Data Loss Prevention and Digital Transformation

INTRODUCTION

Today's digital age has produced unprecedented amounts of data. Much of this data is considered sensitive, such as personal information about customers and employees, financial data, and intellectual property that businesses must keep safe. In another day and age, this information was printed on paper and secured in a locked file cabinet. Now, these highly valuable zeros and ones race from one place to another, more vulnerable than ever.

The need to protect this data is undisputable. It's an organization's lifeblood and it includes information that the organization has been entrusted to keep safe. Certain types of data are, therefore, regulated, and companies face stiff penalties for mishandling it. Not surprisingly, data is also valuable on the dark net, fetching up to five dollars for a single credit card number with address—the type of information many databases store in high volume. For all these reasons, it has become incumbent on organizations to implement comprehensive data loss prevention (DLP) solutions.

THE NEED FOR DLP

A DLP solution is a set of technologies and processes that monitors and inspects data on the corporate network to ensure sensitive data is not lost or stolen. A DLP tool should always be part of an organization-wide data protection initiative, which gets business and IT leaders together to identify what constitutes "sensitive data" and to agree upon how this data should be handled and what a violation would look like. These guidelines can then be translated into a set of rules within a DLP tool. DLP solutions address three major organizational challenges: regulatory compliance, protection against data loss, and visibility.

1

Regulatory compliance:

According to Gartner[1], regulatory compliance is by far the most common DLP use case, being referenced in 75 percent of all recorded DLP deployments. As of May 2018, GDPR, the European General Data Protection Regulation, has brought DLP solutions onto the radar of data protection specialists in organizations outside of regulated industries, which have always been required to have certain measures in place to protect more personally identifiable information (PII) and protected health information (PHI). Although regulations do not explicitly require the use of a DLP solution, data protection requirements often present the concept of DLP to help with compliance.

Sounds like DLP to me...

New York State Department of Financial Services (NYDFS) — 23 NYCRR 500 alludes to the use of a data-in-motion DLP, but does not spell it out:

Section 500.15 (a)

"(...) each Covered Entity shall implement controls, including encryption, to protect Nonpublic Information held or transmitted by the Covered Entity both in transit over external networks and at rest."

[1] Market Guide for Enterprise Data Loss Prevention:
https://www.gartner.com/en/documents/3890116/market-guide-for-enterprise-data-loss-prevention

THE NEED FOR DLP

2 Protection against data loss

The reasons for protecting sensitive information from being exposed to unauthorized parties goes far beyond compliance. It's a frequent target for theft. A good indicator of its value is the willingness of malicious actors to pay much higher prices on the dark web for unregulated data, such as rewards memberships and loyalty program numbers, in comparison to U.S. Social Security numbers[2].

While organizations have incentives to be compliant, like the avoidance of fines or having restrictions imposed on their business operations, data loss bears much broader financial and reputational risks, such as losing customers, refunding or repaying lost membership "points," incurring brand damage, or even facing legal ramifications.

According to the Ponemon 2019 Cost of a Data Breach Study[3], 30 percent of organizations will experience a breach within two years which on average result in:

cost of $3.9M **25,000 lost records**

Industries that are subject to regulatory compliance, such as healthcare and financial services, experience costlier breaches. The average cost per stolen record was:

$429	$210	$150
healthcare	**financial service**	**all industries**

DLP solutions are especially important for avoiding accidental data loss through human error, such as unintentionally sharing sensitive data with third parties via file sharing or social media, or through the failure of IT or business processes[4]. In spite of strict regulations for handling health information, accidental data loss is especially high in the healthcare sector, where it accounts for 57.5 percent[5] of unintended disclosure of data, according to the 2018 Verizon Protected Health Information Data Breach Report. Verizon noted that it is the only industry in which insiders pose a greater data loss threat than malicious external actors.

[2] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; https://www.comparitech.com/blog/information-security/how-much-are-stolen-frequent-flyer-miles-worth-on-the-dark-web/#gref

[3] [4] Ponemon 2019 Data Breach: https://databreachcalculator.mybluemix.net/

[5] Protected Health Information Data Breach Report: http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf

THE NEED FOR DLP

3 Data visibility

Digital transformation confronts organizations and, specifically, CISOs with challenges regarding visibility into what is happening with the data in their networks. With increasing amounts of data, many different data owners and even more places where that data lives, it is difficult to identify all sensitive information and put measures in place to protect it; after all, you can't protect what you can't see. There are three significant trends that all cause blind spots for organizations: cloud adoption, mobility of users, and encryption.

Cloud adoption is forcing organizations to get a handle on all the data stored not only within the data center, but throughout the organization. Before you can move your data to the cloud, you have to know what data you have.

