The Problem
Tracking Threat Actors requires broad, up-to-date, and easily-pivotable Internet-wide scan data. While OSINT tools like nmap, mass scan, and zmap are great (especially for one-offs), they often require significant overhead to manage at scale.

The Solution
The founders of the Zmap Project created Censys to empower organizations with the best visibility into threats with the most reliable, fresh, and highly-indexed Internet-wide scan data.

The Best Data in the Industry
- 2,029 Ports Scanned Across the Entire IPv4 Address Space
- Port-Independent Protocol Detection
- IPv4 Host Deep Scans
- Largest Repository of Certificates

Ingest the Data in the Format that Best Suits Your Team
- Web UI: The WebUI operates like a search engine, with the ability to construct queries using 10k+ unique attributes.
- API: The API powers automation and provides flexibility to scale operations. We also have an open source CLI tool and Python Library.
- Integrations: Censys data plugs into many security products and platforms, including but not limited to Maltego, Recon-ng, ThreatConnect, Phantom, Axonious, FireEye Security Orchestrator, Tines Etc.
- Raw Data: Ingest raw scan data to use with your preferred internal systems. Downloads of JSON Lines are a great fit for organizations who are building a “data lake” or have very strict privacy restrictions.
- Google BigQuery: Run SQL queries across Censys Data in Google BigQuery. We do the ETL, you manage the GCP instance. This method enables you to regex the entire Internet and easily build a data pipeline.

Enhance with Other Censys Products
Censys Attack Surface Management Product
If you’re leveraging Censys Data to find assets belonging to your organization, Censys can help! We have an Attack Surface Management Platform that helps organizations understand their external exposures.

Learn More at Censys.IO/Product