Global Journal of Universal Studies

Volume1:Issue1 **ISSN: 3008-0509**

Article History

Submitted: 29-05-2024

Revised: 13-06-2024

Accepted: 17-06-2024

Corresponding Author:

Noman abid

nomanabid12345@gmail.com

Advancements and Best Practices in Data Loss Prevention: A Comprehensive Review

Noman abid

American National University USA

nomanabid12345@gmail.com

Abstract

DLP solutions are needed because there is more data and more reliance on it which people and businesses need. This paper will provide a further account of what DLP is, its significance, issues it encounters, and prospects in what follows from this article about DLP. Globalization and the rise in the kind and level of cyber threats, uptick in cloud use, and the enhancement of legal requirements for data protection have all moved DLP to higher prominence as a cybersecurity mechanism. In more detail, some challenges that are associated with DLP implementation and that refers to initiation and management, are described, such as data classification, security needs and organization productivity, insiders and their threats, regulation compliance, and others. The article also examines how data protection paradigms are revolutionized by AI, ML, cloud native DLP solutions, Zero Trust architecture, and XDR. Also, it underlines the need of privacy by design, and the controls concerning insider threats in the shift of the paradigm. As the type and functionality of DLP systems will further advance not in the distant future, utilization of such state of the art technologies shall assist organizations to secure data while the latter focus on continued operation. Therefore to meet this ever present need for such smart and dynamic DLP solutions to address data loss consideration in the multiple complex cloud environment there is need to rise new and complex cyber threats.

Keywords: Data loss prevention, cyber security, cloud security, artificial intelligence, 'Zero Trust', Cloud Extended Detection & Response, data privacy, compliance, threat detection, data security challenges, data classification

Introduction

DLP had been defined as a set of procedures and tools used to prevent data loss and leakage by the use of unauthorized parties. It is one of the segments of the rather young and yet rapidly growing field of cybersecurity which has gained high significance nowadays since the primary assets and information for companies, organizations, and governmental institutions are of vital value. Such incidents as continued escalation of data breach attacks as well as other computer-related crimes, plus the looming threats of insider threats have made DLP paramount in several

organizations. If you knock the definition down to its barest level, then DLP is just about safeguarding data from internal and external threats [1]. There is hacking attacks from other people groups or organizations who wish to breach the organization's systems with a view to stealing or tampering with information with the aim of making a profit or so as to further a certain political agenda. External threats on the other hand are those outside activators of the organizational system, the business competitors, rivals and any social persons who are unfitting to enter the organization's territory and have the ill intentions as regards the vital and organizational information. This double approach on both external and internal risks make DLP as unique and critical component of cybersecurity model [2].

The rationale of utilizing DLP in the contemporary world security is because of the expansion of amount of data generated in diverse organizations. Fact recognized in the statistics of the industry reveal that the amount of data generated worldwide is expected to double in the coming years. What this means is that with this sort of growth, is a threat to the data management process because it is very difficult to oversee, regulate, and secure. For instance, the healthcare industry deals with PII and health information, the finance industry, deals with sensitive financial information. Both industries bear submission to regulative frameworks that assert data security over roads the importance of DLP. DLP tools enable organizations to constantly monitor, detect any, and control any adverse data that may pose a threat to security or policy at any one time of any data that is considered sensitive [3]. These solutions typically operate on three primary levels: The specific layers include network and storage, and endpoint. At the network level, DLP solutions monitor and control the movement of data in a company's network to prevent transfer of information to unauthorized users. Endpoint DLP focuses on physical devices like laptops, mobile phones, work stations and among others with an aim of preventing leakage of data at the end-point where these gadgets are used to access, use or transfer data. In contrast with DLP solutions that aim primarily at the correct encryption, backup and protection of data that is stored on local or cloud systems of an organization.

For instance LDP is basically an instrument which is aimed at implementing procedures that specify how a certain individual or an organization should handle protected information. They are set based on one or more parameters among that parameters are data type, location of data type,

and the user role/privilege level. For example, a company may have policies where managers and other workers are prohibited from sending personal data that is unencrypted, or transferring company files to third party cloud storage. These policies can be supported and implemented with the help of DLP tools: data is scanned for compliance and the actions aimed at changing the process are taken – the transfer can be blocked, the user will be alerted, the event can be recorded for the further investigation. DLP is also used in compliance with almost any regulatory model existing within organizations [4]. The EU computer privacy laws like GDPR also created standards that defined how data should be protected while corporations such as HIPAA in USA and PCI-DSS also put into measure, measures to safeguard data. Consequences of failing to follow these regulations include fines that are likely to chime into the company's figures, let alone legal consequences and the effect on image. Therefore, DLP continues to be an essential commodity within organizations that desire compliance and save its image.

These evolutions which control the DLP evolution are the shift toward cloud, the new face of telework, and enhanced cyber threats. Historical on-premises DLP models were somewhat rigid and did not always offer coverage in the current world. Currently, the available types of cloud DLP solutions are gaining popularity due to the ability to preserve data integrity in hybrid and multi-cloud solutions. And also on the list, AI and ML technologies have increased the level of DLP system by enabling the system look at patterns of threats or other inadequate behavior patterns that one would consider inconsequential. DLP is one of the critical components characteristic of the modern trends in information systems' protection. antivirus, as well as backup and analysis of the information and the related data flow which form the base of DLP technologies, Policies and tools to safeguard, control, track, monitor and audit, correspond to the problem of leakage of the sensitive data and are oriented at save the organizations' intellectual and physical property, the compliance with the regulations and at the save of the customer's personal information. As cyber threats continue to evolve, the role of DLP will become even more critical in securing an organization's most valuable asset: its data [5].

Global Journal of Universal Studies
Volume1:Issue1 ISSN: 3008-0509

Fundamental Components of Data Loss Prevention Primary Data of Data Loss Prevention

DLP stands for Data Loss Prevention and is a set of tools, strategies and initiatives meant to stop the leakage, theft or loss of information. These components are essential to managing and securing an organization's network, endpoints & storage. The main areas of DLP can be defined broadly as identification/classification of data, encryption/masking of data and protection/monitoring of end points [6]. Alchemy of these components creates a strong framework, which can protect against data leakage in addition to being compliant with the legal requirement on data protection.

Figure: 1 showing the anatomy of data loss prevention

Data Identification and Classification: The first and the most likely the most important of the above components of a DLP is the categorization of data or the identification of data. The issue arises when commissioned to protect it one does not what is being protected, this is the sensitive data. Data identification can be defined and understood as the process of identifying data in organization's networks, systems and other computing devices. This could be more of an individual's data Social security numbers, financial, credit card, other identification numbers, proprietary information Trade secrets, formulas, algorithms, or any form of data quickly deemed as valuable for sensitive by the business [7]. Once we know what must be kept, we then have to categorize it into levels that are appropriate depending on the level of sensitivity. With this classification, one finds himself or herself right where to enforce or implement various security measures based on the level of security needed for the data in that given organization. For instance, the emails c containing personal customer details and their financial information can be branded as "Confidential," while those meant for internal consumption only are similar labeled "Internal Use Only." Classification structures help organizations determine which section is vulnerable and more critically, which of the vulnerable areas needs maximum protection.

This is done automatically since most DLP instruments use pattern matching, content analysis and context awareness to various forms of sensitive data. Since data is also captured in various types; structured, semi-structured, the unstructured data among others it means that a DLP system must be capable of scanning along the entire data types in order to offer total protection. Data security measures that may be exercised where data is in motion or at rest are twofold: encryption and data masking. Data encryption therefore entails converting available data which are sensitive into a form in which they cannot be utilized or identified by any unauthorized person using a cryptographic key. The only way to decrypt data to return to the first type of data is to use the encryption key. Encryption makes it possible that even if the data ends in the wrong hands, it appears garbage to the interception party [8].

In most cases, DLP systems operate in conjunction with the encryption technologies to ensure that a company's confidential data can be encrypted the moment they are migrated across networks or stored in databases. For example, when an employee in an organization has typed an email containing some sensitive information, then DLP systems can block the information being viewed

by other parties by automatically applying an encryption feature on the message. However, the term data masking means that instead of the rather sensitive information there is information that looks similar but actually is of no concern to the person who is not supposed to access this data. It may be used when sharing information with other users or organizational clients or when in a development/ testing environment. Wearing's help in reducing probability especially where there is testing or formulation of strategy on how to pass certain sensitive information. Encryption and masking both are needed as they have their unique roles in the process of data protection and as shields from consequences of user mistakes or data leakage [9]. Altogether, these methods assist the identification and classification activities so that even if data leaks out, it cannot be used effectively.

