SECURE360

Securing the open source software supply chain

Presented by:

Josh Bressers

Security Strategist - Red Hat, Inc.

@joshbressers

AKA

Open source won
Now what do we do?

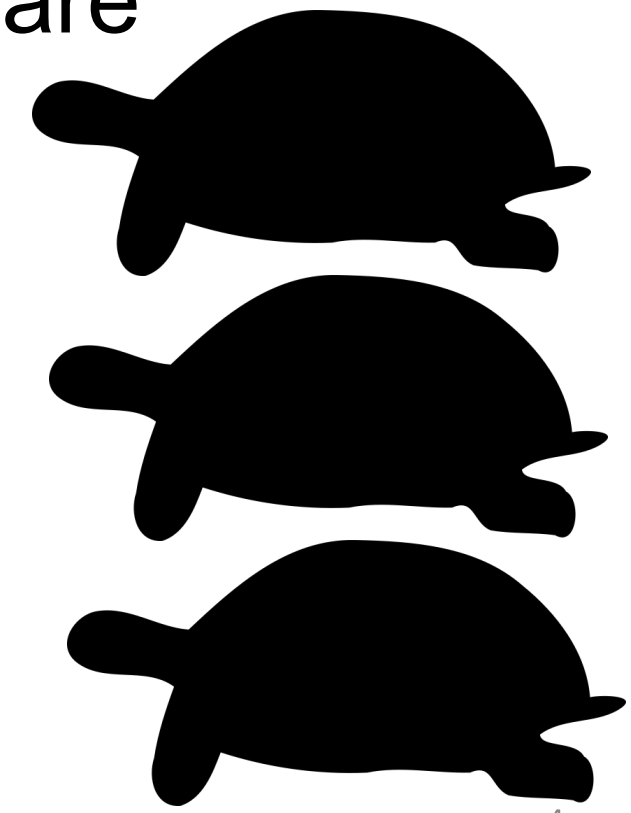
Supply Chain?

Wikipedia says:

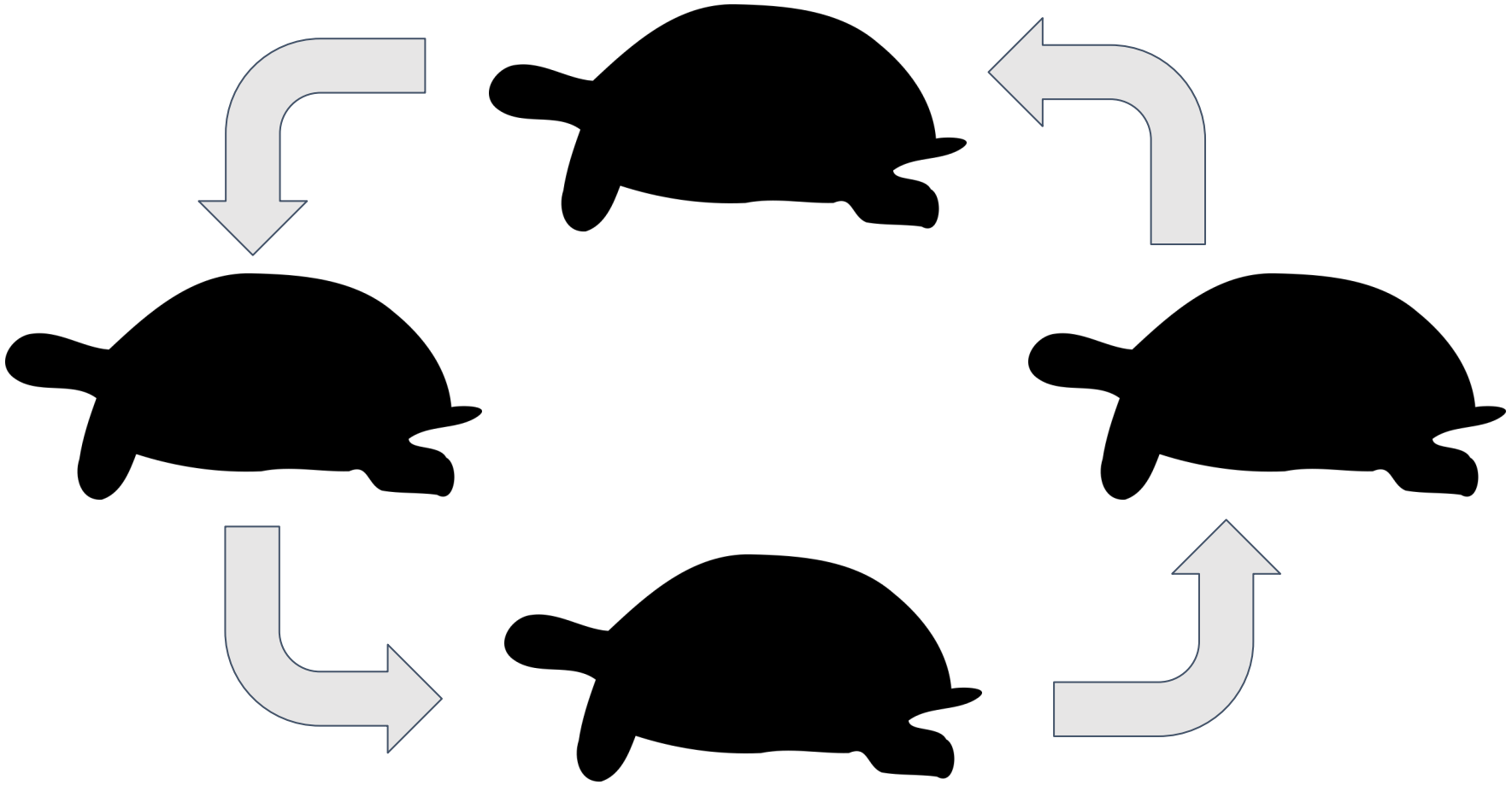
*A **supply chain** is a system of organizations, people, activities, information, and resources involved in moving a product or service from supplier to customer. Supply chain activities involve the transformation of natural resources, raw materials, and components into a finished product that is delivered to the end customer.*

