MALICIOUS COMPLIANCE

@IanColdwater
@bradgeesaman
@mauilion
@raesene

Reflections on Trusting Container Scanners

WHO ARE WE?

@IanColdwater

@mauilion

Ian Coldwater likes breaking rules, breaking computers, and breaking down the walls that divide us.

Duffie Cooley really likes to share knowledge and learn new things!

Brad Geesaman breaks cloud and container security *–for educational purposes only*.

Rory McCune knows some things and writes blogs about them.

@bradgeesaman

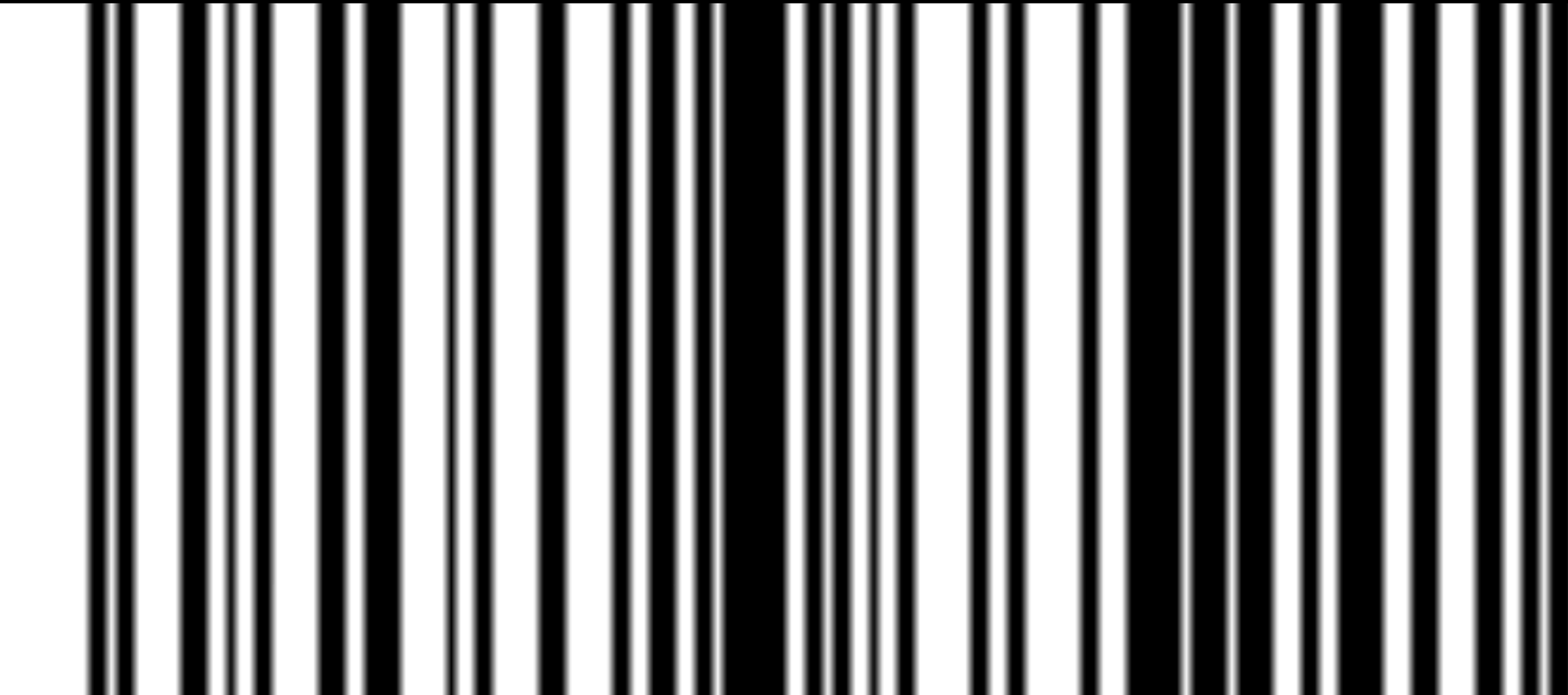
@raesene

SIG-GAGGELEN


"K" LINE
NYK LOGISTICS
& MEGACARRIER
ONE
TRITON
MAXGROSS
TARE WT.
PAYLOAD
CU. CAP.
CAUTION
9.6
HIGH

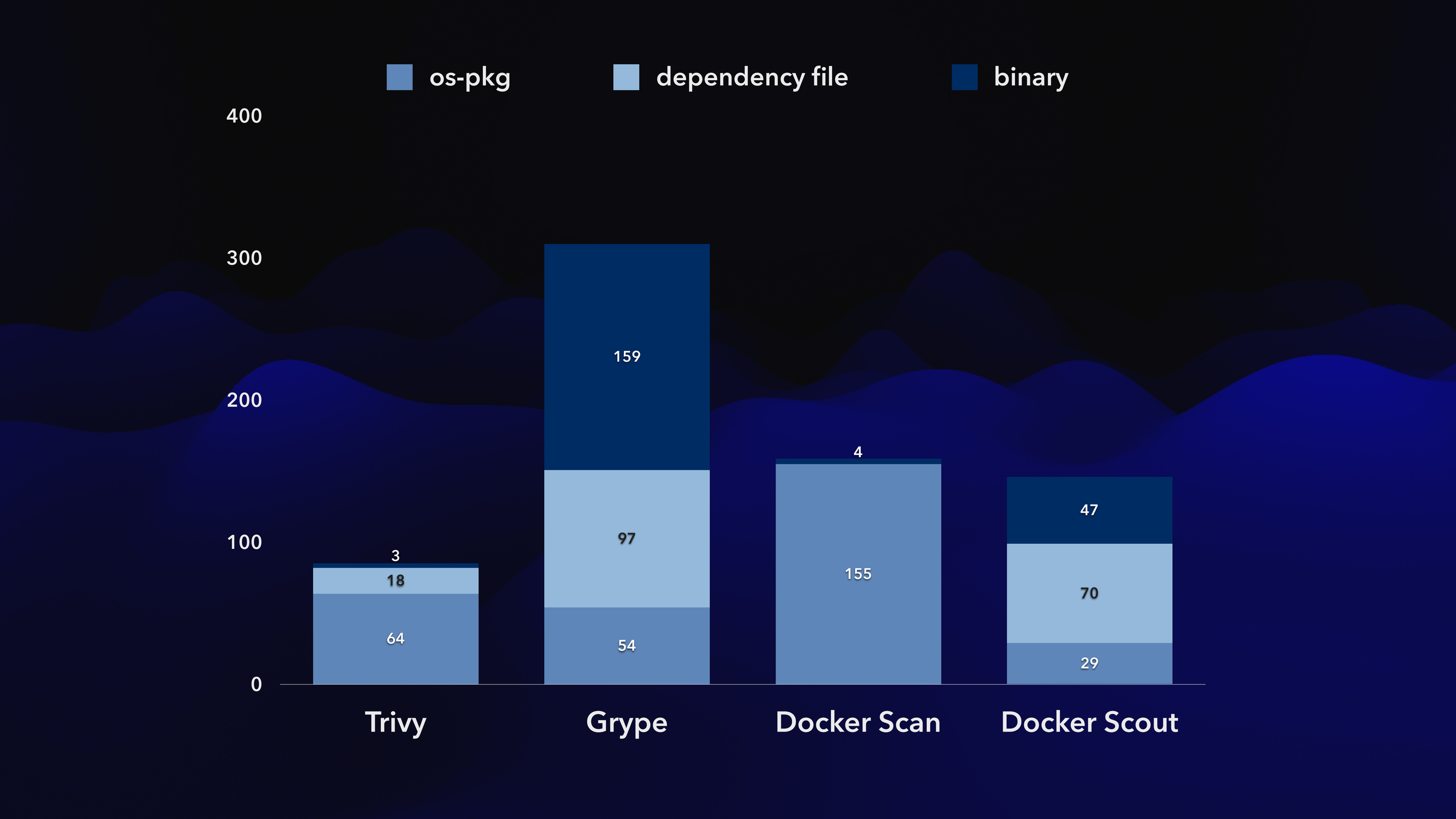
SCAN ALL THE THINGS!