Endpoint protection is a sub set of DLP because endpoints such as laptops, desktops, smart phones and tablets are among the most common entry points for hackers in the organization's systems. Such devices therefore poses other types of risks which include malware, phishing and even physical theft of the devices. Endpoint protection can therefore be described as the safeguard of such devices, as well as the prevention of any transfer or storage of such information, or even manipulation of the same [10]. The specific IT controls built into the DLP solutions, and which might help address the endpoints might include: copying files to removable media or sending documents through e-mail or uploading documents to restricted cloud services. The best approach is to strengthen measures at the end point where it really becomes impossible for the user to compromise the organization by getting it to do something risky to the data. One more aspect of endpoint monitoring leprosy with the dangerous actions of the users that have to be marked and analyzed. For instance, overused sensitive documents detected in the DLP systems, may raise an alarm of an attempt to leak data by an employee or outsider within a short period of time. This kind of monitoring enables organizations to counter threats at a very early stage thus reducing very extensive losses [11].

Hence, together with analyzing user action, which is the goal of monitoring, there is also the protection of the endpoints, that is, the devices. Some of the ways through which the information can be protected under this processes include; installation of the anti-virus and firewalls, and encryption of devices that store information. Besides, MDM solutions can then be integrated with

DLP solutions to ensure that the mobility devices have been configured securely and completely in accordance to organizational policies. Data discovery and indexing, data categorizing, data encryption and obfuscation, endpoint security and audit, are methods of DLP that assist in preventing device data from leaking outside and unauthorized entry. Chiefly, it is quite simple for an organization to incorporate the concept of security measures in data which has been sorted depending on the level of its sensitivity [12]. To the last, let me reflect the brief information that there are two approaches in the case if the data is viewed by an unauthorized person: Irony to encryption and masking. Endpoint protection and monitoring safeguard appliances from threat emanating from outside and inside the network making data secure at the usage end. In recent years the aspect of cybersecurity has enhanced and therefore making it all the more tougher to challenge data meaning that in order to support the currently used DLP systems aspects such as artificial intelligence and machine learning has been incorporated in DLP. All these key elements if well implemented as part of the entire DLP solution will serve prospective negative ramifications such as data loss while protecting the organizations' valuable data and ensuring compliance with legal and regulatory compliance.

Cybersecurity Protection: The Use of DLP Strategies

DLP entails identifying the measures to take in order to protect information within an organization to understand the right steps to take when protecting the information. Among the strategies it is possible to outline the growth, extension, and sustaining models as the signs of loss of data or an attempt at data leakage or breach. Due to numerous reports being published and increased frequency of enhancing cyber-attacks, organizations need implementing comprehensive DLP solutions that target both internal and external malicious parties and unintentional data leakage. DLP solutions meet an organization's need and types include network, endpoint, cloud, and hybrid. Traditional and most common Network Based DLP solutions are aimed at monitoring and controlling data transfer in an organization's network [13]. They aim at preventing the loss of information in communications both from insiders and outsiders and in E-mails, Web applications, FCs and other protocols. In the case of Network based DLP there are configured at strategic places in the network, for instance the email connection point, web connection point or the network firewall point because they define the data move in real-time.

These use content filtering, string search and deep packet filtering (DPI) to detect transfer of such data in the network. When such important data is defined for instance PII or monetary data, the network based DLP tools can either deny transfer or encrypt the data before transfer out of the network. They can also fire an alert to the security teams in case there is more that can be done from the data. The DLP since based on a network is most advantageous in large complex environments where perhaps the data users and devices are many. WLAN security is important to ensure that sensitive data does not go to the wrong hands, to the external extraneous parties and also the internal staff with a vantage access [14].

Endpoint-based DLP addresses the security needs of the data on endpoint – desktop, laptop, mobile phone, USBs and so on. End points are also a critical weakness within organizations 'security measurers because they offer an access to the actual organizational data. Endpoint DLP solutions parenge to protect data on these devices or in active use, to prevent it from disappearing or, worse still, being stolen. Endpoint DLP solutions monitor particular activity and occurrences for instance, file copy and print jobs and data migration from one device to another for instance copying file to USB or uploading to a personal cloud storage. Such solutions, therefore, are preferred because they minimize the risk of the users copying or sharing the specified data, through 'word-of-mouth', owing to strict policies that befit the information technology sector. For Example, endpoint DLP might bar the transfer of specific data to an external storage device and even restrict the printing of some document [15]. In addition to its use in surveillance of existing data, endpoint-based DLP also covers encryption of information stored inside a particular device. This assists in the fact that only the right people that are allowed decoding the file will only be able to do so, hence the hackers if any or in case one misplaced their device.

Initially, cloud based DLP solutions are closely related with today's environment in which organizations are demanding significantly cloud. Cloud-based DLP focuses at information that is situated in cloud solutions such as SaaS, IaaS, and PaaS. Unlike many other IT changes, the move to the cloud introduces new kinds of risks, such as unauthorized access and leakage via third parties. Conventional DLP solutions, therefore, achieve data protection by configuring means of recognizing and managing utilization and access to clouds. Such things can be used to identify situations when the prohibited applications run in the cloud and when new data is uploaded,

updated, or propagated in the cloud application. Another area that Cloud DLP can help protect our data from is interception of the data through encryption when it is at rest and when it is in transit. The utilization of DLP in cloud environment has advantages in the fact that it can secure data in private, public and hybrid cloud systems. All of these solutions can interface with cloud storage solutions like Google Drive, Dropbox or Office 365, in order to ensure that information is protected when it goes from on premise to the cloud back [16].

But yes in real world you can come across cases where Network, Endpoint and Cloud Data Loss Prevention are used to get improved protection to the data. This is especially so since is totally relevant for the organizations that are using a multiple 'clouds' or hybrid IT environment where data can be stored on premise as well as in several cloud services [17]. The hybrid DLP model can be applied to various situations because the program safeguards data in various environments. For instance, there is the network-based DLP which assists in detecting data in circulation within internal conduits, the endpoint-based DLP for data in devices as well as the third-party cloud-based DLP for data in other platforms. The application of several several types of strategies to protect informations in an organization provide a general protection in an organizations' structure anywhere information is found.

In addition, the organizations should consider a mix of both DLP model to promote security but not disrupt functionality. It lowers the risk of very high losses in data and yet at the same time it is possible for the employees to work from any temporal location with minimal interferences. The management of effective DLP strategies is important today as hacker's compromise organization security and internal threats are on the increase. Most conventional DLP solutions have network security, which safeguards data at the time when it is in motion in the organization's network; on the other hand, endpoint security has a security posture for data at the time it gets accessed. Cloud DLP solutions ensure that business information embraced in cloud environments will not be leaked. Fourth, there is the general risk oriented DLP approach that uses all of these methods in order to create a more or less free form protection that will tackle all sorts of risks. This takes me to my last recommendation that as organizations continue to advance their application of Information technology, there is need to enhance the DLP strategies to capture the new emerging problems [18]. This is particularly so in today's applications like more remote working, end user computing,

expanded cloud use, changing and increasingly complex cyber threats; DLP is now a core competency. Thus, the selection of the proper DLP solutions and the combination of single solutions to an overall concept fundamentally support the minimization of the relevant data risks and data losses as well as enable a reliable and compliant manage-ment of enterprise data in relation to internal and external partners.

Challenges to the Integration of Effective DLP

Data Loss Prevention (DLP) is one of the instruments used in enterprise security measures that has several challenges concerning its implementation. These challenges may be occasioned by security/performance, technological elements, compliance and internal threats. Such knowledge is crucial as an attempt towards conceiving DLP programs that afford the maximum defense as much as it does not hamper the functioning of such organizations. Perhaps one of the largest dilemmas that come with implementing DLP is the implementation of strong data security measures on one side of the fence and reasonable usability on the other. Employment of DLP solutions often involves monitoring the transfer, movement or storage of data or other content that can disrupt the usual operations of an enterprise [19]. For instance, limiting the transfer of files to personal cloud storage or the banning of the use of USB in the transfer of files will enhance security of the information as the tools are not secure but will be considered inapt with the working tools by the workers.

The problem with rather generalized DLP policies is that the data remains open and ends up in leaks and even failure of IT projects. It becomes very clear that if you over regulate your employees with DLP they will begin to look for ways in which they are going to bypass the DLP using other tools other than those that are recommended by the organization this is a situation that poses serious security threats to the company. As a result new risks appear which were supposed to be addressed by DLP solutions in the first place. Therefore there must be a middle ground which means that DLP polices are to be aligned with the compliance of the organization's risk tolerance & necessity while employees, on the same note, their work abilities cannot be hindered. One of the most pressing problems formalized when considered is the aftermath of cooperation with extensive difficulties of the technical DLP solutions aspect. Most current DLP undertakings are primarily

dependent on using Rules, content-based scans or heuristics to identify the data that needs protection. Some reasoning Even though these approaches are as effective in most cases, they do not work efficiently with the new, modern, and advanced threats. For example, encrypted data has been reportedly able to pull a bypass on routine DLP tools that fail to scan encrypted traffic or files [20].

