Zach Wasserman - November 30, 2023

Securing the endpoint with open (source) software

fleet

Zach Wasserman

CTO & Cofounder @ Fleet

- Co-creator of osquery, steering committee member
- Climber, biker, skier, Phish fan

16:45
Mittwoch, 20. Februar

chrome
SAMSUNG

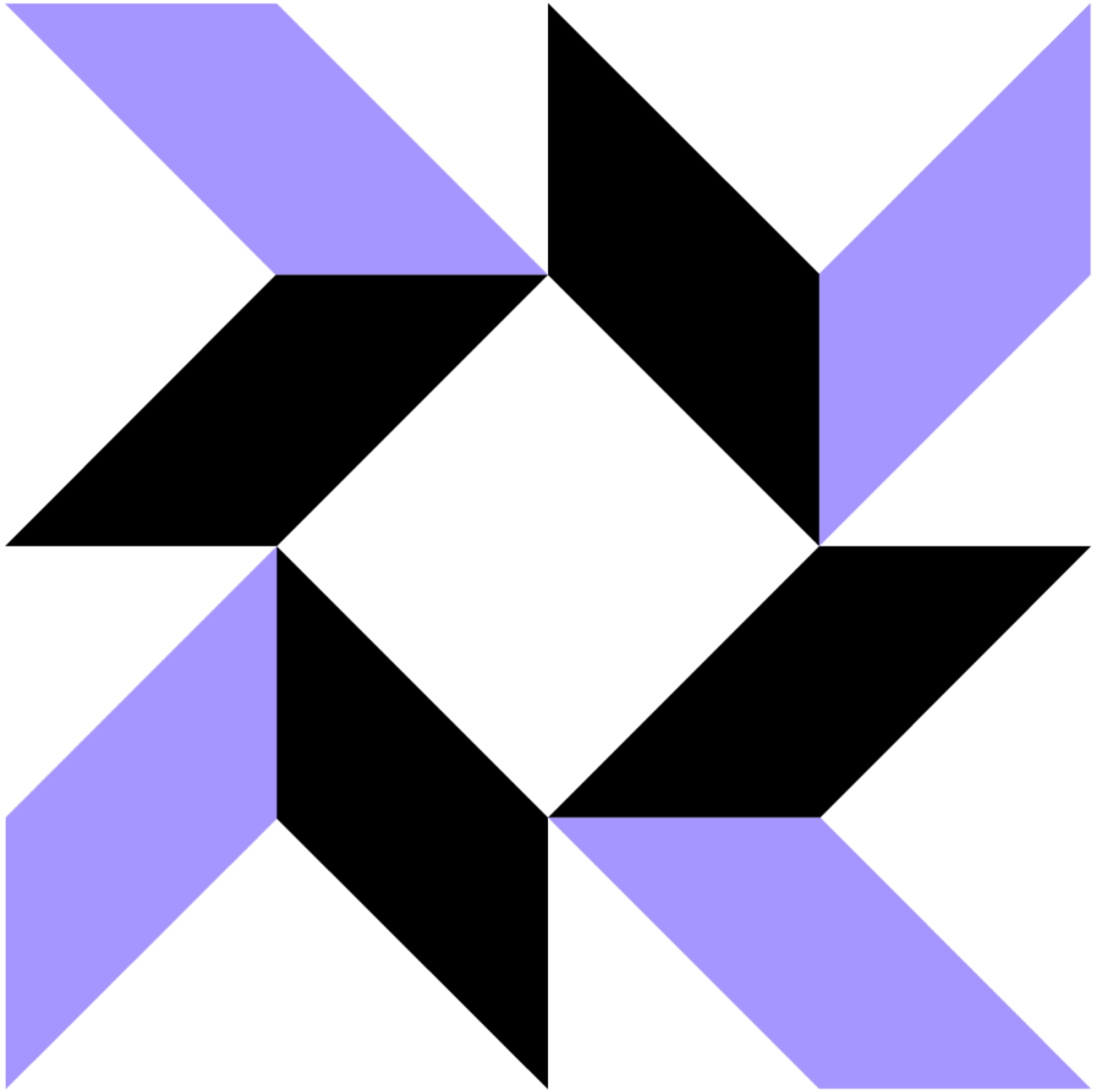
TCNU 427368 9 45G1
CAPITAL
CLHU 902214 7 45G1
ONE
ONEU 022267 9 45G1
ONE
TLLU 556645 0 45G1
FCGU 167620 3 45G1
ONE
BEAU 524904 0 45G1
tex
TEMU 747350 4 45G1
tex
TEMU 730164 45G1
TAL
TCLU 181916 7 45G1
GESU 677715 8 45G1
TAL
TCLU 837136 7 45G1
K LINE
KKFU 758317 1 45G0
TAL
TRLU 751062 0 45G1
TCNU 665678 0 45G1
BEACON
BMOU 660044 7 45G1
ONE
TLLU 544319 45G1
TCNU 441766 2 45G1
NYK LINE
NYKU 4345 16 5 45G1
ONE
FDCU 054699 0 45G1
TCNU 624758 6 45G1
TCNU 599497 2 45G1
NYK LINE
NYKU 4100 21 8 45G1
DRYU 607637 2 45G1
ONE
FFAU 147773 45G1
ONE
TLLU 553526 0 45G1
NYK LINE
NYKU 482331 0 45G1
TLLU 455387 0 45G1
NYK LINE
NYKU 4068 68 8 45G1
K LINE
KKFU 753027 4 45G0
TCNU 443074 6 45G1
NYK LINE
NYKU 481320 3 45G1
TCNU 647538 45G1

