Data Loss Prevention - Risk Assessment Service

All companies risk the loss of sensitive data as confidential or proprietary information escapes through unauthorised channels. Data losses translate to billions in dollar losses every year, in the form of damaged brand equity, fines for regulatory violations, and opportunity costs resulting from stolen intellectual property. Given the high stakes involved, enterprises must implement strong and well-designed safeguards for sensitive data.

Data Loss Prevention (DLP) is the process and methodology to detect and prevent the unauthorised transmission or disclosure of sensitive information. DLP depends on a combination of people, processes, and technology as its strategic control foundation. These control elements work together to help ensure data is utilised in its intended manner. Having hard disk encryption on your laptops while helpful in reducing potential data loss is not a complete solution.

Benefits

Prevent Data Leakage - Prevent accidental or malicious loss of data by insiders or hackers.

Reduce Cost of Investigation and Reputation - A DLP assessment can help reduce costs associated with data losses including remediation costs and brand damage.

Facilitate Early Risk Detection and Mitigation - Conducting a DLP Assessment will help identify data leakage and will help ensure information is protected.

Increase comfort level with senior management - Implementing DLP controls will help assure senior management that proper security safeguards have been implemented, allowing them to concentrate on other critical business issues.

Zinopy can help you reduce your risk of exposure. Our Data Loss Prevention Risk Assessment Service identifies sensitive data that has been copied or is in transit from its original intended location. The assessment captures and identifies assets on the network, on shares, on SANs, in Databases and Email Systems and in transit. We will also identifiy data owners and most common data users.

Zinopy Data Loss Prevention Risk Assessment Gives the Answers:

Zinopy offers a Risk Assessment that allows organisations to quantify and qualify their risk of data loss. At the end of the engagement you will understand:

- Where is confidential data and sensitive information exposed in open file shares?
- Who is transmitting confidential data and sensitive information outside the organisation? (Data-in-motion only)
- What network protocols carry the most violations? (Data-in-motion only)
- What business processes need to be updated?
- What regulations are being violated?

In a typical engagement, the Zinopy Data Loss Prevention Risk Assessment also identifies:

- What are your top security violations by data type and policy?
- What is your risk of non-compliance with regulations?
- What business processes, policies, and awareness programs are required to reduce risk?

Data-in-Motion Assessment

A Data-in-Motion assessment provides information on data travelling through the network. Leveraging the available DLP Technology, Zinopy consultants will configure and connect the system to the network so it can monitor the data travelling through it. The robust appliance has the capability to index incoming and outgoing traffic in real-time. Traffic entering or leaving the network is then analysed against a series of information rules to determine where broken business processes may exist, or detect the presence of a leak of sensitive information.

Zinopy Ltd. | Suite 12-13 | Plaza 256 | Blanchardstwon Corporate Park 2 | Ballycoolin | Dublin 15 | Ireland
T: +353 (0)1 8976750 | **F:** +353 (0)1 8976751 | **E:** info@zinopy.ie | **W:** www.zinopy.ie

Data-at-Rest Assessment

A Data-at-Rest assessment provides information where sensitive data resides. Leveraging the available DLP Technology, Zinopy consultants will configure the system to crawl repositories, where critical data may have been wrongfully copied from its intended storage place. This may include laptops, desktops, file servers, NAS devices, intranet portals, wikis, blogs, document management systems, and more. The data stored on these repositories is indexed and violations to corporate policy are raised as incidents, so they can be investigated.

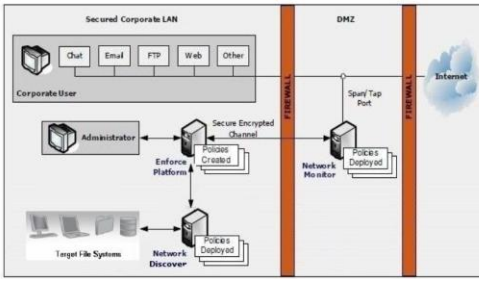
Assessment Methodology

The following diagram displays a visual view of our assessment methodology:

Phase 1 – Obtain Regulatory Requirements

The first step is to identify regulatory requirements that increase the organisation's risk of non-compliance and exposure. We can build standard (PCI DSS, PII, SOX) compliance rules and also custom search rule-sets. Both types of search rule-sets will be used in Phase 4.

Typical Deployment



Phase 2 – Obtain Policy Requirements

The second step is to obtain the organisation's policies. Our consultants will review the policies and build a "search" rule-set for use in phase 4.

Phase 3 – Obtain Classified Data List

The third step requires Zinopy consultants to work with your organisation and obtain a list of specific classified data search items. Non-Public Data (financial, business, HR, legal, and regulatory data), Personally Identifiable Information (social security numbers, credit card information, personal health data), and Intellectual Property (patents, trademarks, design plans) are examples of custom search data rule-sets that can be created. This information will be used to generate a custom search rule-set for use in phase 4.

Phase 4 – Configure and Execute Discovery Scans

Once phases 1, 2 and 3 have been completed, we will then configure the DLP for Data-in-Motion and/or Data-at-Rest to identify company policy violations. The scanning and monitoring processes can take several days to several weeks. Once the information is collected, the analysis phase can begin.

Phase 5 – Analyse Results

The Analyse Results phase is the process of reviewing "flag" information. This process is manual and is part of a decision process to filter out false positive items. Policy violations are recorded and packaged for future investigations. The results from this phase will serve as input for the next phase of "Report Generation."

Phase 6 – Generate Reports

The final phase is Report Generation. Based on our Analyse Results phase, Zinopy consultants will draft a findings report with all the identified policies violations.

Deliverable

The primary deliverable from the Risk Assessment is a Detailed Report with recommendations. The Zinopy Data Loss Prevention Risk Assessment identifies areas of Very High, High, Medium, and Low risk of data across network, and storage systems by data type, based on your evaluation of potential severity and your actual frequency of data loss. Data on desktops and laptops is outside the scope of the RA, but can be included in a full implementation of the DLP Solution.

Zinopy Ltd. | Suite 12-13 | Plaza 256 | Blanchardstwon Corporate Park 2 | Ballycoolin | Dublin 15 | Ireland
T: +353 (0)1 8976750 | **F:** +353 (0)1 8976751 | **E:** info@zinopy.ie | **W:** www.zinopy.ie

Zinopy will provide all software and hardware required to complete the Risk Assessment.