How to secure your business against cyber criminals

- Supply Chain Security
- Edge for IoT

Johnny Westerlund
Solution Architect

Red Hat

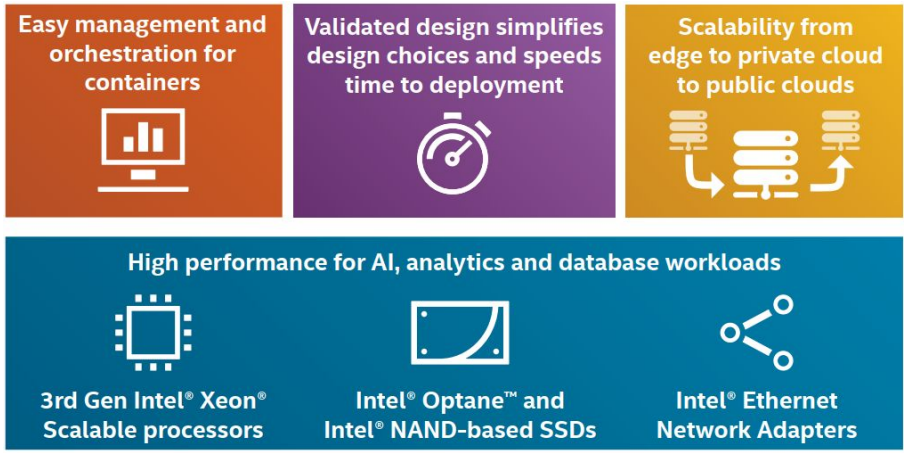
Red Hat OpenShift Reference Architecture

Joint Red Hat and Intel OpenShift Reference Architecture

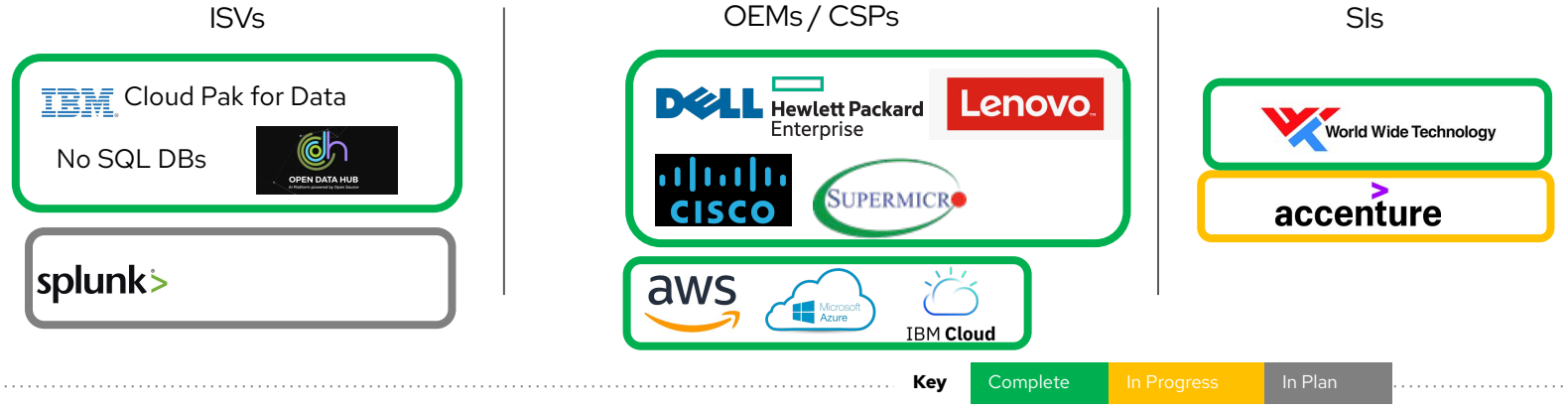
Solution overview

Summary: The RA enables deployment of performant and low-latency container-based workloads onto different footprints, such as bare metal, virtual, private cloud, public cloud, or a combination of these, in either a centralized data center or at the edge

Purpose: A general purpose OpenShift reference architecture to showcase the best of Intel and Red Hat products with key workloads



Solution ecosystem



Intel enabling status

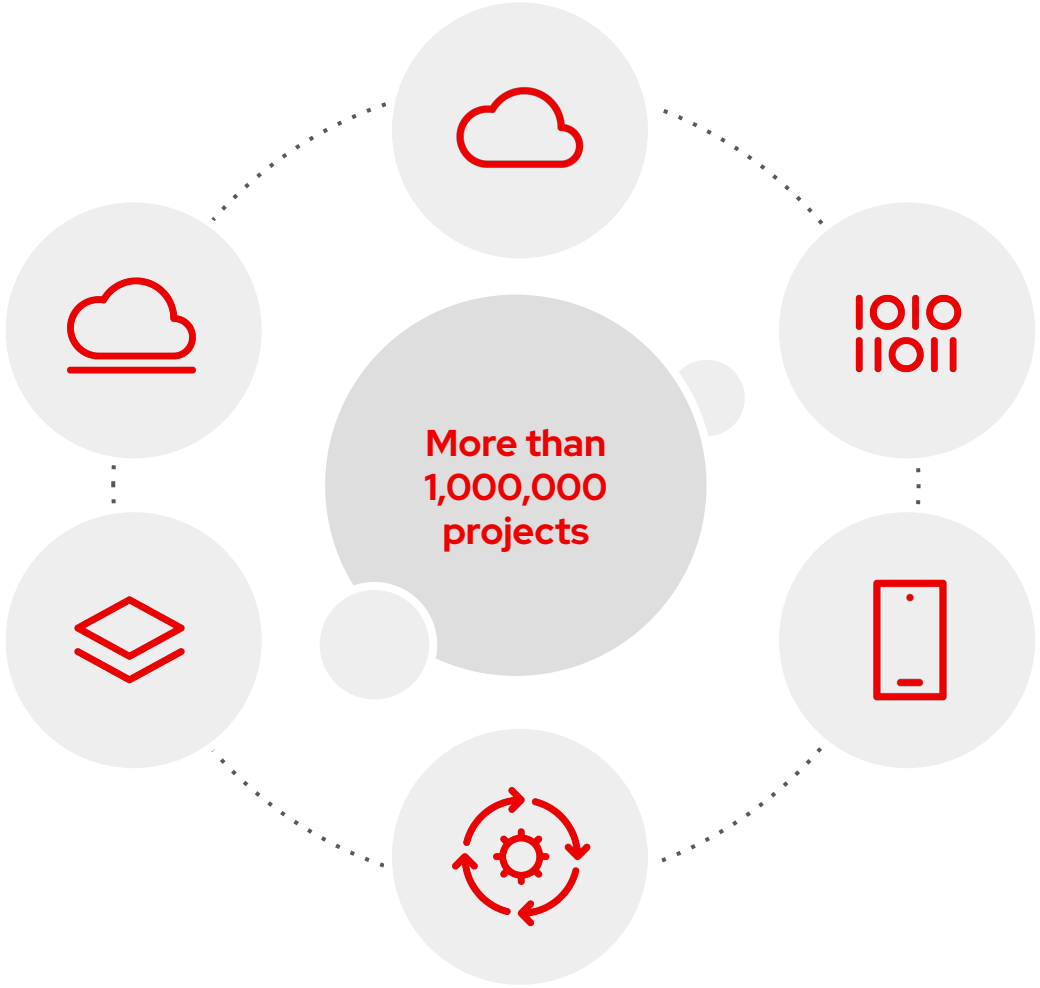
- Intel® Xeon (2nd Gen – Cascade Lake, 3rd Gen – Ice Lake)
- Intel Optane (PMEM, SSD); Columbiaville