KUKA
2.D
KUKA

J4
DISPLAY
GLOBAL_EN
RUN
J2
FCC ID: 2ABCB-RPI4B
IC: 20953-RPI4B
Made in the UK
CAMERA
HDMI
J3
J6
HDMI0
J13
HDMI1
R47
D13U
ACT
PWR
POWER IN

Osquery

- Write queries to collect logs on state of endpoints
- Supports macOS, Linux, Windows
- Enable non-developers to access and aggregate data from disparate sources
- Performance/reliability to deploy across corporate and production infrastructure
- Open source (MIT license)



```
SELECT * FROM users;
```

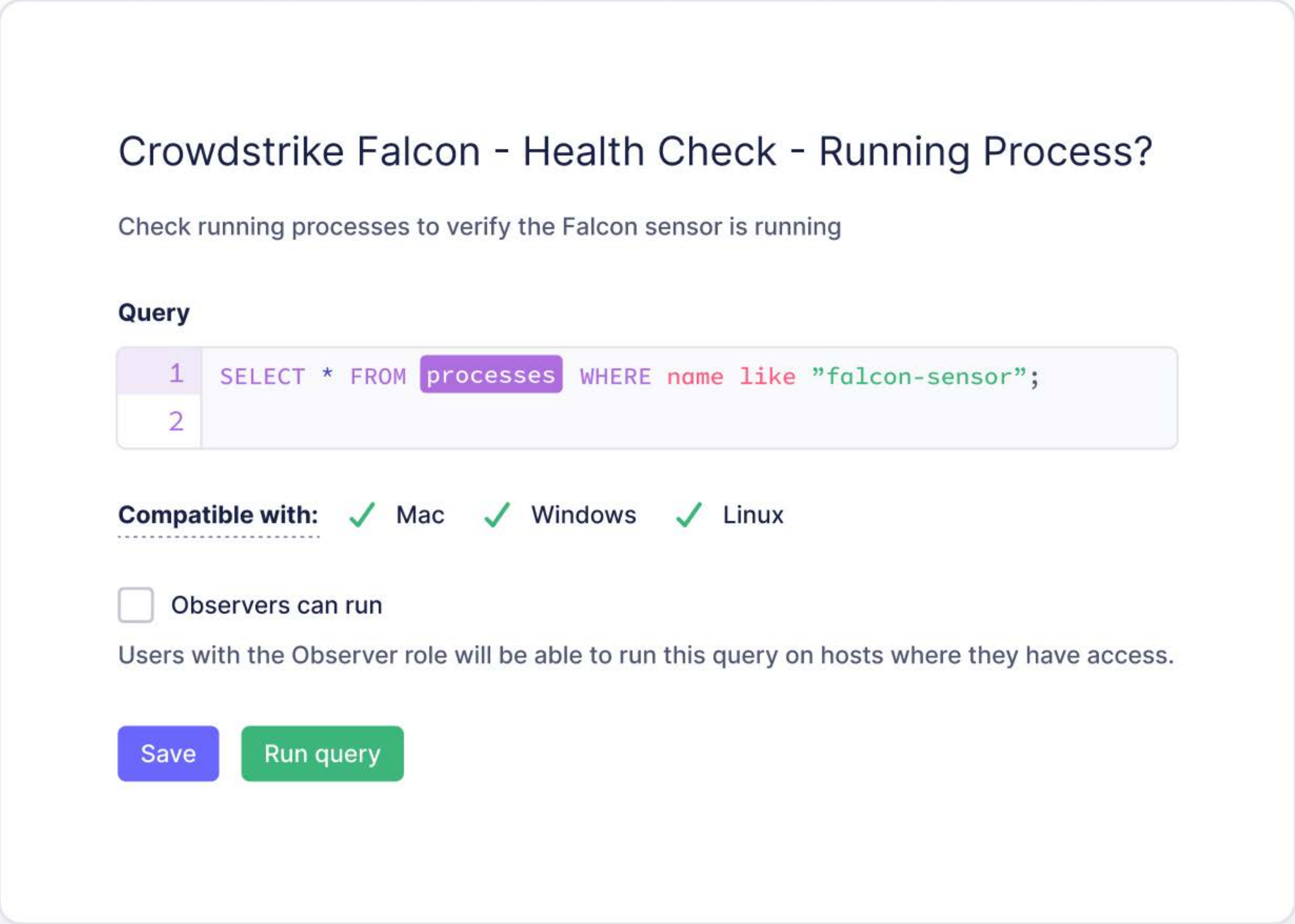
- Flat files (`/etc/hosts`, `/etc/crontab`, `~/.ssh/known_hosts`, etc.)
- SQLite files (`/var/db/SystemPolicy` [GateKeeper configuration], etc.)
- System APIs (Apple System Log, Keychain, SMC, CoreFoundation, etc.)
- Application APIs (Docker, Carbon Black, etc.)
- Event-based APIs (FSEvents, OpenBSM, etc.)
- Filesystem (Shared folders, file hashes, permissions, etc.)
- Plists (`/Library/Managed\ Installs/*` [Munki data], etc.)