SCAN ALL THE THINGS?



DEMO - ALL YOUR BASELINE

https://k8s.rip/demo-base


os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout

WHAT DO CONTAINER SCANNERS LOOK FOR?

- OS detection
- OS package detection
- dependency files
- binary metadata

OS DETECTION

- /etc/os-release
- /etc/lsb-release
- /etc/alpine-release

PACKAGE DETECTION

Alpine

- /etc/apk, /lib/apk

Ubuntu/Debian

- /var/cache/apt/archives
- /var/lib/apt/lists/*

Redhat

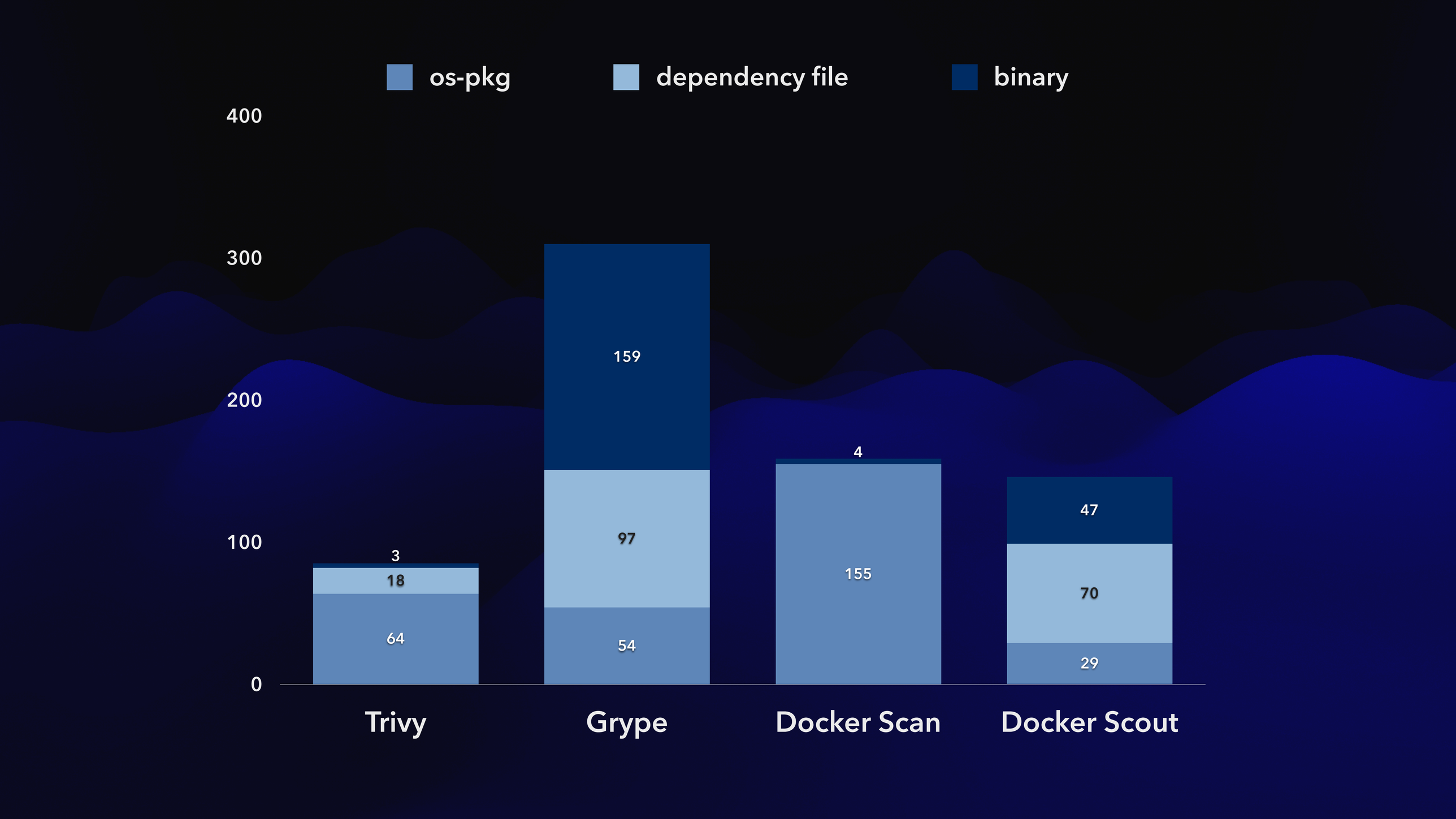
- /var/cache/yum

DEPENDENCY FILES

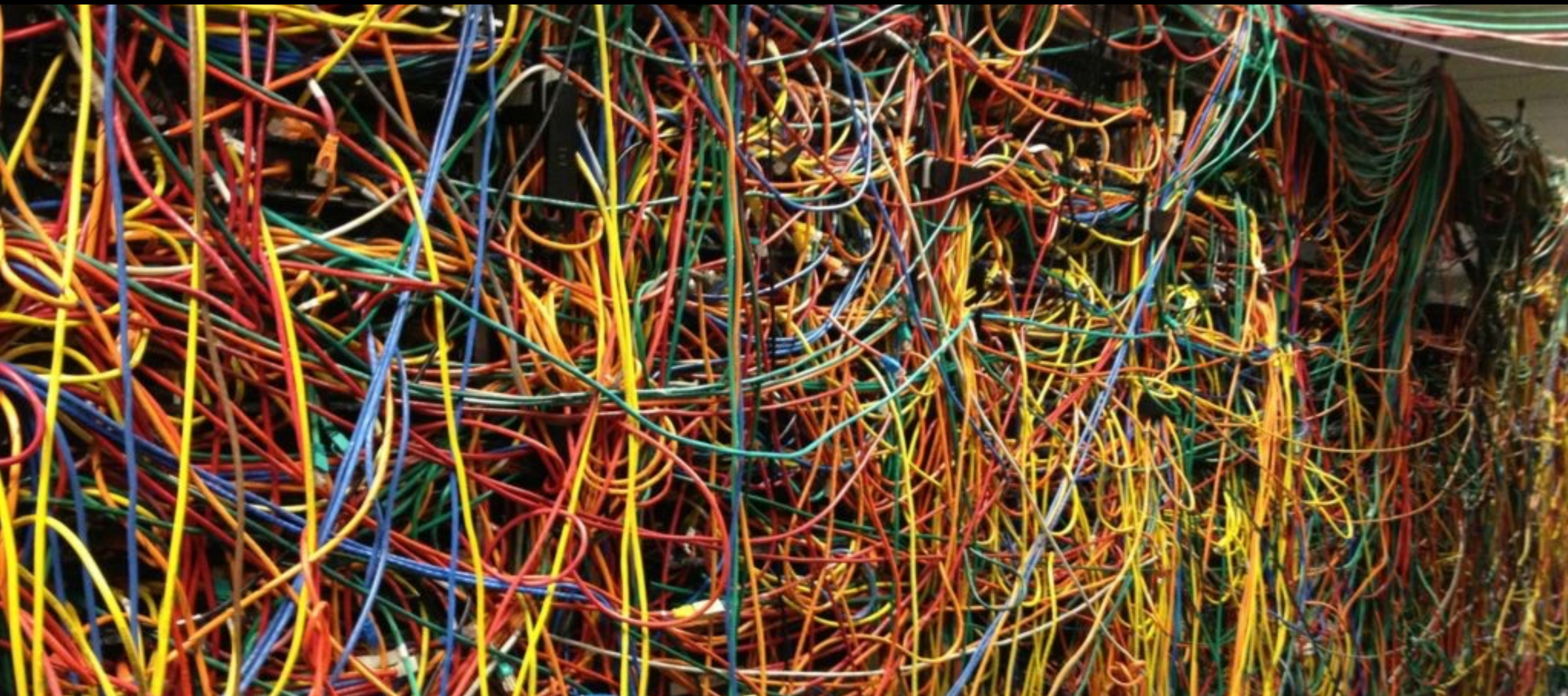
- package.json
- requirements.txt
- gemfile.lock
- Cargo.lock*

