

FOFA

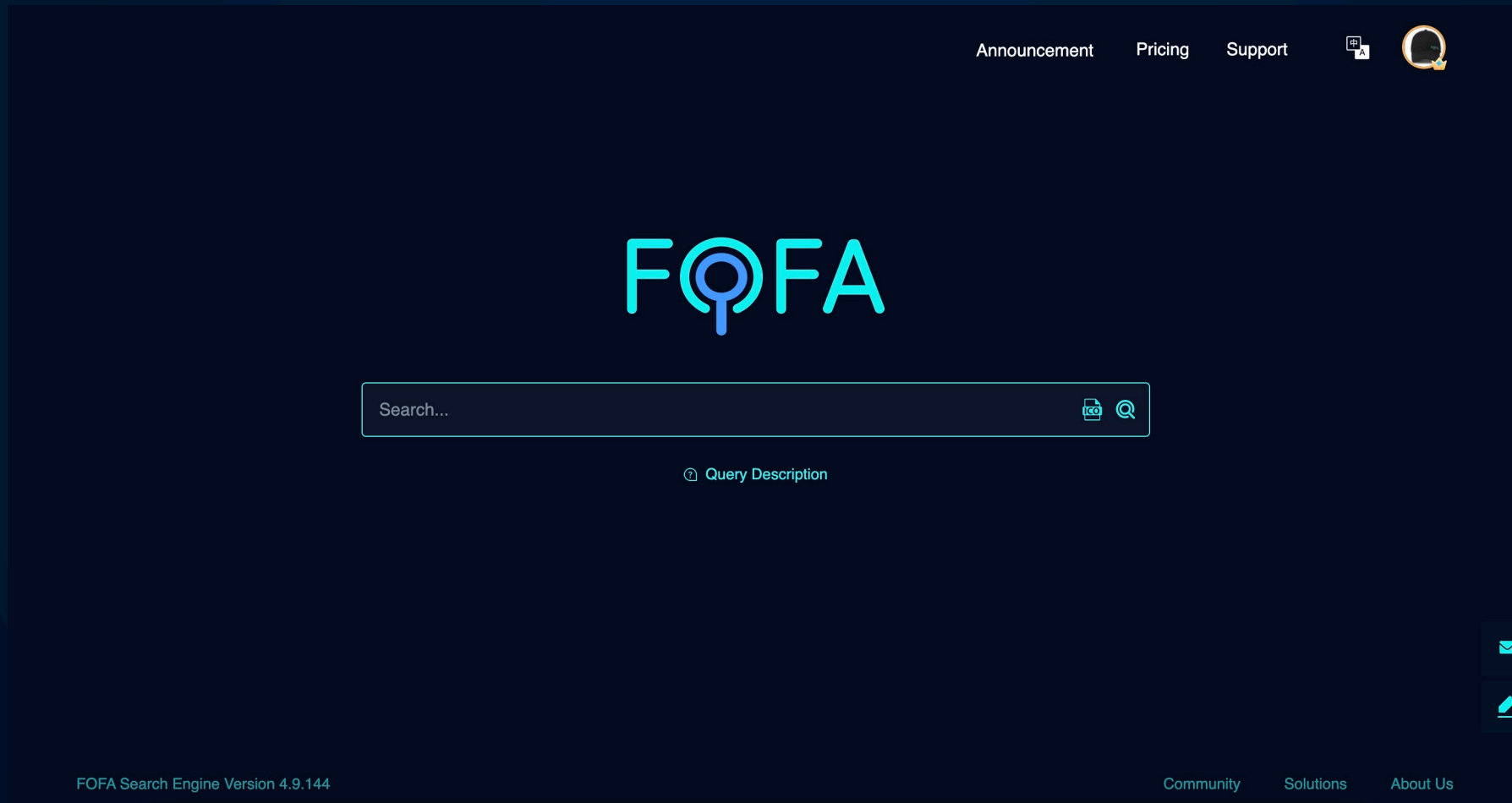
Cyberspace Search Engine ▶▶▶

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.



