DATA CLASSIFICATION FRAMEWORK USE CASES

Finding Sensitive Data

Organizations trying to locate the sensitive data among their vast collection of unstructured data can use the Varonis IDU Data Classification Framework to accelerate the process of finding sensitive data and also ensure that results are actionable.

The Varonis IDU Data Classification Framework can be used either with an existing data classification product, or without one. If you don’t have a data classification solution in place today, the IDU Data Classification Framework includes basic search capabilities that can help you look for sensitive data by scanning content for specific words or phrases, and/or by looking for content patterns that are described by regular expressions.

The IDU Data Classification Framework accelerates the process of finding sensitive data by using the unique meta-data map that the Varonis IDU creates by analyzing your business data, data access permissions, and how data is used by the users in your environment.

If you need to identify credit card data, for example, so that you can comply with the Payment Card Industry Data Security Standard (PCI-DSS), the IDU Data Classification Framework would help in two ways. First, it would help you find that data faster by allowing you to hone in and focus your search to find truly vulnerable data first. If, for example, only three groups in your organization need access to the credit card data, the IDU Data Classification Framework can look first at data accessible by the other groups to see if there is credit card data there. This produces results quickly and helps in a second way as well: by providing a remediation context. The remediation path for credit card data accessible by groups without a business need is implied by the search: remove their access. This remediation context means that the IDU Data Classification Framework produces highly actionable results.

If your organization already has a data classification solution in place, the IDU Data Classification Framework can take the classification results from that solution, and provide business context using its meta-data so you can understand who owns the data, which data is overly accessible and whose access to that data should be revoked. The IDU Data Classification Framework can also help accelerate future scans by feeding your classification solution information about which data was newly added or modified. That will enable future scans to focus on just that data, rather than having to rescan all data.