Collateral

- Intel OpenShift RA for 4.6
- Intel OpenShift Solution Brief for 4.6
- Red Hat: OpenShift Ref Arch – Multiple OEMs
- Dell: OpenShift Offering
- HPE: OpenShift Offering
- Cisco: OpenShift Offering
- Lenovo: OpenShift Offering
- Supermicro: OpenShift Offering
- Penguin Computing: OpenShift Offering

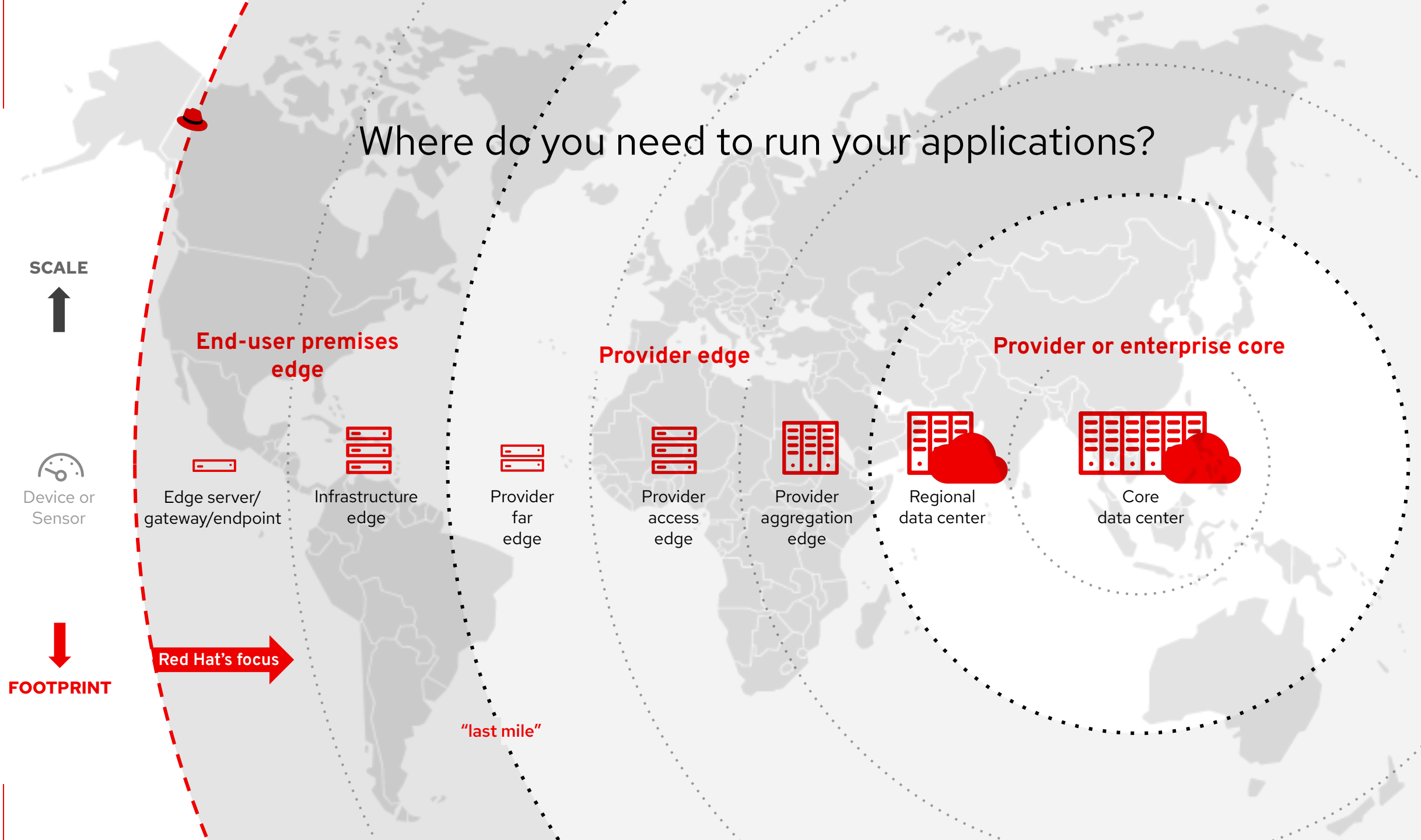
Red Hat | intel

Open source fuels rapid innovation



Red Hat

Where do you need to run your applications?



Security trends

Trend 1: Attack Surface Expansion

Enterprise attack surfaces are expanding. Risks associated with the use of cyber-physical systems and IoT, open-source code, cloud applications, complex digital supply chains, social media and more have brought organizations' exposed surfaces outside of a set of controllable assets.

Trend 2: Digital Supply Chain Risk

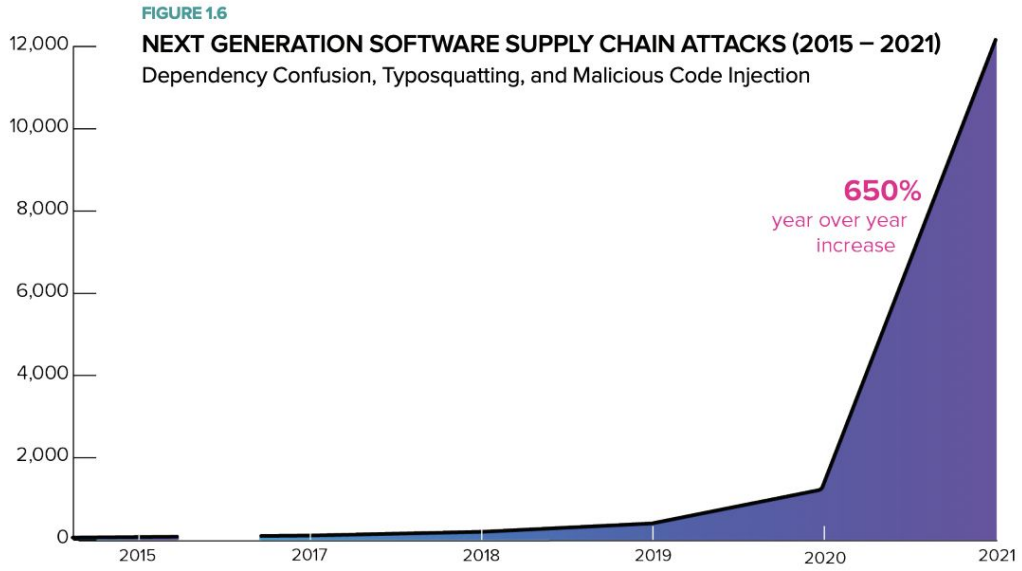
Cybercriminals have discovered that attacks on the digital supply chain can provide a high return on investment. As vulnerabilities such as Log4j spread through the supply chain, more threats are expected to emerge. In fact, Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.