BINARY METADATA

- go version -m kubectl
- cargo audit rust-binary


os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout

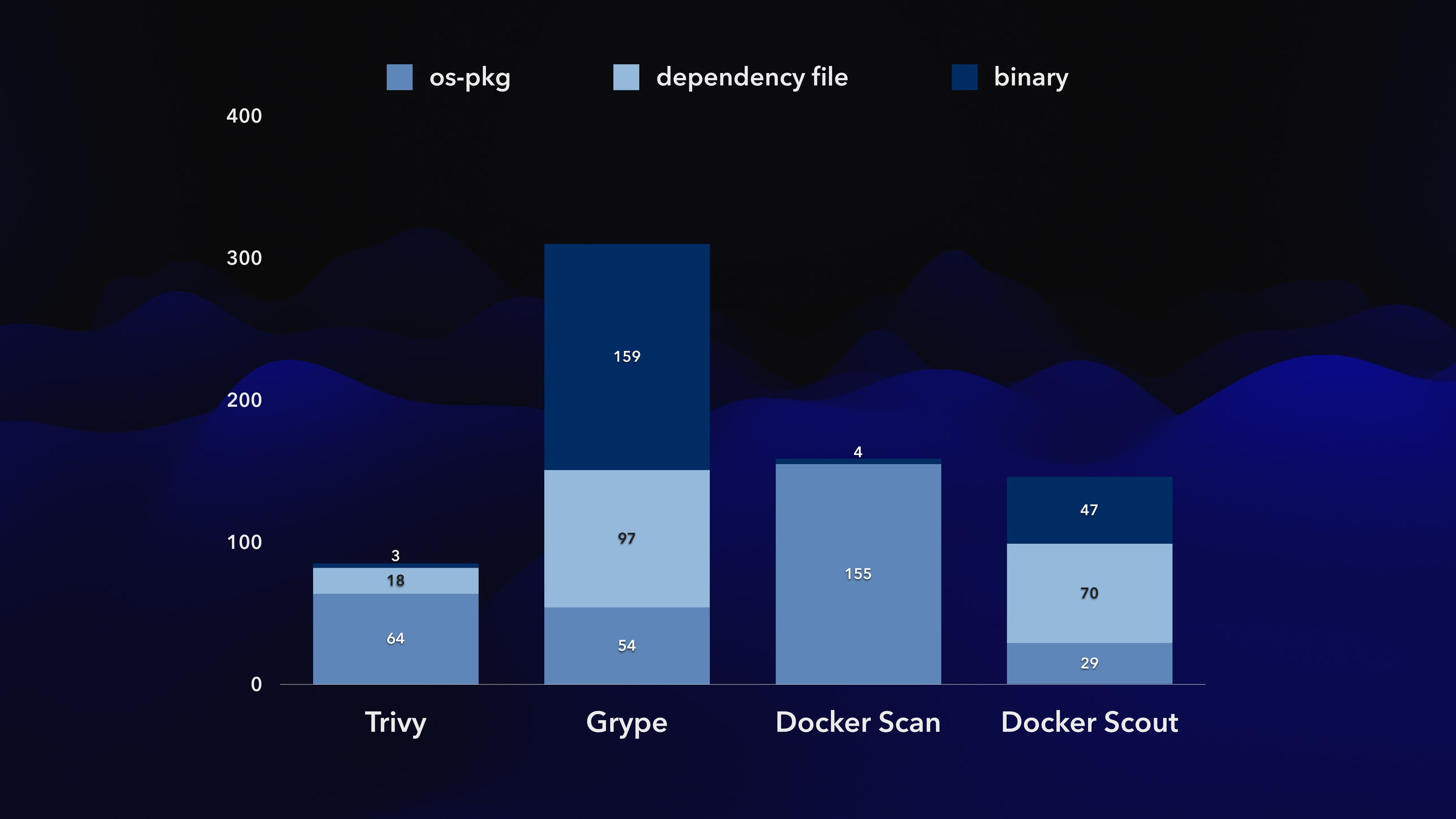
FIXING THINGS IS HARD

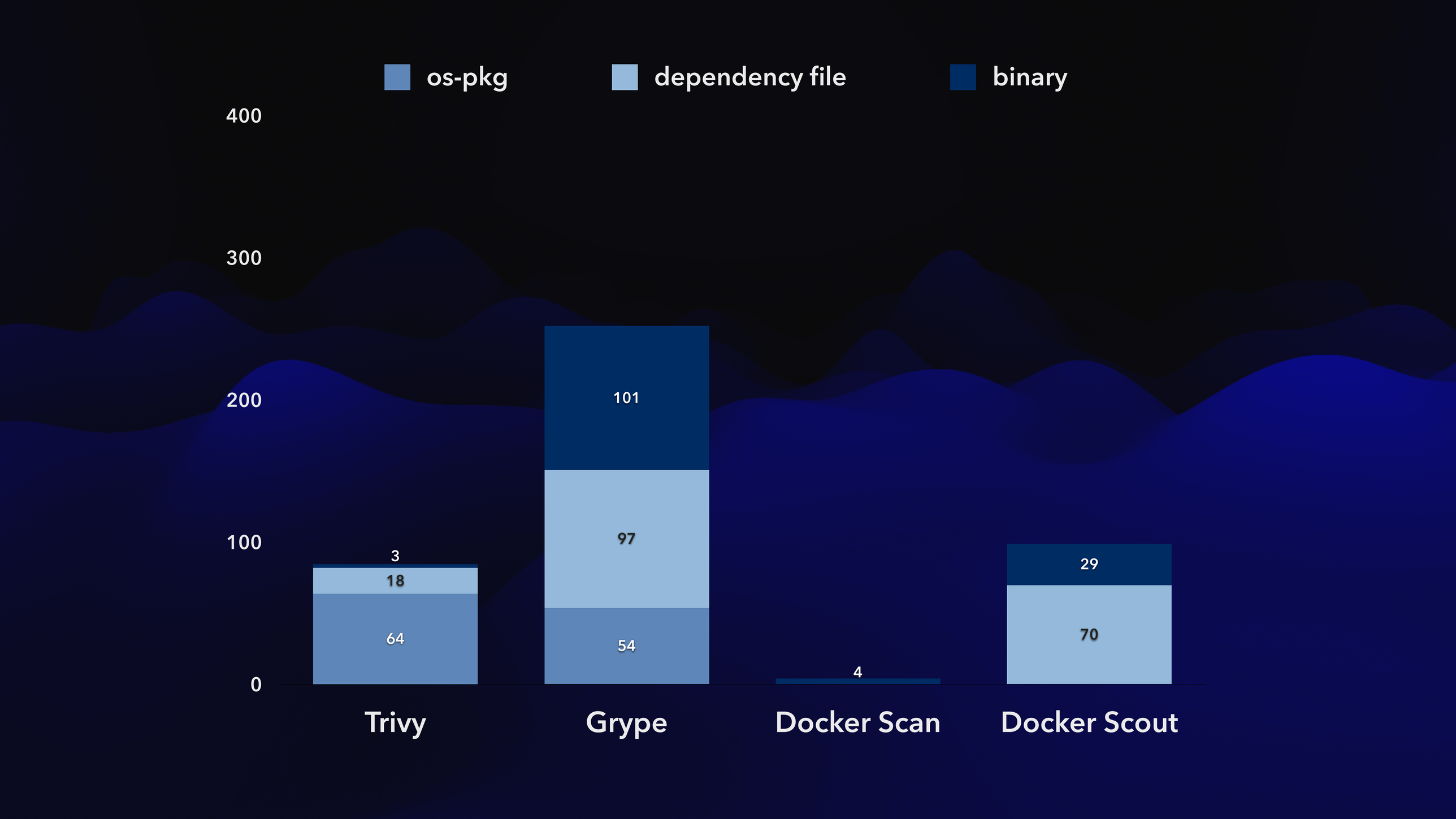


MALICIOUS COMPLIANCE

DEMO - OS RELEASING