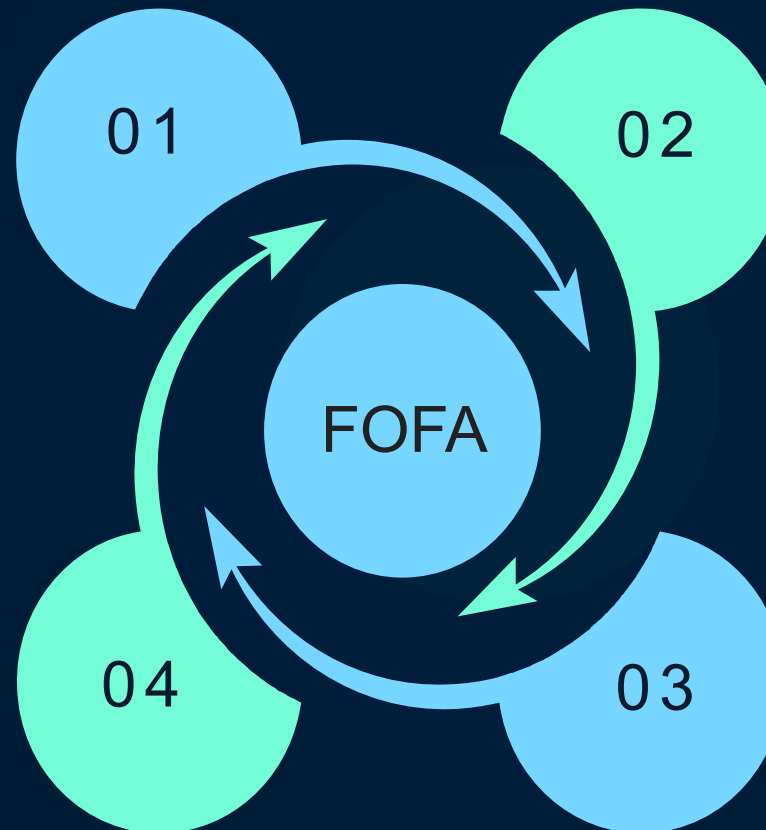
► Cyberspace Search Engine Core

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



Section 1

Core
Functions



Section 2

Application
Scenarios



Section 3

FOFA
Highlights



Section 4

▶ Product Positioning

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

Product
Positioning



Section 1

Core
Functions



Section 2

Application
Scenarios



Section 3

FOFA
Highlights



Section 4

► 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.

Query Description ✕

If the query keyword has no syntax or filter, it will default to search from HTML, HTTP header and URL;
 If the query syntax has multiple AND & OR relationships, try including it with ();
 Add "==" to complete the match, such as finding all hosts of qq.com. It can be domain=="qq.com".

— Advanced Search

Logic Operator	Description
=	Equal matching. When syntax="", it can be queried that the field does not exist or the value is empty.
==	Complete matching. When syntax=="", it can be queried that field dose exist or the value is empty.
&&	And
	Or
!=	Mismatching. When syntax!="", it can be queried that the value is empty.
*=	Fuzzy Search, Use * or? to query, such as banner*="mys??" (Member and above).🔗
()	Confirm the query priority. The parentheses have the highest priority.

