

QOSTODIAN PRIME™

Organizational data risk report

Report name: **HI Risk Assessment**

Reporting period: **Jan 1, 2022 – Jun 3, 2022**

Generated by: **Tom J, VP of Information Security**

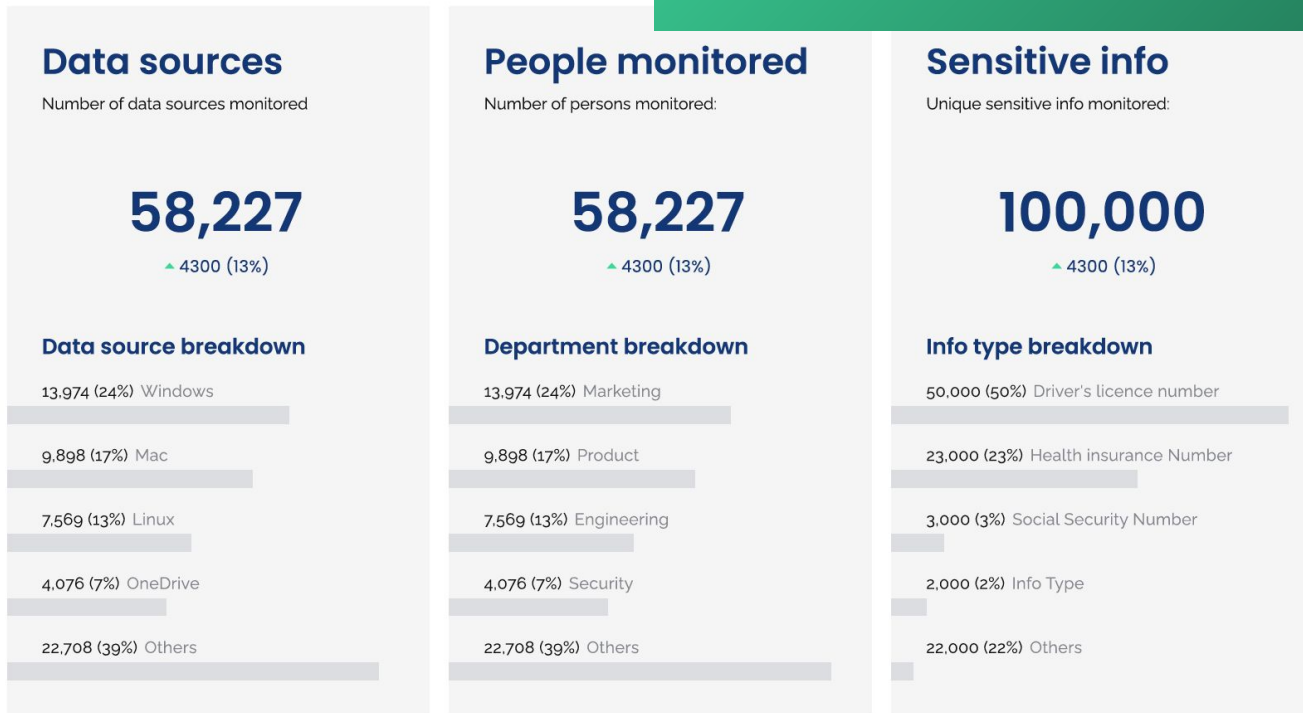
Created on: **Jun 3, 2022**

Tom proactively monitors his business systems and end points with Prime. Employees interactions with sensitive data are monitored 24/7, and Tom is notified the moment risky, non-compliant behavior occurs. Tom downloaded this report to quantify risk levels for his Board and provide a corresponding action plan.

Monitoring overview

At-a-glance, Tom can see the exact quantity of data sources, employees, and sensitive data type being monitored. With flat rate pricing, Tom is able to increase the number of targets as needed to keep the business safe, without incurring additional fees.

Overview of your Qostodian platform coverage and sensitive data holdings.



Reporting period: Jan 1, 2022 - Jan 3, 2022

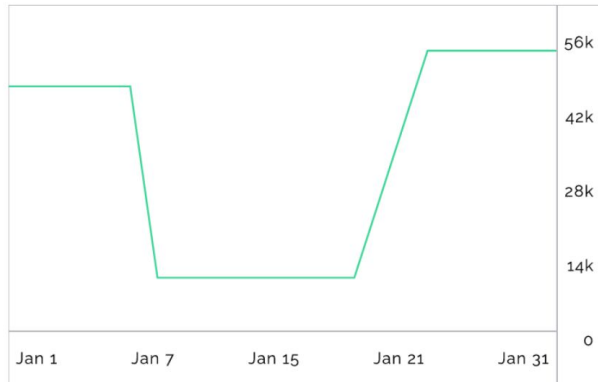
Organizational Risk Score

Total risk : 56,708

▲ 4300 (13%)