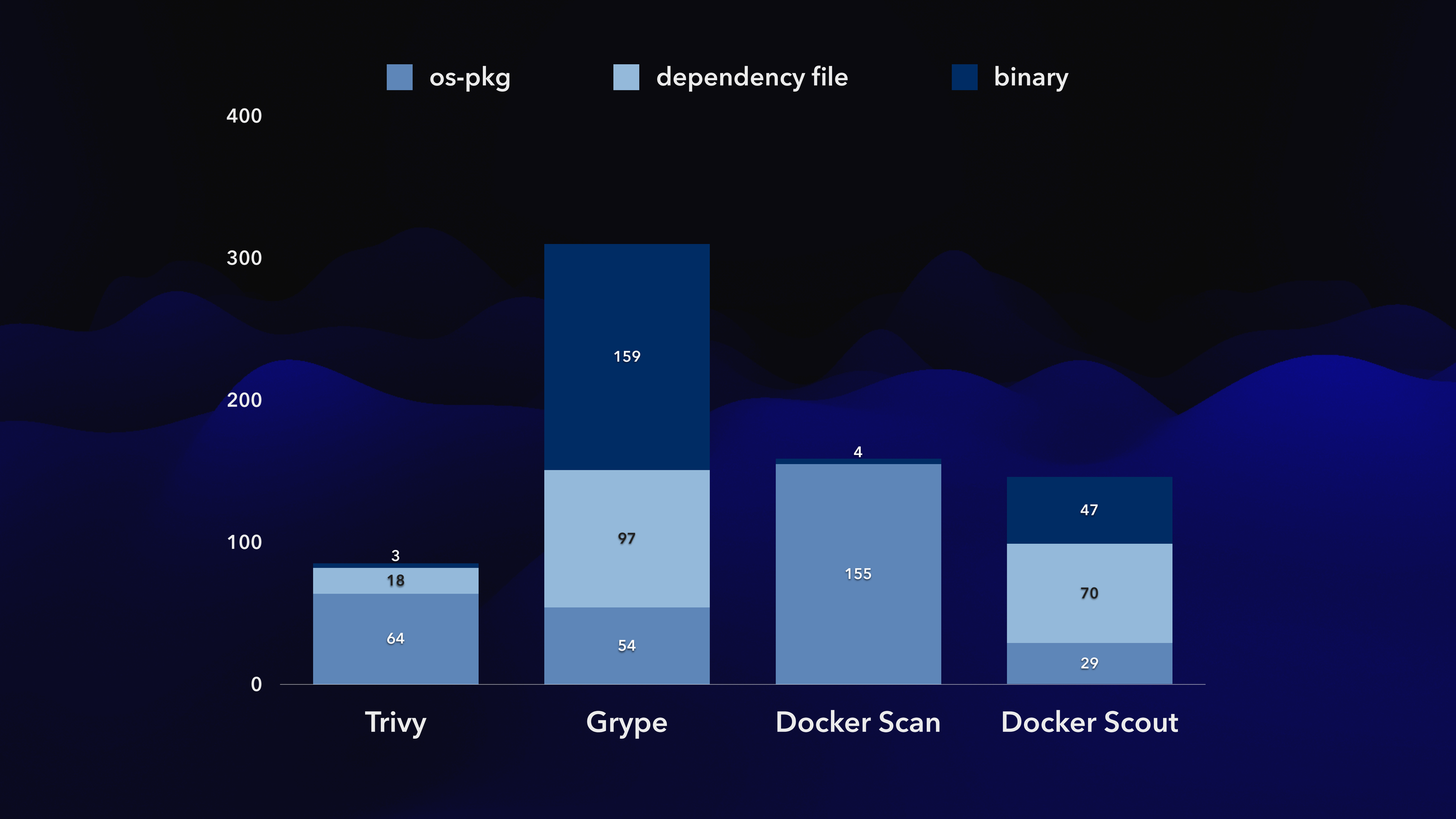
https://k8s.rip/demo-os

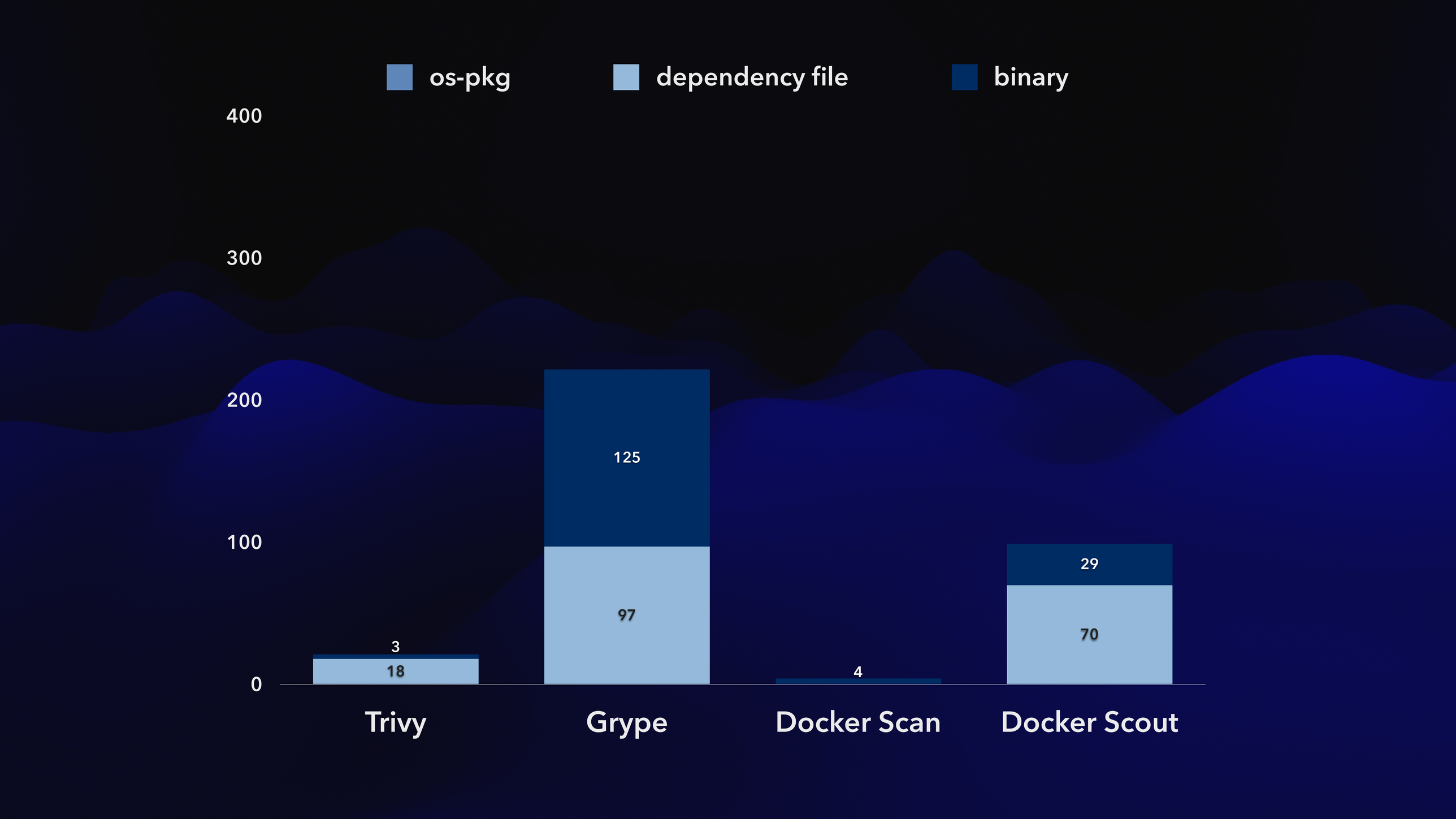

os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout


os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
101
97
54
4
29
70
Trivy
Grype
Docker Scan
Docker Scout

