Demo: Data Security

Today, the world is riskier than it used be. Not a day goes by when another data breach occurs that severely damages business profitability, customer relationships and brand reputation. Estimates of the loss of customer information can range anywhere from $50 to $1000 per customer depending on the number of accounts impacted.

Furthermore, about 70% of security breaches can be attributed to insiders. As a result, data security has become a critical security issue. To adjust, security has to evolve. What was once a model that just focused on securing the perimeter, now requires focus on the data and securing the valuable information residing in your IT infrastructure.

Your data, however, can reside in different forms. In recent years, the world has witnessed exponential growth in the amount of unstructured data. Unstructured data can be documents, spreadsheets, web site content, product images, etc…and is often informal and continuously changing. Furthermore, unstructured data often contains sensitive information, making it difficult to secure. Today, you will see a solution that will classify, secure and monitor your unmanaged, unstructured data.

Steve was hired by Acme Games two years ago as an IT administrator. Acme Games is a cutting edge gaming firm with several wildly popular games. Upon accepting his job offer, Steve chose to receive a higher salary over stock options. Steve has root access to a number of file servers within Acme.

Three months ago, GIANT Inc. announced that it would acquire Acme Games for $300M – a 30% premium over their current share price.   Steve is disappointed he did not take the stock options that were offered to him, but at least he had his job with a high salary….

With his root access, Steve decides to see if what the new organizational structure will look like at GIANT. To his surprise, Steve notices that he is not going to be retained by GIANT. Fuming, he devises a plan to receive his own pay out. Steve decides to copy the source code of Acme's highest selling game and sell it in the black market. To cover his tracks, he deletes the audit trail.

How can your organization protect itself from this type of incident? IBM's Information Security Management solution can secure information in any form from its creation through destruction. IBM's approach is a policy based process that is focused on understanding what classes of data or information exist in your enterprise and what type of security controls should be applied to that information. It continues with the implementation and enforcement of these controls and then the monitoring for the effectiveness of these controls and what is happening to the data and its supporting infrastructure on an ongoing basis. The solution offers you a flexible approach to addressing your most acute information security challenges. One of its building blocks is the Unstructured Data Security solution that classifies, protects and monitors sensitive, unstructured data.

To start, the IBM Classification Module enables you to make more decisions on your content by classifying the sensitive data that resides in your IT infrastructure. At its core, it can automate the classification of content as it is ingested or content that already exists. And its unique learning technology for adaptive classification improves accuracy over time.
In this scenario, you can see we have created four categories – Human Resources, Research and Development, Sales and Legal. Based on natural language processing, the IBM Classification technology builds a statistical profile of the categories created based on sample texts and then compares new content to the category profiles. From here, these previously unmanaged, unstructured files can be collated into respective category folders.

Once classified and collated, how can information be managed for proper access and use? IBM Tivoli Access Manager for Operating Systems securely locks down business-critical applications, files and operating platforms by delivering centralized access control policy management and enforcement. This security capability helps block both insiders and outsiders from unauthorized access to and use of valuable customer, employee and business partner data.

 This has particular significance for super users, like Steve at Acme Games, that have root access. With proper security, Steve would not have been able to access the sensitive information that led to his malcontent.

Additionally, IBM Tivoli Access Manager for Operating Systems allows you to establish central roles, groups and privileges that are aligned to your business needs.

Finally, for the users who have been authorized access, how can you regularly monitor their use and ensure its within proper business guidelines? IBM Tivoli Compliance Insight Manager provides visibility into your organization's security compliance posture through automated, enterprise-wide user activity monitoring. It captures native log data from Tivoli Access Manager for Operating Systems and translates it into common business language for non-technical users. Furthermore, alerts can be established for activity deemed irregular. So in the case of Acme Games, Tivoli Compliance Insight Manager could have highlighted that an IT administrator was access files that he should not have been.

In summary, these three offerings are integrated to deliver a first of a kind Unstructured Data Security solution that classifies, protects and monitors sensitive, unstructured data. It will enhance your organization's security management – particularly those of you who are moving from a perimeter-centric security approach to a data-centric security approach.

To learn more about IBM data security solutions, contact your local IBM representative.