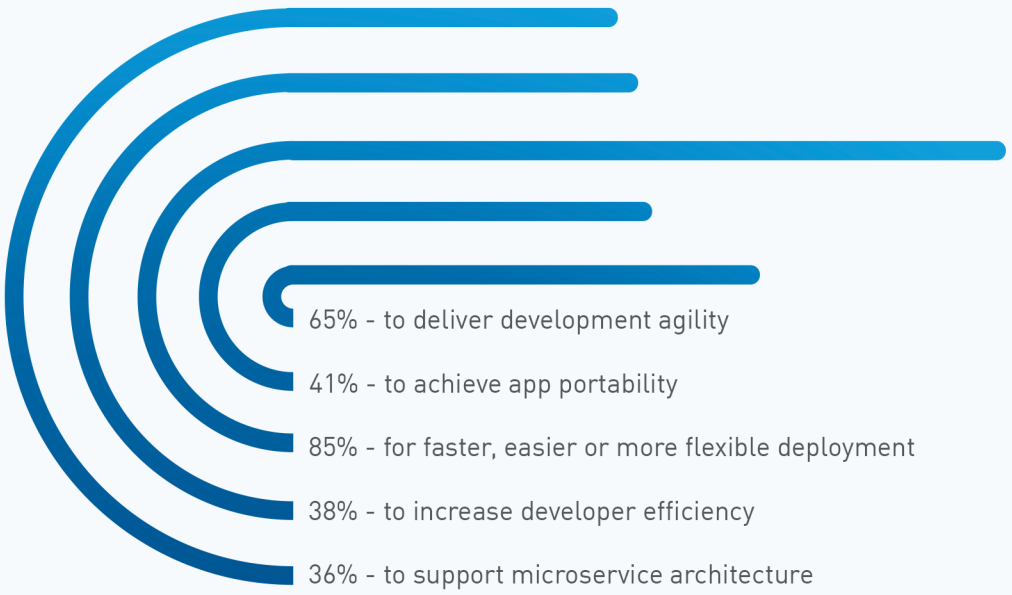
Automated Vulnerability Analysis and Disclosure of Docker Containers in a Distributed Cloud Environment

WHY DOCKER.

Docker is a container platform provider. Docker packages applications with dependencies in a container. It allows to build, ship and run software easily.



Why is everyone using Docker? - kumina (2017)

RISKS.

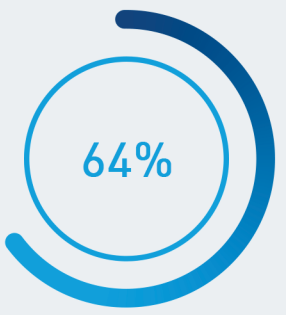
Developers are now responsible for their containers and the dependencies inside. They need to maintain their containers continually.

Using Components with Known Vulnerabilities is very common and listed in the **OWASP TOP 10**.

OWASP (2017)

Over **250 thousand systems** in **150 countries** were affected by the ransomware WannaCry. Only already known vulnerabilities were exploited. It was the most significant ransomware attack in history.

MalwareTech (2017)



64% of **official Docker Images** contain vulnerabilities with High or Medium Priority.

BanyanOps (2015)

VIRITY.

Virity is an open source tool, built for making vulnerabilities of Docker containers visible. It connects existing monitoring tools like Sensu or Elasticsearch with container scanning tools like Clair or Anchore.

01

GATHERING

Virity-Agents automatically gather information of all currently running containers anywhere in the Cloud. This information is saved in a centralised external Data-Store.

02

SCANNING

Virity pulls the stored information and pushes the Docker images to an external Scan Engine. This engine analyses the images and returns all CVEs present in this container.

03

MONITORING

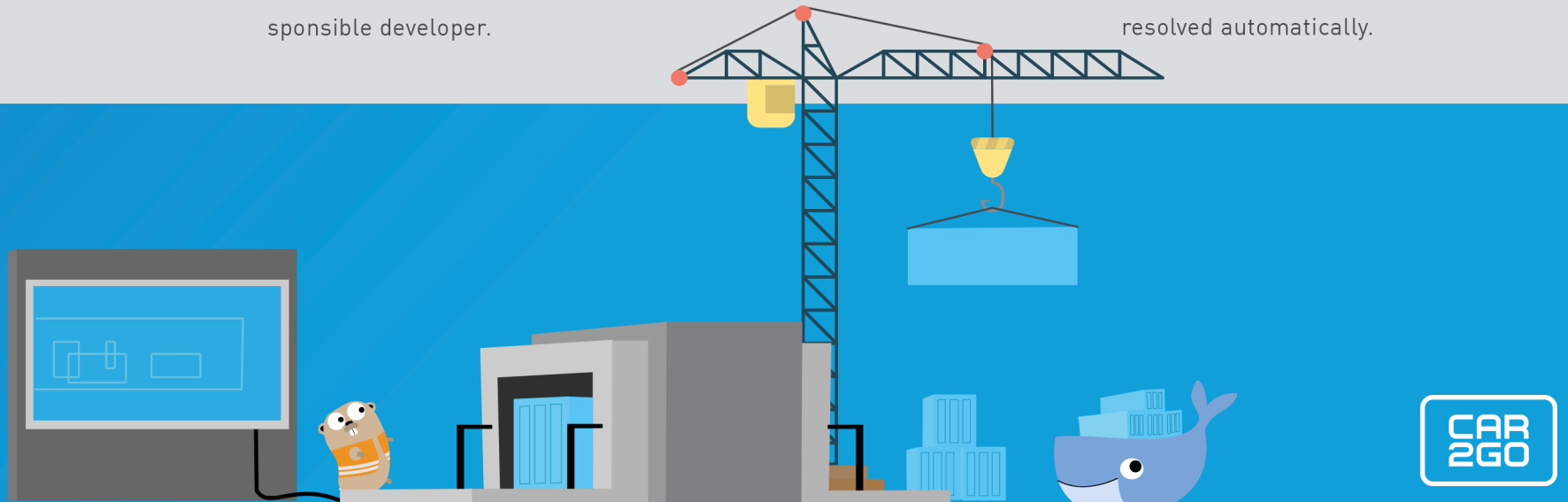
Virity evaluates the scan results and pushes all relevant information to an external monitoring tool. This tool may trigger, e.g. alerts to the responsible developer.

04

TRACKING

Virity enables tracking of vulnerable containers. It creates tickets directly assigned to the responsible developer. Tickets of not running containers are resolved automatically.

HOW IT WORKS.



by Daniel Glinka

CAR 2GO