https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

Where open source lives

Red Hat

Attacks are increasing year on year & targeting OSS projects



650%

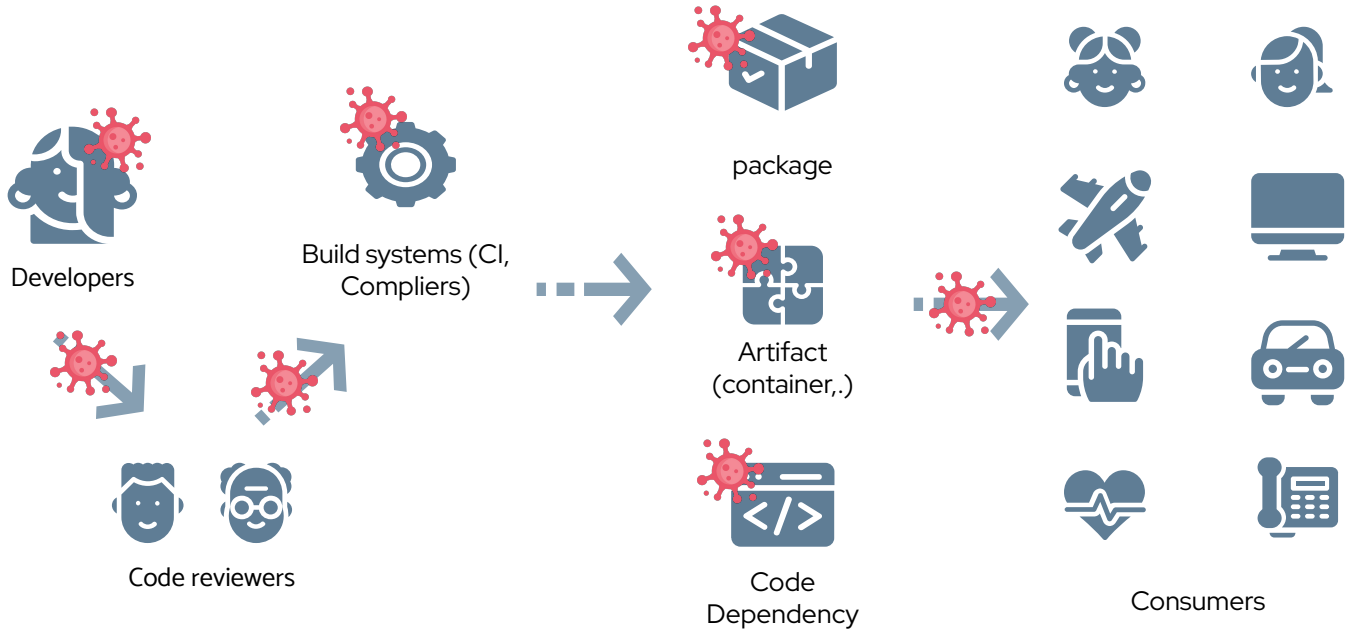
Increase in supply chain attacks in 2021

[Sonatype's State of the Software Supply Chain]

Red Hat

Software supply chains attacks

- Replay / freeze attacks
- Compromised keys
- Account Compromise
- Swapped hashes
- Compromise of build systems
- Easy reconnaissance (open configuration)
- Typosquatting
- Maintainer account takeover



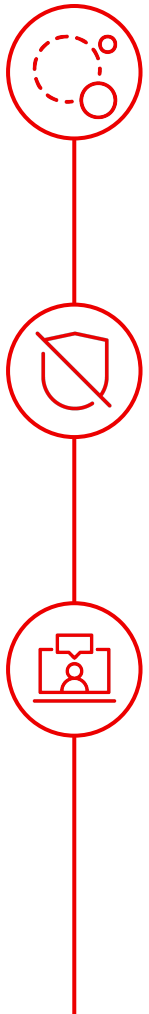
Red Hat

So what do we do about it?

Supply Chain Control

The story of the supply chain is the story of how a vendor creates their offerings and from where they source their materials. Your supply chain is not only what you make and how you make it, but what things exist within the ecosystem of the system that provides that engine.

Security considerations for open source software



How are new vulnerabilities in open source software discovered?

What level of awareness exists around open source software in use?

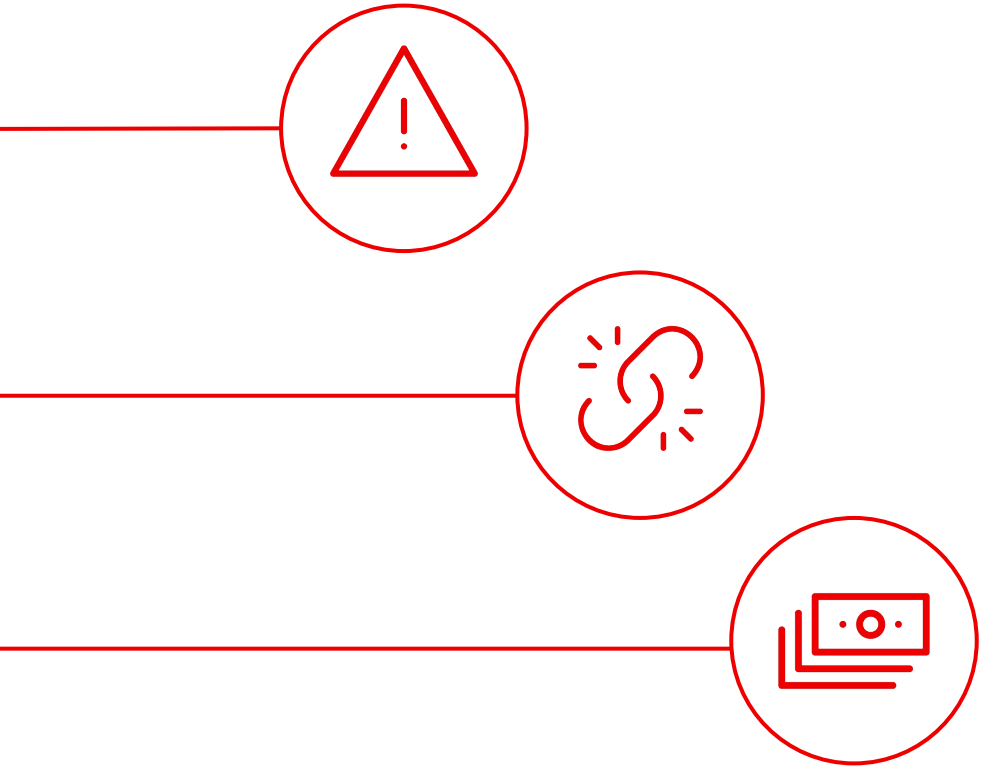
How are the security impact to the software you have assessed?

How are fixes to the software in use addressed?

Is the appropriate expertise to assess and remediate security issues in open source software available in-house?

What about critical and immediate support?

Undermanaged software can have costly impacts



6 million new versions

of OSS introduced in the past year; 37 million component versions now available[1]

650% increase

in open source software supply chain attacks[1]

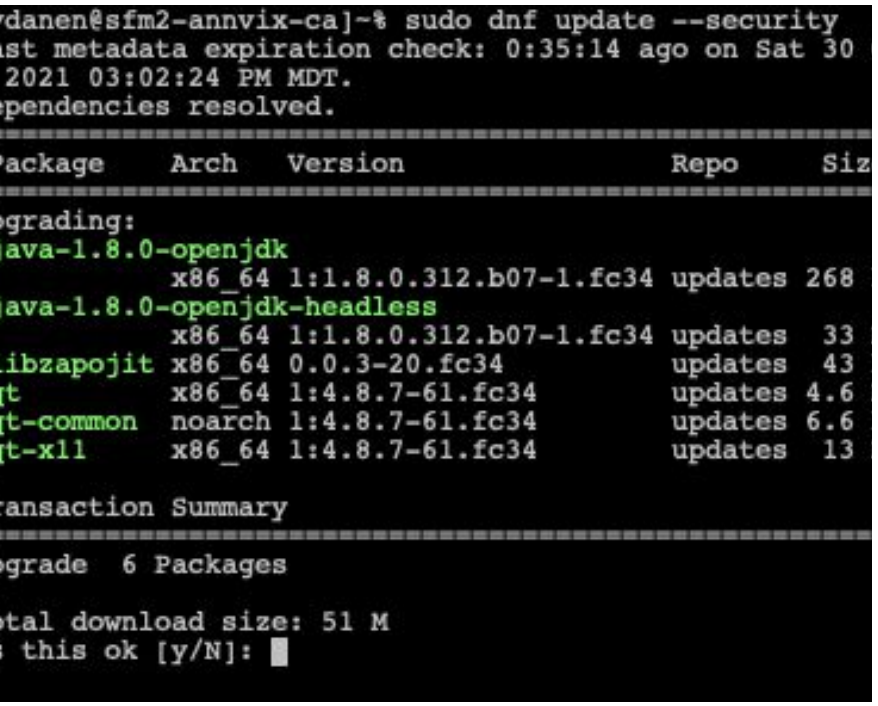
$25 million

the predicted cost of a recent supply chain attack[2]

$2 billion

the cost of a data breach that resulted from an unpatched bug[3]

Source:
[1] Sonatype 2021 State of the software supply chain
[2] SolarWinds Expects Cyber Incident Costs Up To $25 Million In 2021
[3] Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement



"The time to repurpose vulnerabilities into working exploits will be measured in hours and there's nothing you can do about it... except patch."