Furthermore, in relation to the DLP implementation, they may not be able to identify the complicated data leakage patterns or the unauthorized access to data. For instance, today's cyber attackers may use a new or better way of evading programs or organizations that seek to identify, say, use steganography. For this reason, DLP systems must be constantly updated to address latest technologies and threats which is challenging for organizations to stay on the right side on policies and therefore continuing to seek to upgrade their DLP solutions regularly while coming up with new policies to counter new threats. Organizations of today generate massive data – this is one of the technical challenges that the current literature points to. DLP solutions need to be in a position to perform and authenticate big slabs data and all this in real time without the system being overwhelmed. This can be especially challenging in field that involves huge data, say in the health sector, credit industry, or in merchandising [21]. The various laws and regulations of the global business structure where data protection plays an essential role in claiming the company achievements like GDPR and HIPAA, and PCI DSS. These regulations put into place strict measures about how to deal with data and consequences of not adhering to these measures include penalties, legal action and brand damage.

Despite that DLP solutions have a very important mission in ensuring the compliance of an organization, because the compliance standard differ in great degree according to the specificity of the industry or the geographical area, it is not possible to implement the same standardized form of data protection. For example, GDPR has greater specified requirements for the processing of personally identifiable information (PII) when compared to the demands that HIPAA has made on health care information or PCI DSS has made for payment card information. Usually, it is time and cost consuming to ensure that the DLP systems are compliant with so many aspects of regulations and laws are ever evolving and organizations and companies have to make sure they are compliant with current legislation [22]. This implies that apart from compliance rules in terms

of, the use of the IT systems there is has to be checks as well as assessments to ensure that one has to admit that the DLP controls are working as planned. Consequently, both intentional and unintended, end-users continue to pose a significant threat to the viable functioning of DLP systems. In insiders risk is higher because employees, contractors and other people with valid access to the data are more likely to make a bad decision regarding the data or do something wrong unintentionally due to negligence.

Some employee data leakages are accidental and they include cases where an employee forwards sensitive data to the wrong recipient, share sensitive data through the wrong channel or flout organization data security policy. Such mistakes must be detected by the DLP solutions to prevent greatly increasing the level of complication in breaches and leaks. Furthermore, there are employees other than the user, and they may attempt to bring in wrong information with the intent of the gaining monitory advantage and other factors that may attract the attention of the manager [23]. In this regards while DLP systems of course can assist in screening and identification of many of the related abnormal activities such as data use and transfers, identifying intended perpetrator activities which generally entail more elaborate behavioral modeling and surveillance efforts. These threats are sometimes hard to address than the external threats especially since the individuals threatening the organization's information assets already have legitimate access to it. Organizations must also define the human resistance issue to DLP systems as a problem. Resist may be seen by worker as a violation of their rights to privacy or DLP as an interference with the worker's responsibilities hence the resistance to the policies or attempts at circumventing the controls. Three of them are: We have to establish awareness and ensure that we bring on board the employees and or stakeholders so that, they embrace security measures that DLP embraces [24].

If an organization is organized in numerous departments and manages different kinds of IT systems or simply if it is a huge international corporation, the implementation and usage of numerous DLP solutions could be complicated. Business and other organizations use both, a network-based DLP systems and an endpoint-based and cloud-based DLP system to meet several security needs. Nevertheless, the integration of all these solutions inevitably results in the formation of a single system that provides logically consistent protection is a very complex task. Implementation of multiple DLP solutions to where there is combination of multiple DLP solutions that are designed

for implementation is a difficult task because one is likely to find duplication as well as compatibility issues. Moreover, the nature of DLP implementation is more complex than GRC and thus, the policies should cover every system in the organizations and as much as the monitoring procedure of DLP should be distributed, the same way, the reporting procedure of DLP should be centralized [25]. A successful DLP strategy is not without its problems, therefore how do organizations address and tackle the following challenges: Being effective without being endangered, enlightening in the war against technical barriers, meeting today's constantly changing demands of regulations? Besides, it is more challenging due to threats from insiders, mistakes when it comes to DLP systems, and the fact that they have had to implement several systems. The period that demands the DLP solution needs to be realistically measurable, effective and most of all, sustainable each time it is tested against new threats and challenging business environment to operate effectively. On these challenges there is light as addressing them will assist organizations to be in a better place to prevent loss or misuse or access of highly sensitive information within their system.

The future trends of Data Loss Prevention (DLP).

New and more elaborate forms of cyber threats appear while data is now considered as a key asset of any organization, thus, the area of Data Loss Prevention or Data Leak Prevention (DLP) remains in development. The current development drivers of DLP consist of technology advancement, new needs and the need for organizational change. Several future trends are possible to influence further development of the DLP implementations into organizations, making them more efficient, intelligent, and suitable for new and more complex threats. Predicted future trends of DLP require integration of AI and ML in future strategies of DLP as indicated in figure 4. If one were to go looking for DLP in more traditional systems, one might discover that the solution's approach here is to use rules and signatures to identify the data that needs protection [26]. However, these rule-based systems can be so rigid that they are not so useful in the identification that emerging threats.

In partnership with AI and ML, DLP formally enhances DLP systems for big data and potentially identify behavioral risks regarding data loss. For instance, AI can recognize prohibited actions including inclinations that are latent or suspicious in way that entails sharing, downloading or

transferring files that possibly exhibit a leakage scare within internal or external environment. But if the machine learning algorithm is employed to train these systems and if the outlook of the system to analyze information is improved consequent on new patterns of activity observed during experience in combination with feedback received from the prior case, then the DLP system will be better equipped to match the new threat and behavioral characteristics of the existing users. Moreover, some of the conventional DLP system produces a high number of change points which in a way are fake, and this can, in part, be mitigated by listening in AI. AI can improve security while increasing organizational use of DLP by expanding the distance between security threats and noise [27].

Another factor that this paper considers forecasted for DLP is the increase and adoption of cloud environments as part of migration for organizations. As cloud adoption continues to grow and organizations are not only storing applications but also using services and storing space in the cloud the security of data in such structures has become the center of many concerns. At times, it becomes extremely challenging for conventional Endpoint DLP solutions, typically implemented on the company's physical local network infrastructure, to adequately capture and secure data residing in and in transit through cloud storage. Organizations are likely to set the new standard for cloud security by employing DLP solutions developed natively for the cloud. These solutions are particularly designed for cloud assets, and are very quickly integrable with cloud apps, storage and services [28]. By backing SaaS, IaaS, and PaaS, they can always examine the ways whereby data protection policies implemented in the cloud are complied with.

The value that cloud-native DLP brings, is the possibility of actually stopping data leakage or improper handling within cloud providers. For example, these solutions can be used in enforcement of access controls on data or to filter for leakage, as well as, search for leakage. Besides, cloud-native DLP can also be deployed in cases with hybrid cloud where the data is stored both locally and in the cloud, providing protection in both. Another more recent security framework being a bit discussed but which is in fact that is being adopted is the Zero Trust Architecture (ZTA), where no user or device is trusted irrespective of whether he/she is inside or outside the secure corporate perimeter. This approach makes the most sense Now that we are doing remote working and using cloud computing to solve security concerns that are conventional in

their approach. Therefore, it comes as no shock that integration of DLP solutions with the Zero Trust model is the next logical progression. DLP systems will then work hand in hand with IAM systems under a Zero Trust security model to enforce data protection policies relating to the user's position, health of the device or any other thing [29]. For instance, a Zero Trust DLP system may block copying of data to other devices or ports in a scenario where the user device has not been validated or in scenario where a transfer seen in real time appears to be malicious.

When Zero Trust is combined with DLP, additional measures are provided over the information Due to the execution of the 'need to use' principle here, the data has to be given the correct permission and conditions to be accessed by the users. This integration will help organizations when it comes to risk mitigation towards insider threats, stolen credentials and unauthorized access. Today, there are still emerging rules in the world related to the protection of personal data and organizations need to guarantee that data is protected and complies with the GDPR, CCPA and other regional standards. Compliance often presents complex issues, which cannot be solved unless implementation also results in severe financial penalties and negative impacts on the company's reputation. It is predictable that future developments in DLP solutions will be integrated with other compliance automation technologies making compliance to data privacy standards easier [30]. The compliance features which are inherent in DLP systems will help an organization to find where the sensitive data is in the firm, who is allowed to access such information, and how the data is being transferred within the firm. DLP solutions will also be integrated with other components that produce reports showing compliance or the lack of it to set down legal standards and inform an organization that it is due for an audit.

