

# Constellation

By Recorded Future



Illuminate C2 activity, reconnaissance behavior, and emerging risks across network borders — While maintaining the highest standards of compliance.

## Challenge

The primary challenge for threat researchers is visibility. Without global network intelligence insights, blind spots persist, adversaries move unchecked, and investigations stall. Effective defense requires eliminating those blind spots.

## Solution

The **Network Intelligence Query Capability** provides vetted customers and partners with access to global network traffic observations for specific IP addresses of interest. Powered by a distributed network deployed in over 30 countries, this capability supports threat infrastructure, behavioral analysis, and global visibility into malicious activity — all while maintaining strict data minimization and ethical safeguards.

## Access Model

- Access is granted to vetted researchers and organizations only
- Data returned is limited to the exact scope of the request (IP-only queries)
- Users must agree to ethical and legal terms of use prior to participation

## Approved Use Cases

- Tracking adversary infrastructure and malware command and control (C2s)
- Incident Response (IR) analysis
- Supporting public sector or CERT-led investigations
- Threat evaluations of customer owned infrastructure

## How it Works

- **Input:** Users submit IP addresses for investigation (*IPv4 only*)
- **Query:** System searches high-fidelity data from Recorded Future's global Network Intelligence infrastructure
- **Output:** Structured JSON/CSV files with all observed flows for queried IPs within specified timeframe.
  - Source/destination IPs, ports, protocols, flow counts, timestamps
  - Real-time + lookback (60 Days)
  - No payloads, no PII, no DPI — metadata only
- **Usage:** Users can analyze, enrich, and integrate results into research workflows per approved use cases

Unmatched Visibility Powered by a Proprietary Sensor Network

**150+ Sensors**

Across 37 Countries

**100 Billion**

Records per day

**30 Million**

Validated Threat Flow  
Records per day