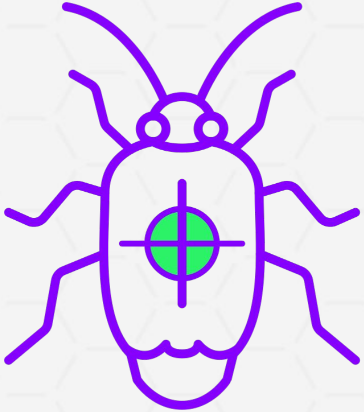
POLYSWARM

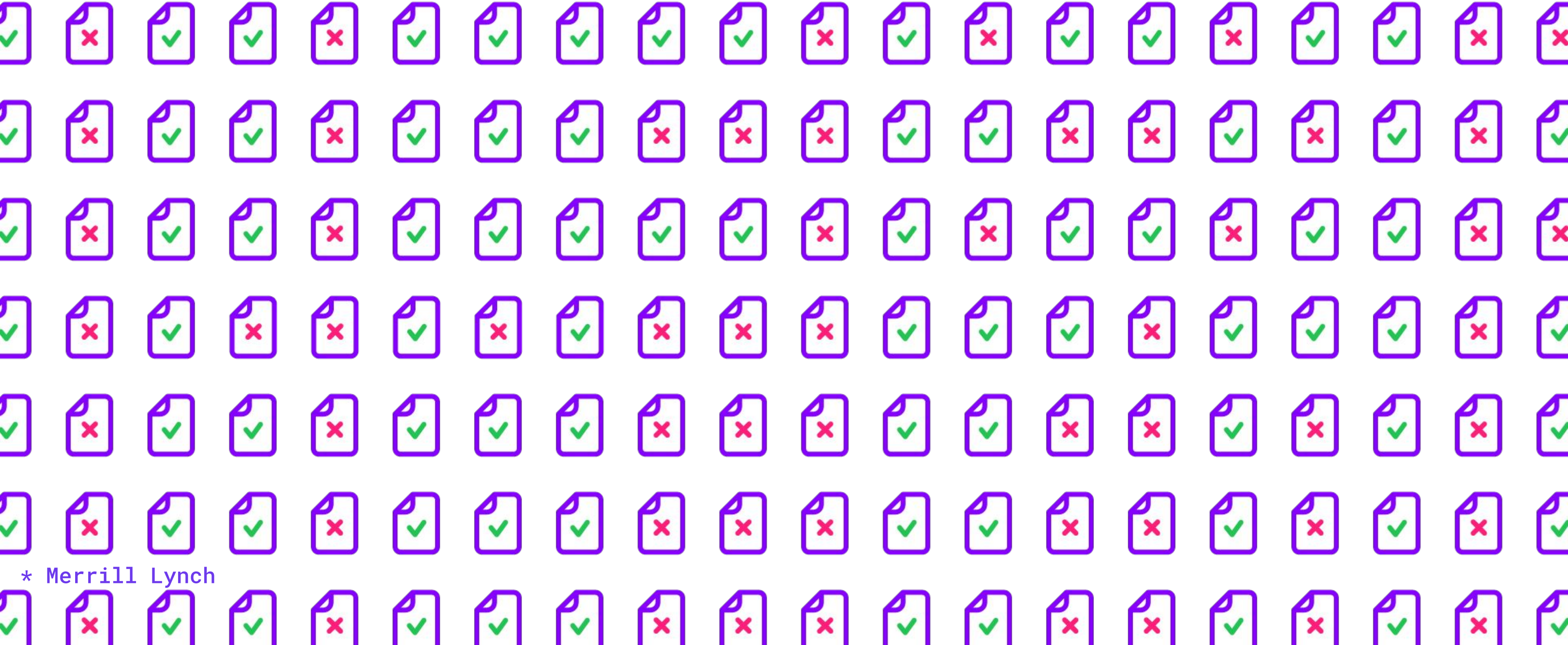
53-74%

Average anti-virus effectiveness against new threats*



* RAP Proactive

400 New threats every minute*



* Merrill Lynch

...Causing

$3T USD in costs, and expected to double by 2021*

* CyberSecurity Ventures (2015)

Today's threat protection economy is broken.

The Problem

Today's centralized threat detection model

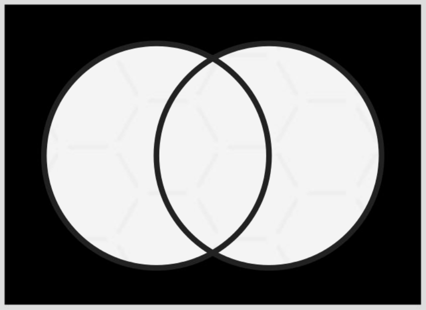
1. Duplicates efforts reducing coverage.
   All AV must detect WannaCry. This creates duplication of effort, cost and coverage, to so some degree (Figure A)

2. Disincentivizes specialized offerings.
   Lowest common denominator wins: invest in common widespread threats.

3. Vendors are not compatible. You can't run both McAfee and Symantec if you wanted to. And you don't want to (Figure B)

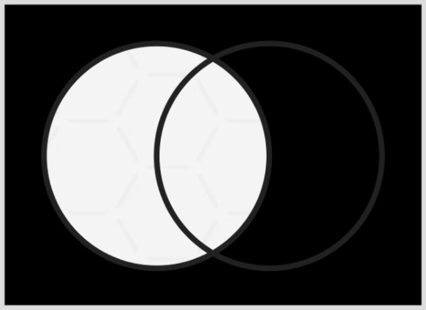
4. Lack of transparency
   Buyers and sellers are in the dark; sellers don't know what threats they're missing and buyers cannot differentiate sellers