DEMO - PACKAGE METADATA

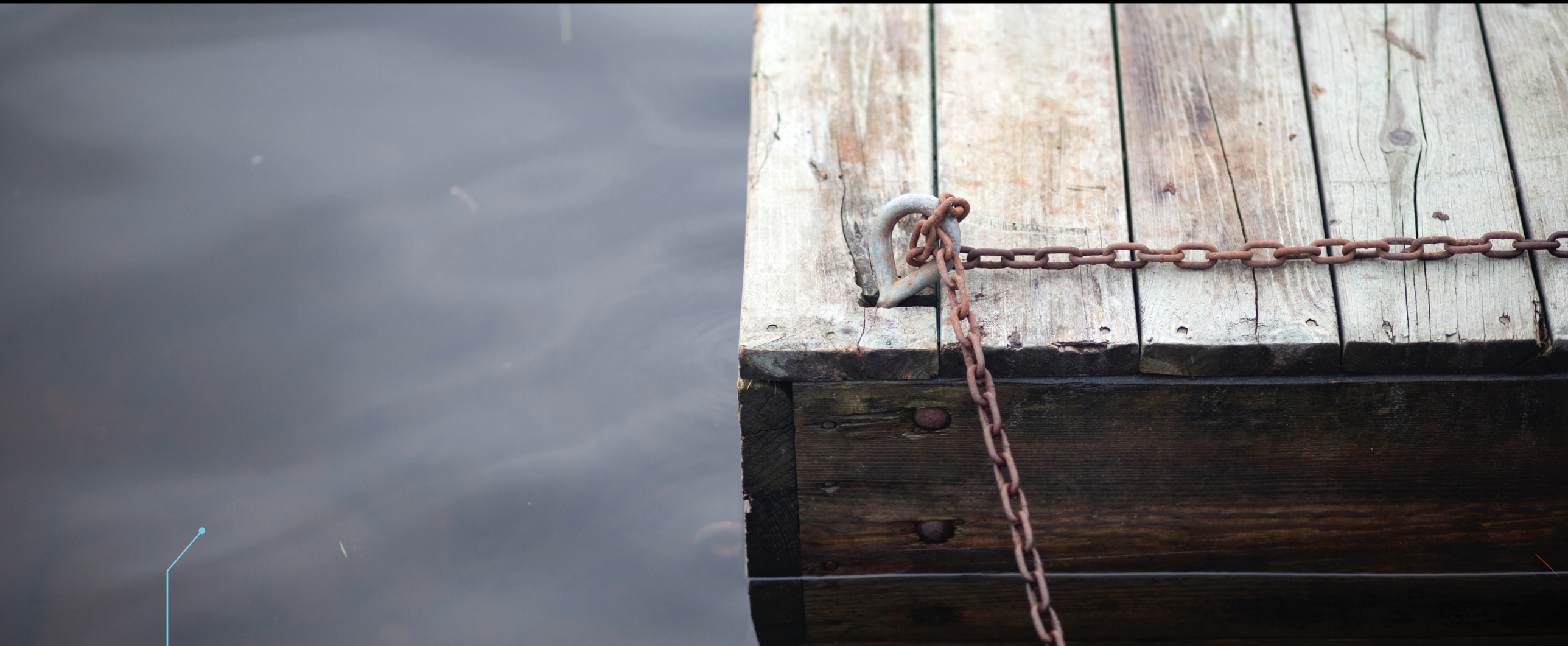
https://k8s.rip/demo-pkg

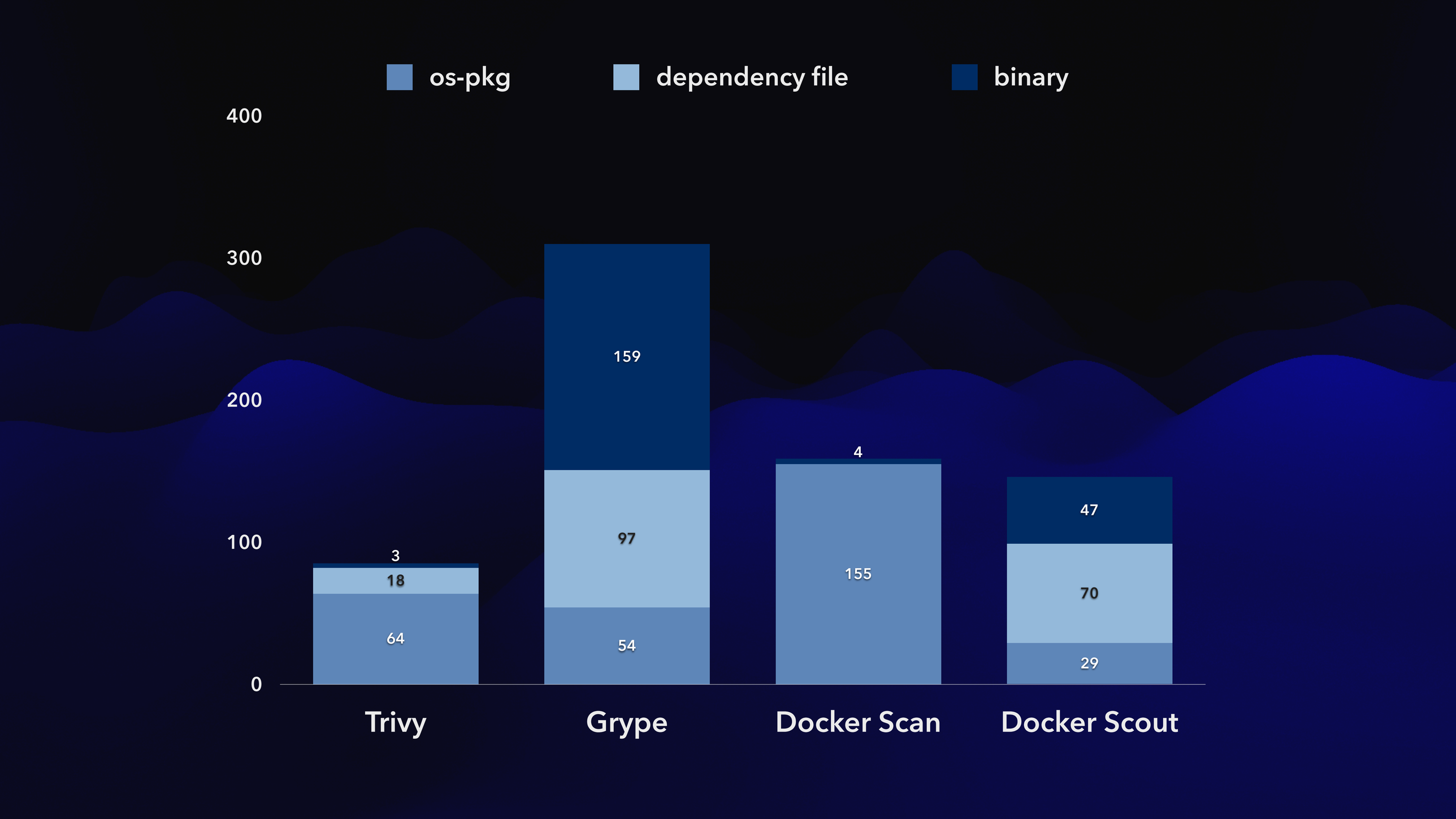

os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout

