltration
Percentage of respondents indicating "very impactful" and "extremely impactful"



Source: Osterman Research (2021)

In looking at the data:

- **Large organizations experience higher impact**
  The impact of each trend always steps up in intensity for larger organizations compared with the average, and always steps down for smaller organizations. This finding is consistent with what we would expect to see, due to the added size, complexity, and breadth of the attack surface at larger organizations.
- **High-profile ransomware incidents affect everyone**
  The trend with the greatest impact is high-profile ransomware attacks against critical infrastructure (e.g., Colonial Pipelines) and using compromised supply chain vendors (e.g., SolarWinds, which impacted large organizations and government agencies, and Kaseya, which had a widespread impact on smaller organizations). Either type of ransomware attack gains widespread news coverage and potentially affects everyone.
- **The work-from-home workforce trend was felt uniformly by all**
  Larger and smaller organizations were within 1% for the rating for the work-from-home workforce trend. The shelter-in-place orders in March 2020 to handle the pandemic did not discriminate between organizations based on employee numbers. For smaller organizations, however, this was the second most impactful trend behind high-profile ransomware incidents, whereas it was the least impactful trend for larger organizations. Smaller organizations appear to have lacked easy availability to cybersecurity professionals and toolkits to assure data security with employees working from home. Many larger organizations, on the other hand, were already pursuing remote work initiatives and many of them were better able to adapt to the new paradigm.

Organizations are most concerned about the impact of high-profile ransomware attacks on data exfiltration.

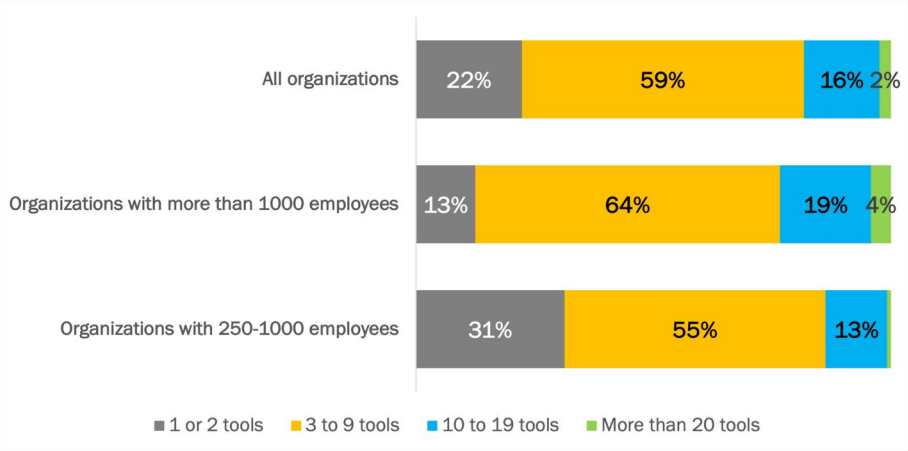
Current Toolsets Are Not Working

Organizations have deployed a range of cybersecurity tools, and yet data exfiltration is still occurring. In this section, we look at the survey findings.

NUMBER OF CYBERSECURITY TOOLS CURRENTLY DEPLOYED

On average, 80% of organizations are currently using up to 10 separate cybersecurity solutions, with large organizations more likely to have a higher number of solutions currently deployed than smaller organizations. See Figure 4.

Figure 4
Number of Cybersecurity Tools Deployed Across the Entire Organization
Percentage of respondents



Source: Osterman Research (2021)

If we group current cybersecurity tools into the four usage bands shown in Figure 4, we can derive a sense of which tools are likely to be used by organizations in each band. For example, as an illustrative (not definitive) grouping of current tools:

- **Organizations using only 1 or 2 tools**
  Anti-virus/anti-spam on devices, plus on-premises backup.
- **3 to 9 tools**
  Everything in the 1 or 2 tools group, plus also tools that offer anti-phishing, anti-ransomware, secure email gateway, secure web gateway, firewall, and multi-factor authentication capabilities, along with security awareness training.
- **10 to 19 tools**
  Both of the previous lists, plus tools such as endpoint protection, threat intelligence, vulnerability analysis, managed security services, data loss prevention (DLP), cloud-based backup, biometric and hardware token authentication, mobile device management, endpoint detection and response or extended detection and response, and a cloud access security broker.
- **More than 20 tools**
  Everything already listed as well as solutions such as managed incident response; security orchestration, automation, and response (SOAR); security ratings services; and external attack surface management tools.