Figure A



left circle: AV 1 coverage
right circle: AV 2 coverage
black: blind spot

Figure B



you went with AV 1
black is still your blind spot

Solution:

incentivize competitive coverage

using smart contracts

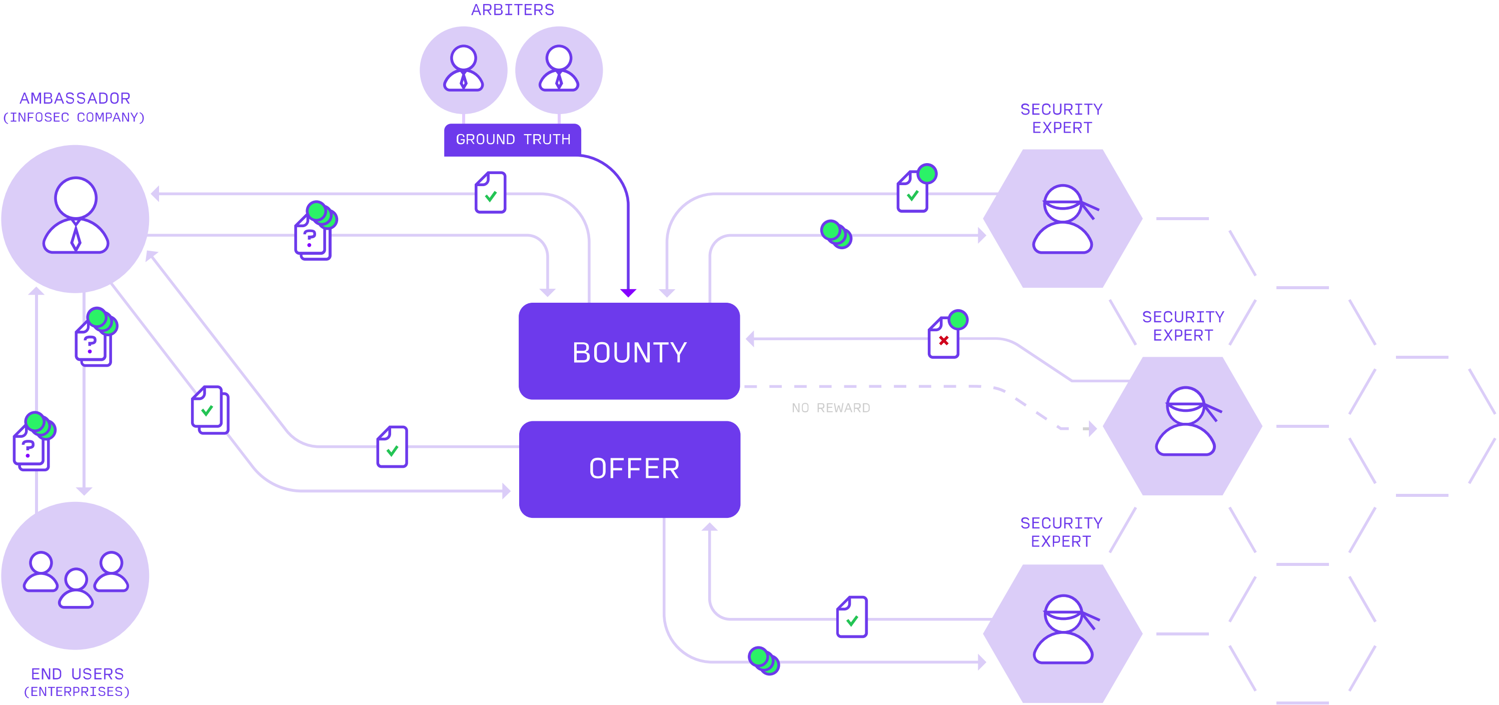
Polyswarm fixes the economics

PolySwarm decentralizes and tokenizes malware threat intelligence.

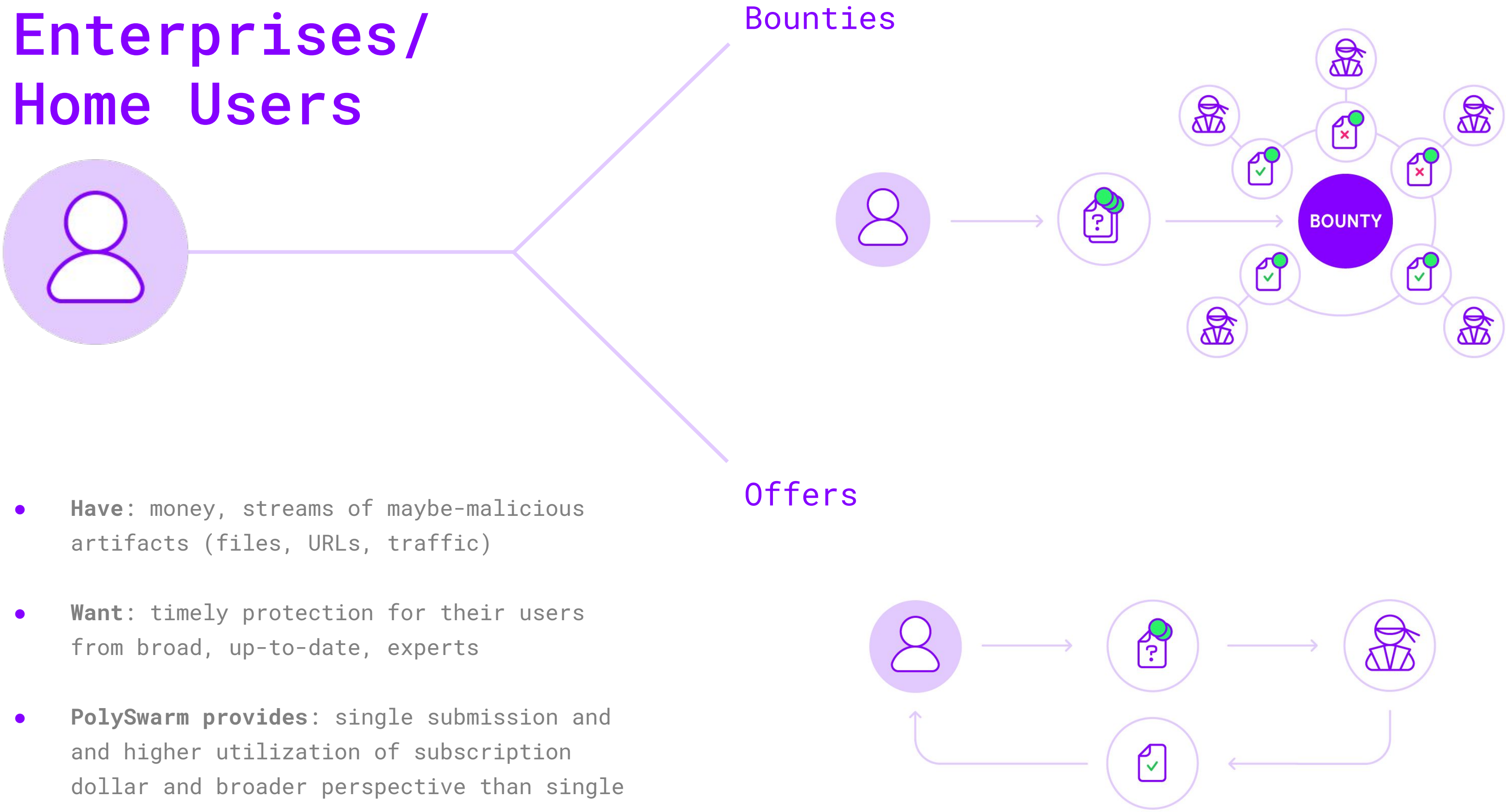
And automatically rewards security experts for timely judgements on the malintent of things submitted by Enterprises & End Users.