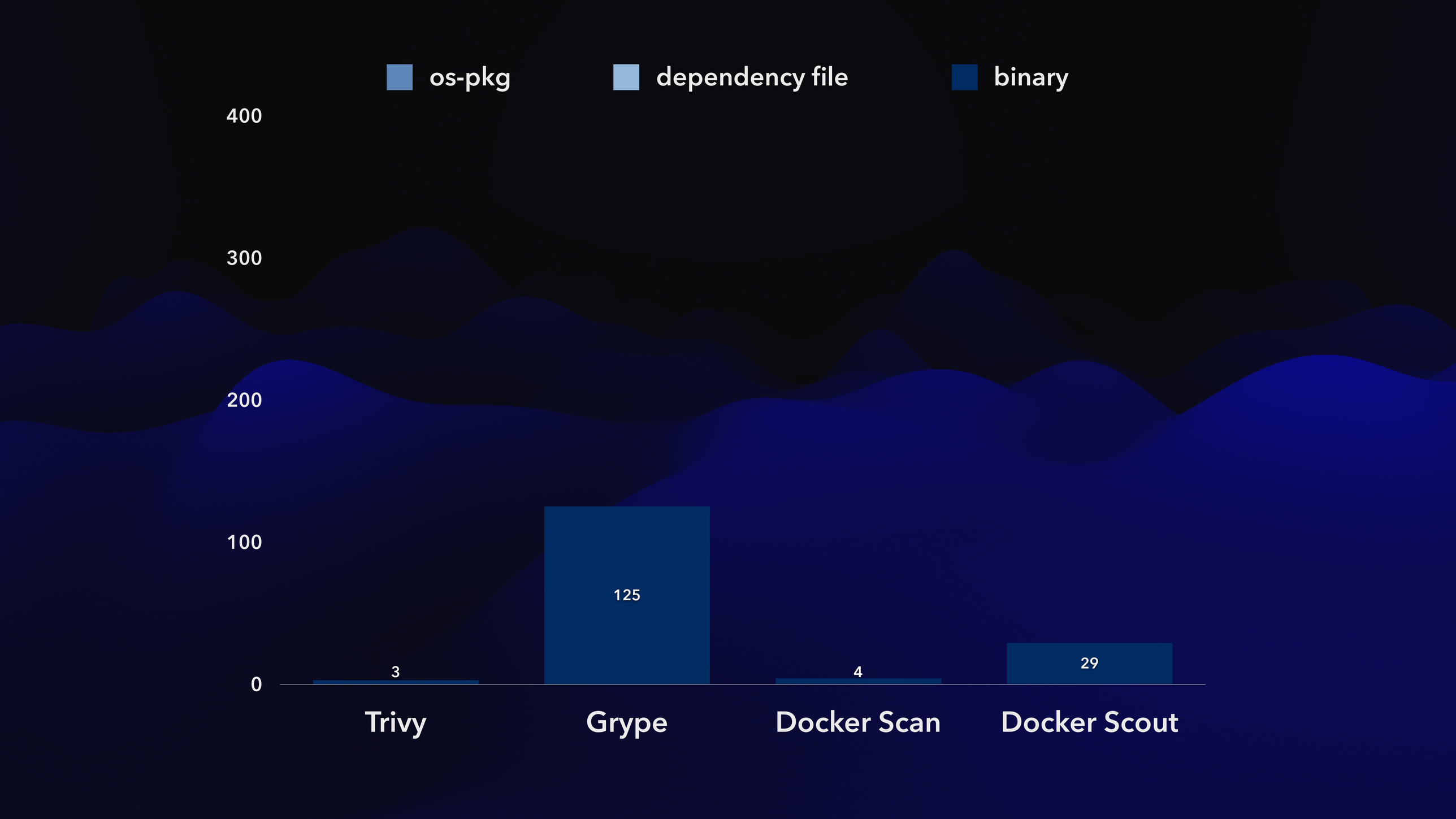

os-pkg
dependency file
binary
400
300
200
100
0
3
18
125
97
4
29
70
Trivy
Grype
Docker Scan
Docker Scout