80% of organizations currently use up to 10 separate cybersecurity solutions; large organizations are more likely to use more.

LARGE ORGANIZATIONS HAVE A COMPLEX SET OF CYBERSECURITY TOOLS

More than 80% of large organizations have between 3 and 19 cybersecurity tools currently deployed. By implication, this means:

- **Using many of the best solutions available**
  Organizations using 10 to 19 tools are using most of the best solutions currently available. Once an organization is using more than 15 separate cybersecurity solutions, there is not a lot they do not have currently deployed.
- **A challenge of efficacy, not solution availability**
  As more tools are added to the overall solutions stack, the challenge becomes one of efficacy across the stack, not the mere addition of yet another tool. Adding more tools is easy; leveraging the security protections of individual tools to improve the overall set of outcomes delivered is much more difficult. As more tools are added, it becomes increasingly difficult to manage offerings from different vendors, coordinate patch cycles, deal with inconsistencies, and integrate new offerings with the current stack.
- **Improvement by consolidation**
  Eliminating, replacing, or otherwise reducing the number of disparate solutions in use provides a pathway for larger organizations using a high number of solutions. Finding vendors with solutions that can help consolidate the number of offerings used while delivering higher effectiveness becomes more critical as the number of solutions increases.

Organizations using 10 to 19 tools are using most of the best cybersecurity solutions currently available.

MANY SMALL ORGANIZATIONS LACK BASELINE PROTECTIONS

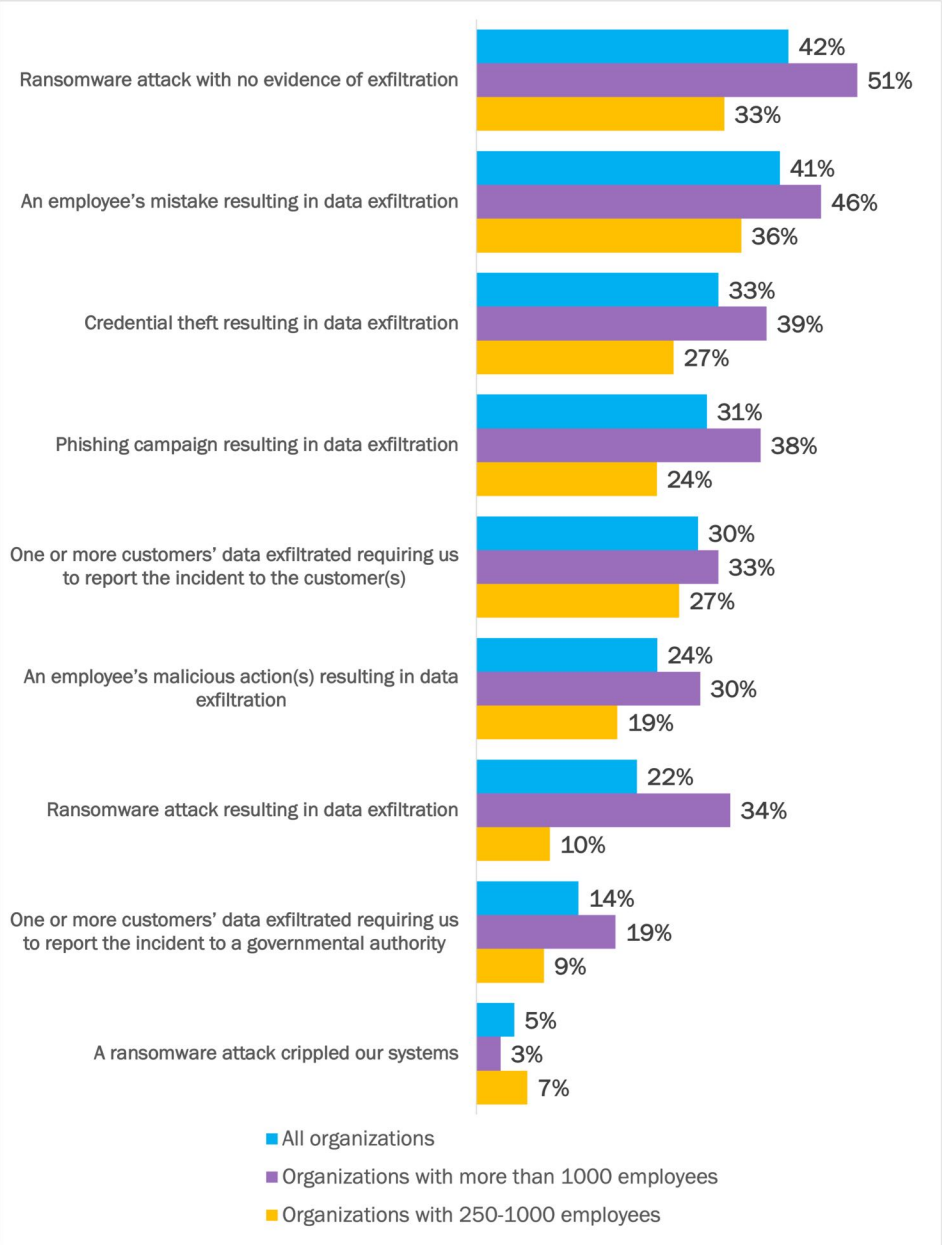
More than 80% of smaller organizations have between 1 and 9 cybersecurity tools currently deployed, with 31% of all smaller organizations currently having only 1 or 2 cybersecurity tools. This may be due to lack of skilled cybersecurity professionals to deploy and configure such solutions, a lack of awareness of what is available, or a perceived lack of need for such capabilities. By implication this means:

