FOFA

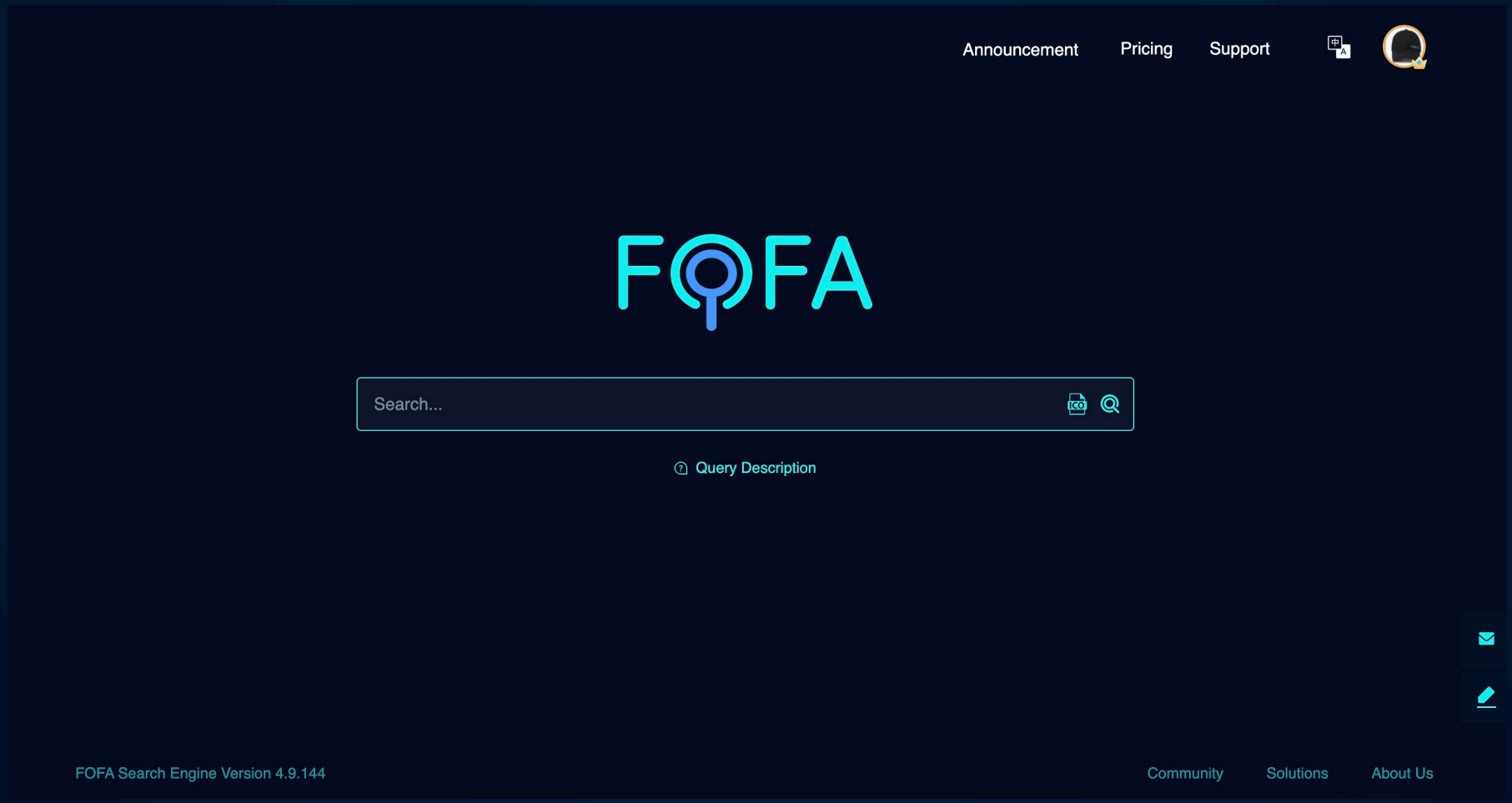
FOFA

Cyberspace Search Engine

March 2023

What is FOFA ?

FOFA platform is a cyberspace search engine for all IT assets on the internet, such as IPs, domains, hosts and product info.



Cyberspace Search Engine Core

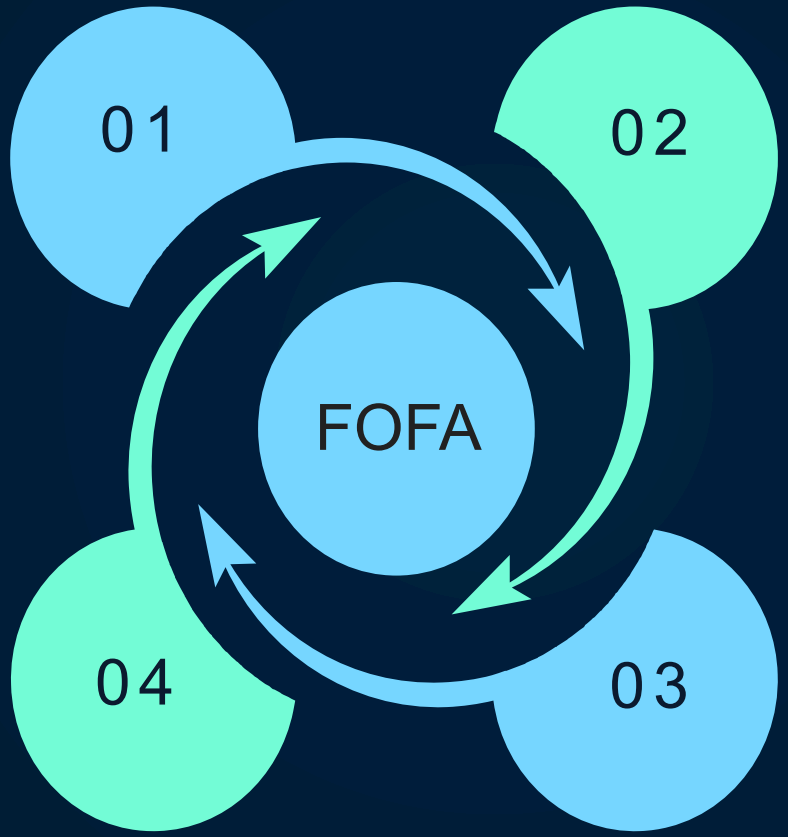
FOFA

Port Scanning

- Asynchronous stateless port scanning technology
- Identifies 1000+ ports
- Flexible & extensible

Vulnerability Scanning

- POCs for vulnerability scanning
- Submitted by white-hats globally
- 5000+ POCs



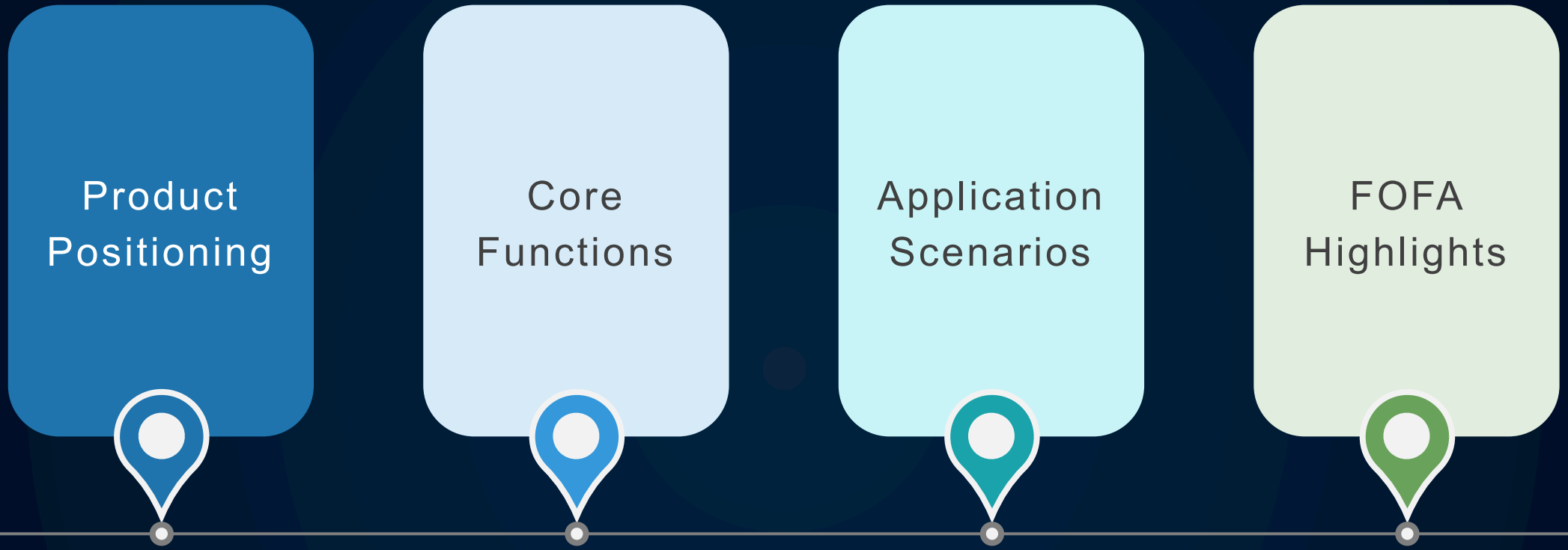
Protocol Identification

- Self-developed scalable protocol identification algorithm
- Supports 1300+ protocols
- Identifies more than 85% open ports