Software Supply Chain?

Your software is build with other software
That software is built with other software
It's turtles all the way down



Software Supply Chain?



SECURE360

Why do we care?

- Security hygiene
- GRC
  - Governance
  - Risk Management
  - Compliance
- It’s a real problem

SECURE360

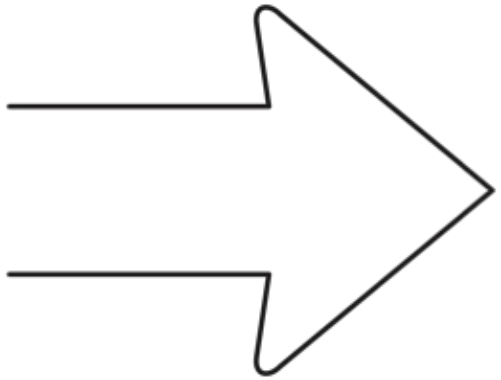
4 Truths

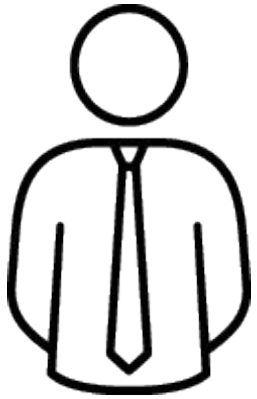
1. Open source won
2. Your organization is full of open source
   a. You may not know this
3. Your developers are using open source
   a. They may not know this
4. We've passed the open source event horizon