PolySwarm rewards accuracy.

threat protection redefined



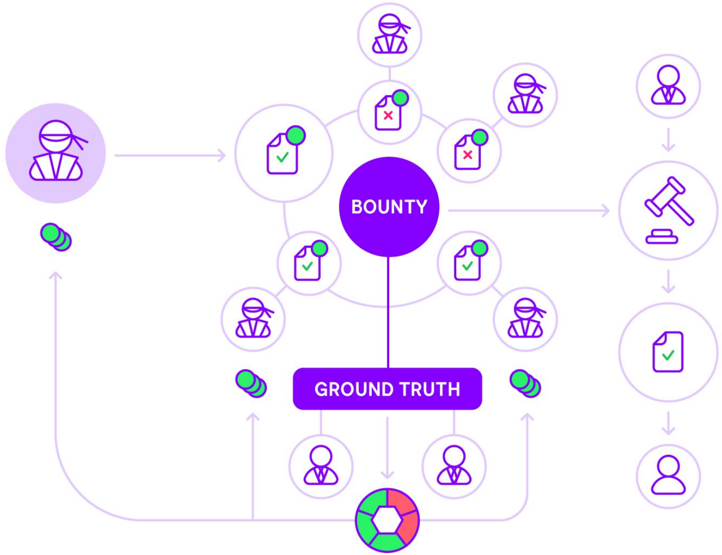
Enterprises/ Home Users



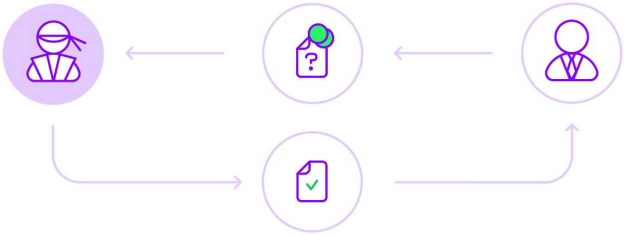
- **Have**: money, streams of maybe-malicious artifacts (files, URLs, traffic)
- **Want**: timely protection for their users from broad, up-to-date, experts
- **PolySwarm provides**: single submission and and higher utilization of subscription dollar and broader perspective than single vendor services

