Classification Module

Add-on for Identity Manager-Data Governance Edition
helps identify content, manage risk and comply with ease.

Even a single loss or mishandling of unstructured data (such as documents, spreadsheets and PDFs) or a single failed audit can have grave consequences: loss of employment, a permanent resume scar, and loss of customers or revenue for the organization.

But securing unstructured data is complex: Virtually everyone in the organization creates, alters or moves unstructured data in their own way, resulting in an ever-growing anarchy of data that is difficult to classify. Does the file SCAN_09:42AM.pdf on an end user's SharePoint site contain any intellectual property, or is it a copy of a receipt that includes a customer's credit card number?

Manually classifying files is impractical. If you open a file to figure out what it is, and it contains someone else's personally identifiable information (PII), you might breach a compliance regulation. Moreover, your organization likely has terabytes of data to classify across Windows files servers, SharePoint and NAS devices—and that data is constantly changing (and growing). What was innocuous yesterday may be sensitive tomorrow after someone alters the file, so you must be constantly vigilant.

Classification Module for Identity Manager–Data Governance Edition, part of the Dell One Identity solutions, automates the process of securing unstructured data. Its "MRI like" ability to find, identify and classify unstructured content minimizes risk, enforces security and takes the stress out of audits.

Don't let your organization be the next security breach headline because of a lack of visibility into unstructured content. Classification Module's "MRI like" ability to find, identify and classify unstructured content minimizes risk, enforces security and takes the stress out of audits.

Benefits:
- Minimizes the risk of bad press and financial exposure associated with sensitive information falling into the wrong hands or a failed audit
- Automatically identifies and protects sensitive data based on policy, eliminating the need to open and examine each file manually
- Offers the flexibility to enable business compliance owners to intervene in the automated process where they need to
- Provides a visual risk map showing hot spots that need to be addressed and enables immediate action to be taken from within the solution
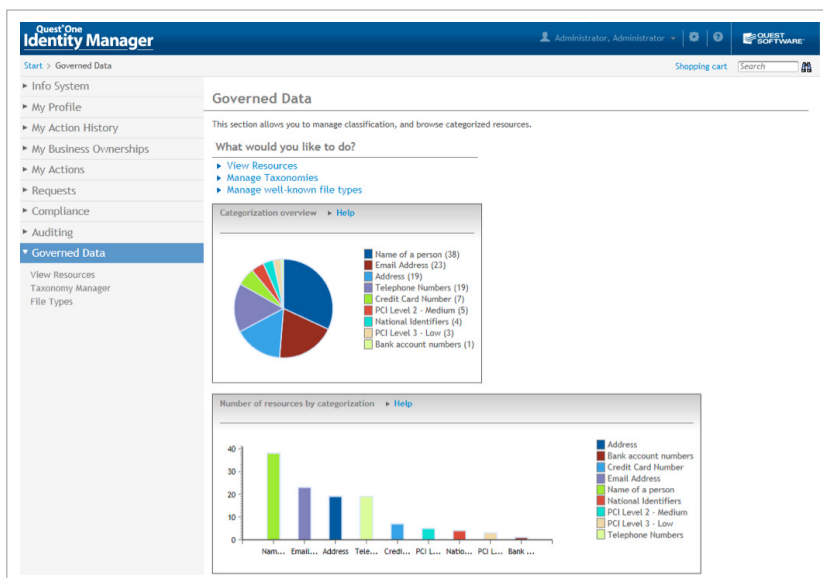- Simplifies the audit process for regulations such as PCI, HIPAA and SOX

Figure 1. Classification Module enables users to search categorized files within their governed data.

Features

An MRI scan for your data

Classification Module delivers a Management Risk Index (MRI) report that shows you a heat map of your organization's infrastructure, so you can focus on the "hot spots" of unstructured data that contain the most risk.

Automate classification of unstructured data.

Understand what sort of sensitive information is contained in your unstructured data files without having to perform the tedious process of manual evaluation. Classification Module can automatically categorize and organize credit card numbers, PII and more.

Tag and secure existing and newly created sensitive data.

Tag sensitive unstructured data throughout your organization as it relates to compliance regulations, use, sensitivity and so on. Then establish and enforce rules for how all existing and newly created sensitive unstructured data is treated, who may access it and where it can be stored.

Deploy a complete all-in-one data governance solution.

The combination of Classification Module working as part of the Identity Manager−Data Governance Edition protects your organization by giving access control to the business owners who actually know who should have access to which sensitive data, with the power to analyze, approve and fulfill unstructured data access requests to files, folders and shares across NTFS, NAS devices and SharePoint.

Additional features supplied by Identity Manager− Data Governance Edition

Restricted access – Define access policies for your organization to ensure that sensitive unstructured data is only accessible to approved users. Identity Manager-Data Governance Edition locks down sensitive data such as files, folders and shares across NTFS, NAS devices and SharePoint.

Data owner assignment – Determine and assign the appropriate owner of data for all future access requests by evaluating usage patterns and read and write access.

Simplified auditing – Aside from using Classification Module to classify the data, Data Governance Edition will identify user access to enterprise resources such as files, folders and shares across NTFS, NAS devices and SharePoint to provide key information during audit preparations.

Automated access requests – Use built-in workflows to automatically direct access requests from the request portal to the appropriate data owner. Approved requests can be automatically and correctly fulfilled, with no burden on IT.

Access verification – Ensure that only approved users have access to specific resources, including those who have left the organization or department or whose roles have changed. Identity Manager-Data Governance Edition enables you to monitor user and resource activity, and configure and schedule a recertification process for data owners to verify and attest to employee access.

Personalized dashboard – View trends and historic and current data access activity, and attestation status on a personalized dashboard with reports that can be used to prove compliance to auditors.

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results. www.dellsoftware.com.

DELL