This means that in the future DLP solutions will have to behave according to the rules of the different jurisdictions as relates to the sovereignty of data. These will help different organizations to adopt different data management principles as they adhere to the laws of nations as more corporations invest in several countries. One of the areas that are thought to offer even greater potential in the future of DLP is behavioral analysis. Traditional DLP tools work with text and/or image analysis generalizing rules for data protection that cannot always be applicable to every user interaction. That is why UEBA can align with DLP to provide additional insight into the user behavior regarding the processed information [31].

Firm with user behavior and usage of software, services or organization application, UEBA solutions differ and distinguish login patterns, access location, file access behaviors and typical data transfer to set up evil or data theft benchmarks. At the same time, when joining UEBA and DLP, it can be subtracted on risk based on suspicious activities despite the fact that, for example, there was an attempt to extend access to data of the highest degree of protection. For example, if an employee begins downloading many files off hours then the DLP system in conjunction with UEBA will flag this as a suspicious activity even if the fact that the files downloaded are not on the list of sensitive files commonly used by DLP rules [32]. This capability makes it possible for an organization to detect insiders, incongruent accounts and other types of information loss at speeds that were hitherto unprecedented.

Therefore, due to this new-style remote work, the idea of managing and containing endpoints has emerged as the objective of DLP systems. Remote employees use their own owned devices or work through insecure networks, and this further amplifies a vulnerability to leakage. Consequently, the future trend of DLP will be to have the endpoint based solutions, which perform the center or core to the above-explained DLP techniques. Current endpoint DLP solutions should have extra features that will be either enhanced or added later; MDM, MFA, and ongoing device health check. Such solutions will watch over the device activity and will prevent unauthorized accesses to data irrespective of the place of the device. There are several trends that define the direction of development of Data Loss Prevention: These are technological trends which we can see in any segment of people's life; the tendencies which are related to the increase in the new level of cybersecurity threats. And as long as all of the related technologies continue to get used, DLP systems will become more proactive, smarter and more adaptive with the help of the added AI, machine learning, cloud-native DLP solutions and behavioral analytics [33]. Additionally, when DLP is combined with true Zero Trust strategies and practices as well as the use of automated compliance and enforcement, organizations are far better prepared to undertake the nearly Sisyphean task of protecting data in an environment that can only be described as effectively dynamic and constantly in flux in terms of regulatory requirements. When adopting these trends, a firm is well placed to enhance it heath for a risk event that affects data that it holds equally meeting emerging laws on data protection.

Largest Trends in DLP Solutions

This paper aims at identifying good practice in Data Loss Prevention (DLP) in order to increase protection of data in organizations against leakage, loss or use by those who should not. DLP technologies are however paramount in this, but the failure to undertake a proper approach in the implementation of a DLP system will in most cases lead to compromise protection or a sign of system glitches. However, it is crucial to consider some recommendation to want a greater effectiveness and efficiency of the DLP system as well as achieve the optimal protection of the data where implementing a DLP solution. When start looking for a DLP solution, organizations should first identify what data is considered sensitive and what may happen if it is leaked. Certain data is of high value than the other hence need to be protected and this include; customers database, ideas and strategies, financials or any personal identifiable information (PII). The fundamental first step though must be the data classification audit [34]. It involves ranking, categorizing and accrediting data according to its character, frequency and use in the business. The process of data classification allows to implement sufficient DLP controls, which correspond to the security needs of the given data type.

As important is to understand what threat is there to that data out there in the market place. These may involve external threats such as hackers and internal threats or agents who incoherently or maliciously interact with data. That way, it is possible to overcome the common risk factors around which the DLP policies are designed. What is more, there are many DLP solutions available today, and even all these solutions are DLP, they may differ with nearly full functionality. Hence when deciding on a DLP system an organization should settle for a system that meets its requirements, its IT framework and level of security. Depending on the deployments type of DLP there are three broad solutions which include; Network based solutions, Endpoint based solutions and the lastly Cloud based solutions [35].

Global Journal of Universal Studies
Volume1:Issue1 ISSN: 3008-0509

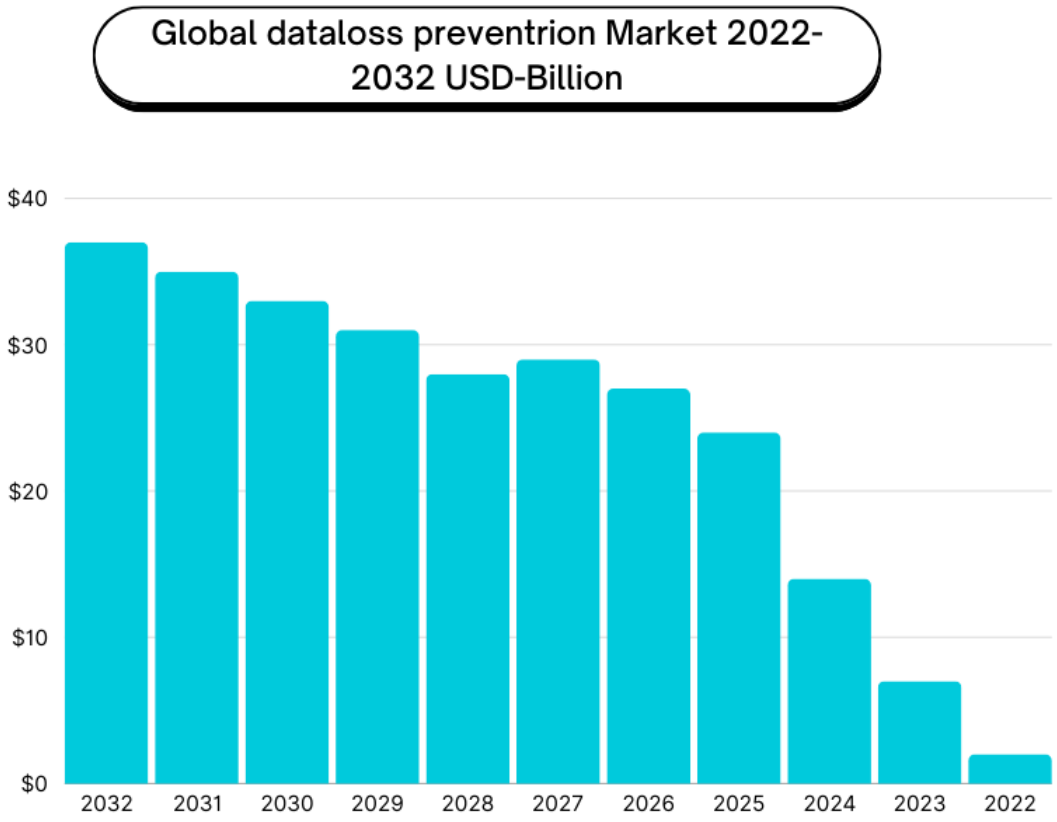

Figure: 2 showing global data loss prevention market

Network-based DLP: An approach that ensures continues monitoring and protection of information during transfer from one point within an organization's network to the other. It is ideal for use with data that is disclosed by e-mail, file-sharing Website and Web traffic.

Endpoint-based DLP: Stresses the protection of records stored in and/or transiting through an individual node, such as PCs, laptops, and mobile handhelds. This solution is important for safeguarding information at the time and place of entry especially in organization where their workers are very mobile [36].

Cloud-based DLP: Protects data that are in active use or transit in cloud systems or while in the process of being provided to cloud programs. Because cloud computing a system that is gaining popularity in organizations today, cloud DLP offers a vital solution component of DLP.

Therefore, the decision is whether to go for the best single solution or whether the hybrid carrying the option of going towards the single best solution as well as other solutions that have been excluded in this process is preferable in the context of analyzed situation in the organization's structure, data usage and potential risks. In the assessment of DLP solutions it is recommended that the metrics used include scalability, installation, integration and adaptability to fresh threats. This is where development of cleat, comprehensive, Admirable and precise organizational policies on such aspects as handling, sharing or storing of the data as becomes a significant component of DLP process [37]. They should be aligned with the organizations data protection direction and compliance requirement and strategy.

Access Control: The question here is who may go to which form of information and in what way. First, it is becoming necessary to implement the RBAC model in order to restrict the access of the employee to only that data which he or she requires in regard to his or her working position.

Data Movement: Define how such data can be transferred and in like manner be cascaded. Stakeholders must define what the policy allows regarding the exchange of data through email or storage in clouds or duplication in an external device such as a USB.

Data Encryption: Choose words that imply choices and decide what type of data should be encrypted during storage or during transfer so that in the event that it leaks while in storage or when it is being transferred it will be safe [38].

User Monitoring: Formulate a policy about how user's actions and their information undergo scrutiny, as well as how it is analyzed and altered without the infringement of user's rights to privacy. Several activities including instances of moving mass quantities of large files, using the 'at risk data' or increasing levels of data sharing are easily noticeable as risky.