Security Experts

Bounties



Offers

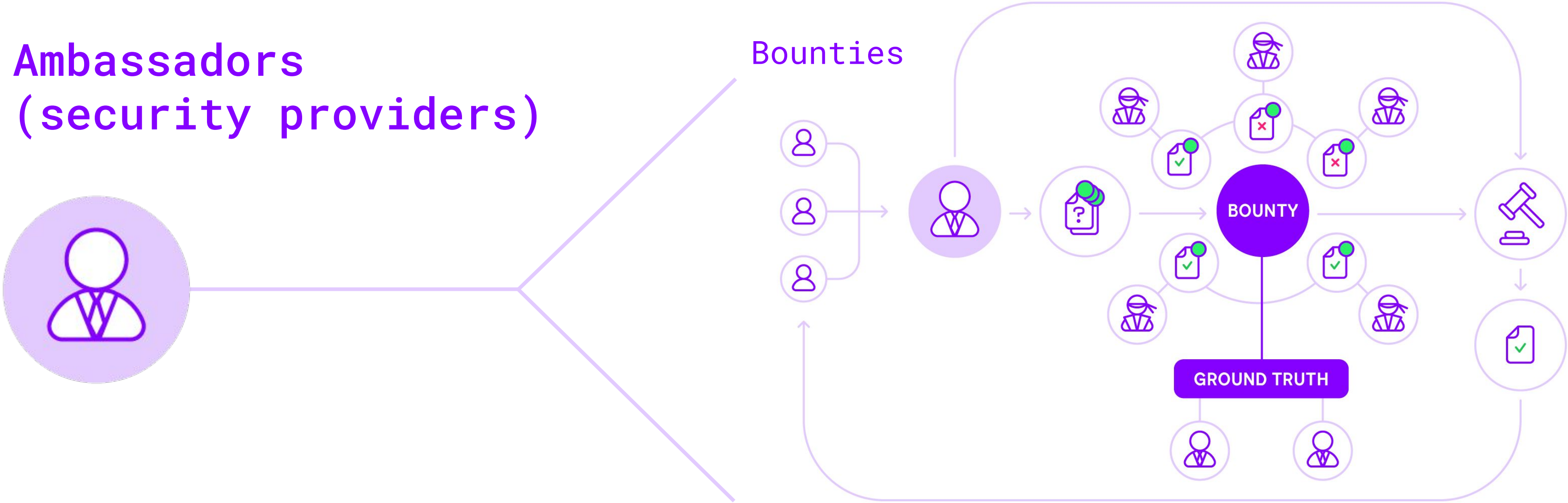


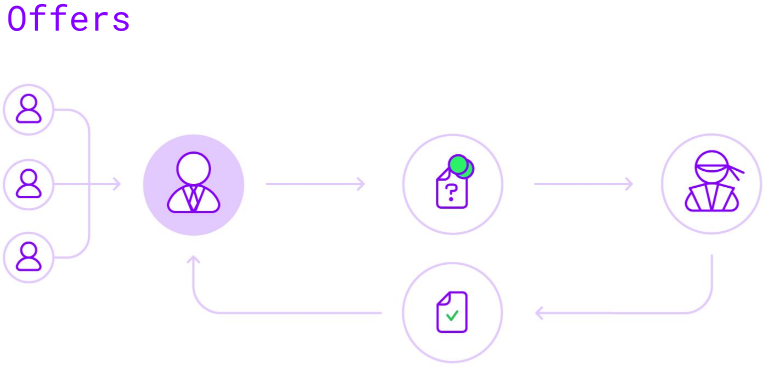
- **Have**: vast expertise in finding badness in files, urls, and network traffic (artifacts)

- **Have**: up to date intel on their slice of the malware underground

- **Want**: passive income from encapsulating knowledge into engine that lives on the market

Ambassadors (security providers)

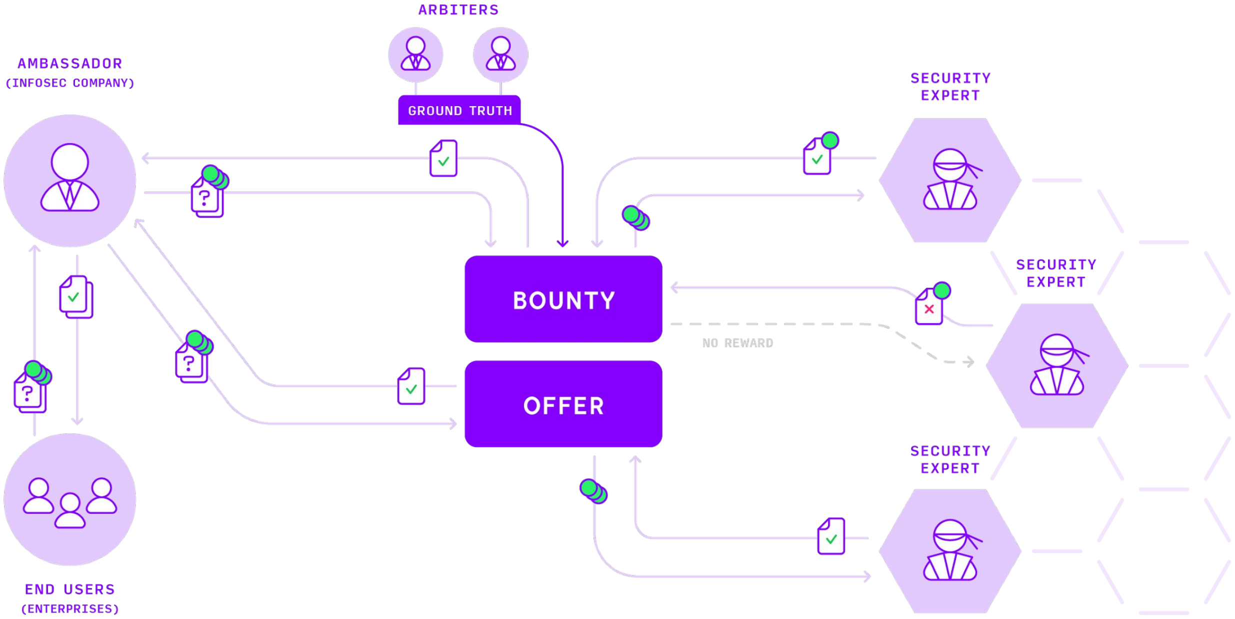




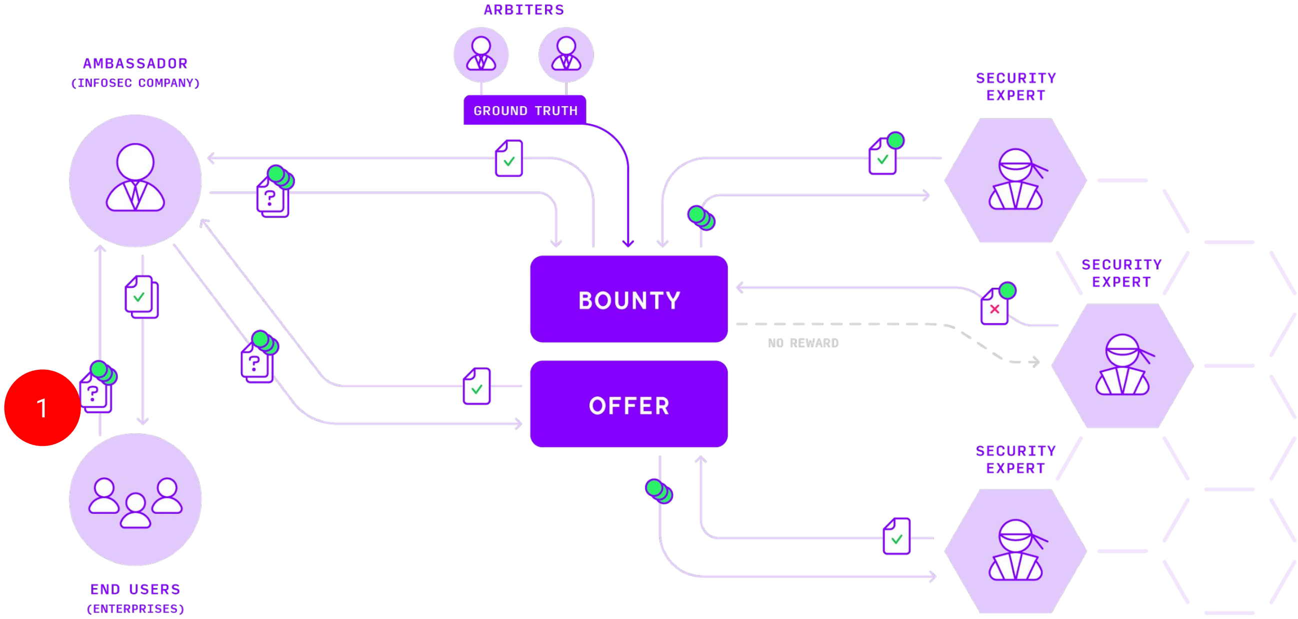
- **Have**: Enterprise customers and accuracy data for PolySwarm security experts.
- **Want**: income from curated offerings to Enterprises.
- **PolySwarm provides**: curated offerings in a simple subscription model to Enterprises. Market maker for experts.