- ... All available under the same SQL interface

```
SELECT *
FROM processes
JOIN process_open_sockets
  USING (pid)
WHERE name = ‘sshd'
  AND local_port != 22;
```

Fleet

- Package, deploy, and manage osquery at scale
- Run live queries, detect vulnerable software, policy compliance, and trigger automations
- Configure scheduled queries (configuration as code)
- Everything is available via API
- Dispatch logs to logging destinations (S3, Elastic, Splunk, Snowflake)
- Bonus: ChromeOS
- Open core (MIT & Enterprise license)



Crowdstrike Falcon - Health Check - Running Process?

Check running processes to verify the Falcon sensor is running

Query

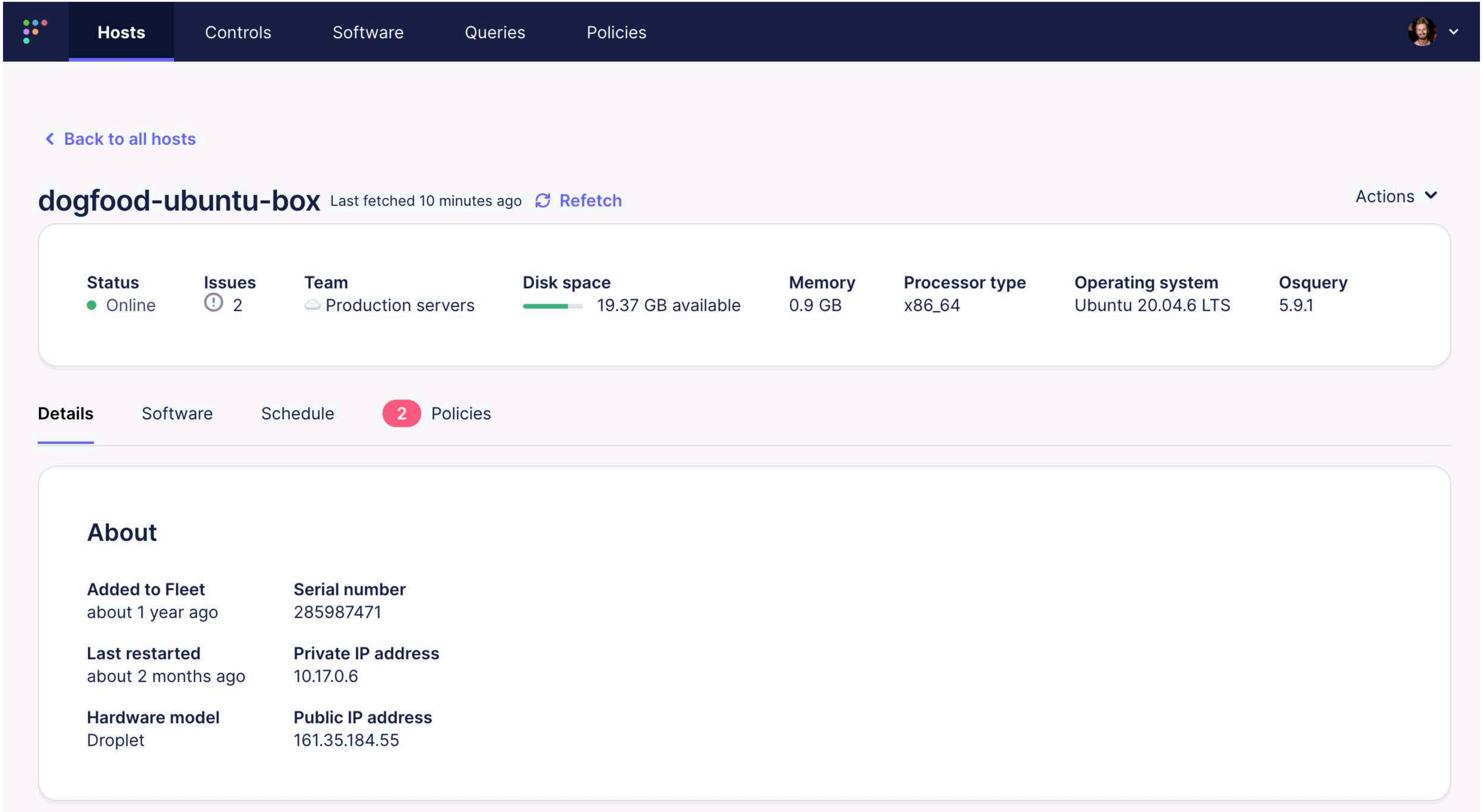
```sql
SELECT * FROM processes WHERE name like ”falcon-sensor”;

```

Compatible with: ✓ Mac ✓ Windows ✓ Linux

□ Observers can run

Users with the Observer role will be able to run this query on hosts where they have access.



dogfood-ubuntu-box Last fetched 10 minutes ago

Status	Issues	Team	Disk space	Memory	Processor type	Operating system	Osquery
● Online	2	Production servers	19.37 GB available	0.9 GB	x86_64	Ubuntu 20.04.6 LTS	5.9.1