There are also social restraints complied with to allow it to address these new threats and challenges when they are discovered due to changes like technology and business. As with other

company policies and procedures, DL policies have to be implemented and communicated to all staff within the organization to help them fulfil their roles when it comes to the handling of data. While it may be relatively simple to paint with a broad brush on deploying DLP controls, it often is in the best interest to filter DLP controls depending on use case scenario or as roles and types of information being dealt with [39]. The advantages of the detailed controls are less false positive, enhanced protection, and less harm to productivity.

Granular DLP controls can include

Context-based policies: Such policies use the information regarding a particular user employing a related data (the role of the user, geographical location, time, or the application) in order to define whether an action is possible.

File-level controls: Limit MODIFY and COPY access rules by classification, dependent on Confidential. For example, there could be some forms of data may be communicated outside the organization, but in an encrypted format.

User-level controls: Limit different parts of the application, web page, functions, or data entry by setting up several user levels and restrictions according to the organization role, division or role/reported organizational clearance of the user. This approach ensures that high risks areas are well protected needing strong controls while other areas of the organization can have little interference by the DLP systems hence cause as little disruption as possible while providing best protection possible [40].

Monitor and Respond to DLP Alerts: Nevertheless, good DLP is not completely about preventing incidents of data loss; it should also be a 24/7 mechanism that is ready to respond to these types of incidents when they occur. Inadequate DLP should be linked to a SIEM solution so that security event review is straightforward, and a rapid response to threats is possible. Another merits are that, as soon as DLP system produces the output for potential data leak the security team needs to react immediately. This involves discovering what caused the alert and then getting to determine the alert if it is really positive or negative before handling it as the case maybe. Alert management procedures have to be clear, the teams have to understand how to work with the incidents correctly [41]. It may also require some form of pausing the transmission of data at any

juncture, quarantining infected files, or notifying the concerned entities. Also, the alerts and response to DLP should be periodically audited in a bid to analyze the effectiveness and discover the loopholes within DLP strategy.

Continuously Review and Update DLP Strategies: This means that DLP strategy is not set in concrete within a particular environment since the structure of data protection is dynamic in nature. The novelties force organizations to recall their DLP policies, technologies and processes more often with a purpose to defend against them. This way, new possible deficiencies appear or previous weak points are revealed as the organization expands, new technologies are integrated, or policies regarding data storage change. Moreover, organizations should get familiar with any other new change in the regulating laws that may impact the need for DLP. The protection laws always evolve and thus the DLP solutions have to be updated in order to ensure that they satisfy those requirements as well as protect data. Other factors include but not limited to the following: The last one is perhaps the most crucial component of any DLP effort; hence the need to rehearse constantly all employees involved. Notifying the users about new data protection policies, threats and measures often reshuffles the relevant perceptions and avoids having the access data opened and shared with the wrong people due to amateurs' negligence [42].

Challenges that can be encountered when implementing Data Loss Prevention Solutions

Data Loss Prevention (DLP) is one of the key components of organizational information asset protection; yet, the practice faces a number of challenges in its endeavor. The following are the main factors behind these challenges: Technical; Organizational; New and continuous threats: cyber threats. Knowledge of such issues is cardinal to organizations aspiring to embark on successful deployment of DLP technologies and to the accomplishment of the goal of providing adequate protection to the data that organizations deem worthy and sensitive. In the subsequent sections of this manuscript, some of these major issues are highlighted. There are major problems associated with the implementation of DLP solutions and how they can be addressed. The first difficulty that any organization is most likely to encounter if it decides to put in place a DLP system is the aspect of classification of data [43]. Data classification is the systematic arrangement of data in relation to risk path, importance or sensitivity to an organization. It is a crucial procedure that

positively affected the enhancement of application and implementation of DLP systems. However, it is not easy to group a lot of information.

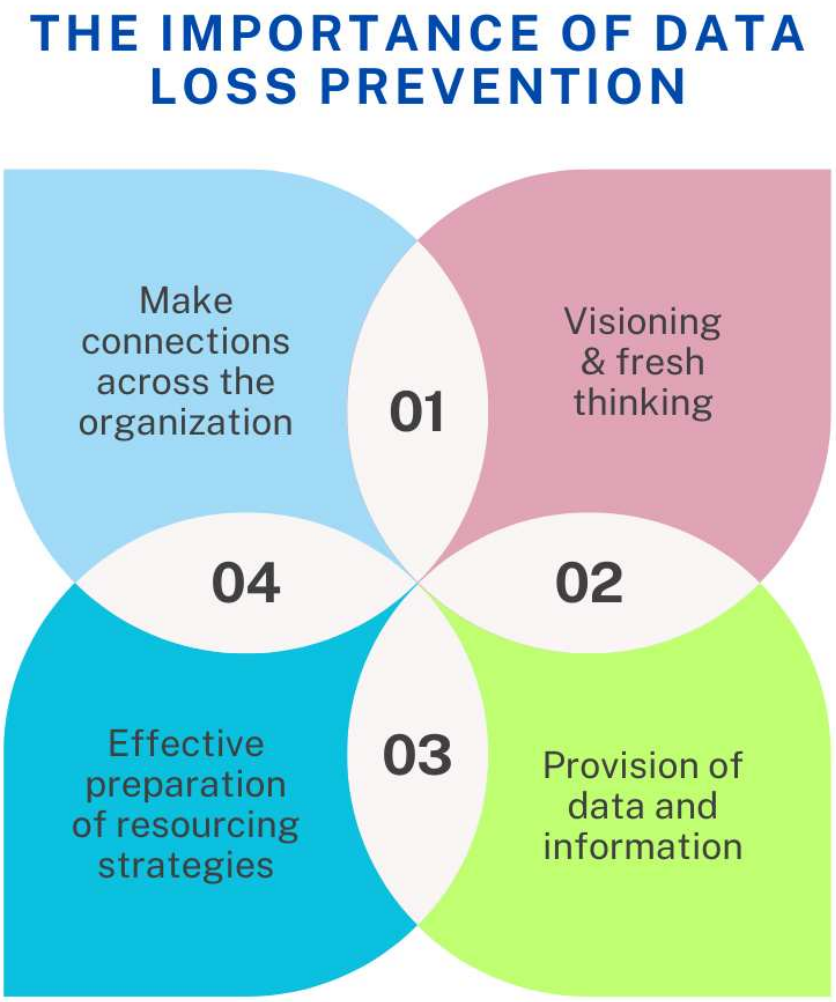

Figure: 3 showing importance of data loss prevention

Because of the amounts of these unstructured data such as emails, documents, image files, etc., the organizations have a difficult time trying to work out which data should be managed more securely. Traditional methods of classification are slow and imprecise and the unconventional methods of classification are decentralized; whereas the climate tools and methods for classification need a fine data to be processed and it might have problems with the complexity of the data. For example, some data may be placed in folder's subfolders, some data may not be tagged unified or with

proper tags for different teams. To solve these problems, organizations can use such advanced technologies as machine learning (ML) and artificial intelligence (AI) in order to classify data. These technologies can patent the usage and contextual and behavioral data and, therefore, more accurately and with less interaction, highlight the data contents of a more sensitive nature. In any case, it is clear that to ensure that such systems are sorting through data appropriately, they must be periodically updated [44].

One of challenges that may be likely to be experienced when organizations install DLP solutions is the problem of balancing security and efficiency. The controls within the DLP concept's goal of implementing safeguards against unwanted access to information: The strict measures can become an obstacle for a workforce. For instance, DLP will fail either to let run or at least raise alarms on real processes such as sharing of project folders with other colleagues or copying data to external peripherals which in this instance will disrupt business. As much as the best DLP system may mimic high false positives employees get annoyed with the system and learn to avoid it or work round it. On the other hand if the levels of interpretations are set at very low and they are also very flexible, then the probability of protecting most of the critical data may also be very low. To overcome this issue, the DLP policies must receive a special focus when being implemented by the organizations [45]. Consistent and forceful implementation of sweeping measures that prevent or recognize the effectiveness of incorporating social media work for all related tasks effectively minimize Interference. In addition, having UBA as an element within the DLP system enables organizations to reassess patterns and modify security. Therefore, context-based policies help to come up with the greatest protection of data loss and the greatest accomplishing of employees' tasks with the least number of constrains.

The outside threats are usually handled by DLP systems while one of the largest risks to organizations is internal; employees, contractors and third parties with access to organizational data. There is another type of threats that are even more challenging to counter since insiders have all the rights to fulfill some tasks and access some systems and information. This means that either malicious or negligent action can be done unobserved and many traditional DLP solutions are likely to miss these threats. Insider threats are not things that can be solved by putting on layers of technologies but it should also involve the employee. While at times DLP solutions may define,

regulate usage and attempt control of data leak, there are other methods like user activity monitoring, behavior analysis, the continuous audit trail which can assist in the identification of unauthorized activity by the actual user. In addition to the above, awareness and training, which both pertain people's education regarding risk touching on data breach and particulars of reporting, are crucial components in organizations [46].