using a prediction market

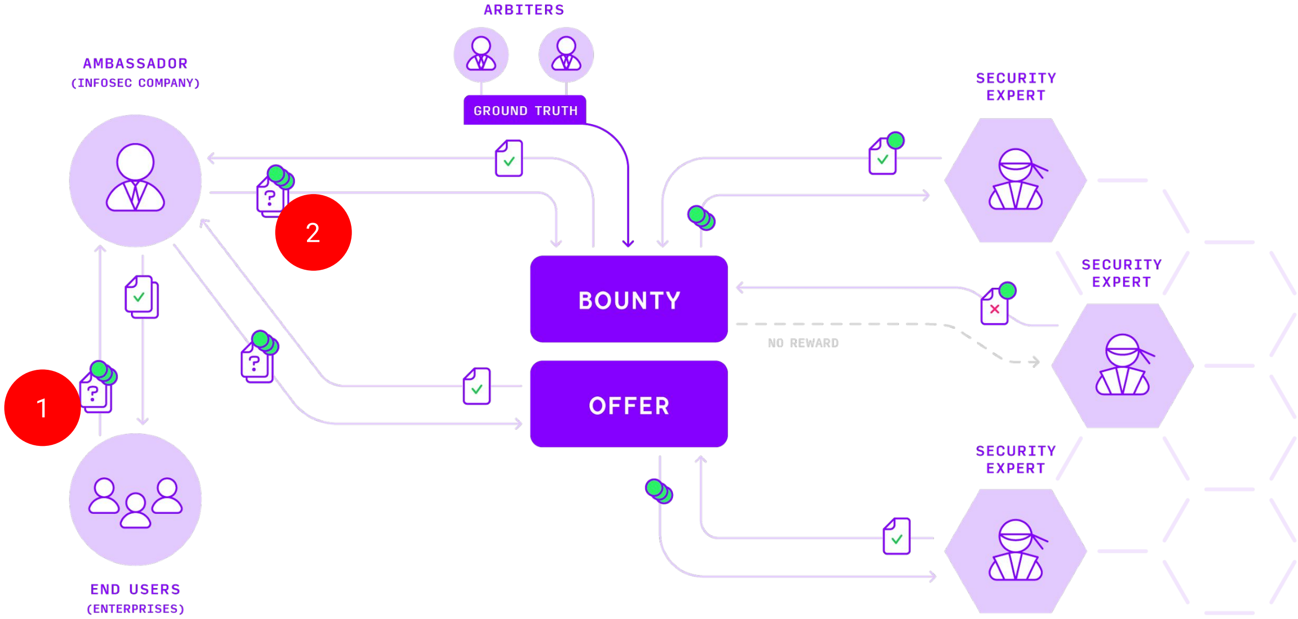
Bounties in depth



Bounties in depth



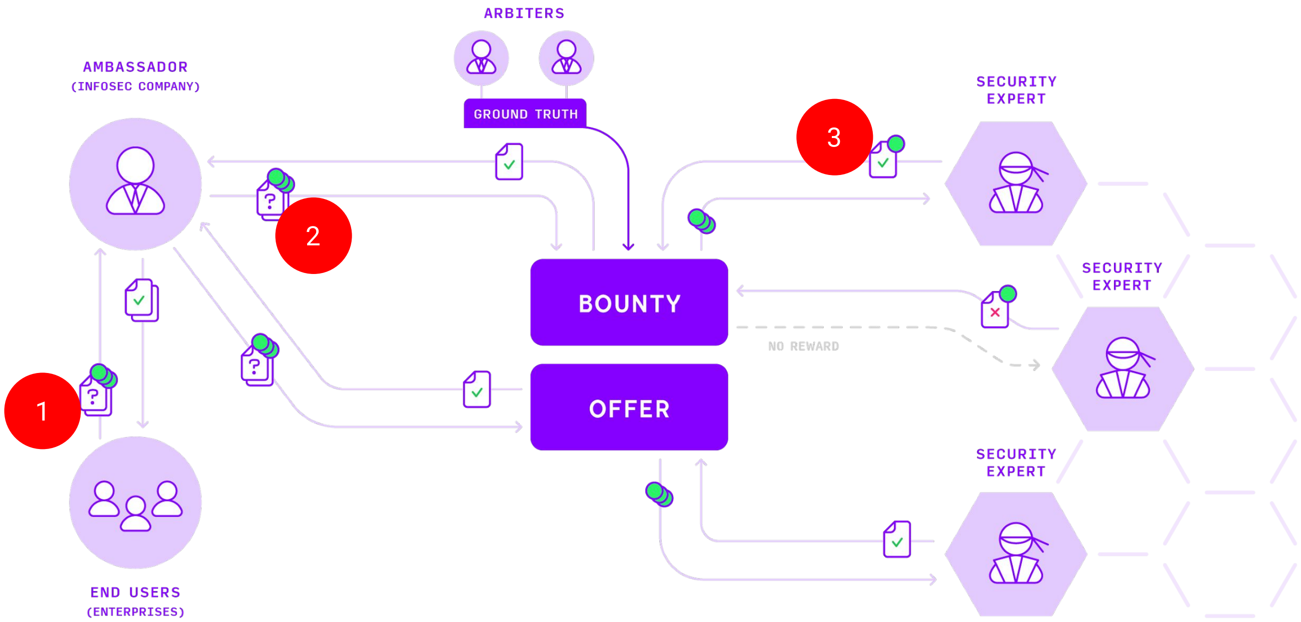
Bounties in depth



no people

all software.