- **Lacking essential protections**
  Many smaller organizations lack essential protections against cybersecurity threats. For organizations currently using only 1 or 2 tools, that is most likely to include desktop anti-virus/anti-spam and on-premises backup.
- **Finding the cybersecurity challenge especially daunting**
  The cybersecurity space is challenging for any organization to navigate, but especially smaller ones. With thousands of security vendors offering a plethora of tools, making intelligent choices among these offerings is an especially daunting task for smaller organizations that lack deep cybersecurity experience and large budgets.

AND YET, DATA IS STILL BEING EXFILTRATED

Despite the protections currently in place for larger organizations and likely due to the lack of protections at smaller organizations, a range of security incidents that include data exfiltration are still happening. See Figure 5.

Figure 5
Security Incidents with Data Exfiltration Over the Previous 12 Months
Percentage of respondents experiencing the security incident



Source: Osterman Research (2021)

Except for ransomware attacks that crippled systems, larger organizations were more likely to experience each of the incident types over the past 12 months.

Despite organizations having a wide range of cybersecurity tools currently in use, data is still being exfiltrated.

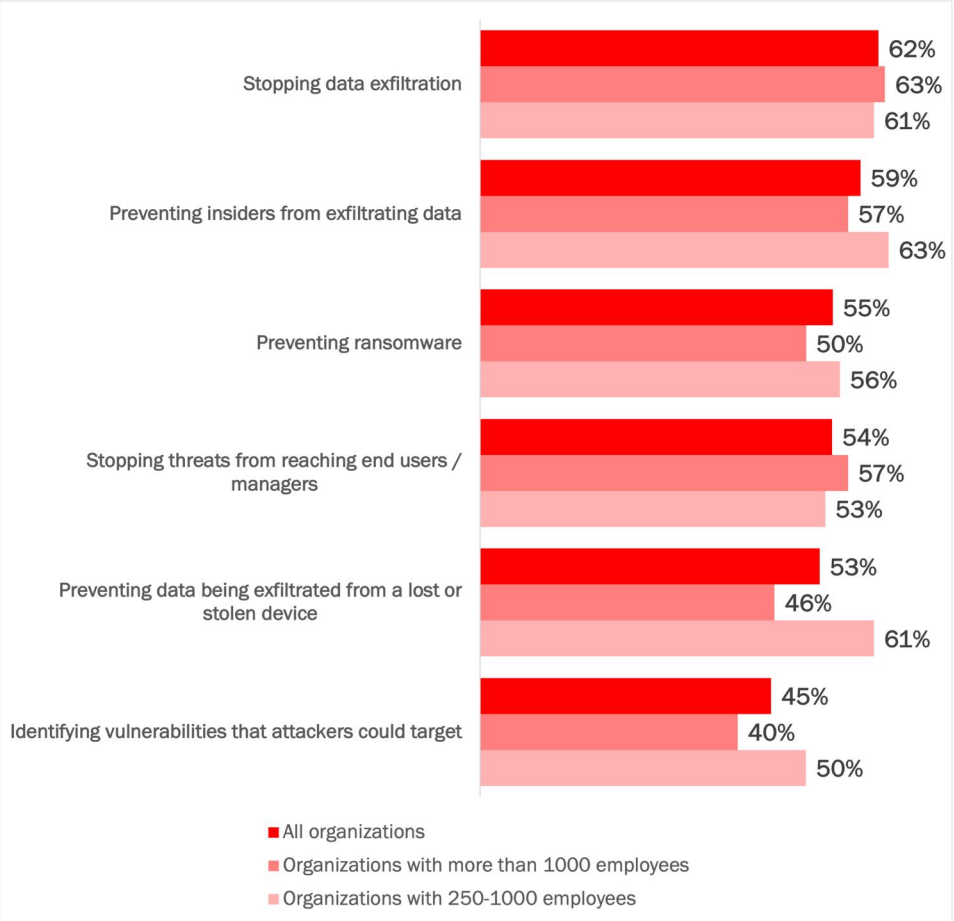
Low Confidence to Prevent Data Exfiltration

Respondents have low confidence in their ability to prevent data exfiltration at their organization. Even though many organizations have deployed DLP to prevent this threat, current DLP solutions are not working. In this section, we look at the data from the survey.

CONFIDENCE IN PROTECTIONS TO PREVENT DATA EXFILTRATION