Asset Identification

- Fingerprint rules covers 7 large categories
- 80+ subcategories
- 360,000+ fingerprint rules

1. Product Positioning



Product Positioning

FOFA

Researchers

Assists target setting and IT asset information gathering

Ethical Hacker

Provides powerful asset collection capabilities

Security Research Institutions

Provides research target and asset collection plan

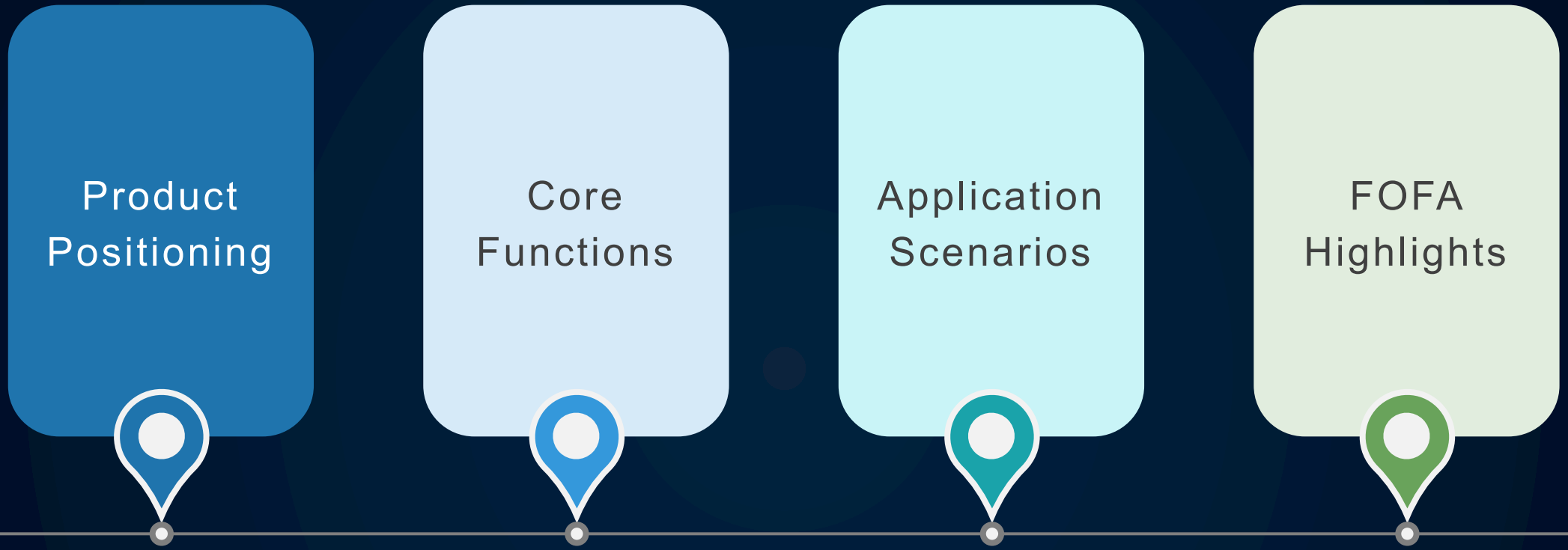
Regulatory Agencies

Provides public network supervision solutions

Enterprises

Provides attack surface mapping solutions

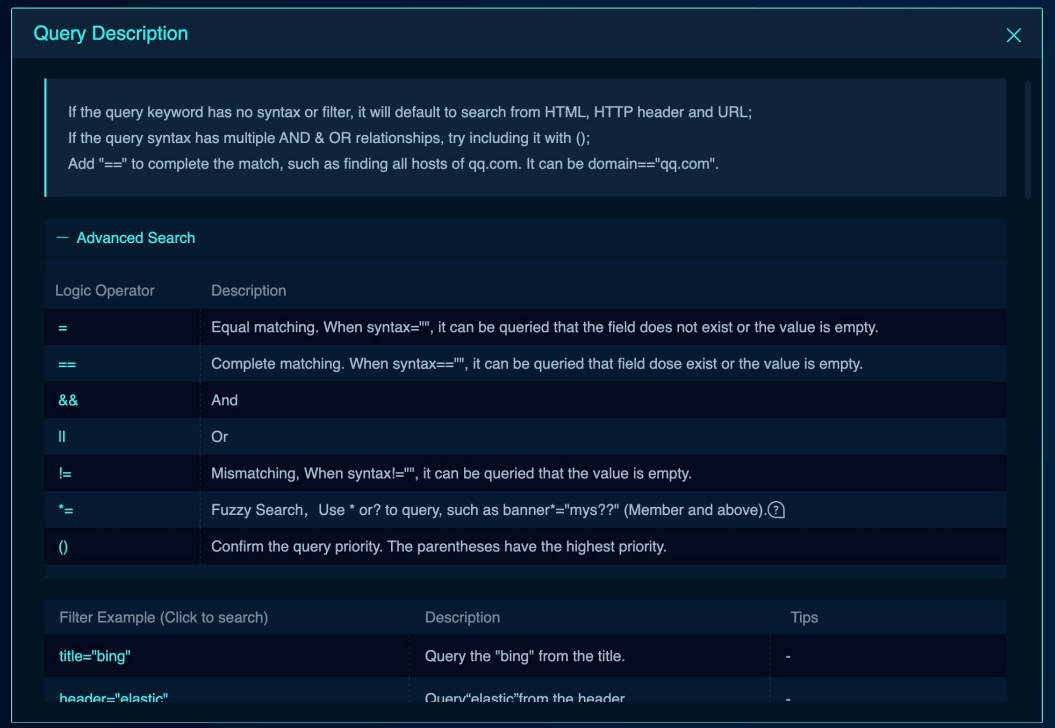
2. Core Functions

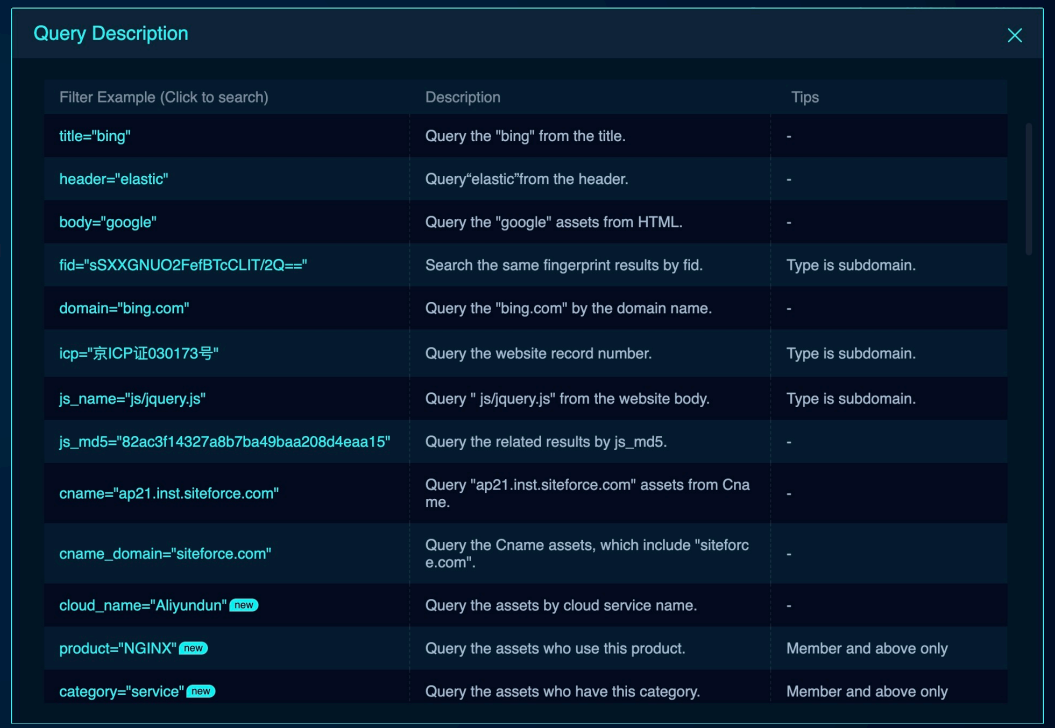


Core Function – Search Engine

FOFA can search all public network IT assets and supports extensive query keywords.