To address this challenge, there is need for organizations to explain the need to protect the data in good details. Another element of training should be the reminder that DLP systems are there to safeguard the organization's and employees' information, not to police behavior. Also, the authors touch upon the importance of giving employment opportunities to work in the development and implementation of the system; this is because the latter might not understand why certain actions are reported, what data is monitored, and so on However, transparency can play a valuable role here: the company should explain to the employees where they can file a complaint and receive an exception [47].

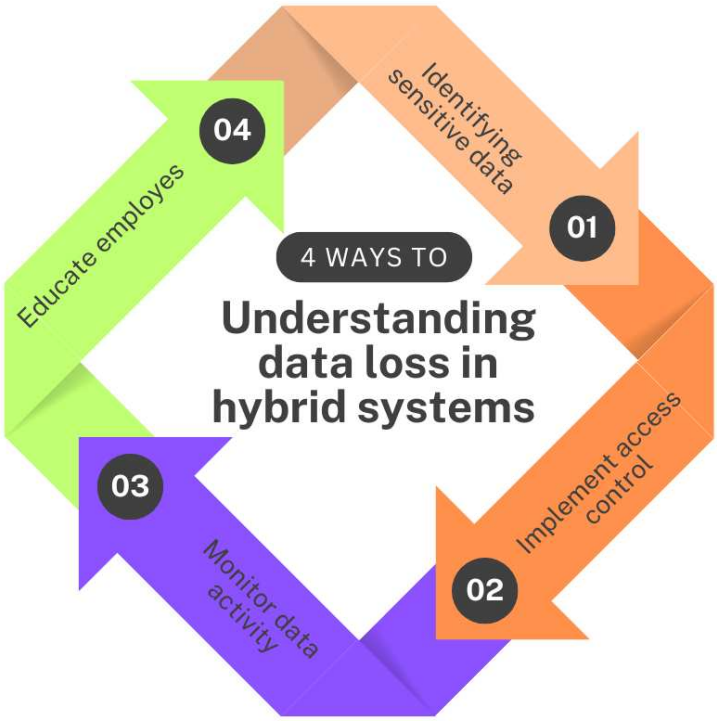

Figure: 4 showing understanding data loss in hybrid systems

Another tough task that comes with deployment of DLP solutions is compatibility of the solution with the network, endpoints, clouds as well enterprise applications in the organization. DLP systems must have capabilities to monitor and secure the data irrespective of the environment they are in, such messaging system to integrate with DLP can be challenging when incorporating with the legacy or With Other type of platforms. For instance, data may be stored on local servers and on remote servers that are hosted by third-party cloud services, as well as on the employees' mobile devices, each of which will pose its own risks. The ability to monitor data in real time across all these environments while at the same time not creating a situation where DLP solutions are separated into distinct areas or indeed excluded from any environments requires careful planning and an understanding of the technicalities that goes beyond the usual project planning. -buying sides have to consider the factors which make DLP solutions to have high flexibility in order to work well with organizations' infrastructure [48]. It is also important to check that DLP solutions integrate with other applications, especially for the cloudscape case. A lot of today's DLP software solutions has native cloud integration which helps in the process of data protection across different platforms. Moreover, a single approach to protect data, accessible on both local networks and the cloud, can minimize risks.

Companies usually need to subscribe with numerous data protection laws including the GDPR, HIPAA, and the CCPA among others. Compliance thus forms a critical part of the DLP solutions but managing the system to conform to changing regulations is a challenge. Compliance mandates always demand the organization to show where the data is, how it is accessed, and who is authorized to get access to it. DLP solutions must be set up to not only to block unauthorized users from accessing sensitive data but also to record, track and report activities that are indicative of a threat [49]. As a way of tackling this challenge, organizations need to recognize that the DLP solution need to be frequently updated to cater for new regulations. Such compliance reporting characteristics as audit trails incorporated in the DLP system must be automated to make it convenient to present compliance with the required legal provisions. Also, the implementation of data protection checks that involves regular review of data handling policies, compliance audits of data handling can also help an organization to stay on track.

An initial issue in having to deal with DLP is the issue of noise, or in other words, the creation of false positives, cases where legitimate conducts are flagged as breaches of security policies. This is rather worrisome especially because organizations that have integrated DLP systems in their everyday tasks will also be most affected. In the long run issues result in greatest threats which is alert fatigue where the security teams get overwhelmed and start using notifications as general indications without really paying attention to them. Due to false positives, organizations need to optimize the DLP rules and policies that have been put in place. However, when these rules are developed they should be reviewed periodically and fine-tuned to reduce possible false positives depending on feedback from users and the security teams. Also, the implementation of DLP systems with AI an machine learning features may increase accuracy as the systems learn from previous events and do not make mistakes with data recognition. Subsequently, despite being necessary tools in the protection of data, the use of DLP systems is accompanied by some complexities [50]. Some of the challenges are classification of data, interoperability of security with productivity, controlling insider threats, dealing with workers' resistance, integrating the security system with existing systems and infrastructure, following legal requirements and addressing the problem of false alarms. When these challenges and best practices be known, DLP solutions can be successfully deployed in organizations to safeguard data without causing interferences ad non-conformity.

Future Trends of Data Loss Prevention (DLP) Solutions

Data Loss Prevention (DLP) is still a relatively young discipline as the amount of pressure rises on the companies to guard the private information in the more flexible and dispersed environment of the modern network. The risks that data faces are evolving in complexity and, therefore, the means that are required to protect the data must change as well. Thus, those trends in DLP that will evolve in the future depending on the increasing complexity of cyber threats and the growing integration of data in cloud and hybrid environments will define further advancements in the sphere. Some of the trends that will define the future of DLP technologies are captured below. Both AI and ML have an incredibly vast impact on cybersecurity, and DLP is not an exception. Historically, DLP solutions depend on pre-determined set of rules and signature-based detection for assessing vulnerabilities of data leakage [51]. However, these systems that are programmed as

artworks to give quick and smart solutions have limitations when presented with large volumes of data, especially within complex and large data landscapes that may ignore even small signs of risk.

AI and ML make DLP fairly more intelligent and automated in a way that these systems aren't just programmed to perform security tasks but also they learn and decide based on the new data set analyzed. For instance, with AI, DLP can monitor user's activities, identify and anticipate data leak incidences and occurrences that have not yet happened. This predictive capability will help to take DLP systems to the next level by greatly diminishing the number of false positives seen in current systems as well as vastly increasing the accuracy of monitoring of data. With advancement in AI and ML, DLP solutions will be able to provide analysis in real-time and will be able to safeguard data with higher accuracy and duplicity and without much input from supporting personnel. All of those technologies will also learn about constantly changing behavior of cyber criminals, which will make DLP solutions much more reliable in stopping newly appearing threats [52].

That is why a need for native cloud solutions, especially in the context of DLP, is emerging together with the further migration of organizations' IT environments to cloud platforms. Data storage is continuously moving towards cloud storage, Software as a Service (SaaS), and Infrastructure as a Service (IaaS) therefore DLP Systems should be compatible with these cloud-based systems. Conventional on-premises DLP solutions act effectively to monitor and safeguard the data within organization owned IT systems but fail to offer proper security for the data in the cloud. Other types of DLP solutions used in the cloud are cloud-native DLP solutions which are developed to tackle the challenges inherent in cloud platforms [53]. They are designed for real-time tracking and protection of data in the cloud, which may be located in the cloud of various types at any geographical location. Native-cloud DLP offers higher agility and availability, so it is evident that data security has the potential to grow with the organization's growing cloud environment. Further, they can be easily connected with Microsoft 365, Google Workspace, AWS, as well as other well-known cloud solutions, providing the best practice security for the cloud-stored data. As cloud growth does not slow down, even on the contrary, organizations will turn to these advanced, cloud natiön DLP solutions to protect data in hybrid and multi-cloud hybrid environments.

Zero Trust Architecture (ZTA) is a relatively new security framework postulating that nobody inside a network should be trusted by default. This model involves constant validation of all access requests and uses identity-based control, device health and usage control. Extending DLP solutions with Zero Trust is emerging as a dominant strategy for protecting sensitive data. It means, in the context of Zero Trust, data is not available for anyone, even if they are within the company's network. Mechanisms that are DLP together with Zero Trust shall make provisions for exceptional access with monitoring of trust in real time. For instance, if a user exhibits behavior that is different from their normal pattern, then DLP systems can either send an alarm or block access to some specific types of information considered sensitive [54].