Most respondents indicate weak levels of confidence that their current cybersecurity protections can achieve a range of outcomes, such as stopping data exfiltration (62% of respondents have weak confidence), preventing insiders from exfiltrating data (59%), and preventing ransomware (55%). The sole outcome for which less than half of respondents had weak confidence was the ability to identify vulnerabilities that attackers could target (45%), which, as the rest of the chart shows, is different from the ability to do something about it. See Figure 6.

Figure 6
Confidence in Current Cybersecurity Protections to Prevent Data Exfiltration
Percentage of respondents indicating weak confidence



Source: Osterman Research (2021)

Respondents believe they can identify vulnerabilities that attackers could target but lack the ability to do anything about it.

LOW CONFIDENCE TO PREVENT DATA EXFILTRATION IN A RANSOMWARE ATTACK

We asked respondents to indicate how confident they are that no data would be exfiltrated if their organization was hit with a ransomware attack "tomorrow." On average, only two out of five respondents were very confident their organization would emerge unscathed (43%). See Figure 7.

Figure 7
Confidence in Protections to Stop Data Exfiltration in a Ransomware Attack
Percentage of respondents (sums to 99% or 101% due to rounding)

Source: Osterman Research (2021)

Ransomware is an especially pernicious form of cyberattack against organizations. It is currently one of the top cybersecurity threats facing governments and commercial organizations. Many of the organizations represented in this study lack strong confidence that they could stop data exfiltration from occurring in a ransomware attack. We have two observations on the answers to this question:

