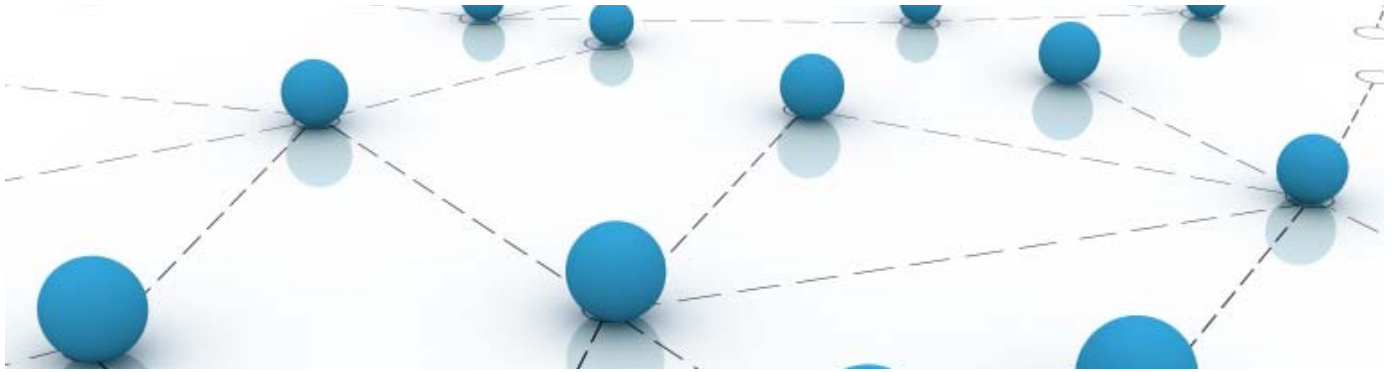


Pentura



Data Risk Assessment

Today's Challenges

Many organisations focus their efforts on controlling and protecting structured data such as databases but according to the IT analyst firm IDC, unstructured data accounts for up to 90 percent of all data stored by organisations.

The amount of unstructured data that resides on the network can be overwhelming in terms of customer data, employee data, intellectual property and confidential business information; all of which need protection from both sides of the firewall.

With limited visibility of access permissions or where the sensitive data resides, many organisations have found themselves falling victim to data loss, error or theft from internal, unauthorised access.

Key Benefits

Visibility of all Unstructured Data

Timely, Accurate Data Audit

Identification of Excessive Permissions to Sensitive Data

Identification of Potential Business Risk

Identification & Classification of Business Critical Data Assets

Remediation Planning

Define a Data Security Strategy

Data Audits help organisations manage change, reduce risk, and ensure compliance. However, these audits are a time consuming and challenging task for Security and IT operations managers. IT staff must search, sort and analyse the data to make sense of it and provide answers to the relevant audit questions.

Unless imposed by regulations, many organisations do not undertake these daunting and resource intensive projects. This results in users having more access to data than is required to effectively conduct business; which poses a security risk to a most valuable business asset, its data.

Introducing Pentura's Data Risk Assessment (DRA)

Pentura's Data Risk Assessment starts at the heart of the data security challenge by providing visibility of all unstructured data to build a current data access model.

Through an assessment process, Pentura assist with the identification of Business Critical Data Assets and then monitor and audit data usage. This provides visibility of the actual data usage profile and an understanding of excessive permissions.

Following the assessment, Pentura provide both technical and business data analysis reports detailing the potential high value data risk. The reports can prove risk reduction through the safe removal of permissions and following a technical workshop, can assist with defining a data security strategy for the business.

Pentura's DRA Service enables organisations to report on data risk accurately and in a timely manner; it also provides clear visibility of data access behaviour on Business Critical Data Assets resulting in improved internal control and understanding of sensitive data.

The Data Risk Assessment Process

Step 1 - Access Model Visualisation



The first stage of Pentura's Data Risk Assessment focuses on gaining visibility over all unstructured data that resides on the network.

Pentura query the Active Directory in order to obtain all the Users & Groups within it and collect the file permission information from the unstructured data on the file servers.

We are then able to correlate this information to provide a current Data Access Model.

Step 2 - Actual Usage Profile Identification & Data Classification

Pentura work with the client to identify the Business Critical Data Assets based on the three key factors when considering Information Security; Confidentiality, Integrity and Availability (C.I.A).

Once we have an understanding of where the sensitive data resides in terms of location (i.e. File Server, Share or Directory), Pentura collect audit data related to these assets.

This audit information allows the visualisation of the user/data relationships which provides us with the actual data usage profile.

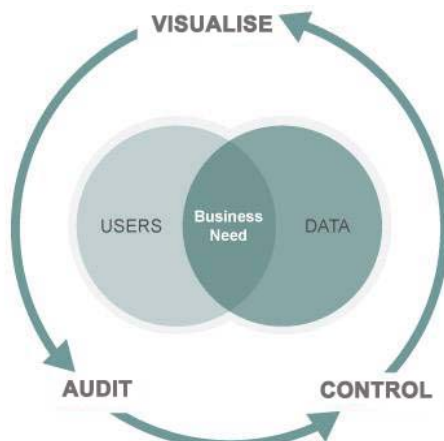


Step 3 - Risk Reports & Remediation Recommendations

Pentura analyse the data collected over the audit period in order to produce both management and technical data analysis reports. These detail the risk level and present methods for mitigating risk on the identified Business Critical Data Assets.

With the visibility gained over the data, Pentura provide remediation recommendations to remove excessive permissions in order to adopt a 'Least Privilege Access Model' on the unstructured data. Following an in-depth technology workshop, Pentura work with organisations to deliver a strong, prioritised data security strategy which meets the needs of the business today and into the future.

In addition, Pentura provide administrators with best practice advice to assist with managing Active Directory in order to address risk from a Data Leakage Prevention aspect — further providing organisations with the assurance that internal information is secure.



Contact:
Pentura Limited
Diddenham Court
Grazeley, Reading
RG7 1JQ

Tel: 0118 976 8960
Email: info@pentura.com