If we can’t stop it, we need to secure it

The ***old*** way

Vendor

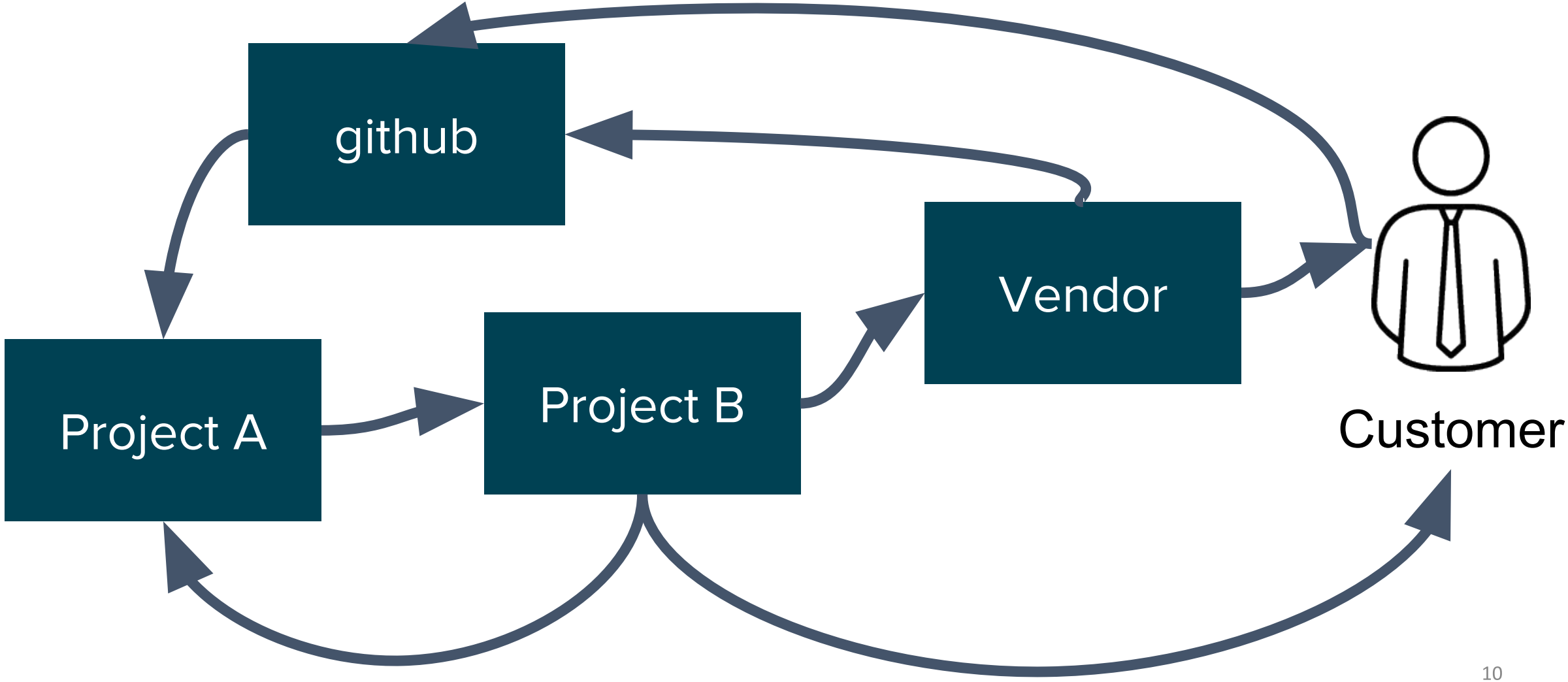




Customer

SECURE360

The *new* way



SECURE360

Before we go on ...

Open source is messy and weird. The only thing more powerful than how scary it can be, is how amazing it is.

This talk is about how awesome open source is and how you can use it, not why you should fear it.