DEMO - SYMLINKS

https://k8s.rip/demo-symlink

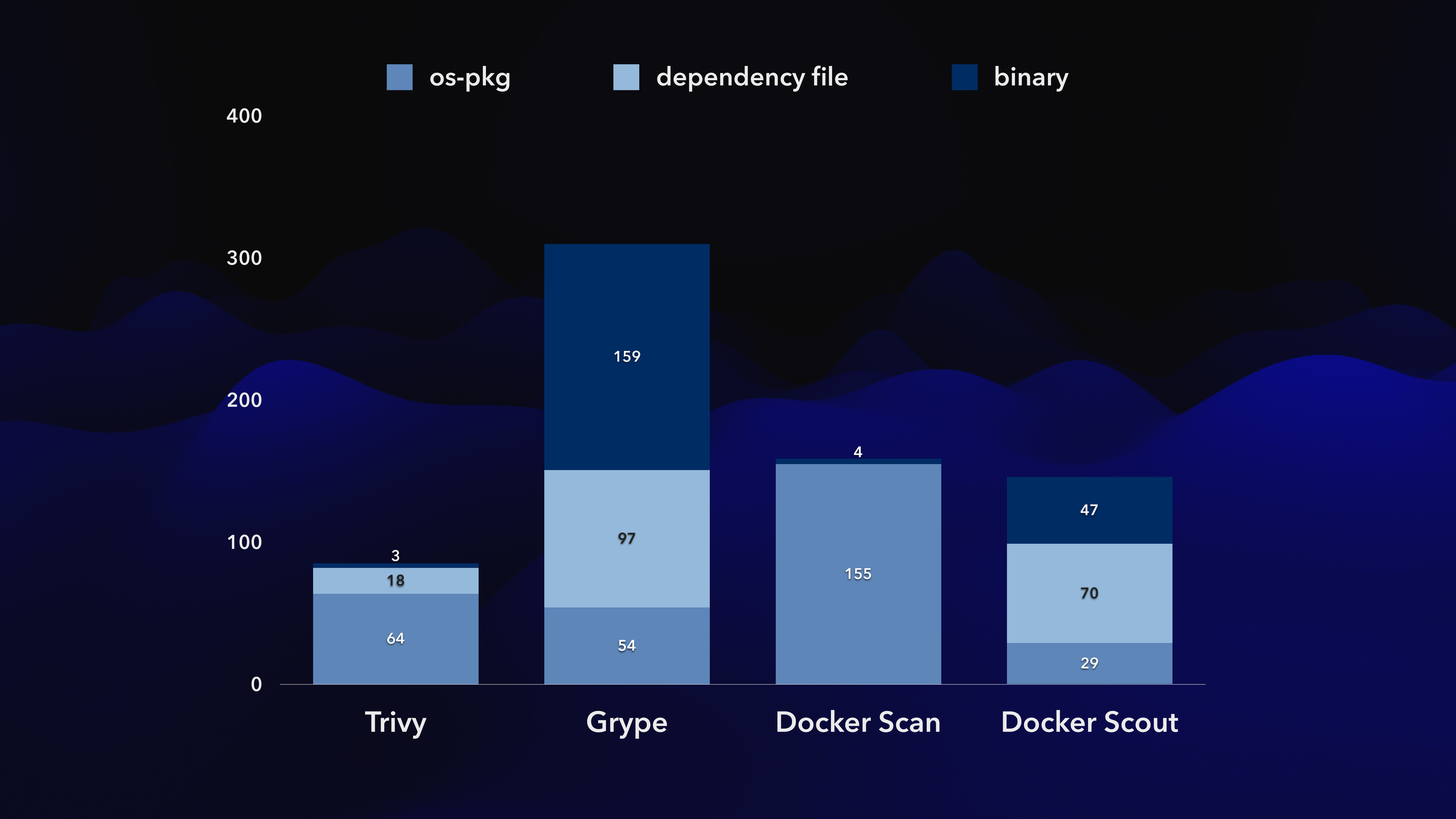


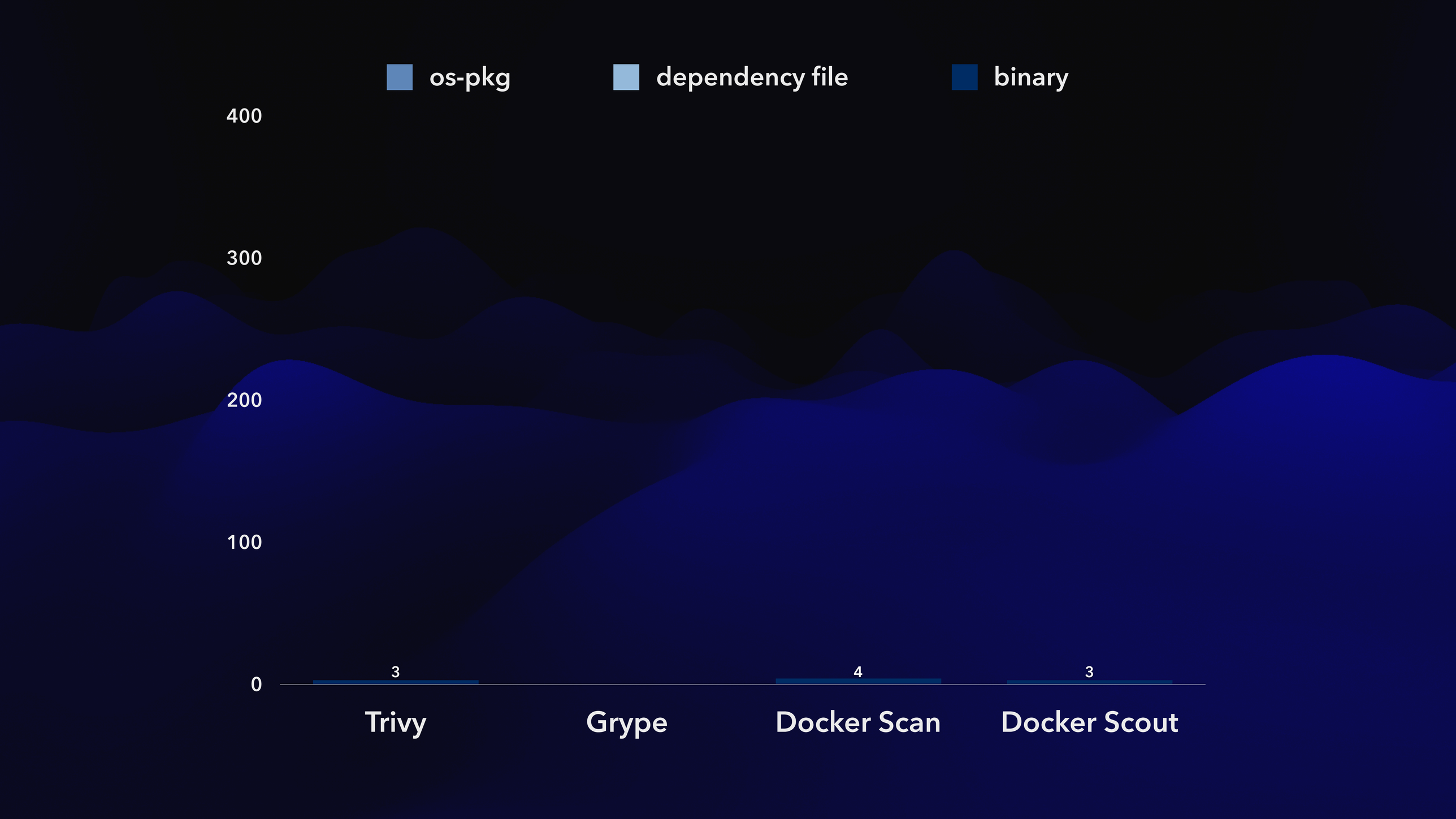

os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout


os-pkg
dependency file
binary
400
300
200
100
0
3
125
4
29
Trivy
Grype
Docker Scan
Docker Scout