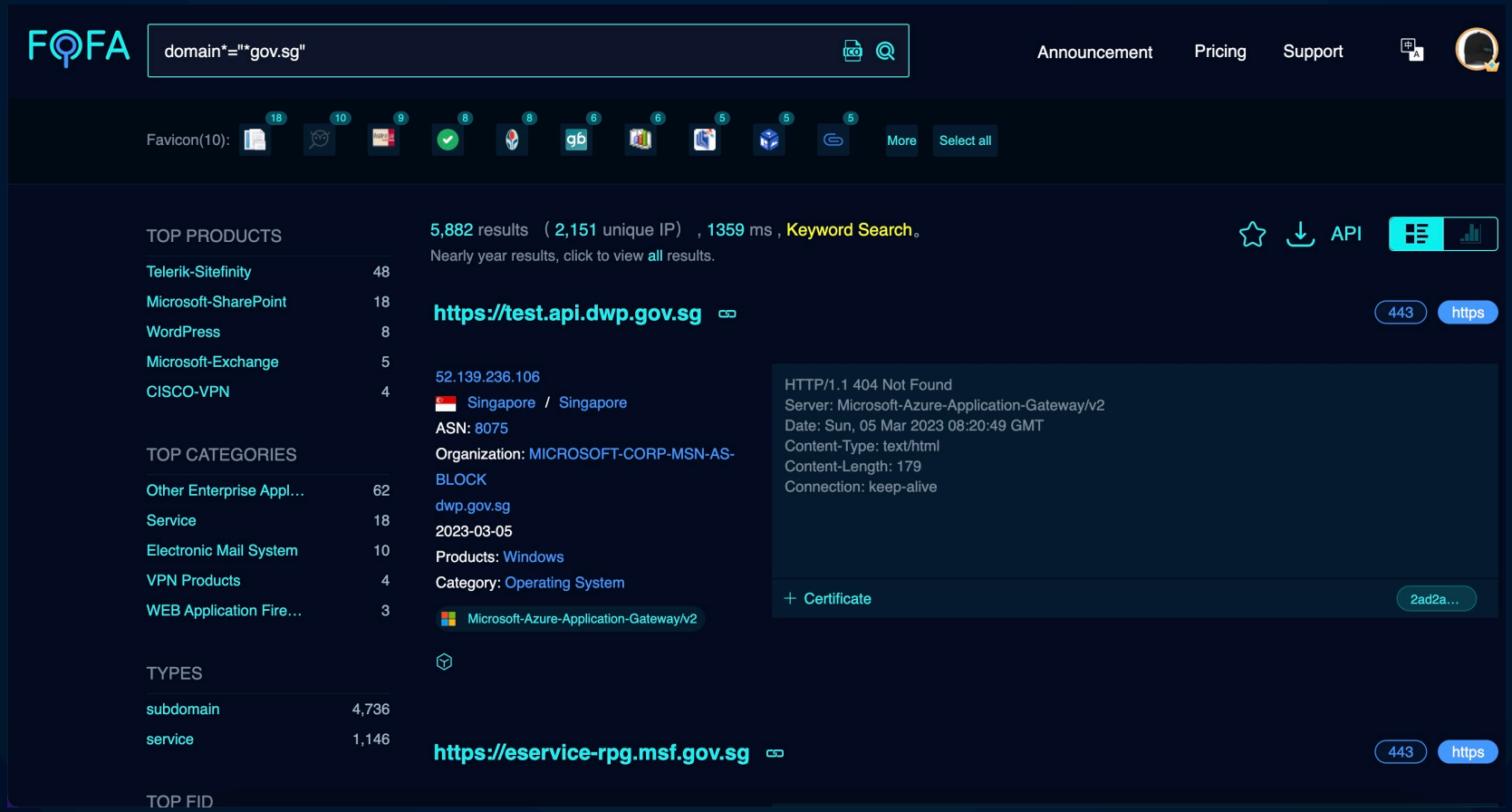
There are currently 52 query keywords, which can cover almost all user scenarios.





Core Function – Search Engine

FOFA can provide detailed information on the searched assets, including but not limited to Top5 ports, products, services, operating systems, certificates, website titles, and more.



Core Function – Search Engine

FOFA can perform statistical analysis on the geographical location of assets.

TOP PRODUCTS

Telerik-Sitefinity	48
Microsoft-SharePoint	18
WordPress	8
Microsoft-Exchange	5
CISCO-VPN	4

TOP CATEGORIES

Other Enterprise Appl…	62
Service	18
Electronic Mail System	10
VPN Products	4
WEB Application Fire…	3

TYPES

subdomain	4,736
service	1,146

TOP COUNTRIES/REGIONS

United State…	2,903
Singapore	2,050
Japan	144
Hong Kong …	69
Germany	26

TOP DOMAINS

seab.gov.sg	454
mom.gov.sg	260
moe.gov.sg	174
singpass.gov.sg	140
nparks.gov.sg	98

TOP IP

45.60.244.0/24	270
52.128.22.0/24	265
199.184.145.0/24	219
122.11.184.0/24	169
35.201.83.0/24	153

TOP JARM

29d29d00029d29d00…	324
29d29d00029d29d00…	233
29d29d00029d29d00…	191
29d29d00029d29d00…	146
29d29d00029d29d00…	115

TOP OPEN PORTS

443	2,784
80	2,198
2095	66
2096	64
2053	57

TOP SERVERS

cloudflare	842
nginx	491
awselb/2.0	458
DOSarrest	403
CloudFront	382

TOP PROTOCOLS

https	604
http	447
smtp	26
tls	20
dns	17

TOP OPERATING SYSTEMS

windows	41
ubuntu	12
cpanel	2
redhat	2
red hat enterprise linux	1

TOP CLOUD NAMES

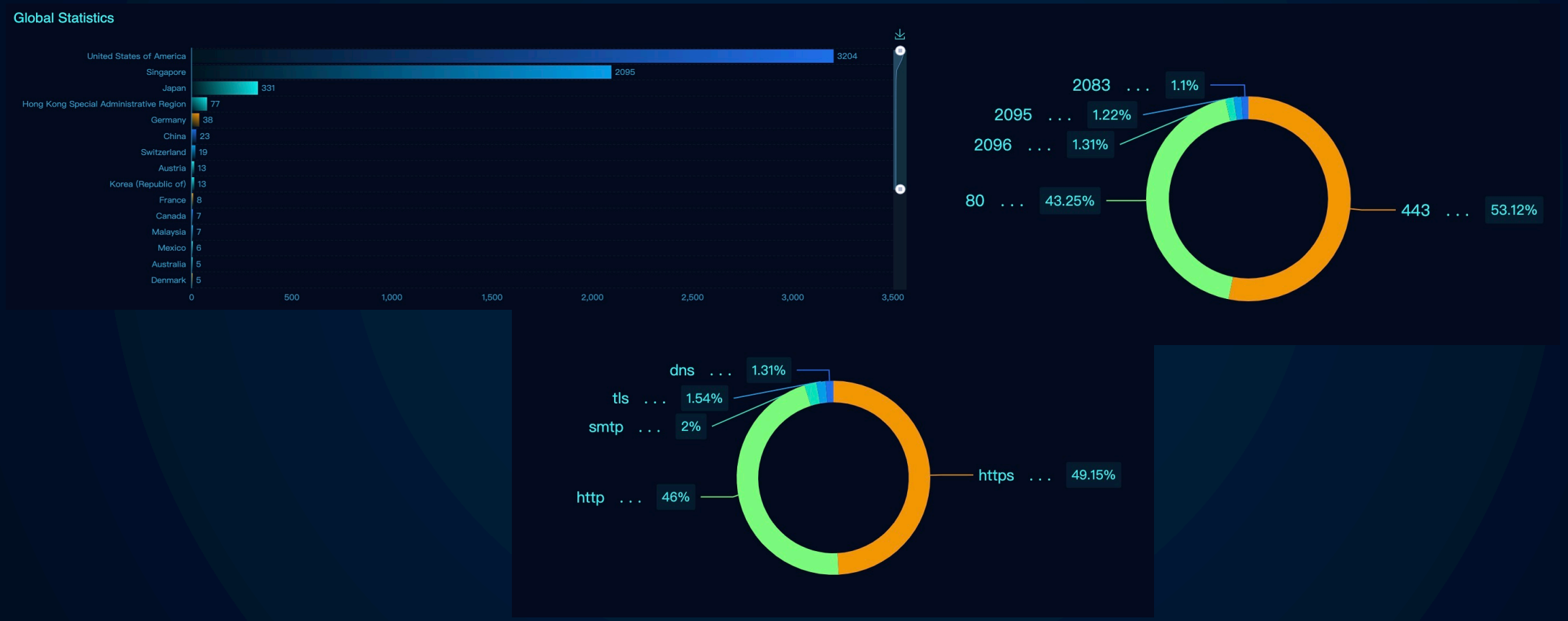
Cloudfront	538
Cloudflare	391
Imperva Incapsula	228
Amazon AWS	224
Akamai	188

TOP CERTIFICATE SUBJECTS

Government Technol…	226
Singapore Examinati…	215
Cloudflare, Inc.	144
Ministry of Social and…	92
Ministry of Manpower	85