SECURE360

4 Stages of open source

1. Denial
2. Confidence
3. Horror
4. Understanding

SECURE360

Denial

SECURE360

Confidence

SECURE360

Horror

SECURE360

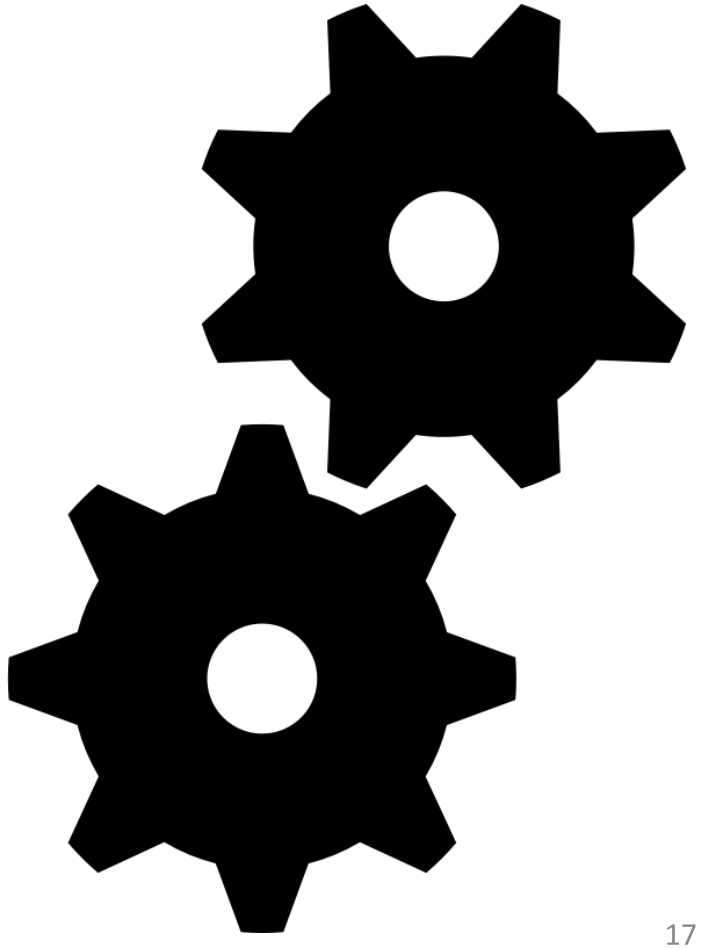
Understanding

SECURE360

How do we understand this?

