QOHASH

Qohash for GenAI

Track and secure high-risk files to reduce oversharing and accelerate GenAI adoption

Ideal customer profile (ICP)

- **Industry**: Financial services with sensitive data
- **Size**: Minimum 1,000 employees with a mature team
- **Technology**: Microsoft-centric, early adopters of GenAI
- **Concerns**: Unstructured data security/file security
- **Culture**: Innovative, enjoy working with scaleup like Qohash

Market trends

- **Files have always been one of the riskiest areas of the business.**
- **Oversharing files previously posed a limited risk** because users were not necessarily aware of the existence or locations of sensitive files.
- **However, GenAI tools like Copilot will identify all accessible data**, including overshared files, dramatically increasing the risk.
- **GenAI is a massive competitive edge for organizations**, and it is happening faster than people think (shadow AI is well underway — employees are already utilizing it).
- **If machines and AI will be using your data in new and unexpected ways**, you need a way to track this data and remediate oversharing.

Qohash's advantage

- **Using files with GenAI is a baseline requirement**, and you need a quick solution.
- **Qohash provides a turnkey solution with a narrow focus** on the riskiest data sources containing files accessible daily by users and machines (NAS, M365, etc).
- **The solution deploys in days and provides a rapid initial response** with a granular data inventory for each employee, department, and data source.
- **Our service partners assesses the results and provides immediate recommendations** for reducing the risk of GenAI and maintaining acceptable data risk posture in future.

Main use cases

1. Baseline file security for GenAI rollout
2. Incident response: Identify the exact data elements involved in incidents.
3. Risk KPIs & metrics