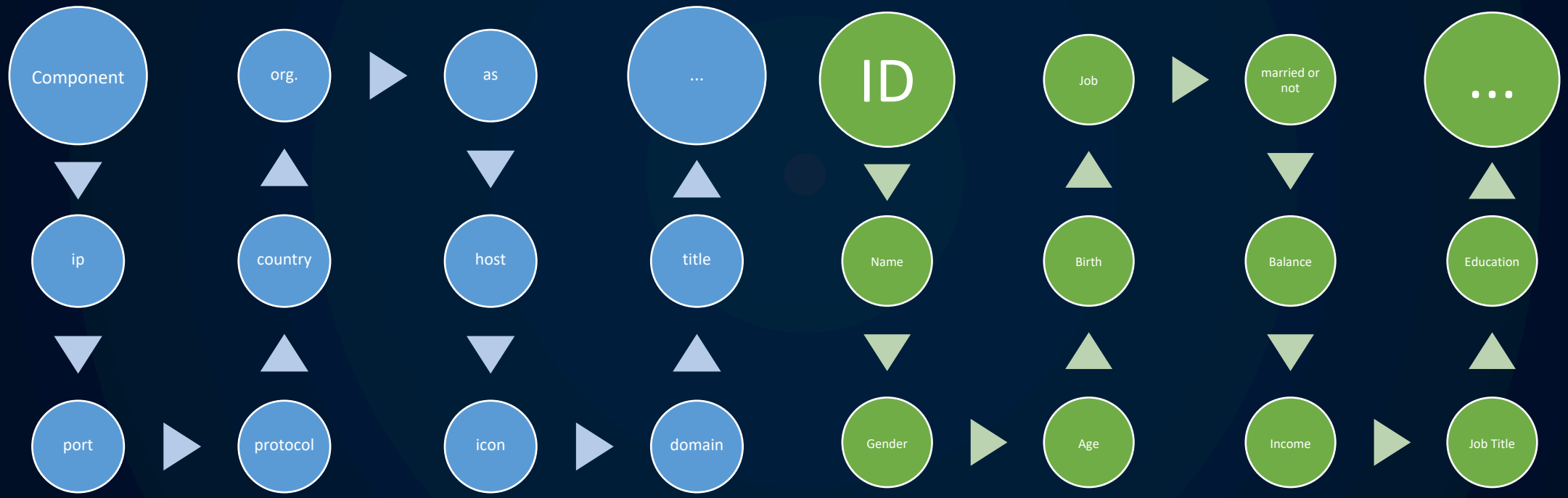
Core Function – Search Engine

FOFA can also display the search results for distribution of assets through visual charts.



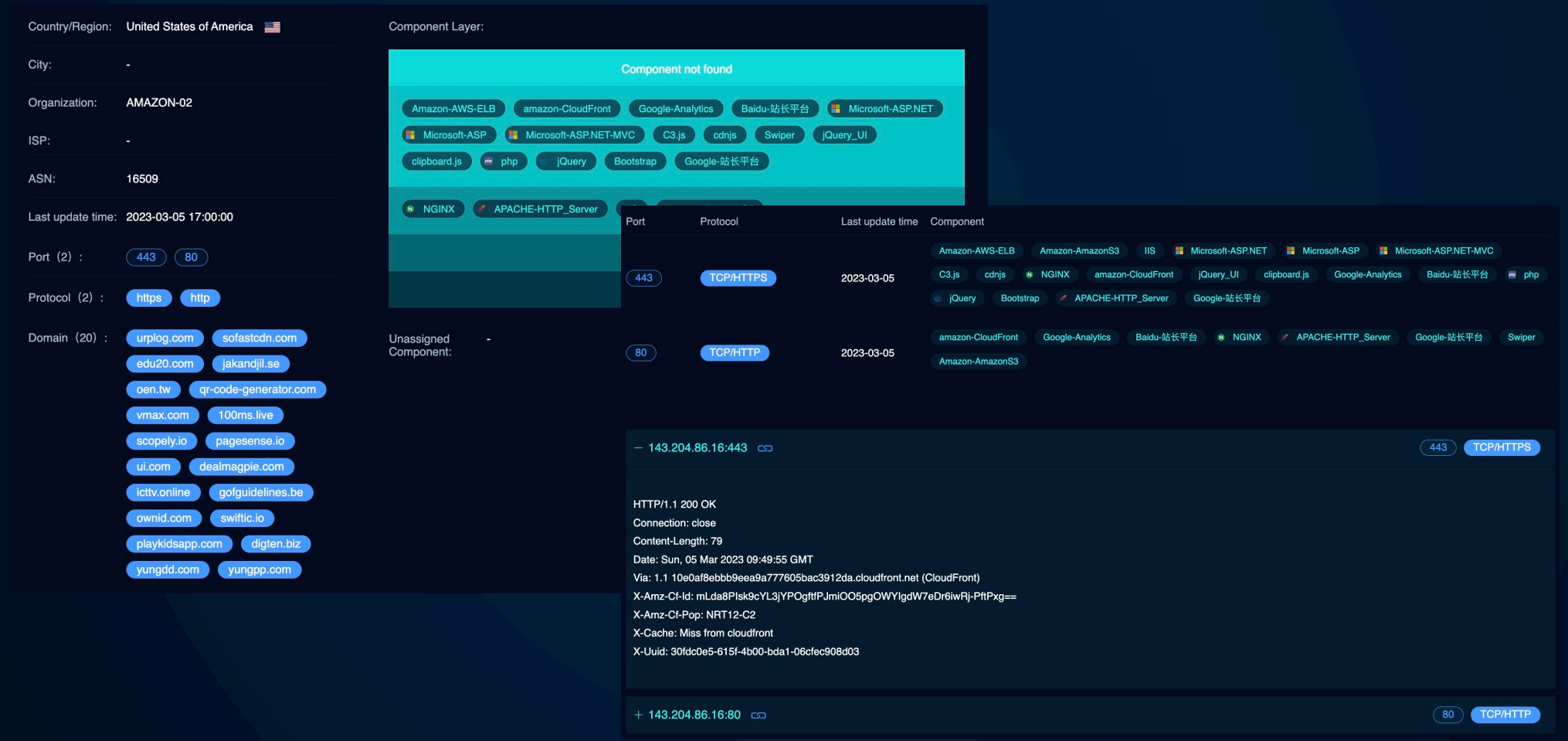
Core Function – Asset Identification

FOFA can accurately identify IT assets through IP, port, protocol, domain name, etc., identify software & hardware products via alive ports, and manage components hierarchically.



Core Function – Asset Identification

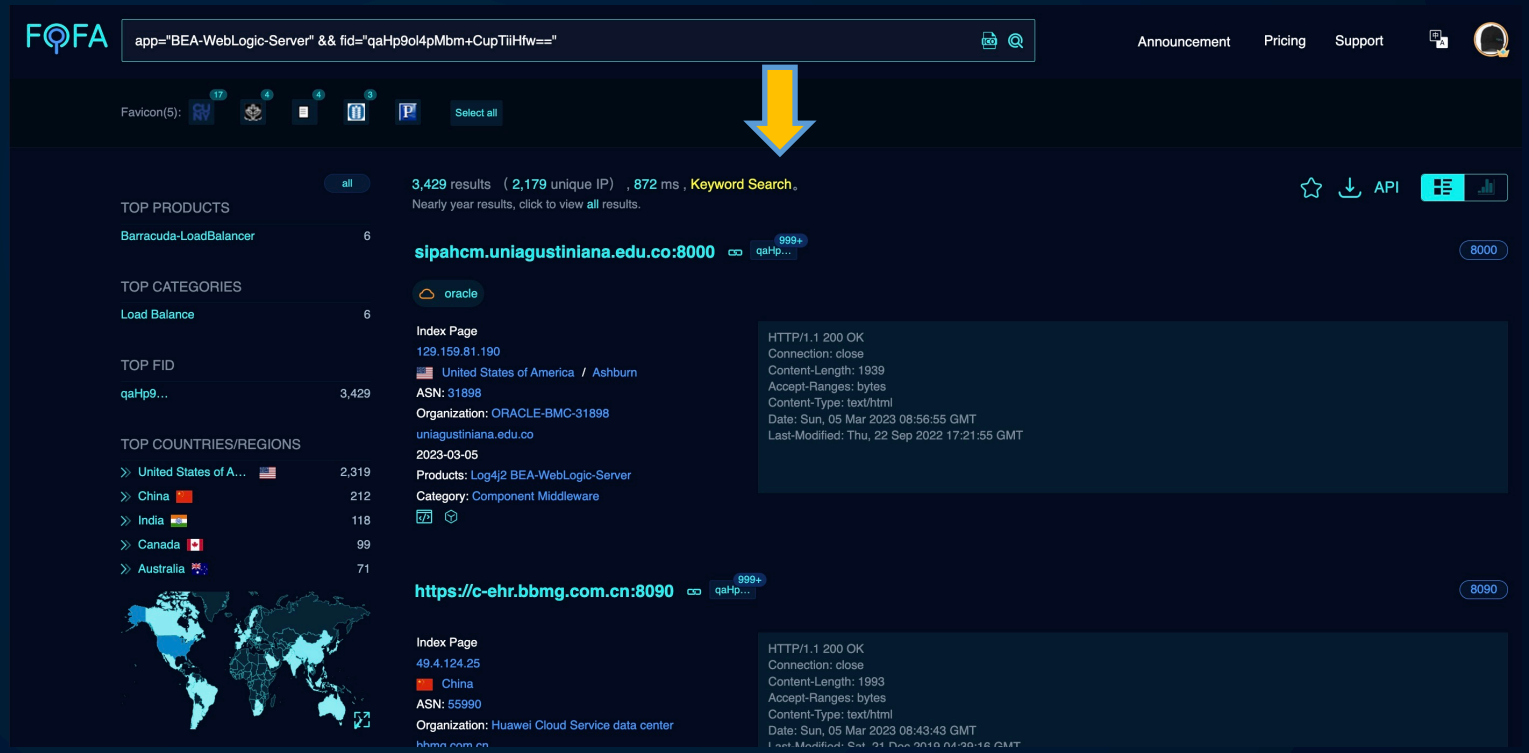
FOFA can accurately identify IT assets through IP, port, protocol, domain name, etc., identify software & hardware products via open ports, and manage components hierarchically.