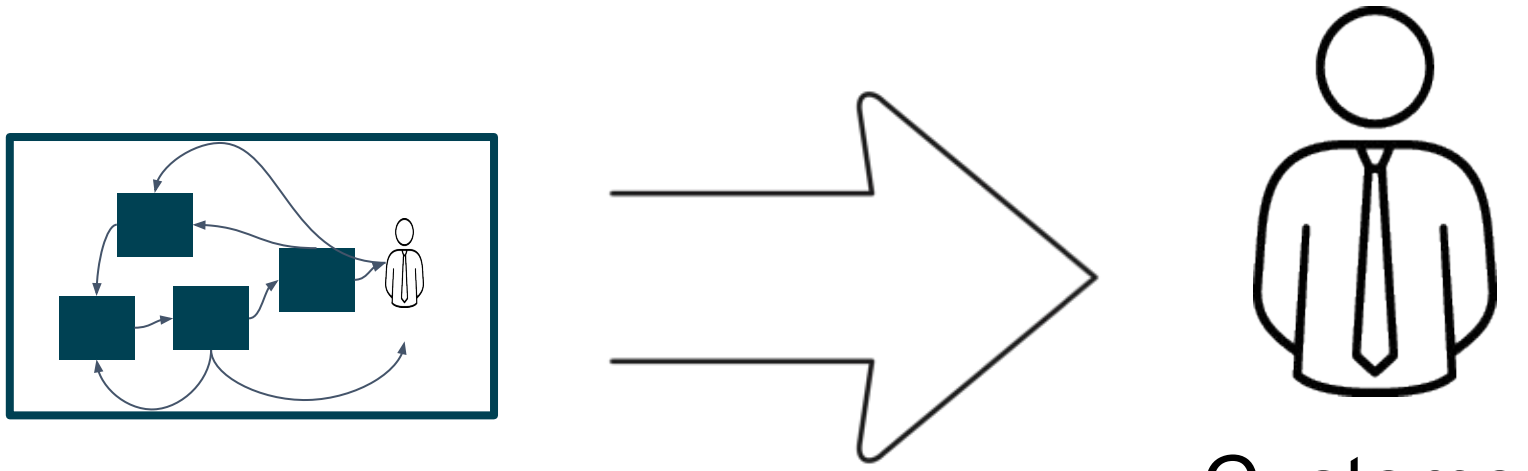
Four easy rules

1. Know what you have
2. Know where it came from
3. Know how to care for it
4. Know who you can work with



SECURE360

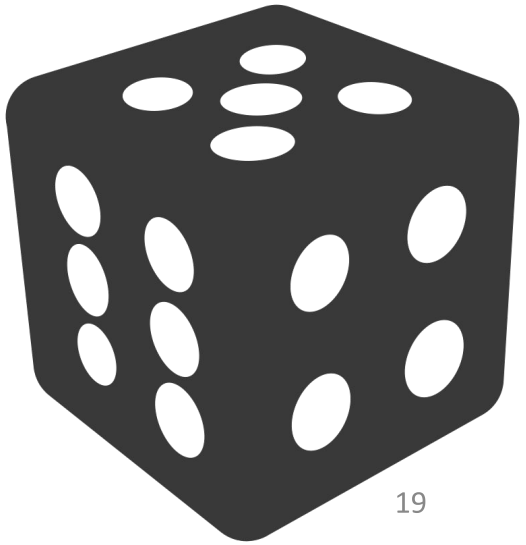
Know what you have



SECURE360

Know what you have

- Manifests
- Nested libraries
- This problem never goes away
  - Even if you have magic containment, you still have to protect the data
- There are partners that can help you do this
  - Find one



SECURE360

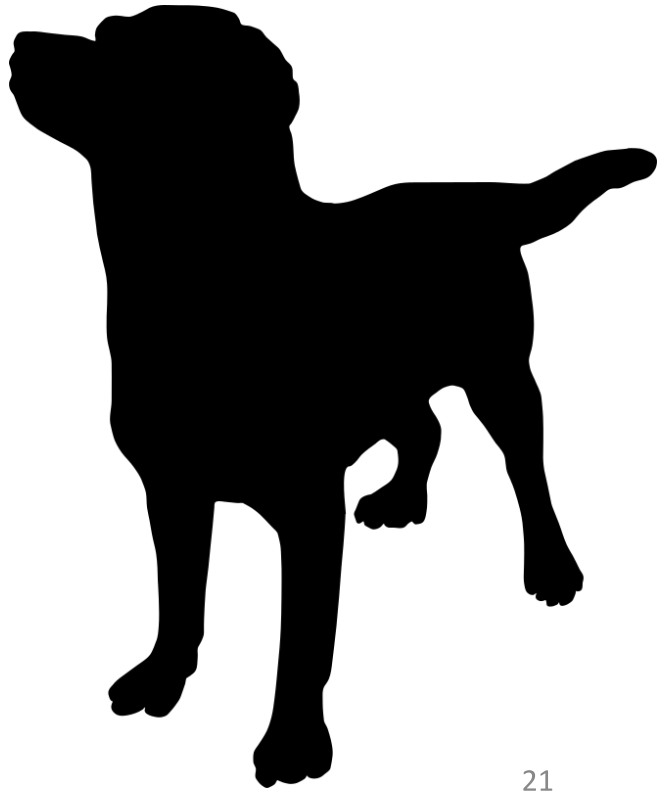
Know where it came from

- Random internet site?
- github?
  - Was it signed?
  - Was it a release?
- What's the license?
- Vendor supplied?
- Dependency?