Fred House
Senior Director at FireEye, Inc.
(*McAfee Enterprise and FireEye 2022 Threat Predictions*)

Source:
https://www.fireeye.com/blog/executive-perspective/2021/10/mcafee-enterprise-fireeye-2022-threat-predictions.html

Backport or rebase?

For enterprise customers sensitive to change, backporting is the best choice

Backporting is taking an upstream change from a later version and applying it to an earlier version. Why backport?

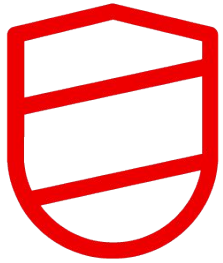
- Isolate code changes to fix a specific issue
- Maintain API/ABI compatibility - existing apps continue to work without change
- Reduce risk of new vulnerabilities introduced in later versions

Rebasing is updating the version of software to the latest available upstream. Why rebase?

- Fixes are too complex to backport successfully
- Desirable functionality present in newer version
- Lack of expertise to backport successfully

Not vulnerable due to backporting

Security value of backports from Red Hat versus grabbing from upstream

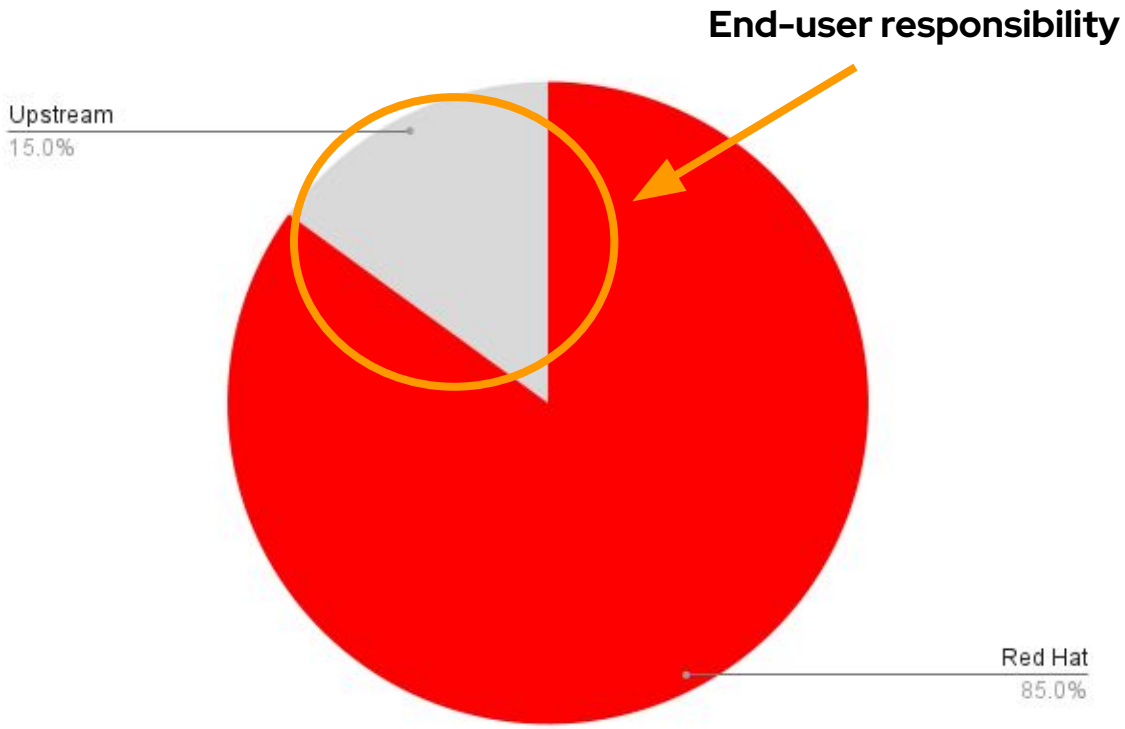


CVE-2020-1967	CVE-2021-3345	CVE-2021-20226	CVE-2020-8835
Important OpenSSL	Critical libgcrypt	Important kernel	Important kernel
Vulnerability was introduced in OpenSSL version 1.1.1d, which we did not ship	Vulnerability was introduced in libgcrypt version 1.9.0, which we did not ship	Vulnerable upstream code was not introduced in any version we shipped	Vulnerable upstream code was not introduced in any version we shipped

Small data sample; there are many more examples where we did not take an upstream version or upstream patches due to our backporting policy.

Whose responsibility? 🤔

Curated (from Red Hat) versus uncurated (self-obtained)



Streamline updates

Updates from Red Hat are easy and low risk; allows for focused time and energy on tracking the rest

Simplify monitoring

Red Hat provides robust security metadata to validate fixes for what is provided so less time is spent tracking and monitoring what isn't

Easily identify what's in use

Use Red Hat inventory metadata to know what is installed and where, track only what other uncurated open source is in use

Red Hat

Trusting your supplier

- All code stored in secure, internal repositories
- Strong distribution mechanisms with signed packages
- Strong safeguards against tampering
- Minimal modifications over product lifetimes protect from unwanted and potentially risky upstream code changes

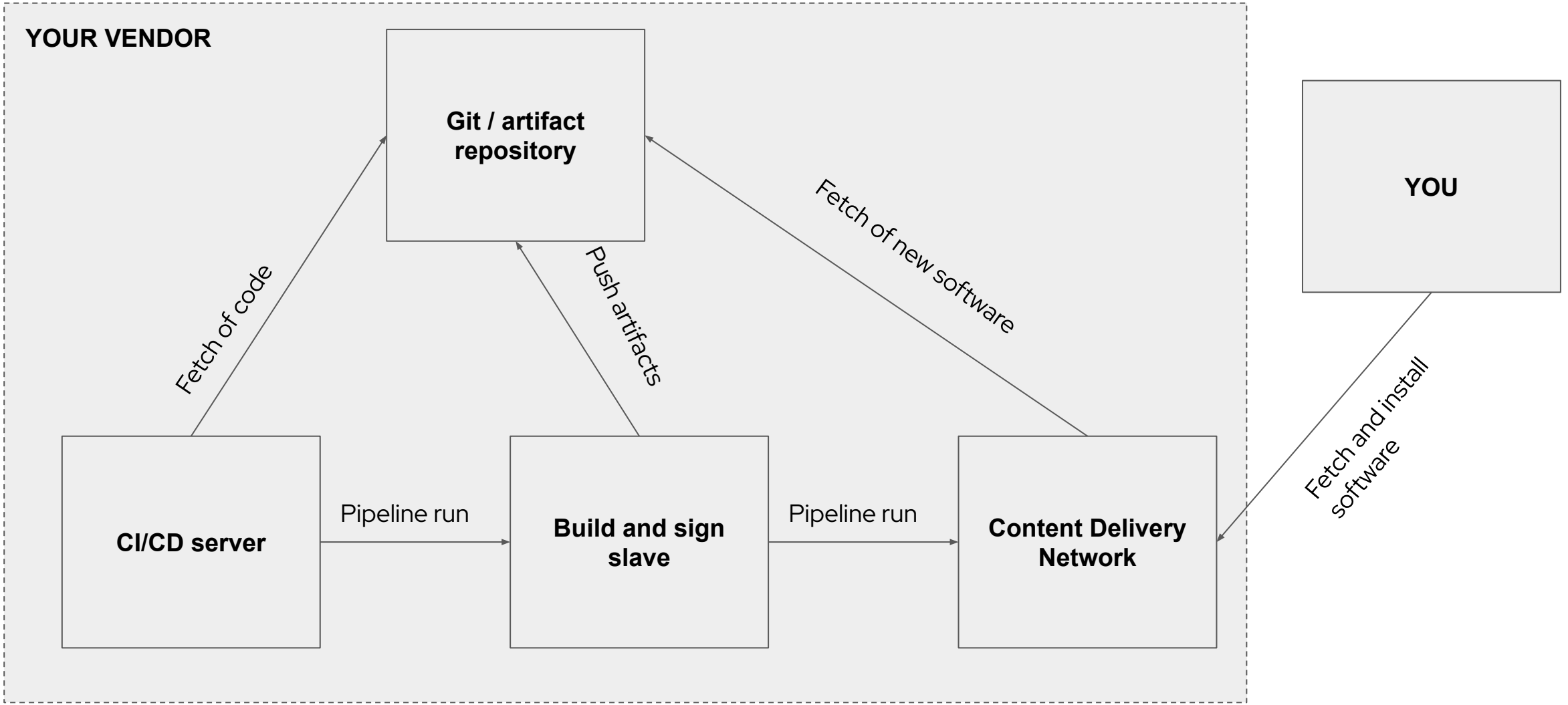
What if signing and key management were greatly simplified...