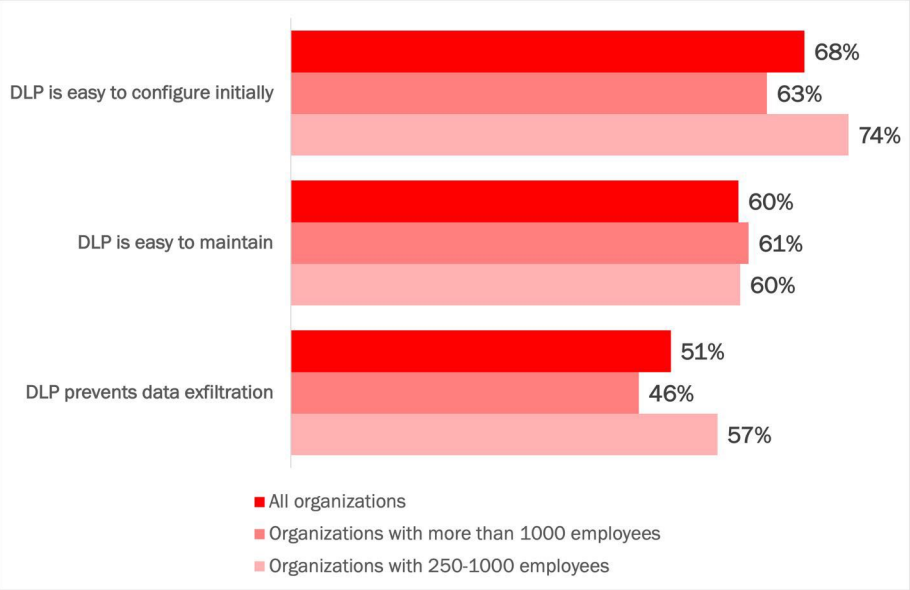
- **Results very similar to how the previous question was answered**
  The results in Figure 7 are very similar to how the "preventing ransomware" incident type in Figure 6 was answered. For all organizations on average and larger organizations the comparative results were within a couple of percentage points. The largest variation was for smaller organizations: 62% "somewhat" and "not at all" confident in Figure 7 compared to 56% in Figure 6.
- **Different answers between larger and smaller organizations**
  More respondents at larger organizations expressed the higher degree of confidence (49%) than respondents at smaller organizations (38%). Overall, more than half of respondents at large organizations expressed the "somewhat" or "not at all" levels of confidence, and more than three out of five at smaller organizations did the same. Larger organizations present more of an opportunity for cybercriminals and must therefore be better prepared than smaller organizations, but for both, the level of confidence is alarming.

Almost three out of five organizations are not confident in their ability to stop data exfiltration in a ransomware attack.

LOW CONFIDENCE THAT DLP CAN PREVENT DATA EXFILTRATION

Data loss prevention (DLP) solutions were introduced more than a decade ago with the intent of detecting potential data exfiltration transmissions and putting a stop to them. Now with widespread availability in cloud platforms such as Microsoft 365, the solution category still gets low scores for achieving this outcome. In our survey, 68% of respondents disagreed that DLP is easy to configure initially, 60% disagreed that DLP is easy to maintain, and 51% disagreed that DLP prevents data exfiltration. See Figure 8.

Figure 8
Ranking the Efficacy of Data Loss Prevention (DLP)
Percentage of respondents indicating weak efficacy



Source: Osterman Research (2021)

Respondents disagree that DLP is easy to configure and easy to maintain, and most say DLP cannot prevent data exfiltration.