Core Function – FID Fingerprints

Based on unique features generated by extracting the structural relationship of the website, website aggregation is carried out through Web Feature Identification fingerprint, where assets with similar structure and content can be found.

It can be used for asset discovery, automatic clustering of websites, asset expansion, and investigative search.



Core Functions – Fuzzy Search

On the FOFA platform, the effect of fuzzy search can be realized by using the wildcard matching function.

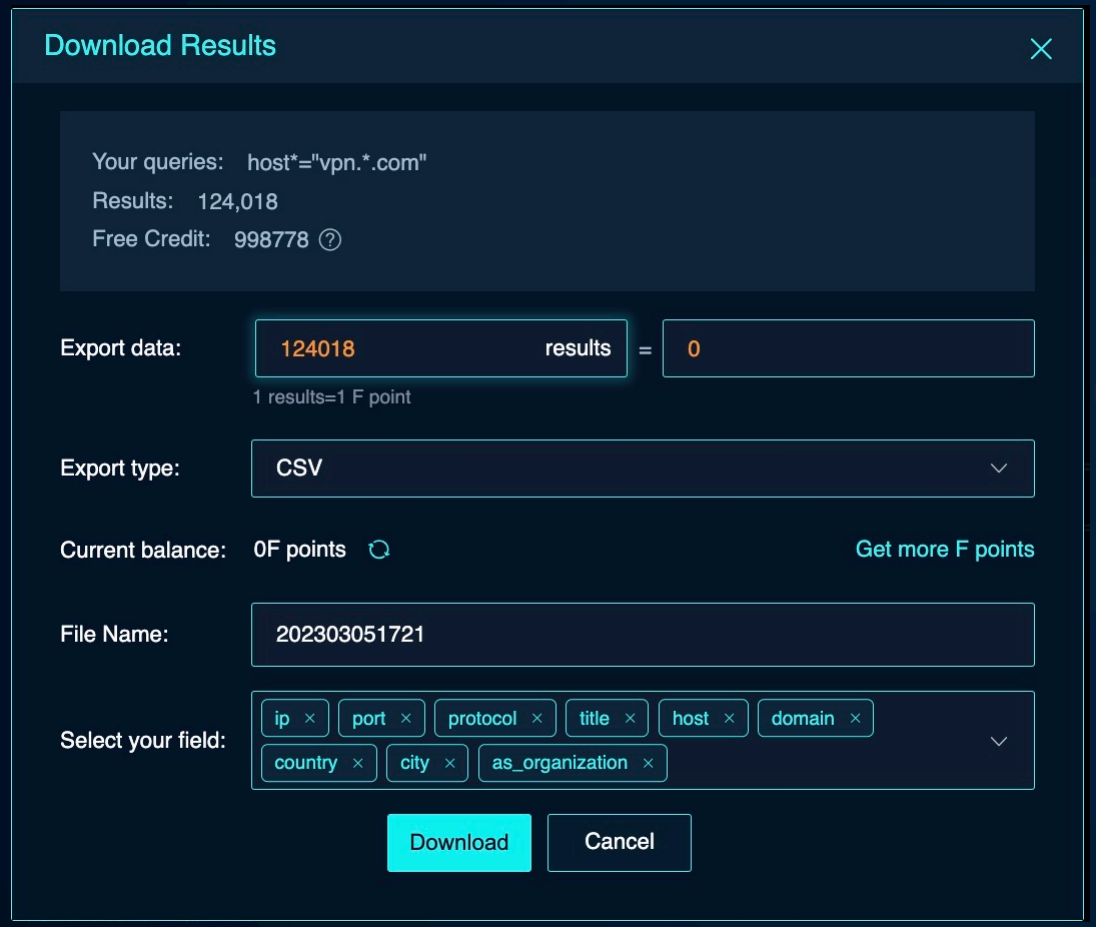
For example, when searching, wildcards "*" and "?" can be used in keywords to match different characters and character strings for fuzzy search.

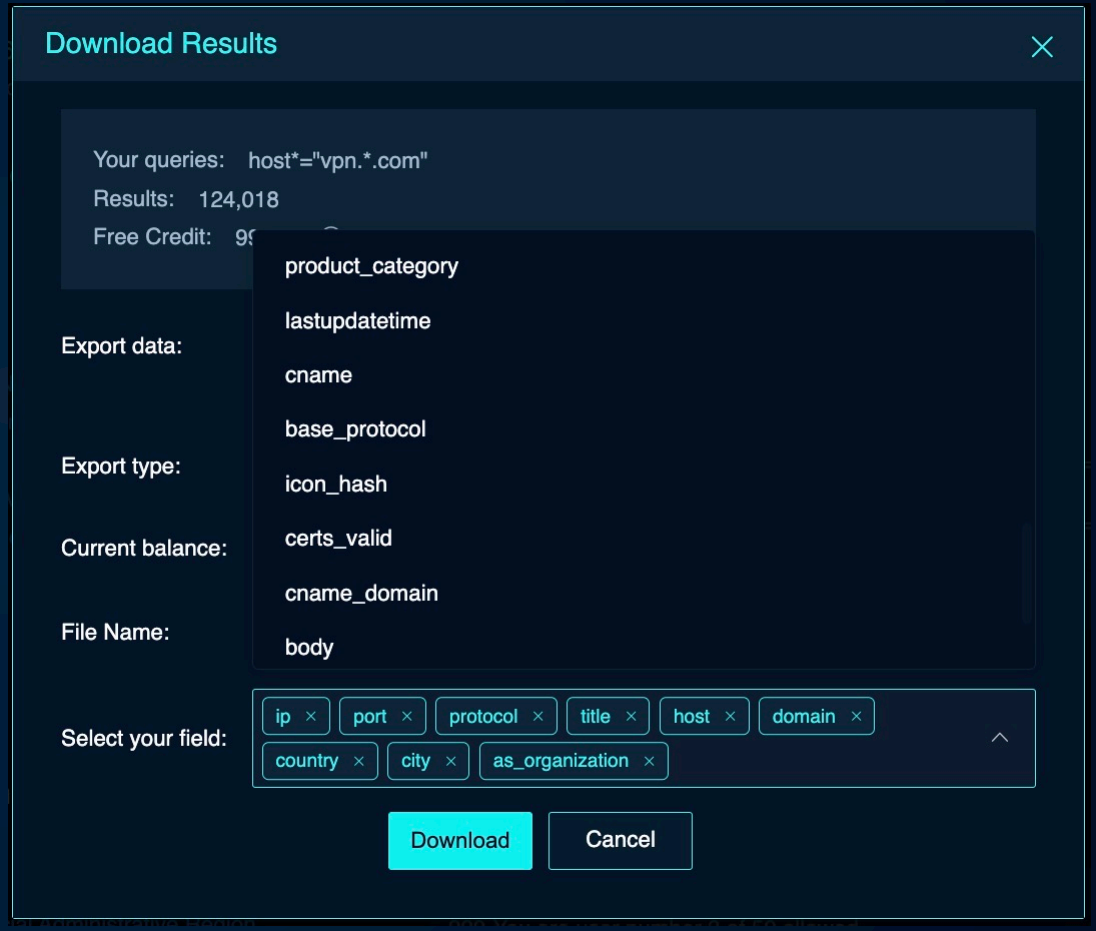
Core Functions – Fingerprint Rules

The core capability of FOFA's fingerprint rule set is to help users sort out assets without manually collecting asset characteristics. Users can directly search for rule names and FOFA makes associated recommendations based on past searches.