Filter Example (Click to search)	Description	Tips
title="bing"	Query the "bing" from the title.	-
header="elastic"	Query"elastic"from the header	-

Query Description ✕

Filter Example (Click to search)	Description	Tips
title="bing"	Query the "bing" from the title.	-
header="elastic"	Query"elastic"from the header.	-
body="google"	Query the "google" assets from HTML.	-
fid="sSXXGNUO2FefBTcCLIT/2Q=="	Search the same fingerprint results by fid.	Type is subdomain.
domain="bing.com"	Query the "bing.com" by the domain name.	-
icp="京ICP证030173号"	Query the website record number.	Type is subdomain.
js_name="js/jquery.js"	Query " js/jquery.js" from the website body.	Type is subdomain.
js_md5="82ac3f14327a8b7ba49baa208d4eaa15"	Query the related results by js_md5.	-
cname="ap21.inst.siteforce.com"	Query "ap21.inst.siteforce.com" assets from Cname.	-
cname_domain="siteforce.com"	Query the Cname assets, which include "siteforce.com".	-
cloud_name="Aliyundun" new	Query the assets by cloud service name.	-
product="NGINX" new	Query the assets who use this product.	Member and above only
category="service" new	Query the assets who have this category.	Member and above only

► 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.

The screenshot displays the FOFA search engine interface. At the top, the search query is 'domain*='*gov.sg'. The search results are categorized into several sections:

- 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 FID:** (partially visible)

The main search results area shows 5,882 results (2,151 unique IP) in 1,359 ms. The first result is for the URL <https://test.api.dwp.gov.sg>. The details for this result include:

- IP: 52.139.236.106
- Location: Singapore / Singapore
- ASN: 8075
- Organization: MICROSOFT-CORP-MSN-AS-BLOCK
- URL: dwp.gov.sg
- Date: 2023-03-05
- Products: Windows
- Category: Operating System
- Product: Microsoft-Azure-Application-Gateway/v2

The HTTP response details for this URL are:

```
HTTP/1.1 404 Not Found
Server: Microsoft-Azure-Application-Gateway/v2
Date: Sun, 05 Mar 2023 08:20:49 GMT
Content-Type: text/html
Content-Length: 179
Connection: keep-alive
```

Below the details, there is a '+ Certificate' button with a certificate ID '2ad2a...'. The second result is for the URL <https://eservice-rpg.msf.gov.sg>.

► 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

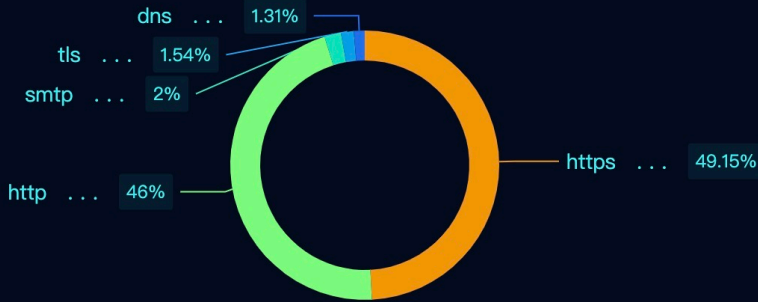
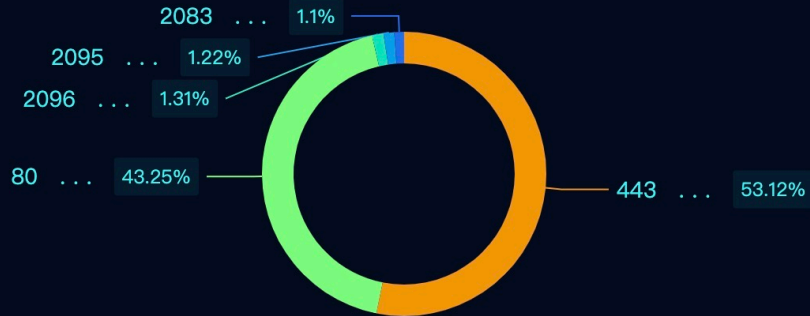
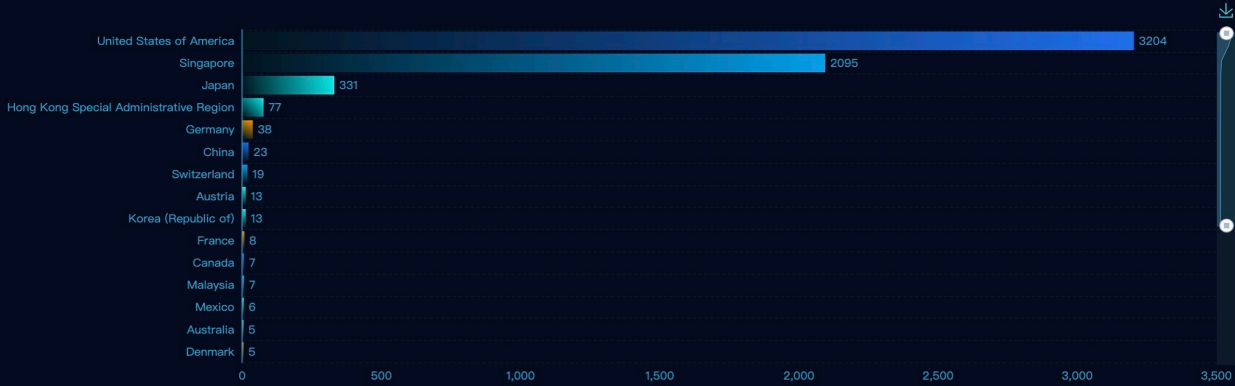
SUBJECTS

