

5 Steps for Securing Sensitive Financial Data



Roughly 73 percent of businesses admit they have suffered at least one sensitive data leak within the past year. Your business can prevent sensitive financial data exposure with these five key steps.



Define the scope of data to protect

Identify all the data created and stored within your organization, including account details, financial records, personally identifying information (PII) and intellectual property. Also define data locations and formats.



Categorize the data

Define data sensitivity categories and map all data to the appropriate category. Factor in any regulatory requirements during categorization.



Discover where data actually lives

Scan all corporate resources and employee devices for a picture of where organizational data truly lives. Make sure all file types and cloud drives are included in the inventory, including those used by remote workers.



Tag data by category

Label each piece of data with the appropriate sensitivity category. Most organizations will automate the process with a data discovery and classification platform that tags data in real-time on an ongoing basis.



Secure data according to classification

Automate the application of appropriate security measures based on category. Security processes will vary according to data type, location, regulatory requirements and level of sensitivity.

Get the guide

Need help? Download **How to Identify and Classify Sensitive Data**, the free Qohash guide that walks you through each step of the process.

[FREE GUIDE](#)