and with open transparency

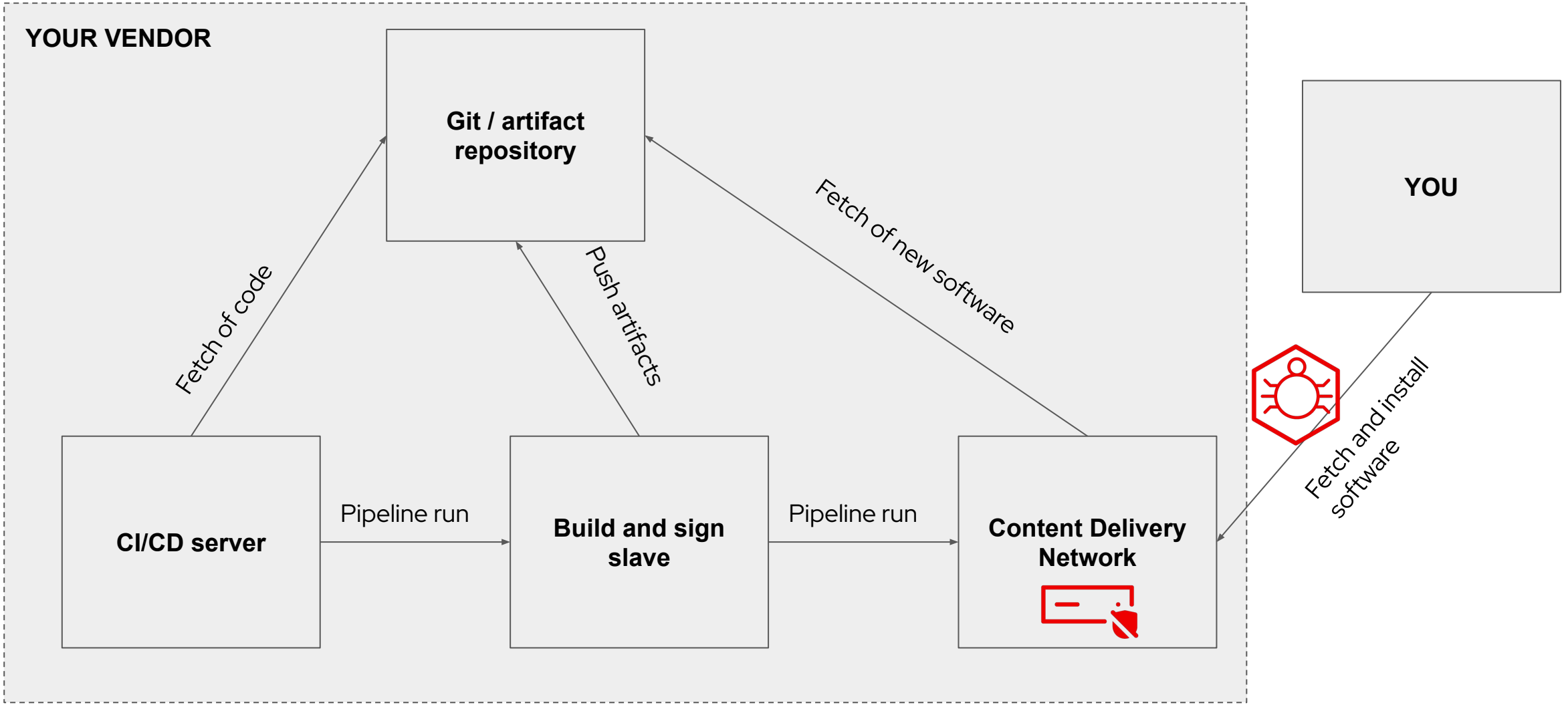
DEMO: sigstore

DEMO: Defending against supply chain attacks

A software supply chain

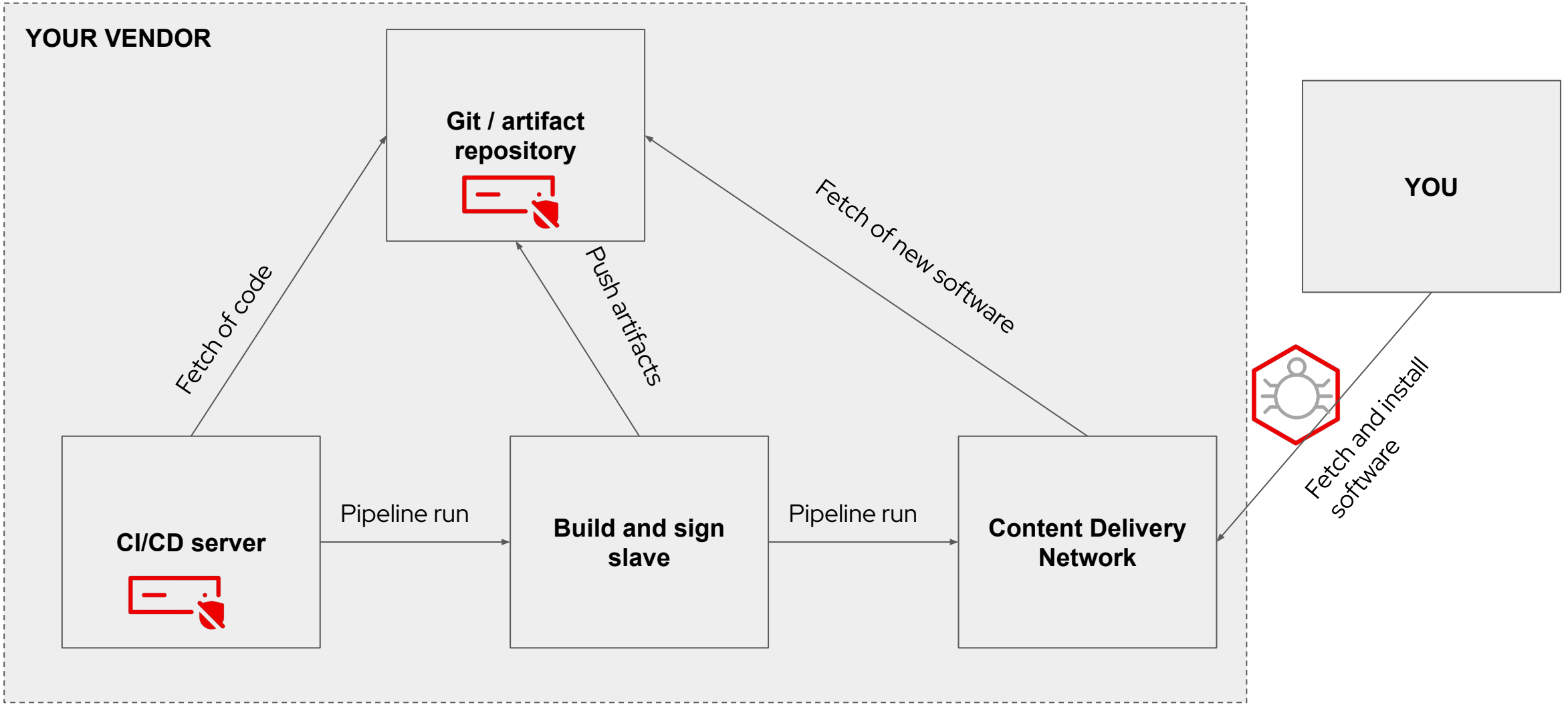


Attack 1: Content Delivery Network breached



Red Hat

Attack 2: Development process breached



Red Hat

Under the hood: **What is SELinux**

```
[root@rhel9c ~]# ls -la /usr/bin/app
-rwxr-xr-x. 1 root root 10912 May 24 10:25 /usr/bin/app
[root@rhel9c ~]# ls -la /etc/shadow
-rw-rw-r--. 1 root root 918 May 24 10:41 /etc/shadow
[root@rhel9c ~]# chown guyfrombar:cluelesspeople /etc/shadow
[root@rhel9c ~]# ls -la /etc/shadow
-rw-rw-r--. 1 guyfrombar cluelesspeople 918 May 24 10:41 /etc/shadow
[root@rhel9c ~]#
```

Discretionary Access System - You have the discretion to shoot yourself in the foot

Under the hood: **What is SELinux**

```
[companyuser@rhel9c ~]$ ls -laZ /usr/bin/app
-rwxr-xr-x. 1 root root system_u:object_r:bin_t:s0 10912 May 24 10:25 /usr/bin/app
[companyuser@rhel9c ~]$ ls -laZ /etc/shadow
ls: cannot access '/etc/shadow': Permission denied
[companyuser@rhel9c ~]$ id -Z
user_u:user_r:user_t:s0
[companyuser@rhel9c ~]$
```

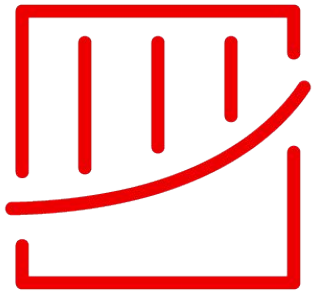
```
[root@rhel9c ~]# ls -laZ /etc/shadow
-rw-rw-r--. 1 root root system_u:object_r:shadow_t:s0 918 May 24 10:41 /etc/shadow