DEMO - BINARY PACKING

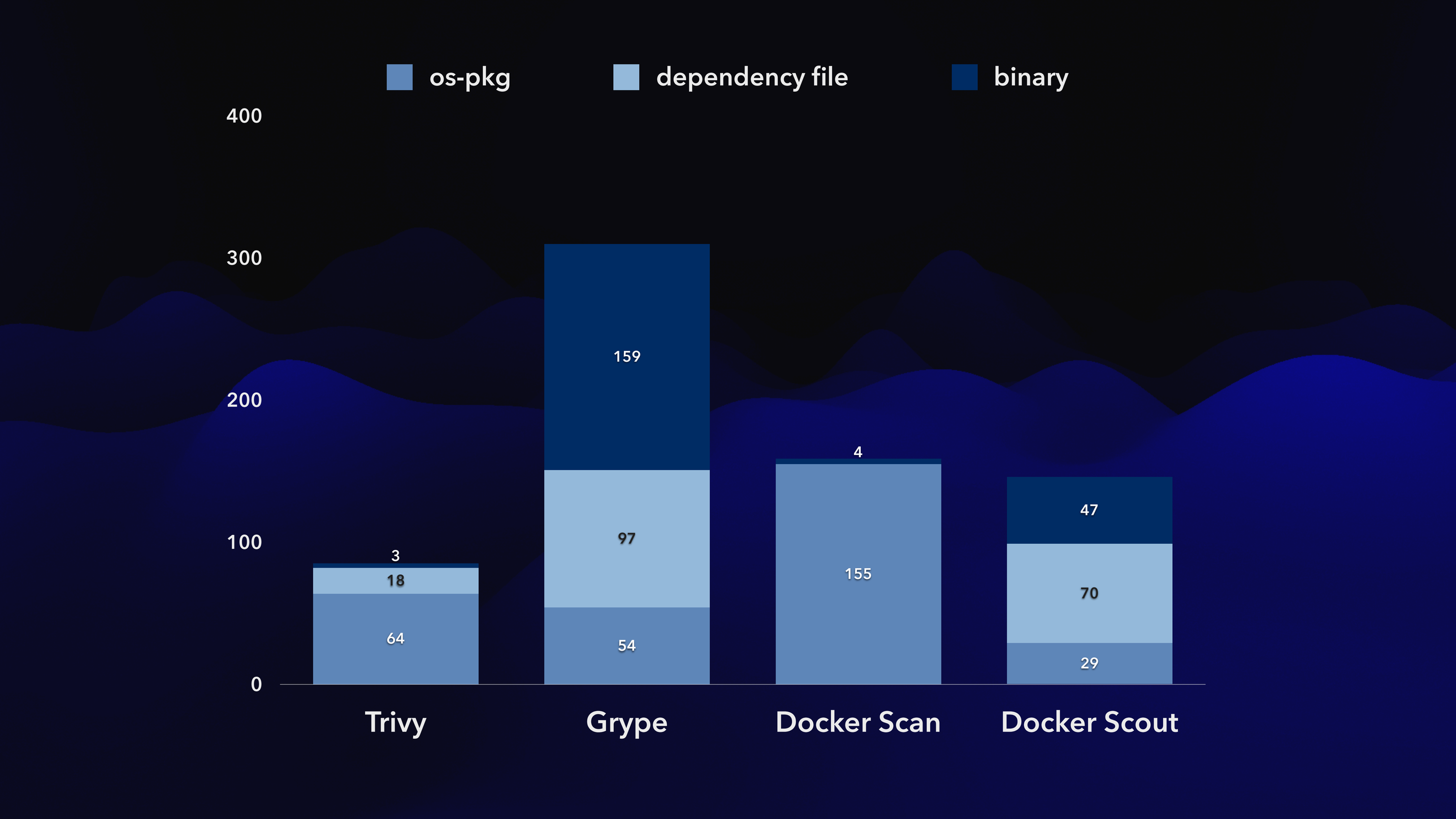
https://k8s.rip/demo-pack

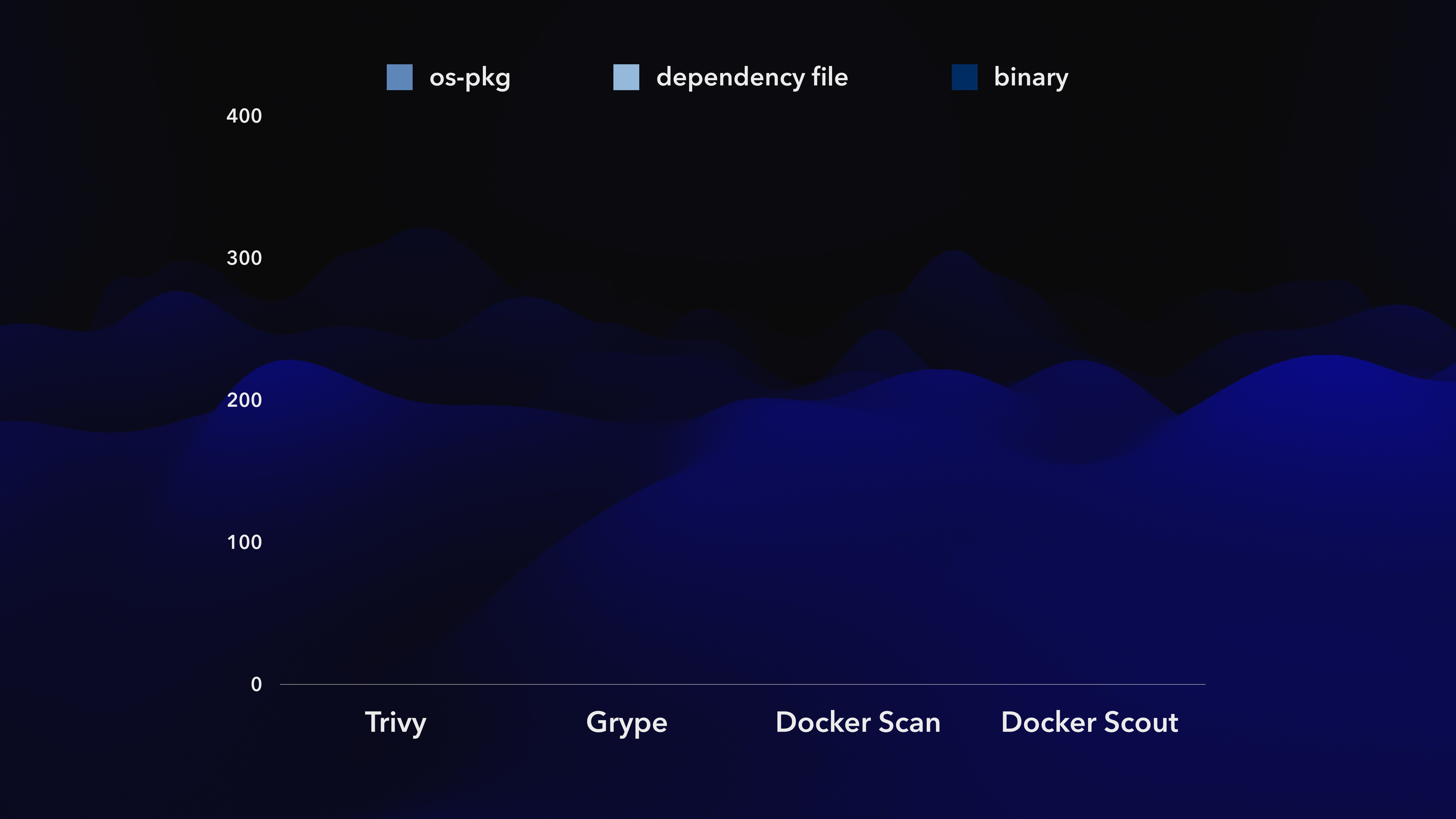

os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout


os-pkg
dependency file
binary
400
300
200
100
0
3
4
3
Trivy
Grype
Docker Scan
Docker Scout

DEMO - ZERO

https://k8s.rip/demo-zero


os-pkg
dependency file
binary
400
300
200
100
0
3
18
64
159
97
54
4
155
47
70
29
Trivy
Grype
Docker Scan
Docker Scout


os-pkg
dependency file
binary
400
300
200
100
0
Trivy
Grype
Docker Scan
Docker Scout

DEMO 6 - S BOMBS

https://k8s.rip/demo-sbom

ALL CONJECTURES ARE BROKEN

WHAT CAN WE LEARN FROM ALL THIS?


SWANSON

WHAT CAN YOU DO?

72C9E7

REFERENCES

- GitHub Repo for this talk - https://k8s.rip/malicious-compliance
- Original base image - https://k8s.rip/mc-base
- Exploiting a Slightly Peculiar Volume Configuration with SIG-Honk - https://k8s.rip/spvc
- Reflections on Trusting Trust - https://k8s.rip/trust
- https://github.com/kelseyhightower/nocode - the best way to write secure and reliable applications!