ZONES™

Data Loss Prevention Assessment

Discover, monitor, and protect sensitive business data

Today, an organization's success heavily depends on the ability to share, access, and disseminate information. The workforce is increasingly working outside the corporate network, accessing documents and databases from anywhere. And exposure to data breaches is compounded as more technologies enter an organization, which makes it easy for data to become lost or leaked. So instead of security that protects the network, it's time to shift attention to securing the data. The best place to start is a Zones Data Loss Prevention Assessment.

> Understand where structured and unstructured data resides in the physical architecture

> Identify the current and ideal state of your data classification and data loss prevention program

> Relate unstructured data to its application(s), from data lifecycle and application criticality perspectives

> Pinpoint where sensitive data is stored, what permissions surround this data, and who is accessing the data

> Gain visibility into data aging, access patterns, and true data ownership based on these patterns

Assessments and Outcomes

To rapidly assess the risk of data loss and to understand what to do next, Zones offers multiple data loss prevention (DLP) assessments.

Our Advanced Solution Group team will help you validate your data security requirements and priorities, and share insights into best practices to proactively secure data wherever it is stored or used.

Some of the key areas addressed are:

> Recommendations for optimizing your storage environment

> Classification of existing unstructured data by file type, age, use, and value to business

> Identification of businesses processes that can lead to risks and non-compliance issues

> Methods of achieving greater return on your investment

Data in Motion DLP Risk Assessment

Identify the sensitive data leaving your organization. During the assessment, the system monitors outbound email, web, file transfer protocol (FTP), and other configured protocols for sensitive content based on configured policy.

Data at Rest DLP Risk Assessment

Identify sensitive data residing within your organization. The system scans network files shares for sensitive content based on configured policy, no actionable response rules are configured during the assessment.

Data Risk Assessment

By combining data in motion and at rest risk assessments, you'll gain insight into sensitive data leaving and residing with your organization. The system monitors outbound email, web, FTP, and other configured protocols for sensitive content based on configured policy. In addition, the system scans network file shares for data at rest.

Project Highlights

Workshop

Prior to starting an assessment, you'll meet with our team to discuss and document your concerns and goals.

Technical Requirements

This portion of the planning phase of the assessment details the technical requirements including repositories to be scanned and samples of any documents to be collected.

Assessment

The typical assessment will run for two to four weeks, depending on the scope of your engagement and how much data/usage metrics you've requested.

The required hardware and software is provided as part of the assessment, and agent installers will be provisioned to be installed on any required repositories. After the assessment, we'll assist with securely wiping hardware before its return.

Reports

At the end of the assessment, you'll receive a report that details the findings from the engagement including remediation paths and next steps. Raw data reports can also be provided to allow for immediate action on high risk repositories.