```

Mandatory Access System - The kernel enforces a policy and users in the system have to follow this policy, no matter what.

IoT /Edge

Red Hat Solutions

Red Hat

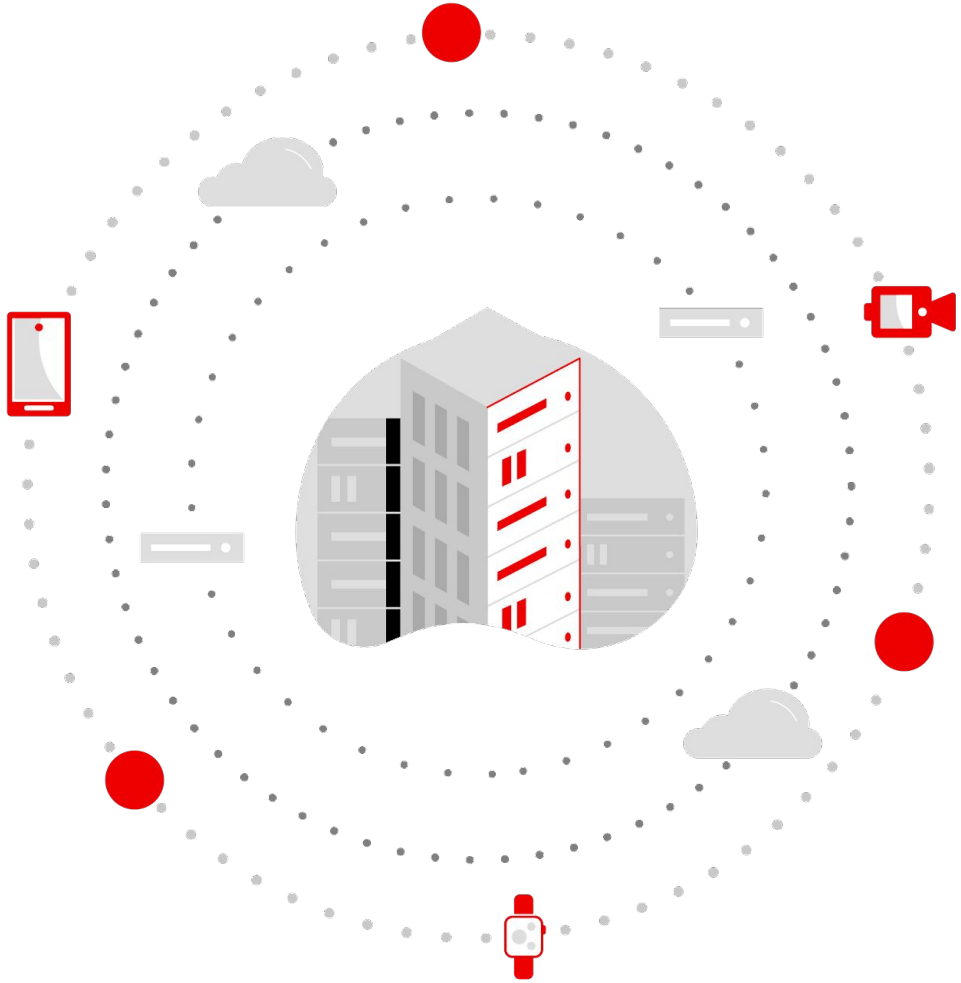


TRENDS!

"96% of customer-obsessed firms adopt new technologies before their competitors do."[1]

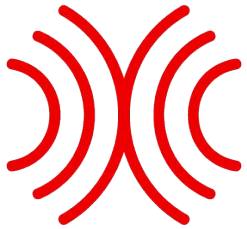
"800% increase in the number of apps deployed at the edge."[2]

"By 2025 more than 50% of enterprise-managed data will be created and processed outside the data center or cloud."[3]



1 Forrester: The Tools That Matter: Demystifying Emerging Technologies, May 2021
2 IDC: IDC FutureScape: Worldwide IT Industry 2020 Predictions, Doc # US45599219, October 2019
3 Gartner: Predicts 2022: The Distributed Enterprise Drives Computing to the Edge October 2021

Red Hat



CHALLENGES!

APPLICATION SECURITY | March 22, 2022

IoT Security and the Internet of Forgotten Things

In 2017, the number of connected devices surpassed the world's human population. That's a lot of things. However, many of them were not built with security in mind. It didn't take long for attackers to take advantage of Internet of Things (IoT) vulnerabilities. One case in 2016 saw threat actors take down Dyn, a company [...]