Employees are no longer bound to their desks, meaning they now access their apps and work files from just about anywhere at any time. These **mobile users** can access data and store files outside of the data center, often leaving the organization in the dark when it comes to this data.

Increasingly, organizations are employing **encryption** techniques in an attempt to protect data. However, hardware-based security systems can't check the content of encrypted files, leaving organizations blind to the type of data contained within.

THE NEED FOR DLP

Data moves across several channels

In our digitalized world, data is moving more freely than ever. At any time, it may be found on one of three channels: an endpoint, in storage, or in transit. Each channel in which data is either stored or passes through requires a different set of tools or techniques to prevent data loss. DLP solutions are segmented according to the three channels they protect:

Data-at-endpoint: Endpoint DLP solutions are agent-based and monitor data that is being processed on the endpoint. Their functionality varies but usually includes printing restrictions, preventing copy/paste between applications, and downloads to portable storage, such as USB.

Data-at-rest: All data sitting on file servers, databases or cloud storage is considered at rest. Data-at-rest DLP scans all repository content to detect sensitive information.

Data-in-motion: Also referred to as web DLP or network DLP, data-in-motion solutions inspect all traffic moving from point A to B over the web (internet) or email, e.g. data that is moved from cloud storage to an endpoint.

Digital transformation has created a shift in user behavior and traffic patterns, which has affected the endpoint and data-at-rest channels. As more data moves to the cloud, data-at-rest solutions are becoming irrelevant because their functionality can essentially be substituted by Cloud Access Security Provider (CASB) solutions. In addition, less data and fewer applications remain on endpoints, placing more importance on securing the data that flows between endpoints, cloud applications, and storage with a **data-in-motion** solution.

WHY HASN'T DLP FULLFILLED ITS PROMISE?

The DLP market is evolving

DLP solutions have been available for 15 years and the market is mature. There's been so little differentiation between competing enterprise DLP solutions that leading analyst firm Gartner retired its Magic Quadrant for Enterprise DLP. Instead, Gartner is focusing on a market guide that highlights the importance of a holistic data protection strategy and provides instruction on the use of integrated DLP solutions.

In comparison to **enterprise DLP** solutions that typically provide a variety of products (agents, physical, and virtual appliances) across all channels, **integrated DLP** solutions are natively provided by technologies such as secure web gateways, content management systems, email encryption, or CASB technology, and hence, have a narrower focus.

Enterprise DLP solutions are notoriously complex and costly. Organizations that purchase enterprise DLP often end up using only a small subset of its capabilities and address only basic use cases that could be solved with an integrated DLP solution, thus sparing the organization from costly and time-intensive setup and integration.

According to Gartner estimates,

> "By 2021, 90% of organizations will implement at least one form of integrated DLP, an increase from 50% today." [6]

However, enterprise and integrated DLP are not mutually exclusive. Organizations that have already made investments into such products should work with their existing infrastructure. Nevertheless, any organization should consider adding integrated DLP to address further use cases that close the gaps in their existing data protection strategy that have been brought about by digital transformation.

[6] How to Choose Between Enterprise DLP and Integrated DLP Approaches
https://www.gartner.com/doc/3757464?ref=mrktg-srch

WHY HASN'T DLP FULFILLED ITS PROMISE

Data loss prevention is an organization-wide initiative, not an IT tool

Despite being a mature solution, organizations continue to report problems with their DLP deployments, many coming from poor planning and other organizational issues.

Most organizations erroneously believe that DLP should be implemented and managed long term by IT security only. Once the DLP rules are established, responsibility for the DLP solution should be transferred to business operations. In addition, those deploying DLP solutions need to secure senior executive buy-in, to get visibility back into the business units or the business risk management teams.

To avoid having to look for additional sponsors and use cases to justify the project, which inevitably adds demands and complexities to deployments, teams must secure internal buy-in and tie DLP projects to specific initiatives or goals.

CLOUD DLP REQUIREMENTS

As organizations move to the cloud, their security should also move to the cloud. But, simply reconfiguring a traditional hardware stack for the cloud is inefficient and doesn't provide the protections and services of a cloud-build solution. This applies as well to DLP. To address the data protection challenges that have emerged with digital transformation and overcome the shortcomings of traditional DLP, a cloud-based DLP solution requires the following three elements:

1. **Identical protection for all users on- or off-network**
   With traditional DLP solutions anchored in the data center, the level of visibility and protection depends on where your users are located. Remote users can bypass inspection when off-network, connecting directly to cloud applications and circumventing VPN and any data protection measures. To provide comprehensive data protection, a DLP solution should provide identical protection to all users, regardless of their location, whether they are in the office, an airport lounge, or a home office.