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

► Core Function – Search Engine

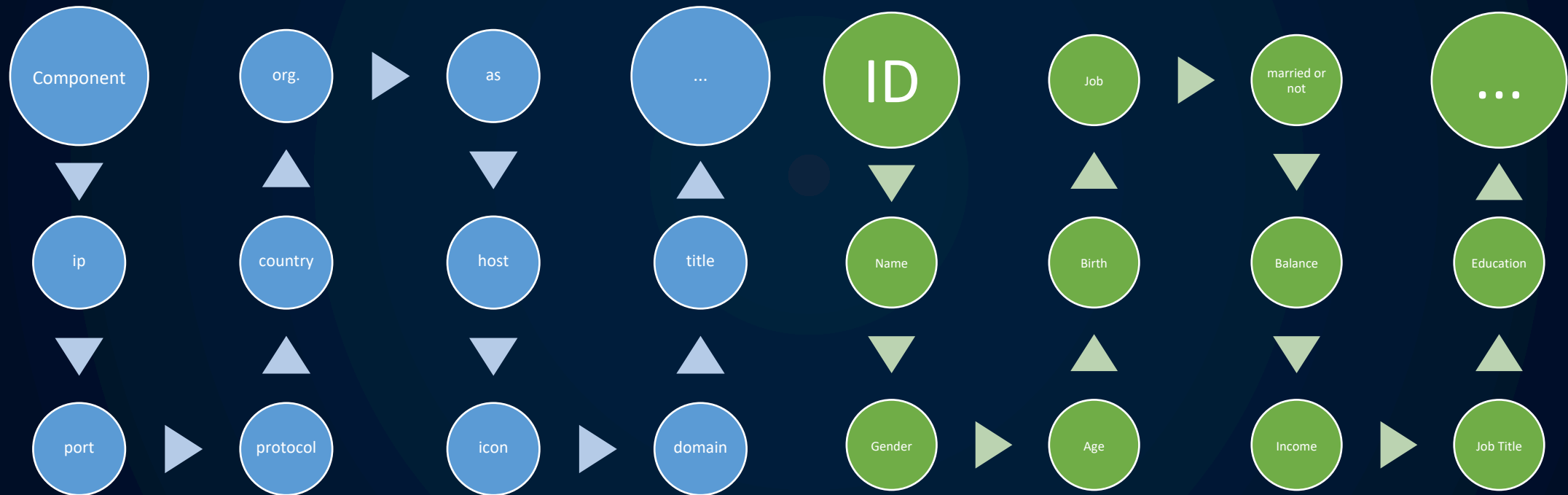
FOFA can also display the search results for distribution of assets through visual charts.