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY SIGN IN SUBSCRIBE

Get WIRED for just ~~$29.99~~ $5. SUBSCRIBE NOW

LILY HAY NEWMAN SECURITY APR 13, 2021 12:01 AM

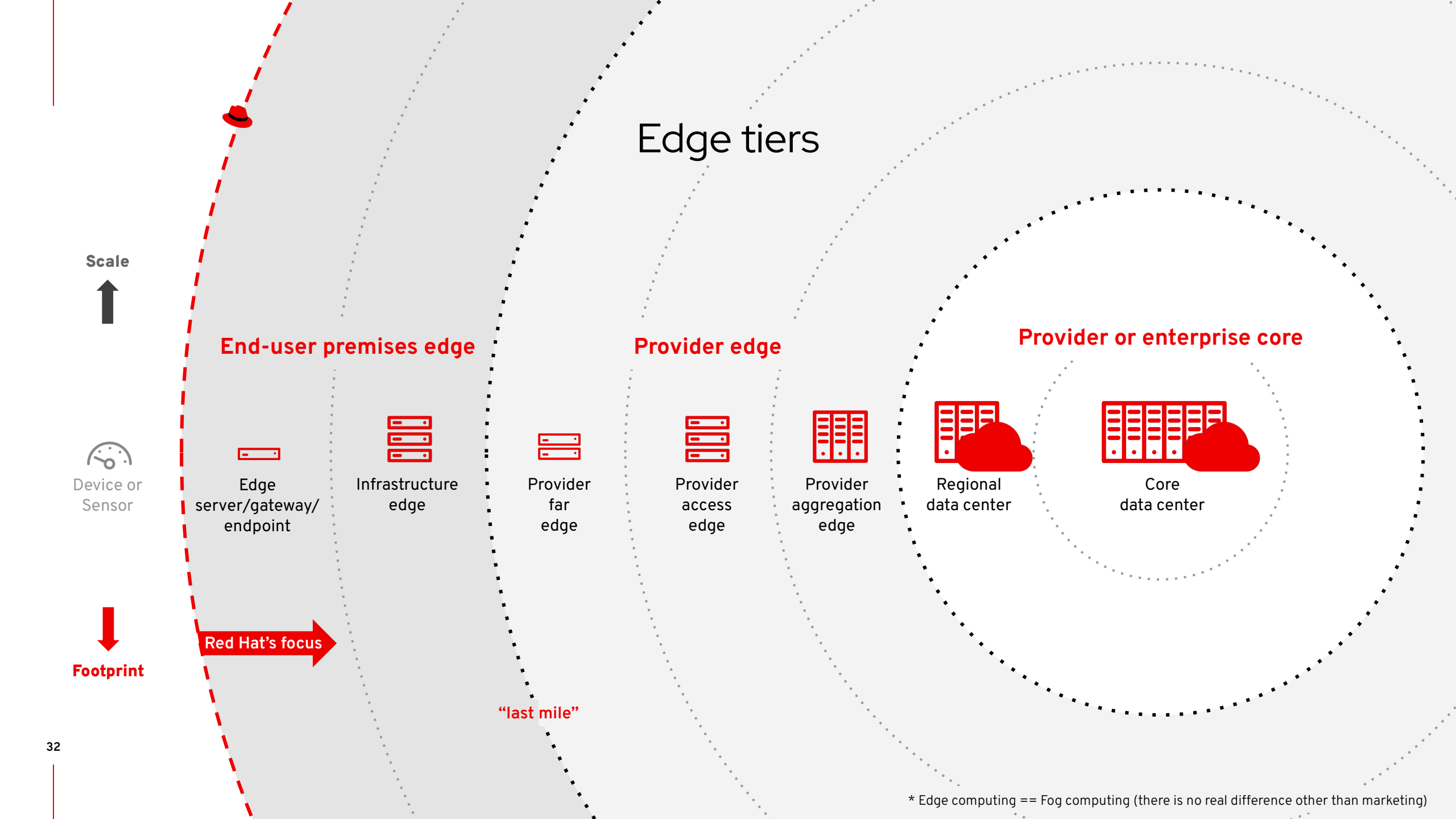
100 Million More IoT Devices Are Exposed—and They Won't Be the Last

The Name:Wreck flaws in TCP/IP are the latest in a series of vulnerabilities with global implications.

Red Hat

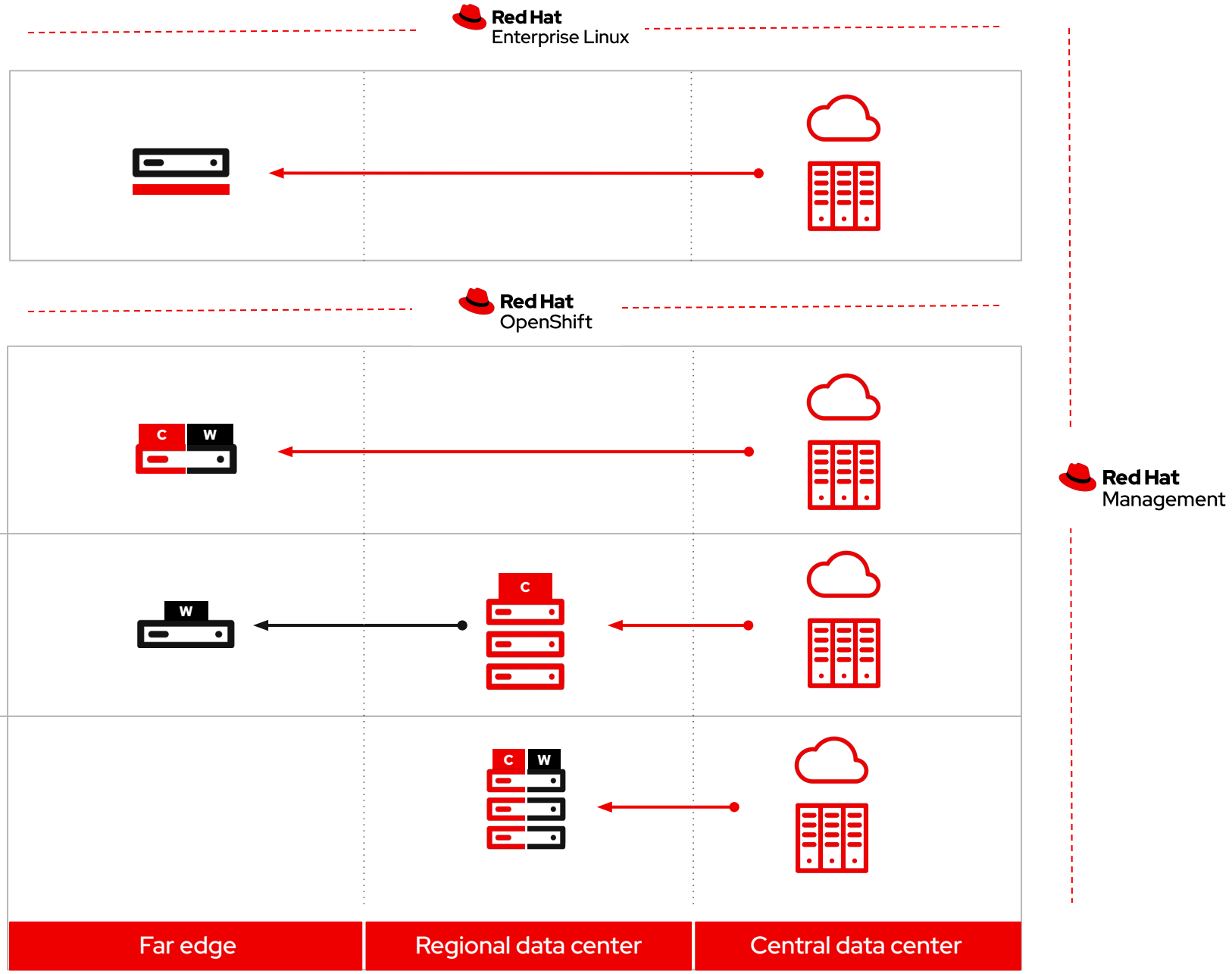
HOW CAN RED HAT HELP?