Risk score evolution

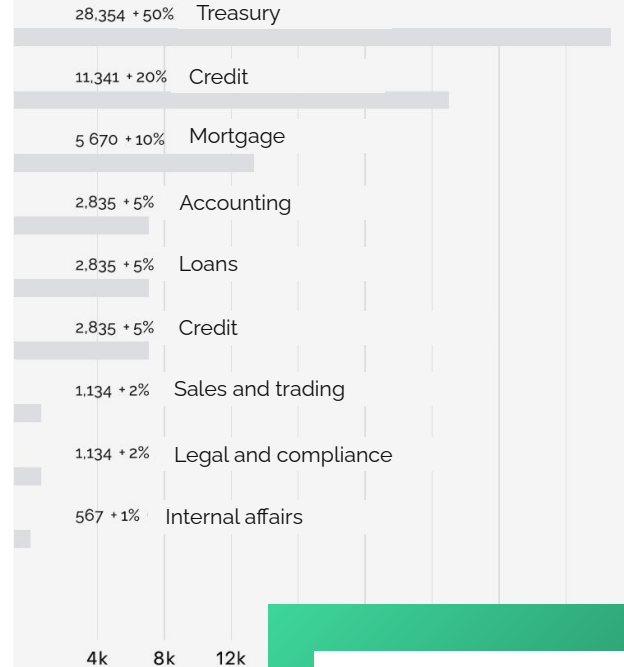
Organizational risk score evolution over time



With risk configured specifically to Tom's business, Prime generates an organizational risk score and provides insight into change over time.

Riskiest departments

Based on total risk score



Tom keeps an eye on the departments with the most sensitive data in their possession.

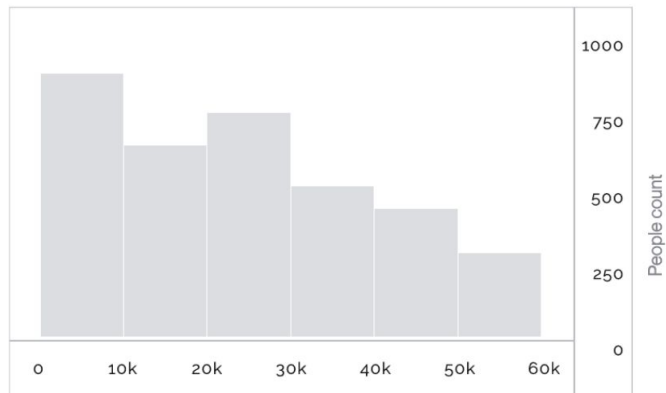
People-centric view

Total monitored people : 56,708

▲ 4300 (13%)

Risk score distribution

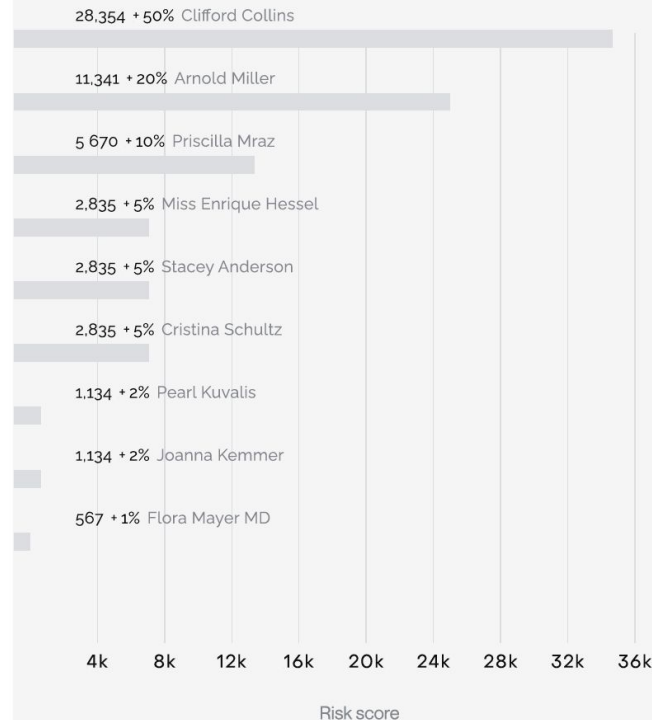
Distribution of monitored people risk scores at report generation.



Risk score segmentation

Riskiest people

Based on total risk score



Configured to Tom's risk tolerance, Tom can keep track of people who handle large quantities of sensitive data. On his risk intelligence dashboard, his team has created a "watch list" with views of percent change over time.

Automatic views of data propagation

Tom can show immediate remediation of a critical incident: a policy violation related to a specific customer's credit card number.

Tom was able to run a search for the credit card number, see which employee first interacted with it, and which additional employees had it in their possession over time.

The screenshot displays a search interface for sensitive information. At the top, a search bar contains the text "4888 8669 8678". Below the search bar, there are several filters: Country, Info Type (set to 1), Sensitive Info, Category, Regulation (set to 1), and Match Ratio (set to 1). The search results are displayed in a table with columns for employee name, risk score, and data propagation details. A tooltip is visible over the first result, providing additional information about the data propagation.

Search results table:

Employee	Risk Score	Data Propagation
Nicolas Thibeault General & Administrative	797	7 infos 6 files Until today (89 days)
Kaiya Lipshutz Credit card	861	24 infos 56 files Until today (23 days)
Kaiya Lipshutz General & Administrative	196	16 infos 39 files 15 days 9 days
Mira Saris Engineering	669	37 infos 109 files ...
Aspen Culhane Engineering	409	37 infos 109 files ...

Tooltip for Nicolas Thibeault:

Nicolas Thibeault possessed a maximum of 7 infos during this period of time across 8 files.
Start date : February 3rd 2021
End date : -