Core Function – Download Reports

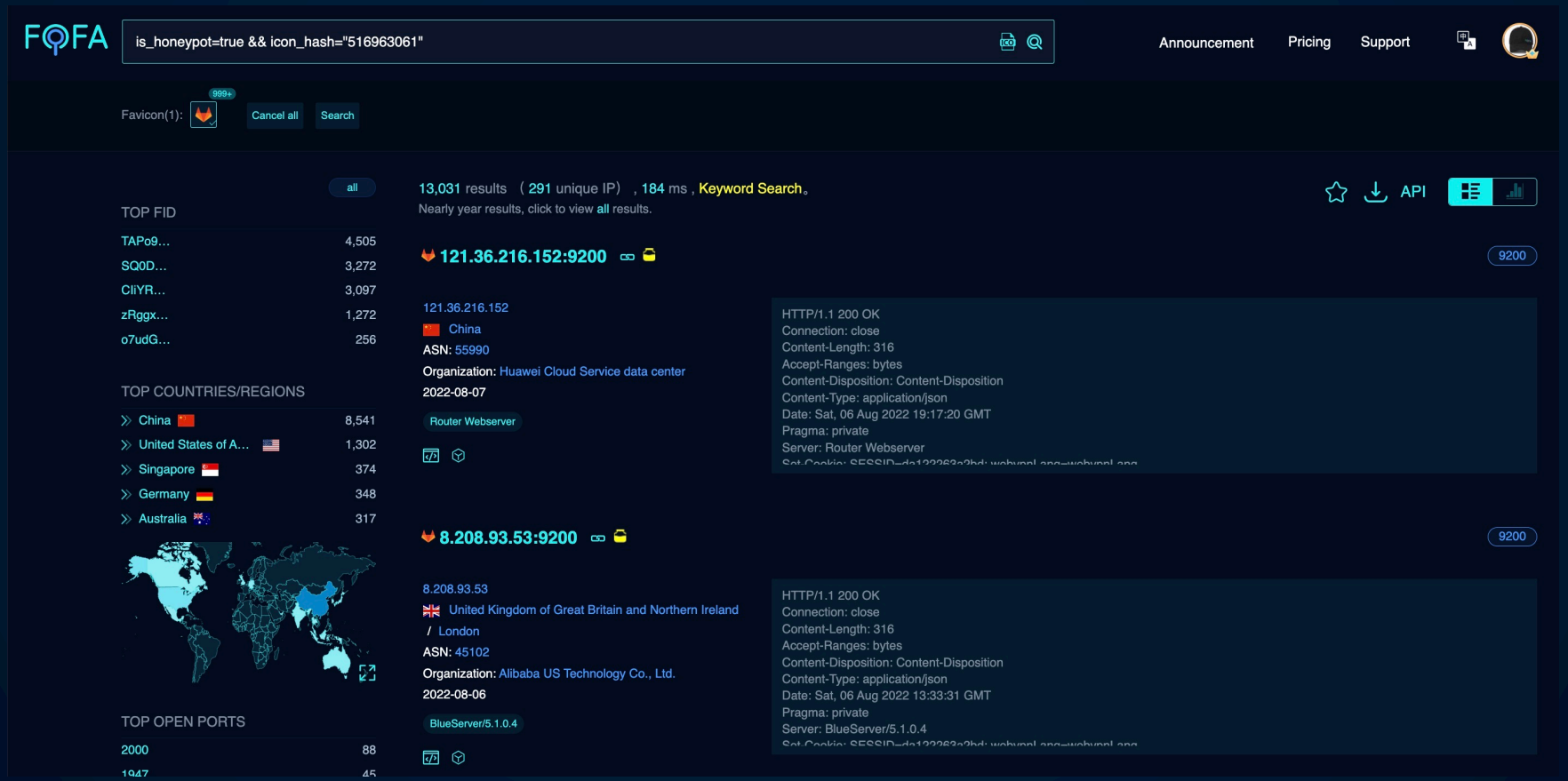
Search results can be exported and downloaded from FOFA web platform.





Core Functions – Honeypot Identification

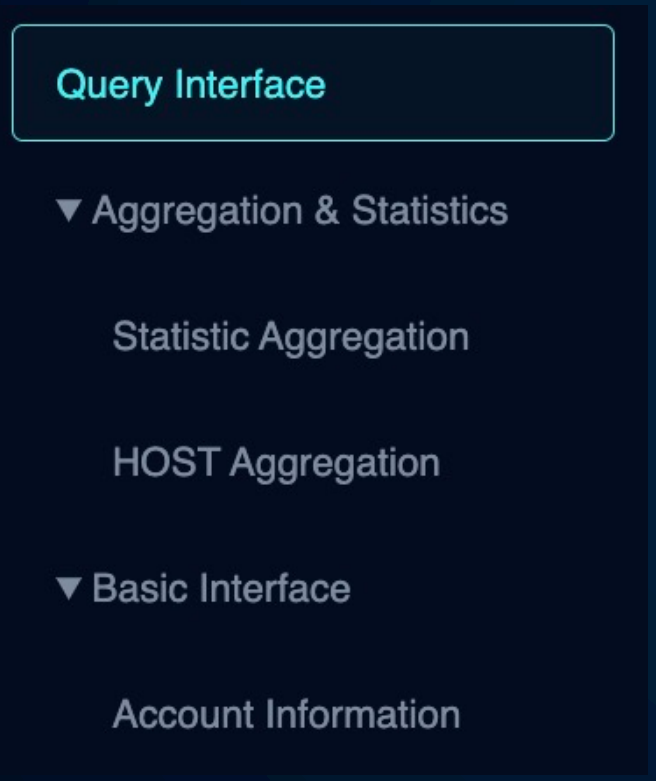
FOFA, as a leader in cyberspace asset mapping, identifies and marks honeypot data through self-developed algorithms to help users avoid honeypot system and locate target assets.

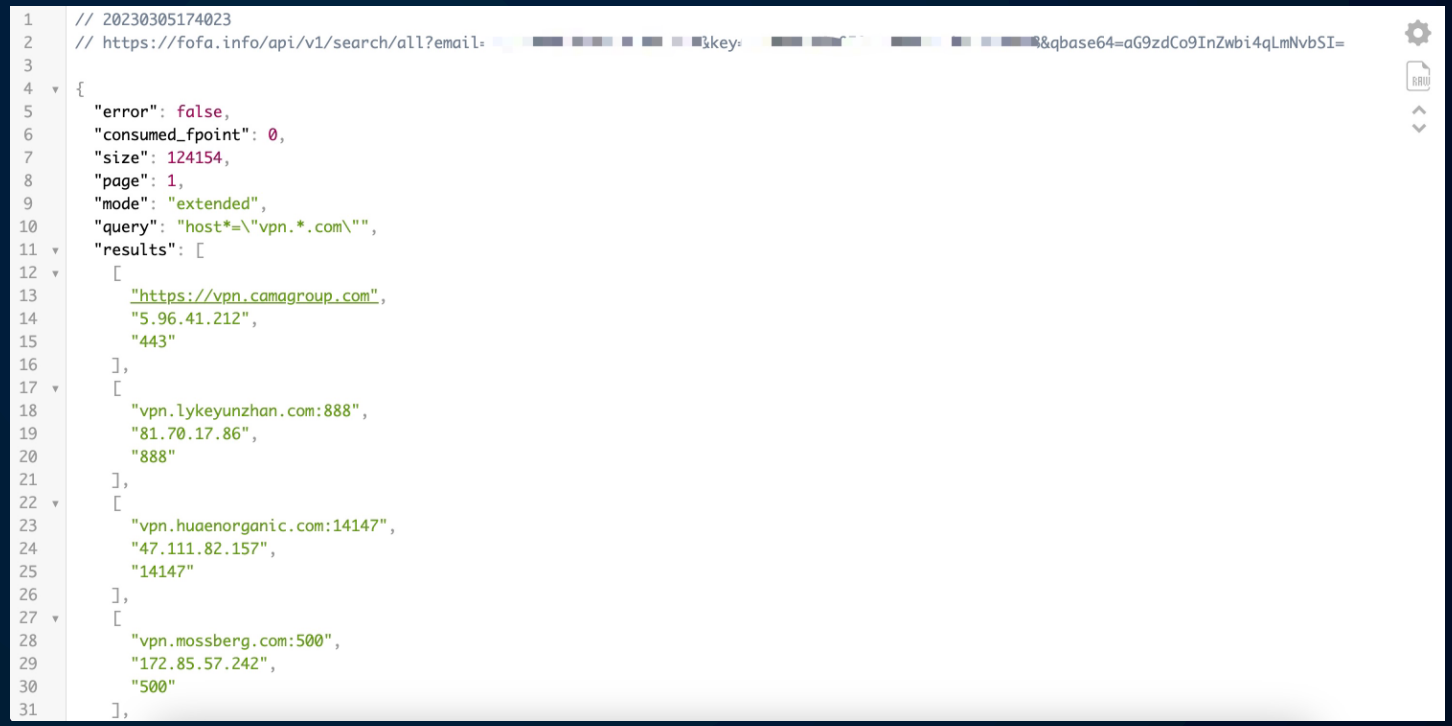


Core Function - API

FOFA provides APIs for one-click direct access to the target, including standard interfaces, statistical aggregation interfaces, HOST aggregation interfaces, and streaming interfaces for quick calls.

Users can also sign up for professional or institutional accounts to adjust speed limit to obtain data more quickly.