Bounties in depth



whoa.

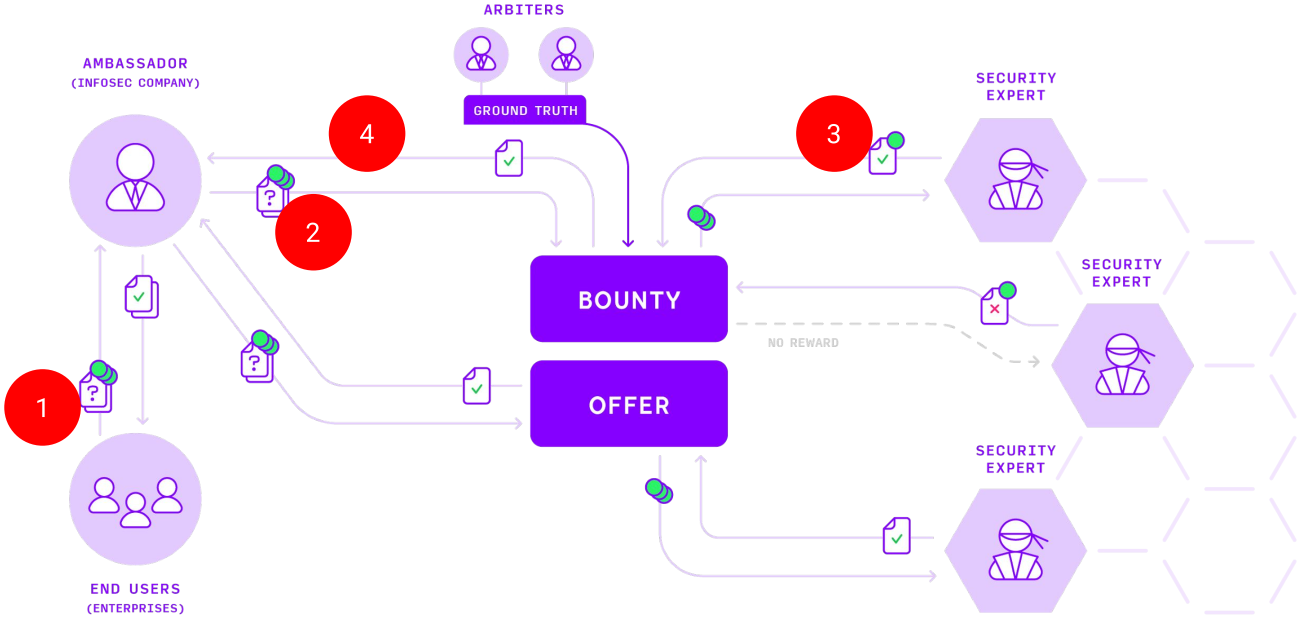
experts

pay to work?

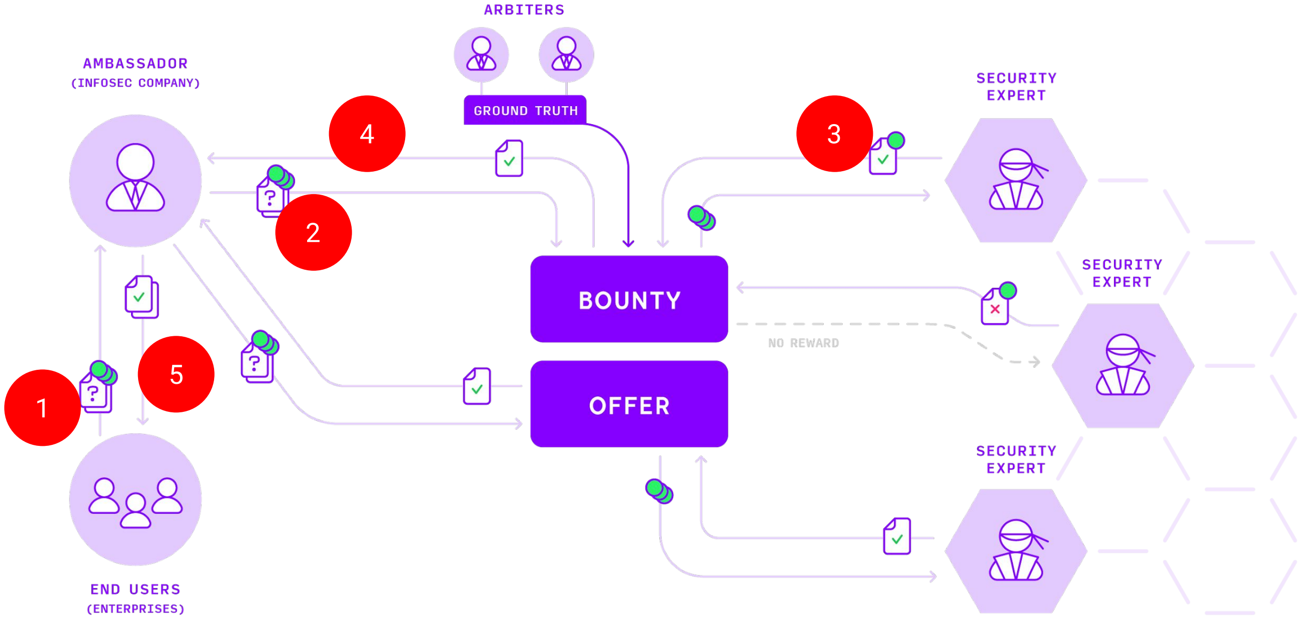
experts stake for fun/profit

- Stake is used as statistical confidence
- Blockchain tracks historical outcomes and rise/fall of engines
- A new trusted data source for cyber risk insurance pricing