Global Statistics



► 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.

Country/Region: United States of America 🇺🇸

City: -

Organization: AMAZON-02

ISP: -

ASN: 16509

Last update time: 2023-03-05 17:00:00

Port (2) : 443 80

Protocol (2) : https http

Domain (20) :

- urplog.com sofastcdn.com
- edu20.com jakandjil.se
- oen.tw qr-code-generator.com
- vmax.com 100ms.live
- scopely.io pagesense.io
- ui.com dealmaggie.com
- ictv.online gofguidelines.be
- ownid.com swiftic.io
- playkidsapp.com digten.biz
- yungdd.com yungpp.com

Component Layer:

Component not found

Amazon-AWS-ELB
amazon-CloudFront
Google-Analytics
Baidu-站长平台
Microsoft-ASP.NET

Microsoft-ASP
Microsoft-ASP.NET-MVC
C3.js
cdnjs
Swiper
jQuery_UI

clipboard.js
php
jQuery
Bootstrap
Google-站长平台

NGINX
APACHE-HTTP_Server

Unassigned Component: -

Port	Protocol	Last update time	Component
443	TCP/HTTPS	2023-03-05	Amazon-AWS-ELB Amazon-AmazonS3 IIS Microsoft-ASP.NET Microsoft-ASP Microsoft-ASP.NET-MVC
443	TCP/HTTPS	2023-03-05	C3.js cdnjs NGINX amazon-CloudFront jQuery_UI clipboard.js Google-Analytics Baidu-站长平台 php
443	TCP/HTTPS	2023-03-05	jQuery Bootstrap APACHE-HTTP_Server Google-站长平台
80	TCP/HTTP	2023-03-05	amazon-CloudFront Google-Analytics Baidu-站长平台 NGINX APACHE-HTTP_Server Google-站长平台 Swiper
80	TCP/HTTP	2023-03-05	Amazon-AmazonS3

- 143.204.86.16:443 443 TCP/HTTPS

```

HTTP/1.1 200 OK
Connection: close
Content-Length: 79
Date: Sun, 05 Mar 2023 09:49:55 GMT
Via: 1.1 10e0af8ebbb9eea9a777605bac3912da.cloudfront.net (CloudFront)
X-Amz-Cf-Id: mLda8Plsk9cYL3jYPOgffPjmiOO5pgOWYlgdW7eDr6iwRj-PftPxx==
X-Amz-Cf-Pop: NRT12-C2
X-Cache: Miss from cloudfront
X-Uid: 30fdc0e5-615f-4b00-bda1-06cfc908d03
                    
```

+ 143.204.86.16:80 80 TCP/HTTP

► 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.

The screenshot displays the FOFA search interface with the following details:

- Search Query:** `app="BEA-WebLogic-Server" && fid="qaHp9oi4pMbm+CupTiiHfw=="`
- Results:** 3,429 results (2,179 unique IP), 872 ms, Keyword Search.
- Filters:**
 - TOP PRODUCTS: Barracuda-LoadBalancer (6)
 - TOP CATEGORIES: Load Balance (6)
 - TOP FID: qaHp9... (3,429)
 - TOP COUNTRIES/REGIONS:
 - United States of A... (2,319)
 - China (212)
 - India (118)
 - Canada (99)
 - Australia (71)
- Highlighted Results:**
 - Result 1:** `sipahcm.uniagustiniana.edu.co:8000` (999+). Organization: ORACLE-BMC-31898, uniaustiniana.edu.co. HTTP status: 200 OK.
 - Result 2:** `https://c-ehr.bbm.com.cn:8090` (999+). Organization: Huawei Cloud Service data center. HTTP status: 200 OK.

► 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.