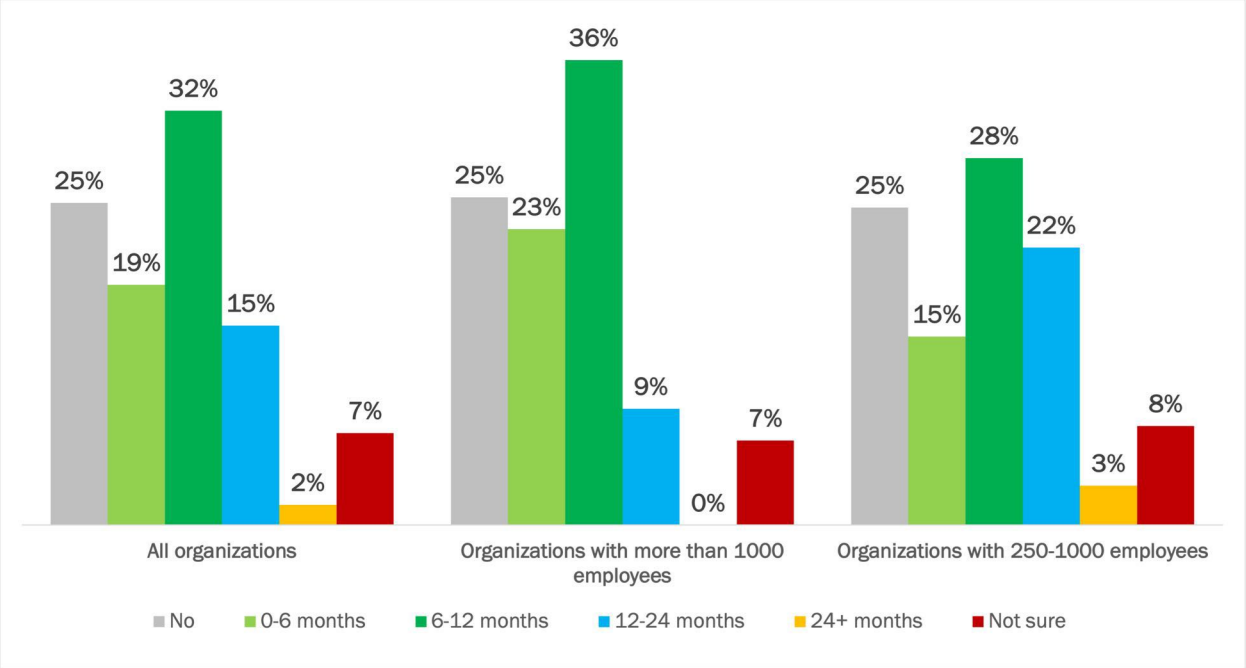
DLP solutions generally require:

- **Configuration of policies to match against data events**
  Policies must be created for identifying sensitive data in motion (e.g., sent by email) and data at rest (e.g., a document stored on a device, file server, or in SharePoint). Policies are required for each type of sensitive data. Organizations require a complex set of policies to capture each type of data loss event.
- **Policies that can match different types of data events**
  The quality of a DLP policy rests entirely on its ability to match policy conditions against different content types, such as email messages and documents. For example, a policy looking for credit card numbers must be able to distinguish credit card numbers from any 16-digit number string.
- **Adaptive designs to handle encryption and deliberate obfuscation attempts**
  Encrypted data is invisible to DLP policies, unless the DLP engine decrypts the data to analyze the document or message to identify a match. Such DLP decryption breaks the security chain and is thus effectively a man-in-the-middle attack. Further, some DLP protections can be circumvented through deliberate obfuscation by an insider, e.g., exchanging digits for words in a credit card number to trick the pattern matching algorithm.

ORGANIZATIONS WANT TO SOLVE THE DATA EXFILTRATION THREAT

Over half of organizations want to solve the data exfiltration threat within the next 12 months, and another 15% are willing to wait for up to two years. One quarter of organizations currently have no timeline for purchasing a solution to prevent data exfiltration, and a further 7% are unsure of their timeline. See Figure 9.

Figure 9
Timeline to Purchase a Solution to Prevent Data Exfiltration
Percentage of respondents



Source: Osterman Research (2021)

In looking at the data, we observe that:

- **Larger organizations want to solve the data exfiltration threat within a year**
  Three out of five larger organizations want to purchase a solution to prevent data exfiltration within the next 12 months. They recognize that despite their current cybersecurity stack they cannot stop data exfiltration currently, and that something specifically focused on data exfiltration is urgently required.
- **Smaller organizations want to solve the threat within two years**
  Respondents at smaller organizations do not feel the same level of urgency as larger organizations, with most wanting to solve the data exfiltration threat within two years. Perhaps this longer timeframe is because smaller organizations feel that implementing new technology like this—whether from a technical, budgetary, or human resources standpoint—is not possible in a shorter timeframe. Alternatively, smaller organizations may hope that attacks targeting larger organizations will take priority over themselves.