About

Added to Fleet
about 1 year ago

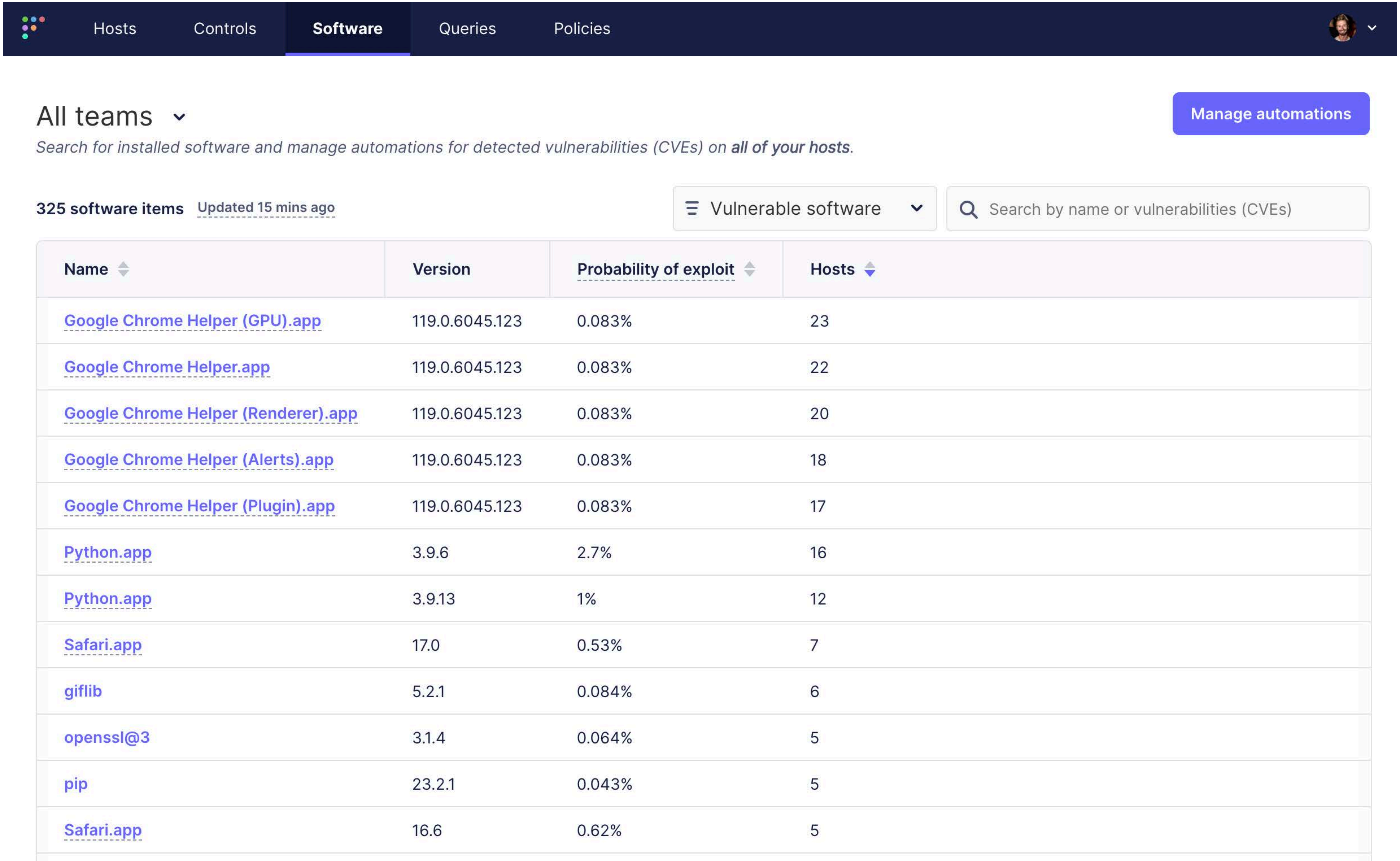
Serial number
285987471

Last restarted
about 2 months ago

Private IP address
10.17.0.6

Hardware model
Droplet

Public IP address
161.35.184.55

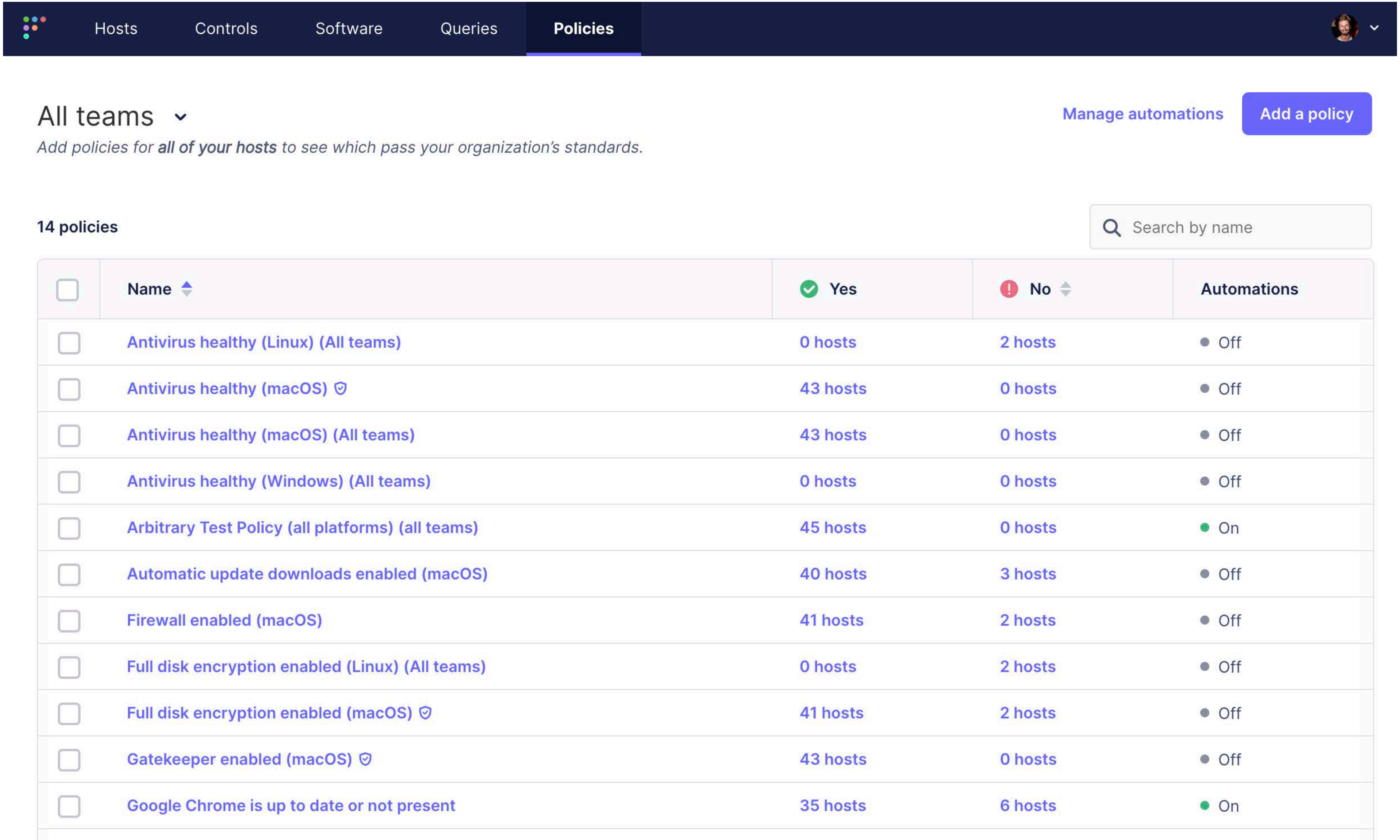


All teams

Search for installed software and manage automations for detected vulnerabilities (CVEs) on ***all of your hosts****.*

325 software items Updated 15 mins ago

Name	Version	Probability of exploit	Hosts
Google Chrome Helper (GPU).app	119.0.6045.123	0.083%	23
Google Chrome Helper.app	119.0.6045.123	0.083%	22
Google Chrome Helper (Renderer).app	119.0.6045.123	0.083%	20
Google Chrome Helper (Alerts).app	119.0.6045.123	0.083%	18
Google Chrome Helper (Plugin).app	119.0.6045.123	0.083%	17
Python.app	3.9.6	2.7%	16
Python.app	3.9.13	1%	12
Safari.app	17.0	0.53%	7
giflib	5.2.1	0.084%	6
openssl@3	3.1.4	0.064%	5
pip	23.2.1	0.043%	5
Safari.app	16.6	0.62%	5