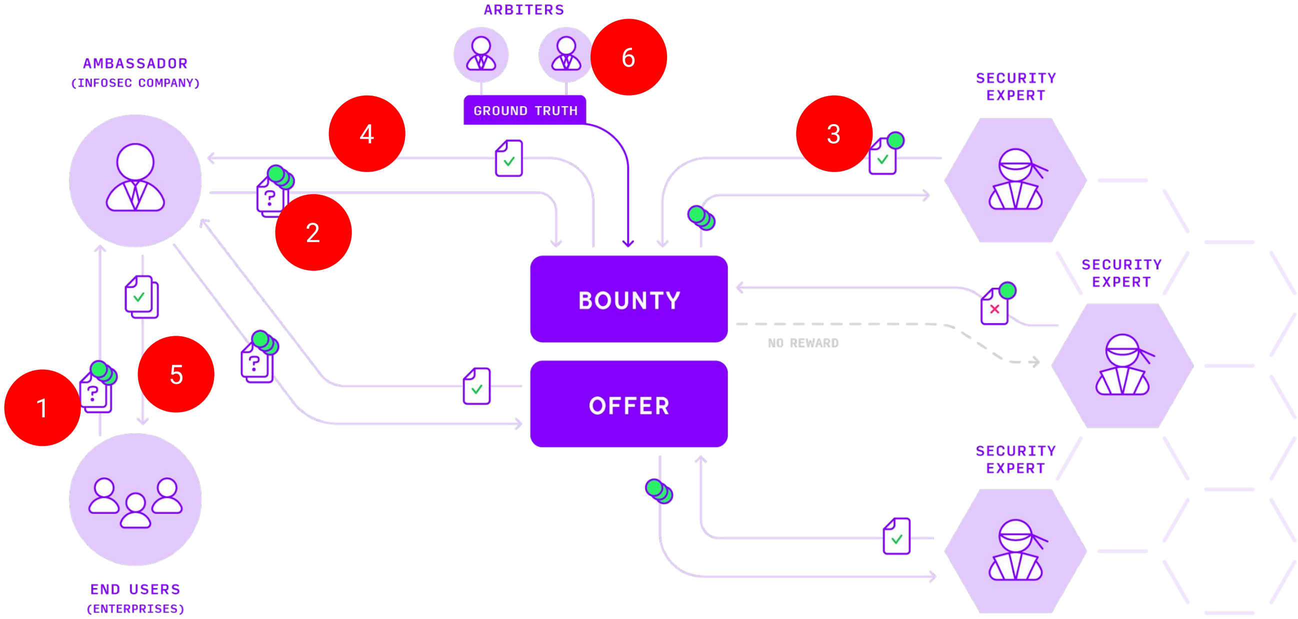
Bounties in depth



Bounties in depth

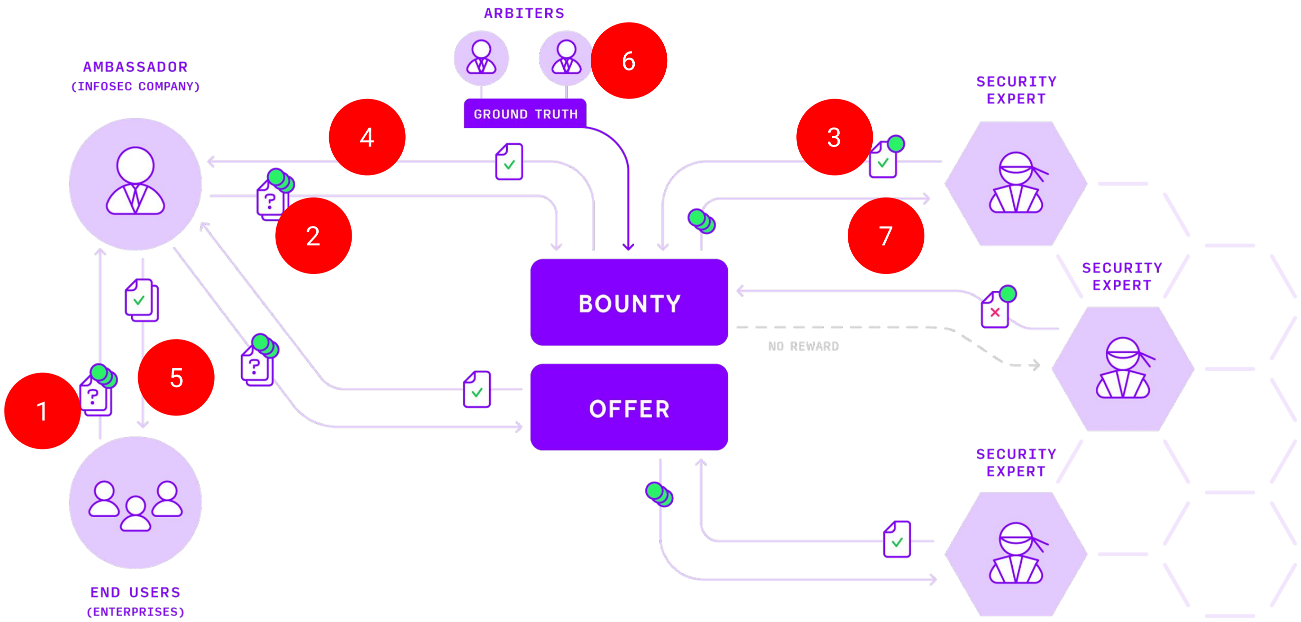


Bounties in depth

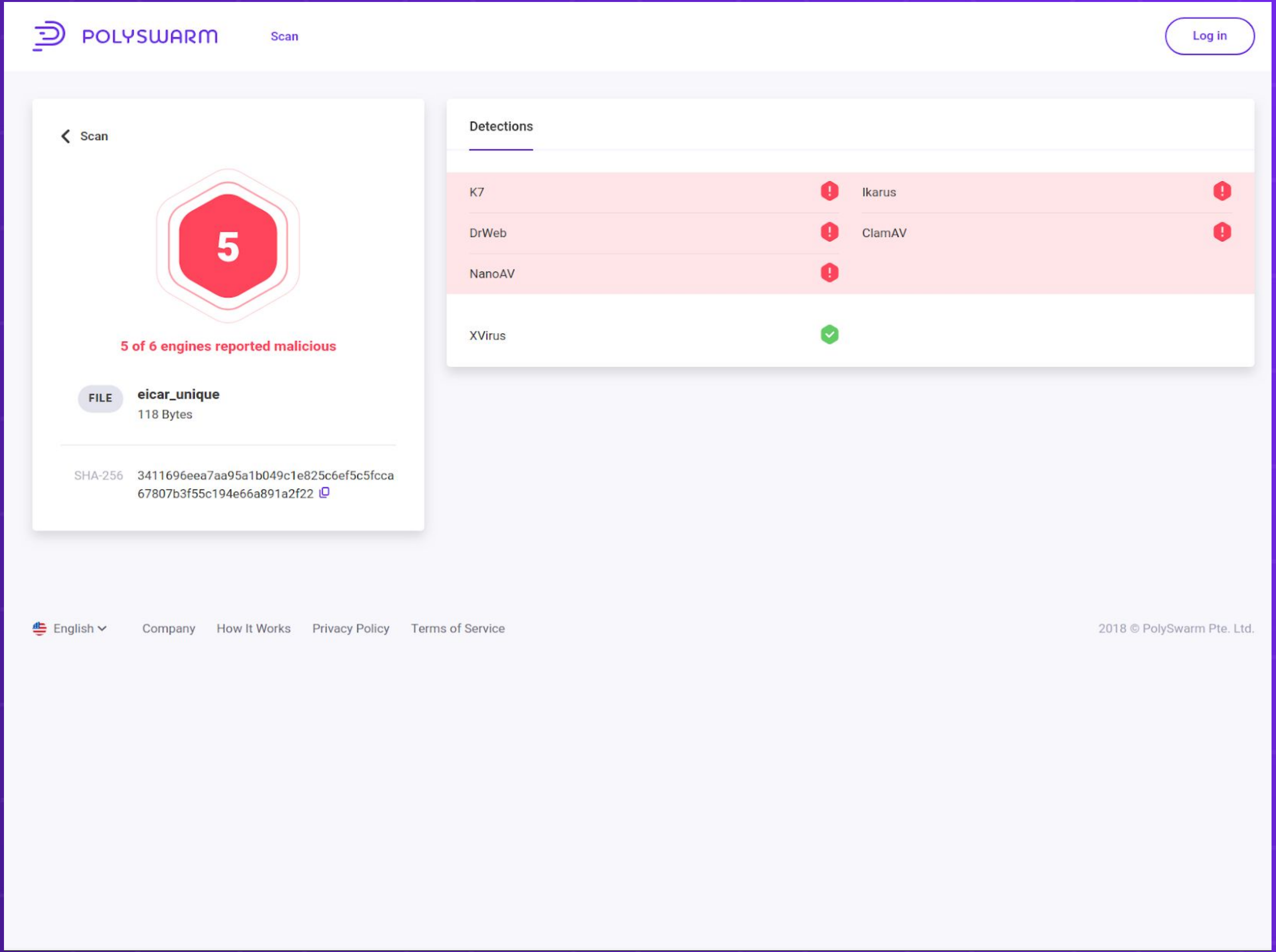


why trust arbiters?

Bounties in depth



bounty response in depth.



5 of 6 engines reported malicious

FILE **eicar_unique**
118 Bytes

SHA-256 3411696eea7aa95a1b049c1e825c6ef5c5fcca67807b3f55c194e66a891a2f22

Detections

K7	!	Ikarus	!
DrWeb	!	ClamAV	!
NanoAV	!		
XVirus	✓		

2018 © PolySwarm Pte. Ltd.

```
{   "size": 189,
    "bounty_guid": "cbbda33b-3167-41b0-9717-57a5b577fe28",
    "bounty_status": "Quorum Reached",
    "assertions": [
        {   "bid": 62500000000000000,
            "author_name": "k7",
            "author": "0xbE0B3ec289aaf9206659F8214c49D083Dc1a9E17",
            "verdict": true,
            "metadata": "EICAR_Test_File" },
       <snip>
        {   "bid": 62500000000000000,
            "author_name": "ikarus",
            "author": "0xA4815D9b8f710e610E8957F4aD13F725a4331cbB",
            "verdict": true,
            "metadata": "EICAR-Test-File" }, ],
    "votes": [
        {
            "arbiter": "0x2E03565b735E2343F7F0501A7772A42B1C0E8893",
            "vote": true
        }
    ],
    "window_closed": true
}
```

what are the
incentives.

