

Elite privacy and intelligence services for people with everything to lose.



Digital Executive Protection

We identify hidden risks across your threat surface, then reduce exposure through targeted removals, identity disruption, and threat monitoring.

Exposure creates risk. Exposure reduction restores control.

The Stakes: Why It Matters Now

Every exposed data point is a liability.

Home addresses, family details, breach data, travel records, and identity fragments circulate across thousands of systems. Adversaries only need one.

For our clients, privacy isn't a preference. It's operational security.

ObscureIQ's Digital Executive Protection program is built for high-risk individuals.

Executives, founders, investors, influencers, and public figures.

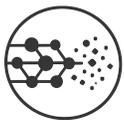
Those who need to control their exposure and stay ahead of emerging threats.

The Digital Executive Protection Framework



01: Threat Surface Mapping

Footprint Audits reveal your full digital exposure across data brokers, the dark web, public records systems, and identity infrastructure. For many clients, the scale of their exposure is surprising - and often alarming.



02: Deep Data Suppression

Footprint Wipe and Bespoke Deletes remove traceable information. No one offers a wider or deeper deletion service.



03: Structural Identity Control

Your identity is not stored in one place. It is constantly being reconstructed. Data brokers, public records systems, delegated exposure, and identity infrastructure play a part. ObscureIQ disrupts those structural identity links.



04: ThreatWatch: Active Threat Monitoring

ThreatWatch detects signals across the threat lifecycle — from online formation to real-world risk. We monitor social networks, dark web forums, paste sites, leak channels, and news platforms. AI aggregates signals. Analysts validate intent and escalate credible threats quickly.

Why ObscureIQ?

Built by intelligence and privacy professionals. Trusted by high-stakes clients.

ObscureIQ combines elite privacy operations with advanced open-source intelligence to understand how exposure forms, spreads, and escalates.

Powered by proprietary technology and CODEX, our internal dataset mapping more than 8,600 organizations that collect, trade, or distribute identity data across the modern surveillance economy.

Most privacy services remove data.

Most security tools scan for keywords.

ObscureIQ analyzes the **entire digital threat environment** around an individual.



The Full Threat Intelligence Picture

Our researchers and analysts study the entire exposure lifecycle.

- **Hostility Signals:** Our internal Hostility Index evaluates client risk and tracks narrative spikes, harassment patterns, and emerging hostility online.
- **Identity Infrastructure:** We analyze how identities propagate across data brokers, public records systems, identity graphs, and verification networks.
- **Surveillance & Identity Infrastructure:** We map the organizations and systems that collect, aggregate, and distribute identity data across the modern surveillance economy.
- **Exposure Pathways:** We study how leaks spread through forums, paste sites, social networks, search engines, and data broker networks.
- **Circulating Breach Data:** Our breach intelligence repository tracks exposed credentials and leaked datasets circulating in underground communities.
- **Adversary Behavior:** Our OSINT research maps how hostile actors gather intelligence, escalate harassment, and move from online targeting to real-world threats.

Privacy + Intelligence: The ObscureIQ Equation

We combine elite privacy operations with advanced open-source intelligence.

This allows us to reduce exposure faster, detect threats earlier, and respond with greater precision.

The result is stronger privacy protection and better security outcomes for our clients.

Schedule a Confidential Executive Briefing

Understand your exposure.

Reduce your risk.