3. Application Scenarios

FOFA

Product Positioning

Core Functions

Application Scenarios

FOFA Highlights

Section 1

Section2

Section 3

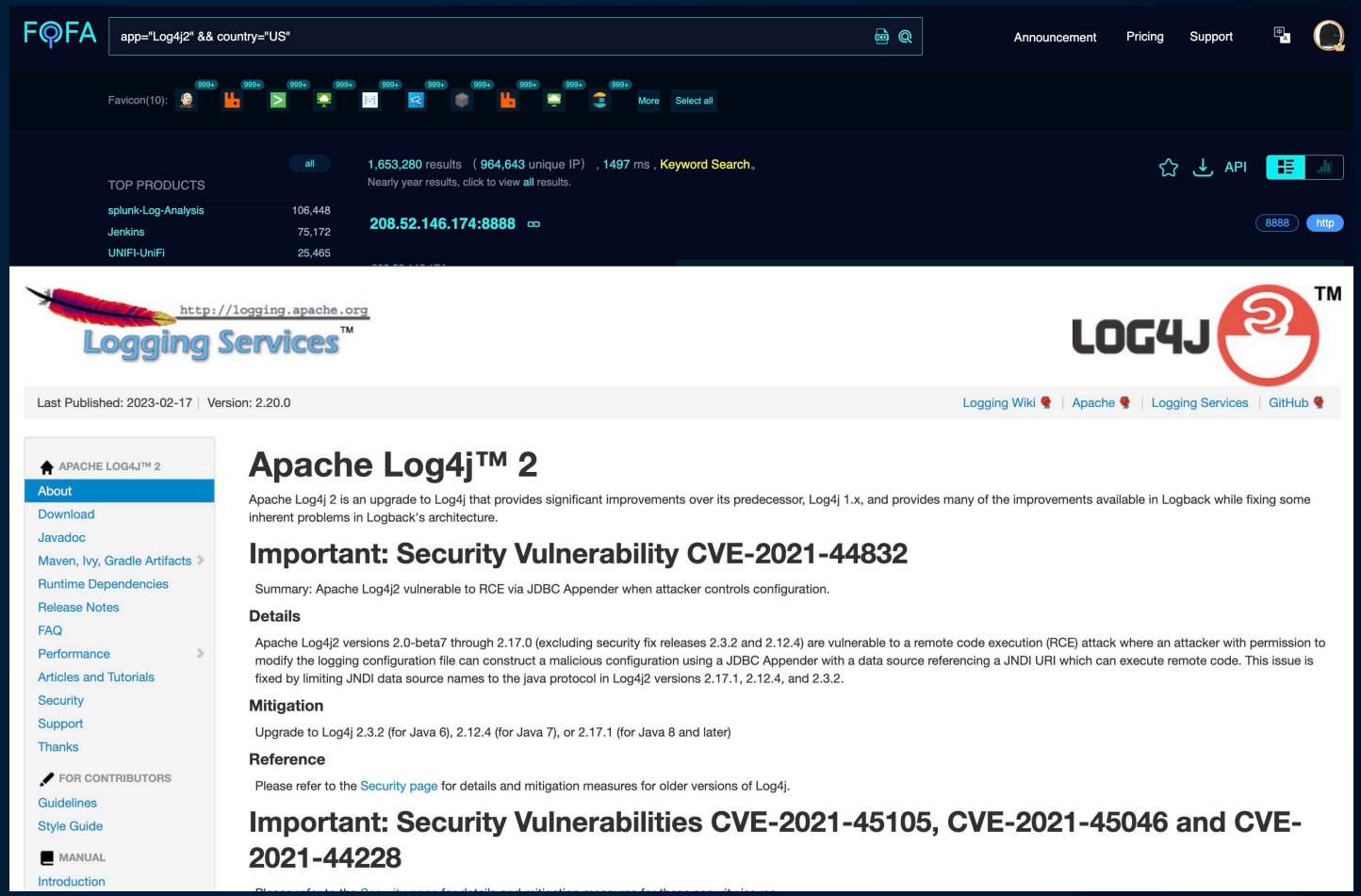
Section 4

Application Scenarios – Vulnerability Warning

Compared to traditional vulnerability database containing vulnerability level, vulnerability name, and potential impact, FOFA adds additional dimensions such as the scope of influence and whether it contains critical assets to its vulnerability database.

This can help regulatory agencies quickly locate risky assets and improve emergency response speed .