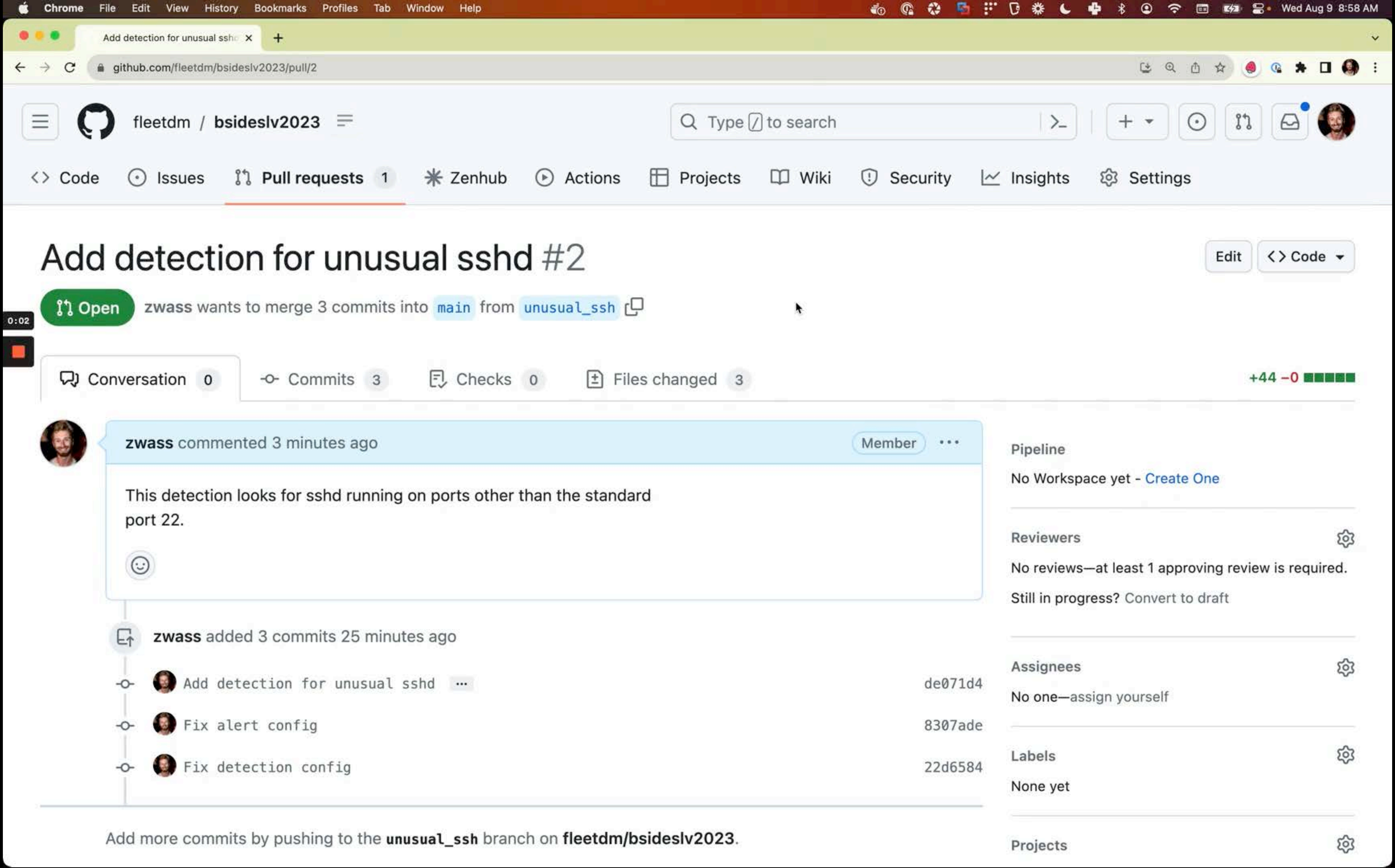


All teams

*Add policies for **all of your hosts** to see which pass your organization’s standards.*

14 policies

□	Name	✓ Yes	! No	Automations
□	Antivirus healthy (Linux) (All teams)	0 hosts	2 hosts	● Off
□	Antivirus healthy (macOS) 🛡	43 hosts	0 hosts	● Off
□	Antivirus healthy (macOS) (All teams)	43 hosts	0 hosts	● Off
□	Antivirus healthy (Windows) (All teams)	0 hosts	0 hosts	● Off
□	Arbitrary Test Policy (all platforms) (all teams)	45 hosts	0 hosts	● On
□	Automatic update downloads enabled (macOS)	40 hosts	3 hosts	● Off
□	Firewall enabled (macOS)	41 hosts	2 hosts	● Off
□	Full disk encryption enabled (Linux) (All teams)	0 hosts	2 hosts	● Off
□	Full disk encryption enabled (macOS) 🛡	41 hosts	2 hosts	● Off
□	Gatekeeper enabled (macOS) 🛡	43 hosts	0 hosts	● Off
□	Google Chrome is up to date or not present	35 hosts	6 hosts	● On



Add detection for unusual sshd #2

Open zwass wants to merge 3 commits into `main` from `unusual_ssh`

zwass commented 3 minutes ago

This detection looks for sshd running on ports other than the standard port 22.

zwass added 3 commits 25 minutes ago

`Add detection for unusual sshd`	de071d4
`Fix alert config`	8307ade
`Fix detection config`	22d6584

Add more commits by pushing to the **`unusual_ssh`** branch on **fleetdm/bsideslv2023**.

Pipeline

No Workspace yet - Create One

Reviewers

No reviews—at least 1 approving review is required.