The screenshot displays the FOFA search interface. At the top left is the FOFA logo. A search bar contains the query `host*="vpn.*.com"`. To the right of the search bar are icons for a document and a magnifying glass. Below the search bar, a row of 10 favicons is shown, each with a count above it: 985, 116, 92, 58, 58, 50, 48, 42, 41, and 34. The text "Favicon(10):" is positioned to the left of the first icon. To the right of the favicons are buttons labeled "More" and "Select all". Below this row, there is a section for "TOP PRODUCTS" with a button labeled "all". To the right of this button, the search results are summarized: "124,018 results (66,239 unique IP) , 1089 ms , Keyword Search." Below this summary, a note reads: "Nearly year results, click to view all results."

► 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.

Download Results

Your queries: host*="vpn.*.com"
Results: 124,018
Free Credit: 998778 ?

Export data: results =
1 results=1 F point

Export type:

Current balance: 0F points [Get more F points](#)

File Name:

Select your field:

Download Results

Your queries: host*="vpn.*.com"
Results: 124,018
Free Credit: 998778 ?

Export data: results =
1 results=1 F point

Export type:

Current balance: 0F points [Get more F points](#)

File Name:

Select your field:

▶ 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.

The screenshot displays the FOFA search interface with the following components:

- Search Bar:** Contains the query `is_honeypot=true && icon_hash="516963061"`.
- Navigation:** Includes links for Announcement, Pricing, and Support.
- Search Results Summary:** Shows 13,031 results (291 unique IP), 184 ms response time, and a Keyword Search filter. A note indicates that nearly year results are shown, with a link to view all results.
- TOP FID:** A list of top identifiers including TAPo9... (4,505), SQ0D... (3,272), ClIYR... (3,097), zRggx... (1,272), and o7udG... (256).
- TOP COUNTRIES/REGIONS:** A list of regions including China (8,541), United States of A... (1,302), Singapore (374), Germany (348), and Australia (317). A world map highlights these regions.
- TOP OPEN PORTS:** A list of open ports including 2000 (88) and 1947 (45).
- IP Details:** Two specific IP addresses are highlighted:
 - 121.36.216.152:9200:** Located in China, ASN: 55990, Organization: Huawei Cloud Service data center, 2022-08-07. Identified as a Router Webserver.
 - 8.208.93.53:9200:** Located in the United Kingdom of Great Britain and Northern Ireland / London, ASN: 45102, Organization: Alibaba US Technology Co., Ltd., 2022-08-06. Identified as BlueServer/5.1.0.4.
- HTTP Headers:** Detailed headers for both IP addresses, including status (200 OK), connection type, content length, accept ranges, content disposition, content type (application/json), date, pragma, and server information.

► 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.

Query Interface

▼ Aggregation & Statistics

Statistic Aggregation

HOST Aggregation

▼ Basic Interface

Account Information

```
1 // 20230305174023
2 // https://fofa.info/api/v1/search/all?email=
3
4 {
5   "error": false,
6   "consumed_fpoint": 0,
7   "size": 124154,
8   "page": 1,
9   "mode": "extended",
10  "query": "host*=\"vpn.*.com\"",
11  "results": [
12    [
13      "https://vpn.camagroup.com",
14      "5.96.41.212",
15      "443"
16    ],
17    [
18      "vpn.lykeyunzhan.com:888",
19      "81.70.17.86",
20      "888"
21    ],
22    [
23      "vpn.huaenorganic.com:14147",
24      "47.111.82.157",
25      "14147"
26    ],
27    [
28      "vpn.mossberg.com:500",
29      "172.85.57.242",
30      "500"
31    ],
32  ]
33 }
```