Such as: log4j2

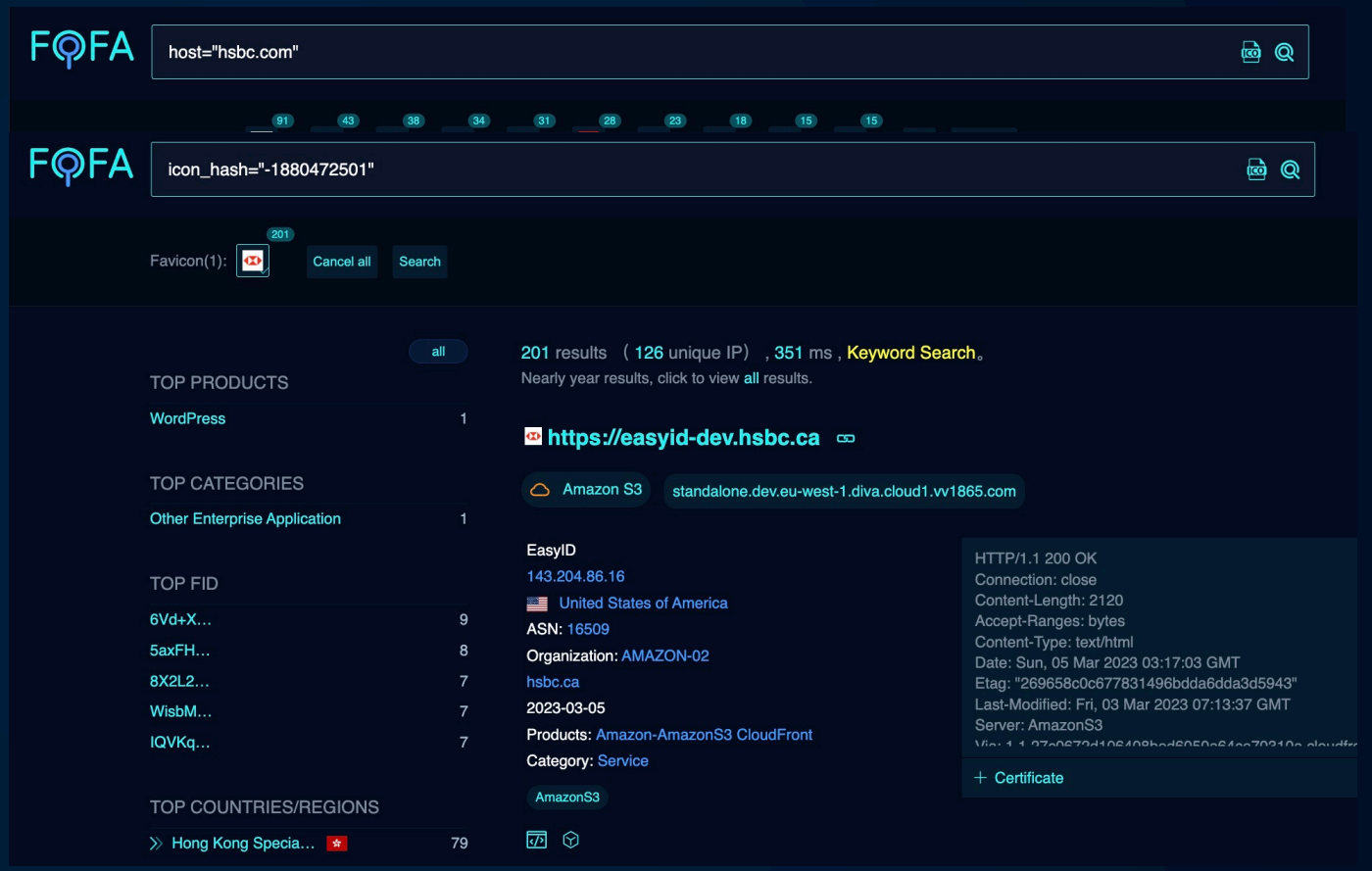


Application Scenarios – Asset Identification

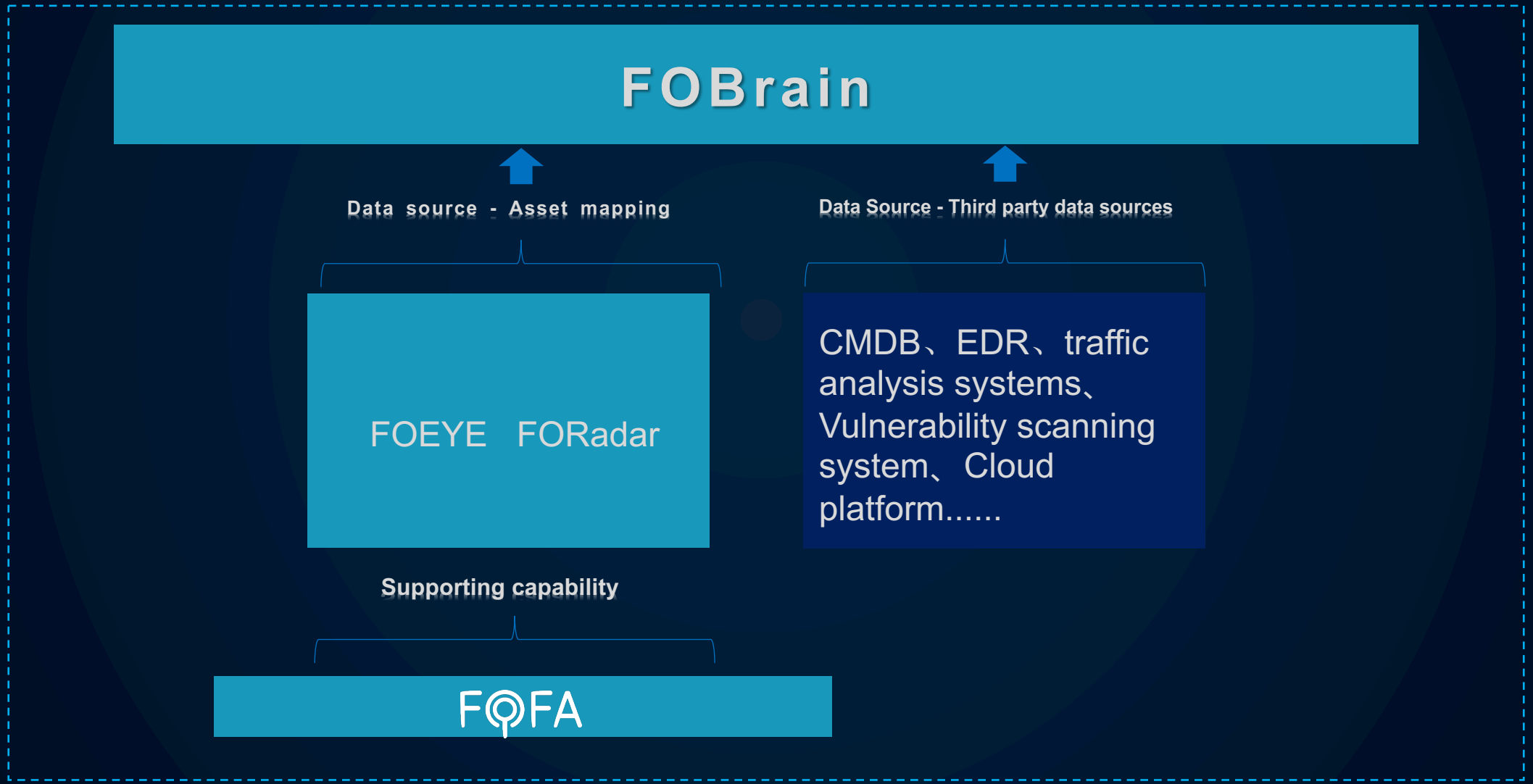
It is often difficult for large enterprise to identify all IT assets connect their network, especially with more data stored in the cloud nowadays.

Large enterprises have the need to clearly grasp the exposed surface of network assets that they need to protect and understand comprehensively the security risks in their network assets.

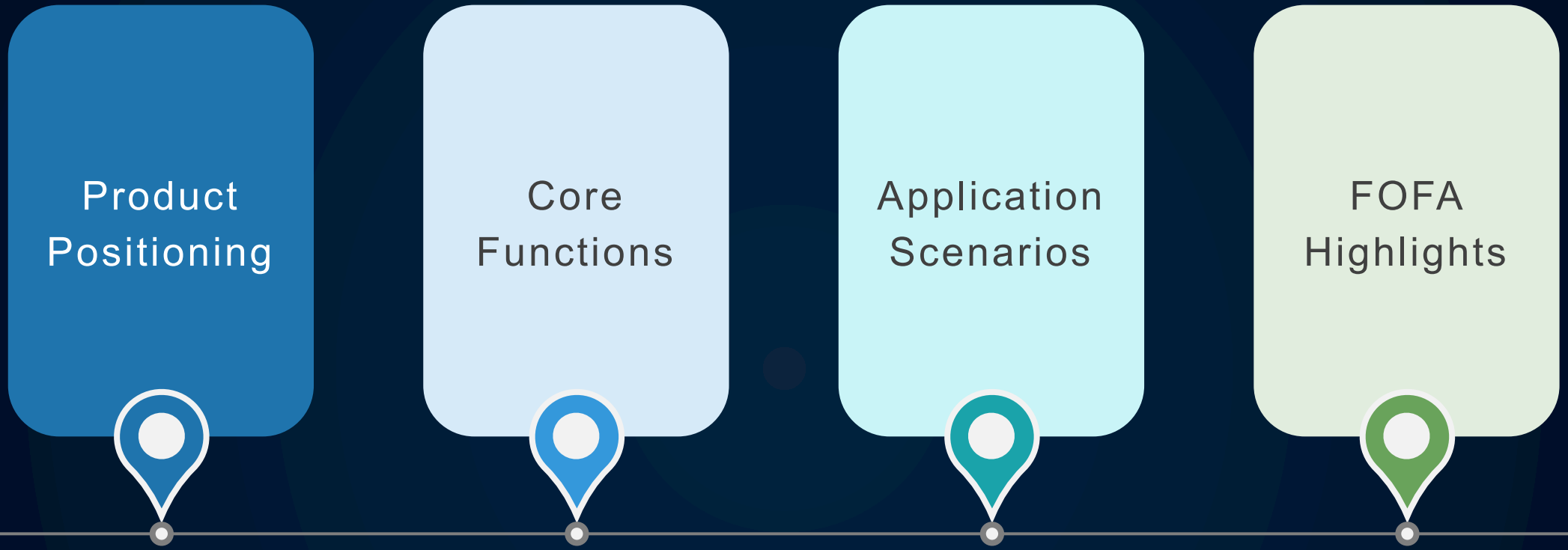
FOFA can extracts the corresponding relationship between assets and enterprises through multi-dimensional domain, cert, icon, etc., allowing security experts to identify open assets of enterprises from the perspective of "attackers".



Application Scenarios – EASM Product



4. FOFA Highlights



FOFA Highlights

Best Search Engine for Network Exposure Globally

Top security team

- Founder Zwell – globally recognized hacker
- Management team with successful entrepreneurial background in security industry
- Core team members come from 360, Huawei, Alibaba and other major tech companies

Leading innovations in tech & product

- FOFA platform can query 6 billion cyberspace assets globally, including IP, servers, applications and data
- Top engine capacity in the world, ranked #1 internationally by Alexa in 2022, platform with the most active users in China
- Developed series of enterprise products including Foeye, Goby, Metasecurity

Rapid and sustainable growth

- >100% revenue growth for 3 consecutive years from 2018 to 2020
- Corporate clients covers industries including critical infrastructure, military, energy, telecom, pharmaceuticals, education, and regulatory agencies
- Rapid expansion across the nation in all industries

FOFA Highlights

https://fofa.info/

FOFA quickly gained global recognition of security professionals and was ranked 17,320 in all internet traffic on Sept 14, 2021, successfully surpassed the top US player - Shodan in popularity and became #1 in the sector.

"FOFA – the Google search engine for all IT assets in network space"

7.3b	IPv4 network coverage	**360k**	Fingerprint rules
52	Query syntax search	**800+**	0Day Vulnerabilities
300k	Global security professionals	**5000+**	Vulnerabilities POC
17min	Ave. Time on site	**Fastest POC update globally**	

Most accurate network asset scan results

Support flexible query syntax combinations

AI-based search recommendations

FOFA Highlights

FOFA is the only platform with 95% accuracy rate within 24h, and 100% accuracy rate within 48h.

Test Criteria

- Time: Oct 2021
- Goal： Random scan of 23 IPs in key areas over the global
- Testing method： record and compare the scanning results of target IPs using 5 top network scanning platforms

Performance Results

	FOFA	ZoomEye	QUAKE	SHODAN	censys
In 8 hours	**17** / 23	0 / 23	0 / 23	0 / 23	0 / 23
In 24 hours	**22** / 23	2 / 23	0 / 23	2 / 23	8 / 23
In 48 hours	**23** / 23	10 / 23	2 / 23	4 / 23	4 / 23
In 72 hours	**23** / 23	21 / 23	6 / 23	10/ 23	23/ 23

The core capability of network search engine requires long term accumulation of asset database, which is also the unbreakable competitive advantage of FOFA platform.

FOFA Highlights

Offers flexible cybersecurity solutions and products using core FOFA search engine.

Solutions

For 8 key industries

- Finance
- Telecom
- Regulatory Agency
- Military
- Industrials
- Transportation
- Energy
- Education

Core Engine

FOFA

Data Collection

7.5 billion network assets, broadest coverage in the cybermapping industry

Data Analytics

10+ AI-based data analytics engine developed in house

Data Library

800+0Day，5000+POC，5000+EXP……

Largest fingerprinting & POC database in the industry

FOFA Highlights

"This could be really cool if open source or extensible"

"Can't believe it is done by Chinese people"

"How to build a network scanning analysis Platform-Part I: medium.com/@fapro0…"

"All our security and IT team use your platform on daily basis"

CNCERT/CC

H3C

FOFA

https://fofa.info/

17min Ave. Time on site

12k Individual IP access
5% from US

FOFA platform actively used by cybersecurity professionals, largest security expert community.

Thank you!