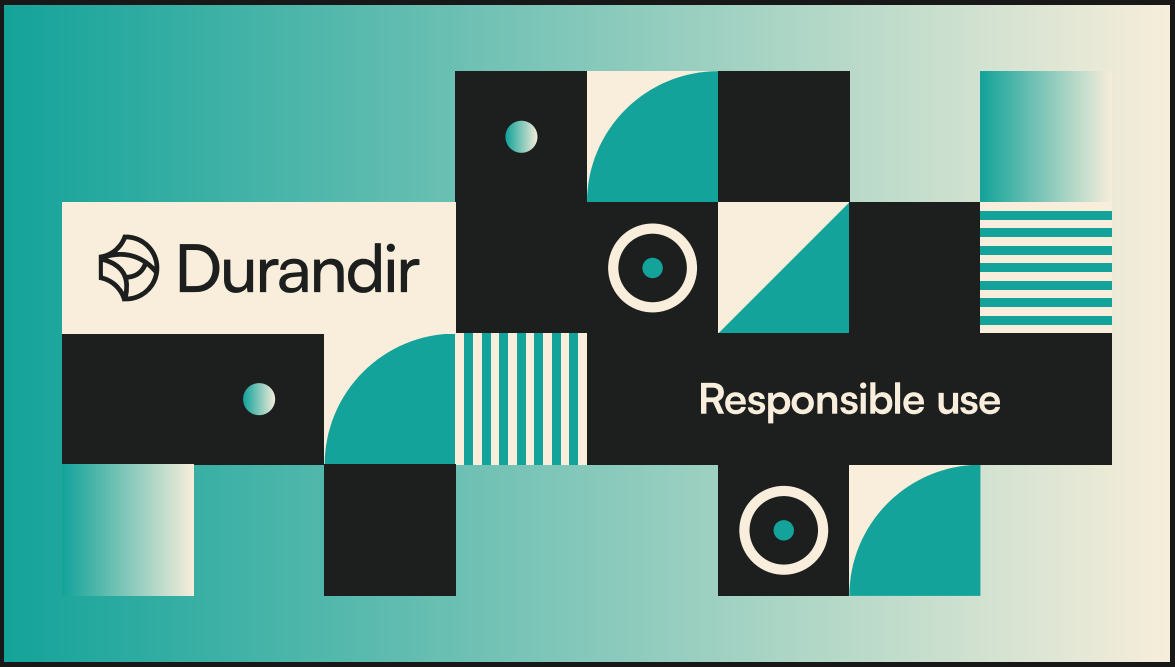
Responsible use



Published	Aug 26, 2026
Last updated	Nov 14, 2026
Category	Policy

Durandir software is built for lawful professional work. How it is used, and against whom, is the responsibility of the person using it.

Durandir Harness and the tools around it are investigation, OSINT, forensic analysis and security research software. They are meant for lawful professional use: investigators, analysts, security teams and researchers who work with a legitimate purpose and the authority to act.

Your responsibility

You decide how to configure and operate our software, and you are responsible for making sure that every investigation, query, scan, collection activity and system interaction is lawful and properly authorised.

Before you use it against a person, account, device, network, service or information system, you need a valid legal basis and whatever consent, ownership right, contractual authority, professional mandate, judicial authorisation or other permission the law requires.

Having access to a feature does not authorise you to use it against any particular target.

What our software must not be used for

- Gaining or facilitating unauthorised access to systems, accounts, devices or data.
- Intercepting non-public communications or bypassing security controls without authorisation.
- Deploying malware, stealing credentials, disrupting services or damaging information systems.
- Unlawfully harassing, intimidating, discriminating against, surveilling, profiling or exposing another person.
- Collecting, processing, publishing or transferring personal data without a lawful basis.
- Concealing, falsifying, fabricating or misrepresenting evidence or attribution.
- Breaking intellectual property, confidentiality, export control, sanctions, criminal, data protection or cybersecurity law.

Dual-use by nature

Security testing, forensic analysis, OSINT, network administration and cyberintelligence are dual-use activities: the same techniques serve defence and attack. We do not design, adapt, market or document our software primarily for unauthorised access, unlawful interception, malware deployment, credential theft, harassment or any other criminal activity. Our product design and documentation keep the legitimate professional purpose of these techniques in front and put authorisation first.

Our Safeguards add a further limit: they stop requests that the law prohibits and reserve sensitive capabilities for accounts authorised to use them.

Enforcement

Where the licence agreement and the law allow it, we may suspend or revoke access to our licensing services when there is reliable evidence of licence fraud, compromise of our infrastructure, deliberate exploitation of a product vulnerability, or use that directly exposes Durandir to unlawful conduct. Those decisions are documented, proportionate and limited to the systems we control, and they do not imply that we control every action taken with a locally installed copy.