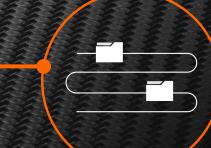
# Data Classification

## A NEW PERSPECTIVE

Enable the creation of attributes for data identity to determine how to manage and secure data through proper classification.

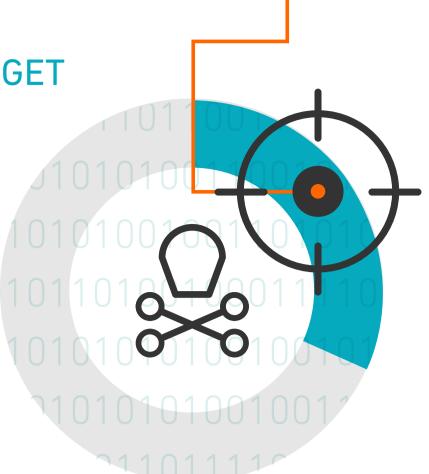


## THREAT ACTORS ACTIVELY TARGET

THAT HAS
SIGNIFICANT
VALUE

OF YOUR DATA VALUE.

How can you protect important data assets? First, understand what they are. And that's why 39 percent of North American and European decision makers utilize data classification tools.



# **DATA CLASSIFICATION: SIMPLIFIED**

In order to be one step ahead of threat actors, it's vital to get familiar with the data within your organization.



#### This type of data is subjected to local

ELEVATED DATA

or national compliance regulations and, if lost, may violate a business agreement or result in significant economic harm. Technical controls, combined with managed security that integrates intelligence with defense, will ensure its protection.

#### Could harm customers, employees and

**HIGH-RISK DATA** 

earnings, while also causing brand damage. You should protect high-risk data through detailed policies and procedures, plus unified security controls that are customizable by the workload. **UNCLASSIFIED DATA** 

#### May be handled as public information

without harm to an organization. As its sensitivity decreases, a company can reclassify it.



designed to scan resources that could contain confidential information to later be classified.

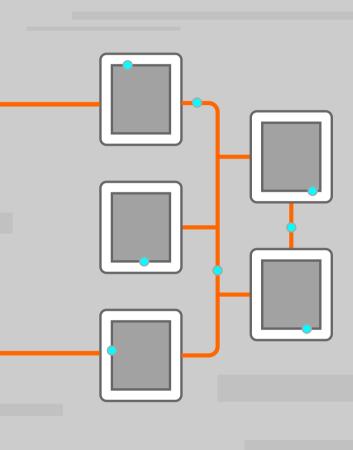
Determine how data is handled by

allowing the tools associated with

Data discovery tools are specifically



data classification to deterministically match data, such as credit cards and SSNs, then apply labels so that information can be protected.



THE DATA RED FLAGS

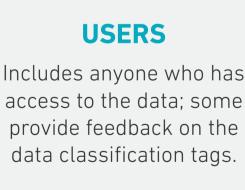


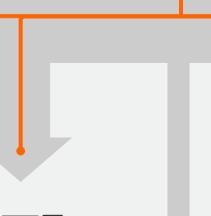












### **AUDITORS** Manage risk and

compliance, or are an officer for privacy and data. They also review feedback from the users.



@armor

1 844 682 2858

**CLOUD COMPANY™** 



armor.com