When implemented hand in hand with DLP, Zero Trust will help an organization work around the principle of least privilege: even if an internal user has been compromised, the system will only allow them to access as much data as is necessary. Having this additional layer of security will be highly effective against internal threats as well as external threats. XDR is a new generation security solution that provides threat detection and response across endpoint, network, and cloud layers using a single platform. Through integration and subsequent comparative analysis, different XDR tools will potentially provide a more extensive perspective on the threats within an organization's IT landscape. The integration of DLP with XDR will strengthen data protection in a very big way [55]. DLP solutions focus on stopping data leakage, whereas XDR offers wide coverage of the entire IT environment which will help organizations have more effective threat detection and response. For instance, if DLP system finds some data leakage in a cloud application then XDR system identifies that data with endpoint and network activity then it will be easy for security analyst to handle the situation.

With the XDR, DLP solutions can enhance from automating the mundane alerting of DLP and can include a lot more of value giving deeper context to a leaked data instance. This integrated approach to data security will allow organizations to counter threats instantly in order to minimize loss. Despite the growing crosses by cross external threat actors who remain a real threat to organizations, insiders threats end up being ranked among the most reported. This is one of the main reasons why insider threats are often considered complicated since employees, or contractors, for instance, have legitimate access to the data. In the future, DLP technologies will have better

features to focus on insiders threats. This will require improved levels of user behavior analytics (UBA) which can spot 'abnormal' actions such as accessing critical data after business hours or transferring extensive data to removable media devices [56]. Proactive intervention will be made possible by machine learning model in detecting any possibly malicious insider activity since the program will work based on deviation from the normal set behavior.

Higher-end DLP systems will also link with the user identity and access management (IAM) solution, to risk manage every user according to his role and risk appetite across the organization. This way, the control on who has an access to the specific data and at what stage of the process will be more tightly regulated, thus in consequence minimizes the threat which insider could pose. Because of the Enhanced Data Privacy Regulation Industry, organizations are under pressure not only to secure crucial data but also adhere to different privacy laws and regulations like GDPR, CCPA, HIPAA, etc. These regulations will ensure organizations safeguard privacy and Monitor the collection, processing, use and sharing of the personal data and ensure the individuals are informed of the data processed. These are being introduced as privacy-first DLP which will contain provisions to meet these regulatory needs regarding data management. For example, DLP systems will ensure that PII will be automatically recognized, indexed and secured, alongside making sure that it is saved and transferred based on privacy laws [57].

These systems will also have solid reporting and auditing capabilities to support organizational claims of compliance with the legislation. Mainly, because when gained privacy principles will comprise into DLP solutions, the organization's data security will be enhanced, and the threats related to data privacy breaches avoided. This is especially the case when foraying into more collaboration means using tools, including cloud-based document collaboration systems, like Google Workspace, Microsoft 365 and others. Typically, future DLP solutions will be in complete harmony with these tools to enable an organization to regulate the flow of information both within the organization and with and external third party [58]. Modern DLP solutions will allow applying detailed access controls to the possible collaboration actions, e.g. file sharing, working on the same document concurrently, or transferring data between cloud applications. Through coming up with measures that regulate those activities depending on the type of information, the organizational data is secured while at the same time enhancing the data sharing among the various party.

The intensified volume of data flows, coupled with the complexity of contemporary IT environments, and raises the need for extending the functionality of manual monitoring and intervention in DLP systems. Consequently, key future trends of DLP will entail its increased automating and orchestration features [59]. Policies specify how messages are sent, how data is quarantined or the actions are prevented based on contextual data provided by context- adequate automated workflows. Orchestration is now expected to give higher efficiency to the DLP systems by integrating them with other related security structures such as SIEM systems, firewalls, and EPPs (Endpoint Protection Platforms). This feature makes the DLP solution respond faster and more efficiently to the needs of data protection by providing automated responses and directly interfacing with other security applications. Technology trends that will define the future development of Data Loss Prevention (DLP) solutions are as follows: Artificial intelligence and machine learning; Shift to cloud-based DLP; Zero Trust Strategy; and, Privacy-First. Because of these pressures, these innovations will help DLP systems become smarter, more efficient and more capable of meeting organizational needs. The knowledge about these trends will allow organizations to be ready to protect against data loss in the context of growing threats.

Conclusion

DLP solutions are required variant for effective cybersecurity strategies based on their specialization to protect different types of data in diverse landscapes. In this paper, the importance of DLP in the modern world, the changes in threats and concerns it faces, as well as the trends that characterize the direction of the development of DLP have been investigated. In this blog entry I will discuss how advances in cyber threats are slowly eroding the capabilities of traditional DLP systems. The problems organizations experience with execution of DLP solutions, including data classification, securing work interdependence, insider threats, integration with other systems, and legal requirements, prove that there is a demand for further development and enhancements in this area. The future expectations for DLP shall involve systems that can develop learned behavior from users, become fully adaptive to various interfaces and environments, as well as provide a feed to various threats in as real time mode as possible.

AI, machine learning, and cloud natives DLP solutions are emergent technologies that are changing the methods through which organizations are safeguarding data by providing increased automation, accuracy, and elasticity. In addition, the expansion of DLP networks through synergies with other security concepts like Zero Trust Architecture and Extended Detection and Response will strengthen the management of data security because it will include more extensive views of an organization's security landscape. While growing numbers of organizations embrace more friendly collaboration and cloud-based structures, DLP systems will have to be tailored to offer constant, real-time protection across different grades of environments. The growing emphasis on privacy and the necessity to meet the insider threat challenge contributes to the ongoing development of DLP systems that not only protect data but also help organizations meet data protection legislation. Thus, following a more integrated approach is possible to provide organizations operating in the modern conditions, achieving the desired balance between security risks and business processes.

Although getting and managing DLP systems has its challenges, the development in DLP technology does reassure an optimistic future in data protection in various environments, risk avoidance, and compliance to privacy laws. It is in this light that the role of DLP carries on in the struggle against data loss and other menacing cyber ventures in view of the dynamic advances in tools, architectures, and strategies by organizations.

References

[1]. Albugmi, A., Alassafi, M. O., Walters, R., & Wills, G. (2016, August). Data security in cloud computing. In 2016 Fifth international conference on future generation communication technologies (FGCT) (pp. 55-59). IEEE.

[2]. Arefin, S., Chowdhury, M., Parvez, R., Ahmed, T., Abrar, A. F. M., & Sumaiya, F. (2024). Understanding APT Detection Using Machine Learning Algorithms: Is Superior Accuracy a Thing.

[3]. Alenizi, B. A., Humayun, M., & Jhanjhi, N. Z. (2021, August). Security and privacy issues in cloud computing. In Journal of Physics: Conference Series (Vol. 1979, No. 1, p. 012038). IOP Publishing.

[4]. Arefin, S., Parvez, R., Ahmed, T., Ahsan, M., Sumaiya, F., Jahin, F., & Hasan, M. (2024, May). Retail Industry Analytics: Unraveling Consumer Behavior through RFM Segmentation and Machine Learning. In 24th Annual IEEE International Conference on Electro Information Technology (eit2024).

[5]. Bender, D. (2012). Privacy and security issues in cloud computing. The Computer & Internet Lawyer, 29(10), 1-16.

[6]. Duffany, J. L. (2012). Cloud computing security and privacy. In 10th Latin American and Caribbean Conference for Engineering and Technology (pp. 1-9).

[7]. El-Yahyaoui, A., & El Kettani, M. D. E. C. (2018, May). Data privacy in cloud computing. In 2018 4th International Conference on Computer and Technology Applications (ICCTA) (pp. 25-28). IEEE.

[8]. Friedman, A. A., & West, D. M. (2010). Privacy and security in cloud computing. Center for Technology Innovation at Brookings.

[9]. Gupta, R., Saxena, D., & Singh, A. K. (2021). Data security and privacy in cloud computing: concepts and emerging trends. arXiv preprint arXiv:2108.09508.

[10]. Kshetri, N. (2013). Privacy and security issues in cloud computing: The role of institutions and institutional evolution. Telecommunications Policy, 37(4-5), 372-386

[11]. Pearson, S. (2013). Privacy, security and trust in cloud computing (pp. 3-42). Springer London.

[12]. Sen, J. (2015). Security and privacy issues in cloud computing. In Cloud technology: concepts, methodologies, tools, and applications (pp. 1585-1630). IGI global.

[13]. Shaikh, R., & Sasikumar, M. (2015). Data classification for achieving security in cloud computing. Procedia computer science, 45, 493-498.

[14]. Shankarwar, M. U., & Pawar, A. V. (2015). Security and privacy in cloud computing: A survey. In Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014: Volume 2 (pp. 1-11). Springer International Publishing.