expert incentives

specialized and timely intel reaps rewards

1. Reward for specialty
   Engines can focus on broad or narrow scope, only assert if confident

2. Access to sample stream
   Level the playing field to data access

3. Wide Distribution.
   No language barriers or marketing beauty contests to win.

4. Reputational Record
   Testing firms don’t matter, long term performance recorded to blockchain that we can’t modify.

user incentives

broad protection without vendor bakeoffs

1. Second, Third, and Nth opinion
   Many opinions, one artifact, experts put money/reputation on the line

2. Reputation based weighting
   Past performance indicates trust in expert verdicts

3. Competitive Detection
   Experts race to be the first to detect 0day

4. Self Configuring
   Regional differences between AV vendors go away

25 Engines online in 1.0

many additional engines on the pipeline

Dr.WEB®
Anti-virus
NANO
antivirus
INTEZER
TRUSTLOOK
Zillya
ANTIVIRUS
HATCHING
TYLABS
LIONIC
IKARUS
security software
SecureAge
XVirus
TACHYON
Alibaba.com
RISING
LION-STRONG SECURITY
EMSISOFT
ANTIY
K7
IRIS-H

get involved

- write a micro-engine
- become an ambassador
- get in touch

  bens@polyswarm.io

  https://polyswarm.network

POLYSWARM

https://polyswarm.io