▶ 3. Application Scenarios

Product
Positioning



Section 1

Core
Functions



Section 2

Application
Scenarios



Section 3

FOFA
Highlights



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`

The screenshot shows a FOFA search interface with the query `app='Log4j2' && country='US'`. The search results show 1,653,280 results (964,643 unique IP) in 1,497 ms. A search result for 'Logging Services' is highlighted, showing the URL `http://logging.apache.org` and the IP `208.52.146.174:8888`. The page content includes the Apache Log4j logo and a section titled 'Apache Log4j™ 2' with a warning for 'Important: Security Vulnerability CVE-2021-44832'. The warning summary states: 'Apache Log4j2 vulnerable to RCE via JDBC Appender when attacker controls configuration.' The details section explains that Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack. The mitigation section advises upgrading to Log4j 2.3.2 (for Java 6), 2.12.4 (for Java 7), or 2.17.1 (for Java 8 and later). The reference section points to the Security page for details and mitigation measures for older versions of Log4j. Below this, another warning for 'Important: Security Vulnerabilities CVE-2021-45105, CVE-2021-45046 and CVE-2021-44228' is visible.

▶ 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.

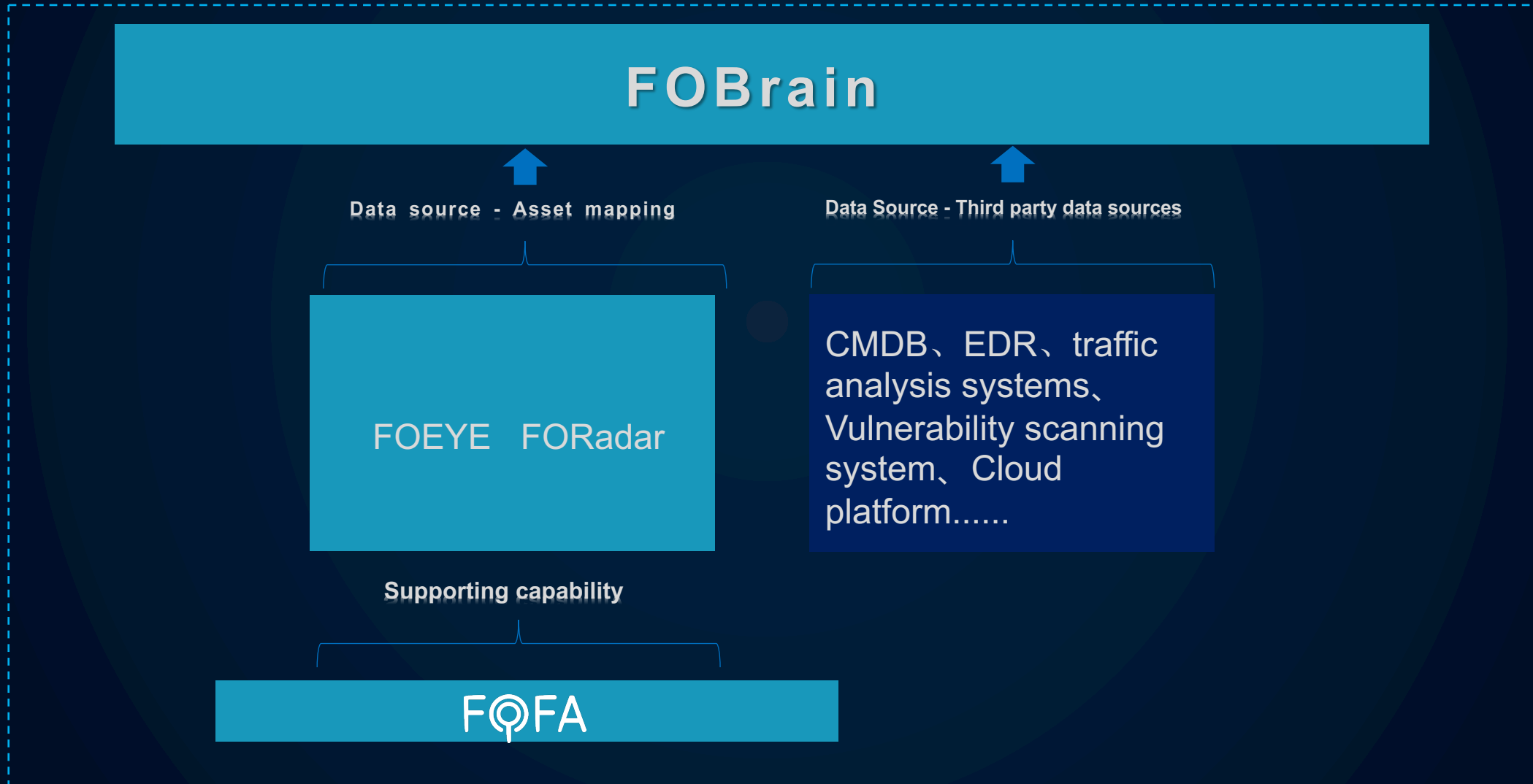
Large enterprises have the need to clearly grasp the exposed surface of network assets that they need to protect and understand comprehensively the security risks in their network assets.