[15]. Sun, P. J. (2019). Privacy protection and data security in cloud computing: a survey, challenges, and solutions. Ieee Access, 7, 147420-147452

[16]. Tari, Z., Yi, X., Premarathne, U. S., Bertok, P., & Khalil, I. (2015). Security and privacy in cloud computing: vision, trends, and challenges. IEEE Cloud Computing, 2(2), 30-38

[17]. Yang, C. N., & Lai, J. B. (2013, July). Protecting data privacy and security for cloud computing based on secret sharing. In 2013 International Symposium on Biometrics and Security Technologies (pp. 259-266). IEEE.

[18]. Yalamati, S. (2024). Data Privacy, Compliance, and Security in Cloud Computing for Finance. In Practical Applications of Data Processing, Algorithms, and Modeling (pp. 127-144). IGI Global

[19]. Zhou, M., Zhang, R., Xie, W., Qian, W., & Zhou, A. (2010, November). Security and privacy in cloud computing: A survey. In 2010 sixth international conference on semantics, knowledge and grids (pp. 105-112). IEEE.

[20]. K. Abouelmehdi, A. Beni-Hssane, H. Khaloufi, and M. J. P. C. S. Saadi, “Big data security and privacy in healthcare: A Review,” vol. 113, pp. 73-80, 2017.

[21]. S. Kauser, A. Rahman, A. M. Khan, and T. Ahmad, "Attribute-based access control in web applications." pp. 385-393. 133 Habeeb Omotunde et al, Mesopotamian Journal of Cybersecurity Vol.2023, 115–133

[22]. Hamza, and B. Kumar, "A review paper on DES, AES, RSA encryption standards." pp. 333-338

[23]. T. Zitta, M. Neruda, L. Vojtech, M. Matejkova, M. Jehlicka, L. Hach, and J. Moravec, "Penetration testing of intrusion detection and prevention system in low-performance embedded IoT device." pp. 1-5.

[24]. H. Kettani, and P. Wainwright, "On the top threats to cyber systems." pp. 175-179.

[25]. H. J. Hejase, H. F. Fayyad-Kazan, I. J. J. o. E. Moukadem, and E. E. Research, “Advanced persistent threats (apt): an awareness review,” vol. 21, no. 6, pp. 1-8, 2020.

[26]. S. Moin, A. Karim, Z. Safdar, K. Safdar, E. Ahmed, and M. J. F. G. C. S. Imran, “Securing IoTs in distributed blockchain: Analysis, requirements and open issues,” vol. 100, pp. 325-343, 2019

[27]. D. J. J. o. R. i. B. Mohammed, Economics, and Management, “US healthcare industry: Cybersecurity regulatory and compliance issues,” vol. 9, no. 5, pp. 1771-1776, 2017.

[28]. D. Vinayagamurthy, A. Gribov, and S. J. P. P. E. T. Gorbunov, “StealthDB: a Scalable Encrypted Database with Full SQL Query Support,” vol. 2019, no. 3, pp. 370-388, 2019.

[29]. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. J. C. Koucheryavy, “Multi-factor authentication: A survey,” vol. 2, no. 1, pp. 1, 2018.

[30]. R. YERRAMILLI, and D. N. K. J. J. SWAMY, “A comparative study of traditional authentication and authorization methods with block chain technology for egovernance services,” pp. 149-154, 2019.

[31]. E. Pagnin, A. J. S. Mitrokotsa, and C. Networks, “Privacy-preserving biometric authentication: challenges and directions,” vol. 2017, 2017.

[32]. Olade, H.-N. Liang, C. Fleming, and C. Champion, "Exploring the vulnerabilities and advantages of swipe or pattern authentication in virtual reality (vr)." pp. 45-52

[33]. Lopez, and J. E. J. C. N. Rubio, “Access control for cyber-physical systems interconnected to the cloud,” vol. 134, pp. 46-54, 2018

[34]. D. Servos, and S. L. J. A. C. S. Osborn, “Current research and open problems in attribute-based access control,” vol. 49, no. 4, pp. 1-45, 2017.

[35]. N. Kashmar, M. Adda, and M. Atieh, "From access control models to access control metamodels: A survey." pp. 892- 911

[36]. Z. Tang, X. Ding, Y. Zhong, L. Yang, K. J. I. T. o. I. F. Li, and Security, “A self-adaptive Bell–LaPadula model based on model training with historical access logs,” vol. 13, no. 8, pp. 2047-2061, 2018.

[37]. T. Xiaopeng, and S. Haohao, "A zero trust method based on BLP and BIBA model." pp. 96-100.

[38]. T. Tsegaye, S. J. I. Flowerday, and C. Security, “A Clark-Wilson and ANSI role-based access control model,” vol. 28, no. 3, pp. 373-395, 2020

[39]. P. Cruz, Y. Kaji, and N. J. I. A. Yanai, “RBAC-SC: Role-based access control using smart contract,” vol. 6, pp. 12240-12251, 2018.

[40]. Rezakhani, H. Shirazi, N. J. N. C. Modiri, and Applications, “A novel multilayer AAA model for integrated applications,” vol. 29, pp. 887-901, 2018.

[41]. H. A. Abdulghani, N. A. Nijdam, A. Collen, and D. J. S. Konstantas, “A study on security and privacy guidelines, countermeasures, threats: IoT data at rest perspective,” vol. 11, no. 6, pp. 774, 2019.

[42]. Ghouse, M. J. Nene, and C. Vembuselvi, "Data leakage prevention for data in transit using artificial intelligence and encryption techniques." pp. 1-6.

[43]. Megouache, A. Zitouni, M. J. H.-c. C. Djoudi, and i. sciences, “Ensuring user authentication and data integrity in multi-cloud environment,” vol. 10, pp. 1-20, 2020.

[44]. C. Liu, Y. Cui, K. Tan, Q. Fan, K. Ren, and J. Wu, "Building generic scalable middlebox services over encrypted protocols." pp. 2195-2203

[45]. S. Shastri, V. Banakar, M. Wasserman, A. Kumar, and V. J. a. p. a. Chidambaram, “Understanding and benchmarking the impact of GDPR on database systems,” 2019.

[46]. J. Zeng, Z. L. Chua, Y. Chen, K. Ji, Z. Liang, and J. Mao, "WATSON: Abstracting Behaviors from Audit Logs via Aggregation of Contextual Semantics."

[47]. E. Whitman, and H. J. Mattord, Principles of information security: Cengage learning, 2021.

[48]. G. Aceto, V. Persico, and A. J. J. o. I. I. I. Pescapé, “Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0,” vol. 18, pp. 100129, 2020.

[49]. S. Fischer-Hbner, and S. Berthold, "Privacy-enhancing technologies," Computer and information security Handbook, pp. 759-778: Elsevier, 2017.

[50]. K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, Y. J. J. o. H. Jin, and S. Security, “Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice,” vol. 2, pp. 97-110, 2018.

[51]. T. Mahmood and U. Afzal, “Security analytics: Big data analytics for cybersecurity: A review of trends, techniques and tools,” 2013 2nd national conference on, 2013

[52]. K. Gai, M. Qiu, and S. A. Elnagdy, “A novel secure big data cyber incident analytics framework for cloud-based cybersecurity insurance,” on Big Data Security on Cloud …, 2016.

[53]. E. Hossain, I. Khan, F. Un-Noor, S. S. Sikander, and M. S. H. Sunny, “Application of big data and machine learning in smart grid, and associated security concerns: A review,” IEEE Access, vol. 7, pp. 13960–13988, 2019.

[54]. A. Gheyas and A. E. Abdallah, "Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis," Big Data Analytics, vol. 1, no. 1, pp. 1–29, Aug. 2016. International Journal of Information and Cybersecurity 56

[55]. F. Kache and S. Seuring, "Challenges and opportunities of digital information at the intersection of Big Data Analytics and supply chain management," Int. J. Oper. Prod. Manage. vol. 37, no. 1, pp. 10–36, Jan. 2017.

[56]. D. B. Rawat, R. Doku, and M. Garuba, "Cybersecurity in big data era: From securing big data to data-driven security," IEEE Trans. Serv. Comput., vol. 14, no. 6, pp. 2055–2072, Nov. 2021. [7] H. Vijayakumar, A. Seetharaman, and K. Maddulety, "Impact of AIServiceOps on Organizational Resilience," 2023, pp. 314–319.

[57]. T.-M. Choi, S. W. Wallace, and Y. Wang, "Big data analytics in operations management," Prod. Oper. Manag., vol. 27, no. 10, pp. 1868–1883, Oct. 2018

[58]. . Hu and A. V. Vasilakos, "Energy big data analytics and security: challenges and opportunities," IEEE Trans. Smart Grid, 2016.

[59]. V. N. Inukollu, S. Arsi, and S. R. Ravuri, "Security issues associated with big data in cloud computing," International Journal of Network Security & Its Applications, vol. 6, no. 3, p. 45, 2014.