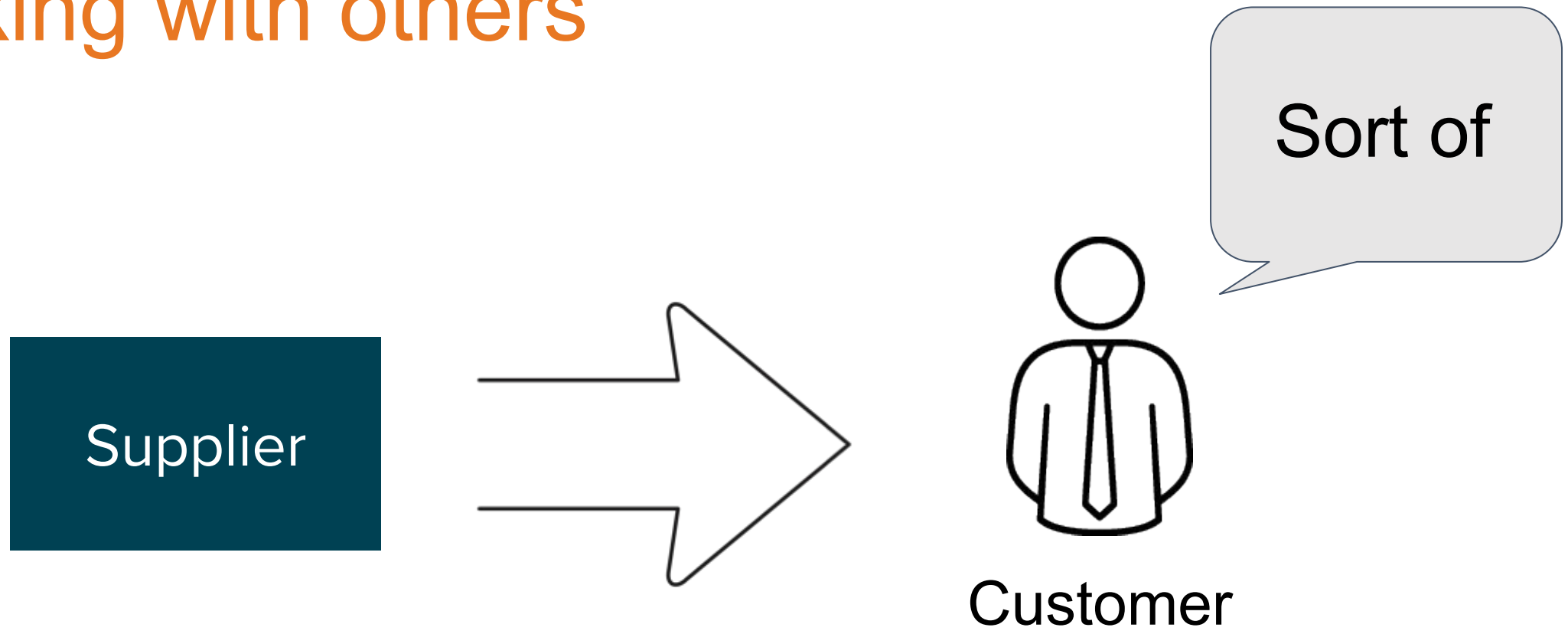
SECURE360

How do we care for it

- Security updates
- End of life
- Support
- New versions
- Features



Working with others

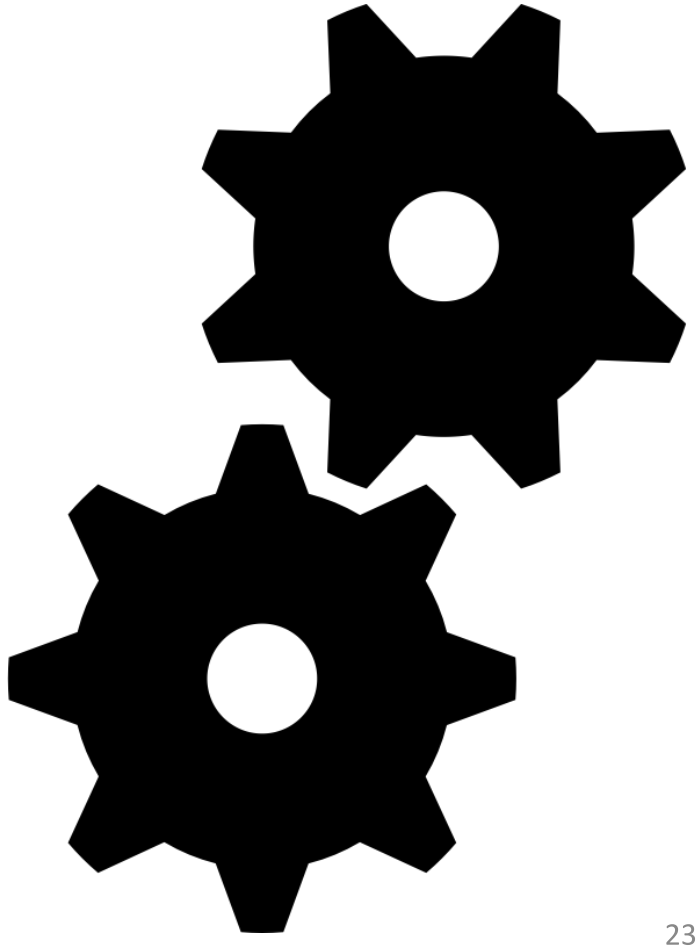


SECURE360

Now what?

What you can do right now

1. Accept reality
2. Modify your GRC
3. Start building an inventory
4. Find a trusted partner
5. Build your community
6. Embrace Open Source



Questions?

Josh Bressers
bressers@redhat.com
@joshbressers