

Digital Executive Protection

Protective intelligence for high-risk people and organizations.

We map the exposure around a principal, remove what can be weaponized, disrupt the systems that rebuild it, and keep it from re-forming.

OBSCUREIQ · SERVICE OVERVIEW

MMXXVI · REF. DEP-02

ANALYST-LED FOOTPRINT AUDIT	1,000+ BROKER REMOVALS	DAILY BREACH & DARK WEB SCANNING	DEDICATED ACCOUNT MANAGER
-----------------------------	------------------------	----------------------------------	---------------------------

Home addresses, family connections, breach records, travel patterns and identity fragments circulate across thousands of systems, and an adversary needs only one. ObscureIQ identifies and removes publicly discoverable personal information, uncovers hidden exposure through deep investigative audits, and maintains awareness as new exposure appears.

For our clients, privacy is not a preference. It is operational security.

HOW EXPOSURE BECOMES CONTROL

MAP · NEUTRALIZE · MAINTAIN

01 Map Footprint audits reveal full exposure across data brokers, the dark web, public records and identity infrastructure. For most clients the scale is unfamiliar, and clarifying.	02 Suppress Broker removals and bespoke deletions pull traceable information out of circulation, including the downstream aggregators most services never reach.	03 Disrupt Identity is not stored in one place. It is rebuilt continuously by brokers and identity graphs. We break the links that let reconstruction happen.	04 Maintain Removed records reappear. We monitor the broker ecosystem for repopulation and re-file removals, and scan breach and dark web sources daily for new exposure.
--	---	--	--

CAPABILITIES

OPERATED BY ANALYSTS, NOT DASHBOARDS

Footprint Audit An analyst-built exposure report, delivered in a private review session with a personalized action plan.	Broker Removal Removals across 1,000+ brokers, plus custom deletions for records that standard opt-outs will not reach.	Breach & Dark Web Daily scanning for compromised credentials, leaked records and stealer log data tied to your protectee.
Identity Disruption Work against the records systems, identity graphs and verification networks that rebuild a profile after deletion.	Facial & AI Exposure Locate a protectee's face across the open web and test whether AI tools surface their personal data.	Residence & Circle Address exposure checks across multiple locations, extending to family and the staff closest to the principal.

Scope: Digital Executive Protection covers the data layer, meaning brokers, public records, breach and dark web sources. Continuous monitoring of adversaries, narratives and harassment is delivered through ThreatWatch, a separate program.

WHO IT PROTECTS

BUILT FOR HIGH-RISK INDIVIDUALS

- Executives, founders and board members
 - Investors and high-net-worth principals
- Public figures and media personalities
 - Families and teams facing elevated exposure

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

Program Levels

Two levels of coverage, scoped per protectee, both delivered by named analysts with direct access to the people doing the work.

LEVEL 01

Premium

For high-profile leaders whose exposure demands deeper attention.

Premium covers 1,000+ brokers and adds the capabilities that matter when someone's profile carries weight. Dark web scanning goes deeper, using advanced investigative tools to surface compromised credentials that consumer searches miss. We check whether AI tools are exposing your protectee's personal data, and locate their face across the open web. The audit is analyst-driven: a bespoke report, a private review session, and a personalized action plan. Each protectee gets a dedicated account manager, regular check-ins, implementation support, and direct contact by email, text or Signal.

LEVEL 02

Diamond

For individuals who have been threatened or face elevated, ongoing risk.

Diamond includes everything in Premium plus the capabilities that matter most when someone is actively at risk. Dark web coverage expands to stealer log analysis, the malware-harvested data that exposes saved passwords, session tokens and device details. We run a social media and threat sweep, account takeover analysis, a news visibility audit, a residence exposure check across up to five locations, and an Active Threats report. Senior leadership is involved in sensitive situations and all communications are handled on priority. Diamond is for people whose exposure is already being used against them. At that point the work is not cleanup. It is containment, with analysts on the file.

WHY OBSCUREIQ

PRIVACY OPERATIONS AND INTELLIGENCE, ONE TEAM

Most privacy services remove data. Most security tools scan for keywords. We analyze the full threat environment around an individual, then act on it.

CODEX · 8,600+

Our internal dataset maps more than 8,600 organizations that collect, trade or distribute identity data across the modern surveillance economy. It is the index behind every removal decision we make.

Hostility Signals	Narrative spikes, harassment patterns and our internal Hostility Index.
Identity Infrastructure	How identities propagate across brokers, records and verification networks.
Exposure Pathways	How leaks spread through forums, paste sites, social platforms, search engines and broker networks.
Breach Intelligence	A repository of exposed credentials and leaked datasets circulating in underground communities.
Adversary Behavior	How hostile actors gather intelligence, escalate, and move from online targeting to physical threat.

Service Comparison

What is included at each level. Scope is set during a confidential briefing and quoted per protectee.

COVERAGE	PREMIUM	DIAMOND
Best for	Senior leadership	Under threat
DATA WIPE		
Broker removals	1,000+	1,000+
Custom deletions	Simple requests included	Complex, with credit toward intensive removals
FOOTPRINT AUDIT		
Audit delivery	Private session and personalized action plan	Private session, action plan and implementation help
Dark web & breach scanning	Advanced investigative scanning, compromised credentials	Comprehensive scanning with stealer log analysis
AI exposure scan	✓	✓
Facial recognition	Search, optional removal	Search, optional removal
Residence exposure check	1 location	Up to 5 locations
ADVANCED CAPABILITIES		
Social media & threat sweep	—	✓
Account takeover analysis	—	✓
News visibility audit	—	✓
Active Threats report	—	✓
SUPPORT		
Support channel	Email, text or Signal	Email, text or Signal
Account manager	Dedicated per protectee	Dedicated, plus senior leadership
Check-ins	Regular	Regular and priority
Implementation support	Included	Included, hands-on

Coverage is per protectee. Programs are scoped and quoted after a briefing.

The ObscureIQ equation

Privacy operations + open-source intelligence

Faster exposure reduction. Earlier threat detection. More precise response.

Schedule a confidential executive briefing.

obscureiq.com/coin 1-855-763-7273 Signal: PrivacyStan.10

Conversations are private and off-the-record by default.