Still in progress? Convert to draft

Assignees

No one—assign yourself

Labels

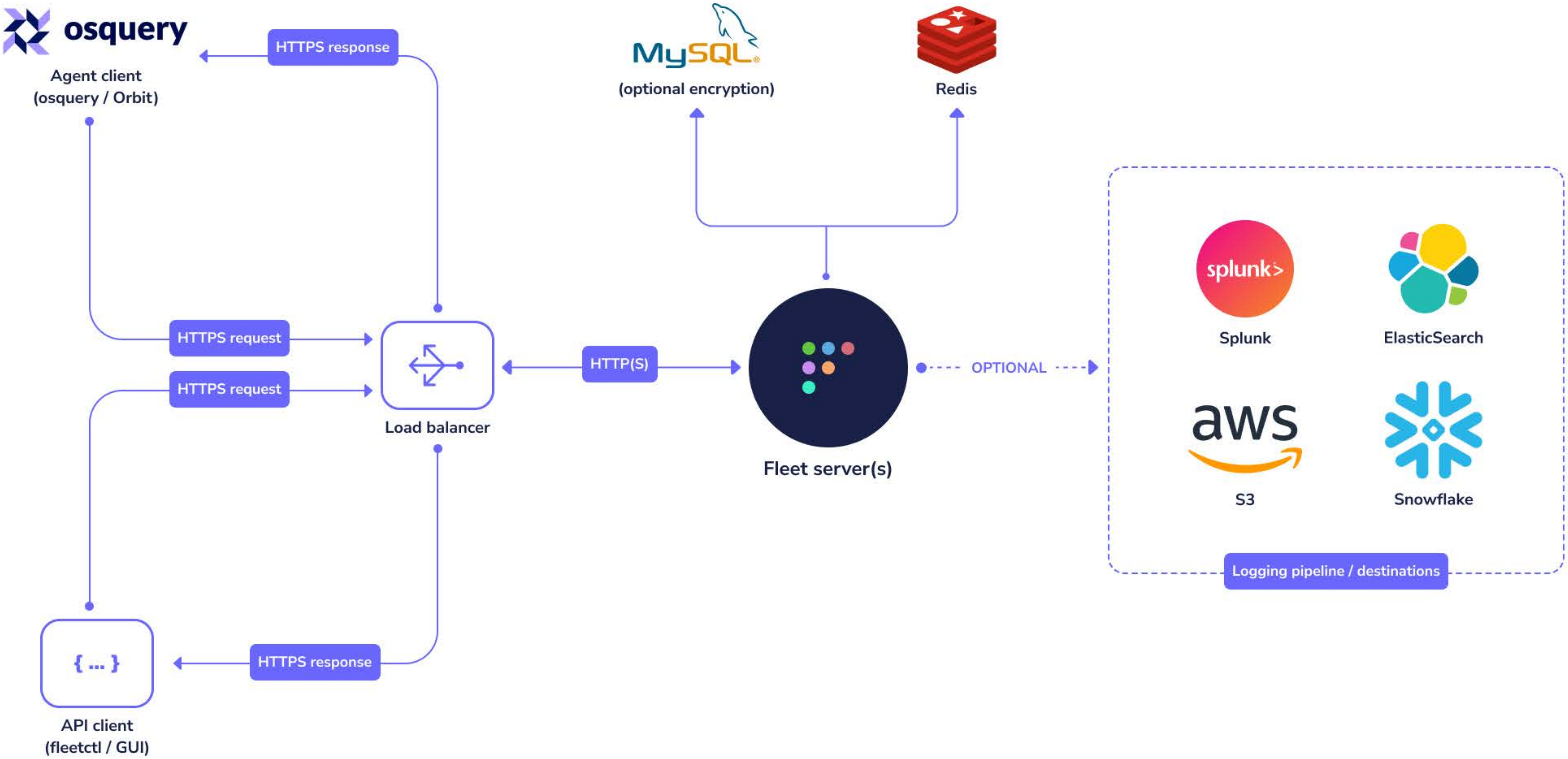
None yet

Projects

Deployment

Fleet

- Deploy in AWS via provided Terraform
  - Deploy manually to any suitable infrastructure
- Expose to the public internet (or not)
- Install `fleetctl` command-line tool for management & packaging
- See https://fleetdm.com/docs/deploy/introduction


osquery
Agent client
(osquery / Orbit)
HTTPS response
MySQL
(optional encryption)
Redis
HTTPS request
HTTPS request
Load balancer
HTTP(S)
Fleet server(s)
OPTIONAL
splunk>
Splunk
ElasticSearch
aws
S3
Snowflake
Logging pipeline / destinations
{ ... }
HTTPS response
API client
(fleetctl / GUI)

Deployment

Osquery

- Generate installation packages via `fleetctl`
  - Windows `.msi`
  - MacOS `.pkg`
  - Debian/Ubuntu `.deb`
  - CentOS/RHEL `.rpm`
- Install packages via standard management workflows (eg. Chef, MDM, etc.)
  - Or bake it into VM/container images
- See https://fleetdm.com/docs/using-fleet/enroll-hosts

Thank you!

zach@fleetdm.com

@thezachw

@zwass

linkedin.com/in/zacharywasserman

fleet