Addressing the Data Exfiltration Threat

Something new is needed that specifically addresses the modern threat dynamics of data exfiltration. Despite the best of what the cybersecurity industry has to offer, incidents that include data exfiltration are still frequently occurring. In this section, we introduce the "something new."

INTRODUCING ANTI-DATA EXFILTRATION (ADX)

We propose a new category of cybersecurity tool to address the data exfiltration threat: Anti-Data Exfiltration (ADX). Attributes of ADX solutions must include:

- **Reimagining how to stop data exfiltration**
  ADX solutions are not reliant on prescriptive policies that attempt to match the policy against a data event—such as an email message being sent, a document being scanned on a file server, or movement of data off a device. ADX solutions offer a fundamental reimagining of how to stop data exfiltration by disrupting exfiltration attempts rather than trying to fix a broken approach.
- **Direct protection on endpoints, not an afterthought in the network**
  Endpoints store organizational data, access organizational data stored elsewhere, connect to both network and cloud repositories, and use other wireless networks in addition to the corporate network. Since only some data movements will flow through a DLP solution on the network, the endpoint as its own entity must be protected directly to put a stop to data exfiltration. ADX solutions use a footprint that is light enough to work directly even on mobile devices and smartphones.
- **Zero-touch "set-and-forget" approach**
  Anti-data exfiltration solutions adhere to the same principle as endpoint anti-virus solutions: zero-touch and "set-and-forget." A complex set of customized policies that match against sensitive data should not be required to prevent data exfiltration.
- **Reliance on behavioral profiling, not sensitive data matching**
  ADX solutions monitor outbound traffic on an endpoint looking for abnormal behavior in traffic patterns and signals of compromise that are reflective of malware, ransomware, and other malicious processes. These include attempted communication with command-and-control servers, endpoint processes that should never send network traffic that suddenly are doing so, traffic being routed to known locations of cyberthreat (e.g., China and Russia), the use of Dark Web protocols, and reliance on direct IP addresses, among many others. Whenever these patterns and signals are detected, it is likely that data exfiltration is happening and must be stopped.

See Figure 10.

ADX solutions offer zero-touch "set-and-forget" protections against data exfiltration.

Figure 10
Comparing ADX and DLP Solutions

Attribute	ADX solutions	DLP solutions
Need for policy development	None to low	High
Need for ongoing management of policies	None to low	High
Detection method	Profiling of network traffic, behavioral indicators, and other signals of exfiltration	Signature and pattern matching against sensitive data templates
Location of deployment	Endpoint	Network Cloud
Handling of encrypted data	Honors the security chain for encrypted data	Breaks the security chain for encrypted data
Amount of IT effort to manage	Low	High
Ability to fool the technology	Low	High
Cost	Low	High
Expertise required	Minimal	Significant

Source: Osterman Research (2021)

Conclusion

The consensus across the world is that attempts at cybercrime are not going away. Cybercriminals are perfecting a range of attack methods that steal data, wage cyber warfare, and disrupt critical operations at victim organizations. Embracing effective strategies to stop data exfiltration attempts and break the cyberattack chain are increasingly important for organizations. Products in the new ADX category of cybersecurity solutions offer a reimagining of how to prevent data exfiltration in a world where the stakes are higher, more costly, and increasingly deadly.

ADX solutions offer a reimagining of how to prevent data exfiltration in a world where the stakes are higher, more costly, and increasingly deadly.

Sponsored by BlackFog

Founded in 2015, BlackFog is a global cybersecurity company that has pioneered on-device Anti Data Exfiltration (ADX) technology to protect companies from global security threats such as ransomware, spyware, malware, phishing, unauthorized data collection and profiling. Its software monitors enterprise compliance with global privacy regulations and prevents cyberattacks across all endpoints. BlackFog uses behavioral analysis to preemptively prevent hackers from exploiting vulnerabilities in enterprise security systems and data structures.

BlackFog's preventative approach to security recognizes the limitations of existing perimeter defense techniques and neutralizes attacks before they happen at multiple points in their lifecycle. Trusted by corporations all over the world, BlackFog is redefining modern cybersecurity practices.

www.blackfog.com

info@blackfog.com

@blackfogprivacy