



**IDLake™ powering
IDENTITY INTELLIGENCE**



*The traditional approach to building a virtual wall to protect data cannot be counted on.
That's why hundreds of "secure" networks are compromised every day.
By going where hackers buy, sell, trade and dump data,
4iQ provides a layer of protection never before available.*

4iQ scans deep and dark web sources for stolen, leaked or lost login credentials and other personal identifiable information (PII). **With team and technology**, 4iQ indexes billions of identity records exposed in hacked and dumped breach corpuses across the world.

As breach hunting pioneers, the 4iQ intelligence team has spent over eight years developing tools and techniques to both continuously crawl and manually access:

- **Very restricted forums.** These can be joined after a vetting process or by special invitation. These forums are transient - they often close, reopen, disappear and are re-constituted. Some are global while others are regional, using a specific language and local slang.
- **Semi-restricted forums.** These are also transient and found both in Tor networks and the surface web.
- **Tor and I2P networks.** The Tor Network fluctuates between 25k-60k sites, many of which come and go.
- **Dumped/leaked text -> file storage sites** (e.g. Pastebins).
- **P2P networks** containing millions of live torrents or files.
- **Surface web directories** leaking identity data.

4iQ automatically scans open and exposed data repositories daily:

- Open **MongoDB** with no authentication or access controls.
- Live **Cloud Sharing** sites like Mega, Google Drive.

98+Billion
Breach Attributes

20+Billion
Curated Records

6+Billion
Validated Passwords

16Million
Malicious Actors

54,000+
Breaches

24x7Service

The 4iQ breach team also monitors hundreds of actors on **Twitter, Discord, Live Torrents**, and other **social media, chat rooms / (IRC / Jabber)** who are actively engaged in chatter about breaches and exposed PII.

Finally, a significant portion of data is provided by private sources or from breaches and leaks not commonly known or available from any other vendors or underground forums, discovered for the first time by the 4iQ breach hunting team, or shared by underground actors to only 4iQ. 4iQ does not buy data.

As a result, 4iQ has built the world's largest and most accurate datalake of exposed identities - the **4iQ IDLake™** - that includes cryptocurrency wallets and addresses, IP addresses, phone numbers, passwords, credit card numbers, cvvs, social security numbers, birthdays, drivers licenses and other identity attributes.

MOST ATTRIBUTES TRACKED