FOFA can extract 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".

The screenshot shows the FOFA search interface with two search queries: `host="hsbc.com"` and `icon_hash="-1880472501"`. The results for the second query are displayed, showing 201 results (126 unique IP) in 351 ms. The results are categorized into Top Products, Top Categories, Top FID, and Top Countries/Regions. A detailed view of a result for `https://easyid-dev.hsbc.ca` is shown, including its IP address (143.204.86.16), location (United States of America), organization (AMAZON-02), and products (Amazon-S3, CloudFront). A technical details panel on the right shows HTTP status (200 OK) and various headers.

Category	Item	Count
TOP PRODUCTS	WordPress	1
TOP CATEGORIES	Other Enterprise Application	1
TOP FID	6Vd+X...	9
	5axFH...	8
	8X2L2...	7
	WisbM...	7
	IQVKq...	7
TOP COUNTRIES/REGIONS	Hong Kong Specia...	79

▶ Application Scenarios – EASM Product



▶ 4. FOFA Highlights

Product
Positioning



Section 1

Core
Functions



Section 2

Application
Scenarios



Section 3

FOFA
Highlights



Section 4



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



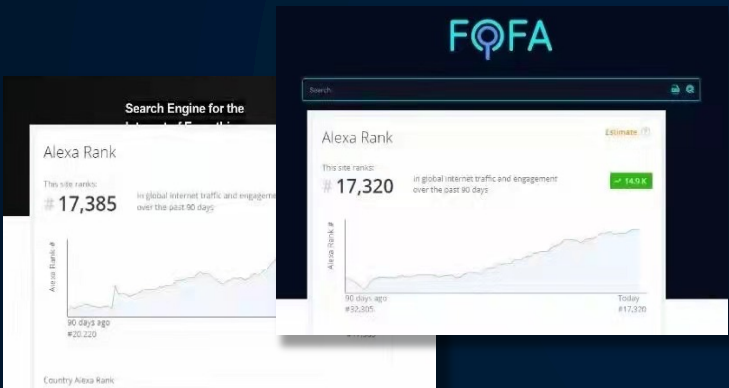
Rapid and sustainable growth

- >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	Performance Results				
	FOFA	ZoomEye	QUAKE	SHODAN	censys
● Time: Oct 2021					
● Goal : Random scan of 23 IPs in key areas over the global	In 8 hours	17 / 23	0 / 23	0 / 23	0 / 23
● Testing method : record and compare the scanning results of target IPs using 5 top network scanning platforms	In 24 hours	22 / 23	2 / 23	0 / 23	2 / 23
	In 48 hours	23 / 23	10 / 23	2 / 23	4 / 23
	In 72 hours	23 / 23	21 / 23	6 / 23	10 / 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

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"



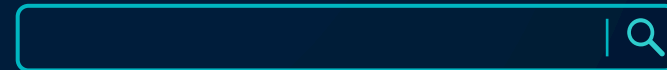
"Can't believe it is done by Chinese people"



"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"



<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!