2. **Inspection of encrypted traffic**
   With more than 70 percent of today's traffic using encryption, it is incumbent upon organizations to inspect this traffic. However, as encryption was originally created as a security measure, traditional security solutions don't natively inspect this traffic. As a result, organizations tend to inspect only a fraction of their encrypted traffic—and what is a DLP solution worth if it sees, perhaps, only 30 percent of the total traffic? Increasing your security posture by adding SSL appliances is probably not financially feasible, nor is it acceptable in terms of IT complexity. The only way to get visibility into encrypted traffic is to use a DLP solution that natively inspects SSL.

3. **Elastic scalability for inline inspection**
   The tremendous growth of internet traffic requires constant updates to traditional, appliance-based DLP solutions, as their finite inspection capacity is quickly drained. In an attempt to overcome the complexity and cost of this endeavor, many organizations resist deploying a DLP solution inline from the start. Unfortunately, this only allows organizations to do damage control after their data has been compromised. A cloud solution allows for elastically scalable inspection capacity that can prevent data loss by inspecting all traffic inline—before data can be compromised.

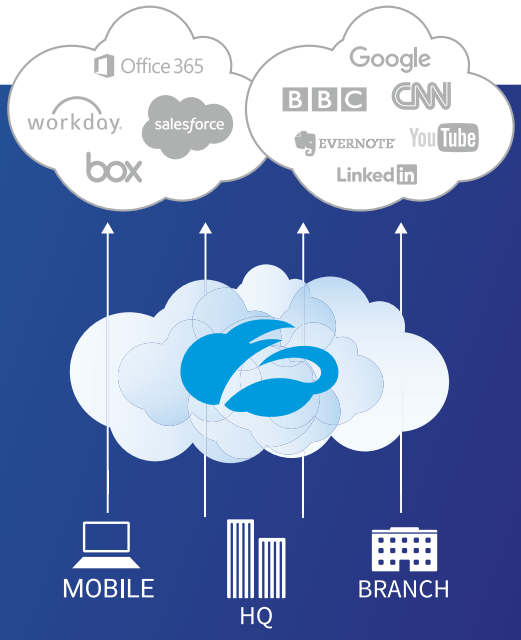
ZSCALER™ CLOUD DLP

Part of Zscaler Internet Access

Zscaler Internet Access™ (ZIA™) is a secure internet and web gateway delivered as a service from the cloud. ZIA sits between your users and the internet, inspecting every byte of traffic inline across multiple security techniques, even within SSL, providing full protection from internet threats. This purpose-built cloud platform includes Cloud Sandbox, Next-Generation Firewall, and Cloud Application Visibility and Control, as well as Cloud DLP.

Cloud DLP Overview

Zscaler Cloud DLP offers complete data protection with full context and content inspection for all data in motion, as well as advanced features, including Exact Data Match, machine learning, and granular policies for optimal protection.



Zscaler Cloud DLP fulfills the three requirements

Zscaler Cloud DLP provides the same level of security to all your users by moving your data security to the cloud. Zscaler sits between your users and the applications they are connecting to. Cloud DLP policy follows users where they work—on- or off-network—and provides the same level of protection to all users at all times.

It also provides full inspection of encrypted traffic. Around 70 percent of outbound traffic is encrypted and thus not subject to inspection by traditional DLP solutions. With Zscaler, there are no capacity constraints for enabling SSL interception at scale. Zscaler is a proxy by design, performing SSL inspection on all traffic without the inspection limitations of appliances.

In addition, Zscaler is architected to sit inline, so it can block sensitive information before it leaves your network—instead of being limited to damage control after data has been compromised. The Zscaler security architecture was built in the cloud from the ground up and the service is user-based, not capacity-based, allowing your Cloud DLP inspection to scale elastically with performance guaranteed by SLAs.

CONCLUSION

DLP needs to be viewed as a well-defined security process that is bolstered by well-managed supporting technology. However, even at this late stage of DLP solution maturity, organizations continue to struggle with DLP deployments. This is primarily due to misrepresentation of the DLP solutions internally within the context of a security program. In addition, many in the market overstate the simplicity of deployments, the level of out-of-the-box accuracy in identifying content and visibility, and the control over all applications.

With increasing risks and expanding regulations for data protection, organizations must close security gaps created by cloud and mobility. In the past, that would have meant adding more appliances to an already complex security stack. Zscaler offers a better way. With Zscaler Cloud DLP, you can close data protection gaps, regardless of where users connect or where applications are hosted, without costly, complex appliances.

About Zscaler

Zscaler enables organizations to securely transform their networks and applications for a mobile and cloud-first world. Zscaler connects users to applications and cloud services, regardless of device, location, or network, while providing comprehensive security and a fast user experience. All without costly, complex gateway appliances.

zscaler™