Edge tiers



* Edge computing == Fog computing (there is no real difference other than marketing)

Red Hat platforms for the edge



Cluster management and application deployment

Kubernetes node control

C Control node

W Worker node

Red Hat

Edge solutions demos

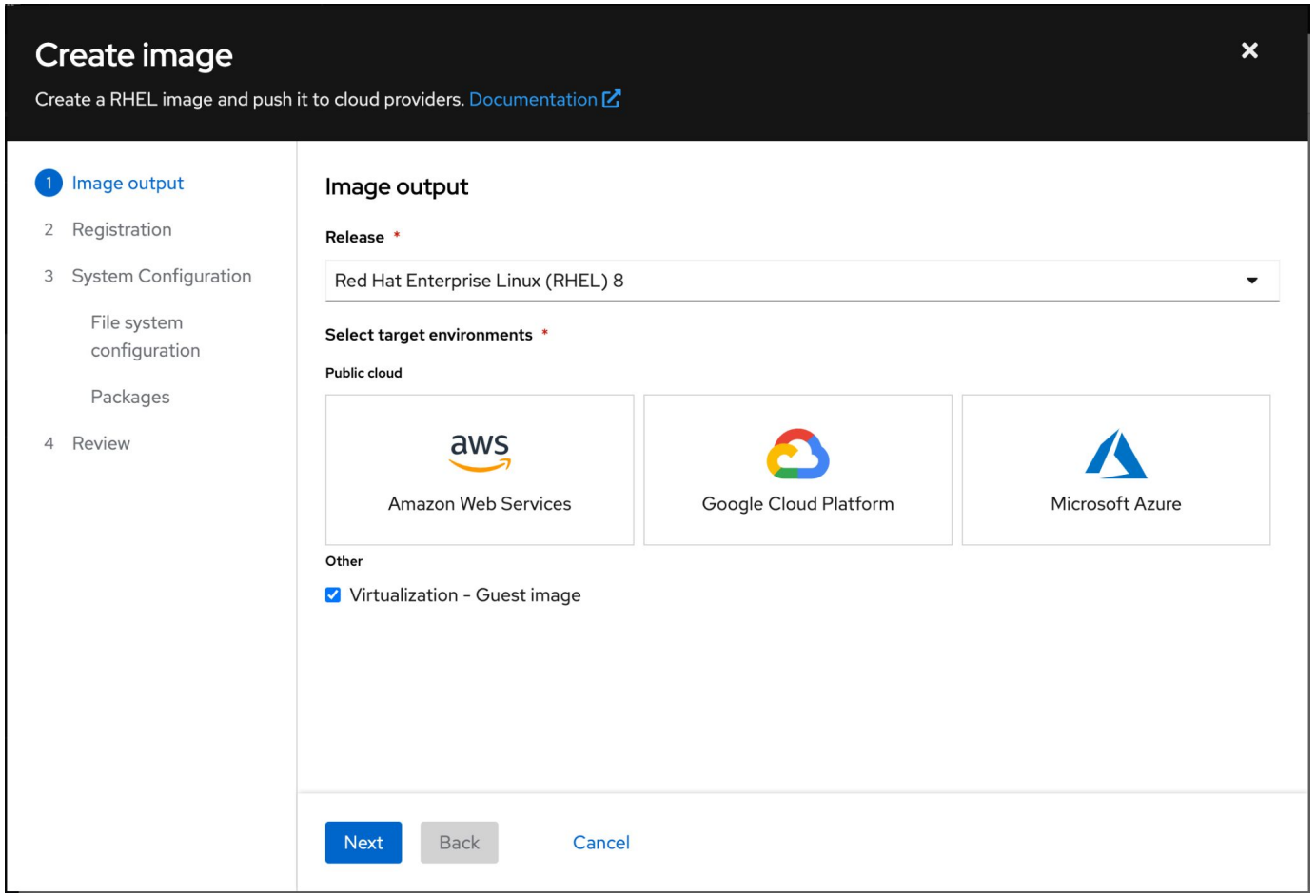
1. Image Builder - RHEL for Edge
2. Container deployment to the edge

Edge solutions demos

1. Image Builder - RHEL for Edge
2. Container deployment to the edge

Red Hat Enterprise Linux image builder

Save time and ensure consistency when deploying RHEL systems at scale



- **Support for Bare Metal Deployments**
  Install a customized RHEL OS image directly on physical hardware by creating installation media with a built-in kickstart file to automate the process.

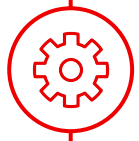
- **Customized Filesystem Support**
  Assemble RHEL OS images that have multiple, distinct, non-LVM filesystem mount points rather than a single, large root filesystem.

Red Hat

Steps for using image builder

1. Choose platform

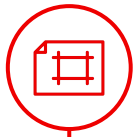
Physical, private cloud, public cloud, or edge



2. Select image builder tool

Image builder service
console.redhat.com

Image builder
On-premises private build



3. Create blueprint

Define and customize the image

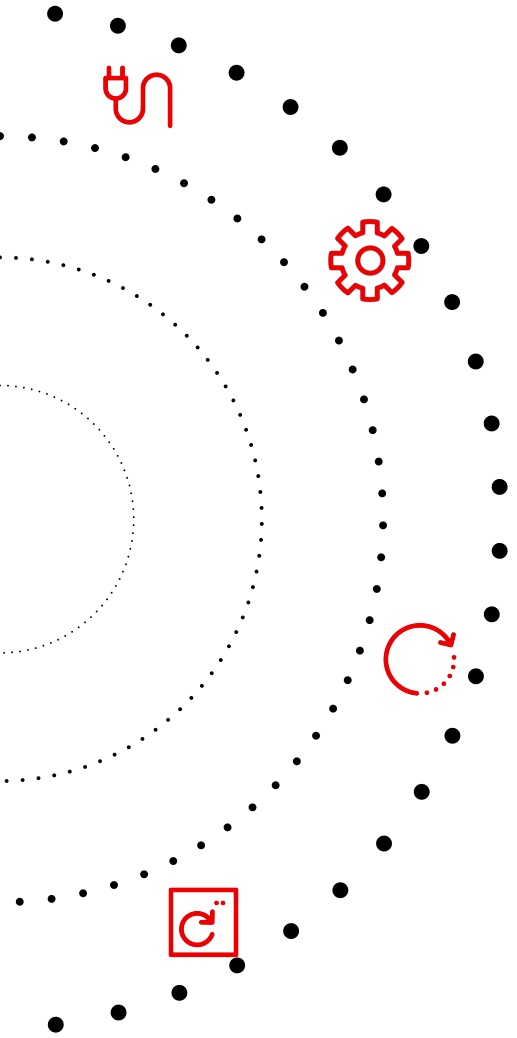
4. Build the image

Create a variety of images including Red Hat OpenStack, Amazon Web Services, VMware, and Microsoft Azure, and more

5. Deploy instance

Push image to the cloud provider of your choice or download to your datacenter

Red Hat



Red Hat Enterprise Linux for edge

Ensured stability and deployment flexibility

Edge Management

Zero-touch provisioning, health visibility, and security remediation

Automated container updates & rollback

Download, deploy, and update images with built-in auto-rollback

Major release upgrade support

Transparently stage OS upgrades in the background

Simplified install and on-boarding

Deploy images through the network or physical install media

Edge solutions demos

1. Image Builder - RHEL for Edge
   Easy to use image builder
2. Container deployment to the edge

DEMO TIME!

Edge solutions demos

1. Image Builder - RHEL for Edge
2. Container deployment to the edge

podman

Running containers on Edge

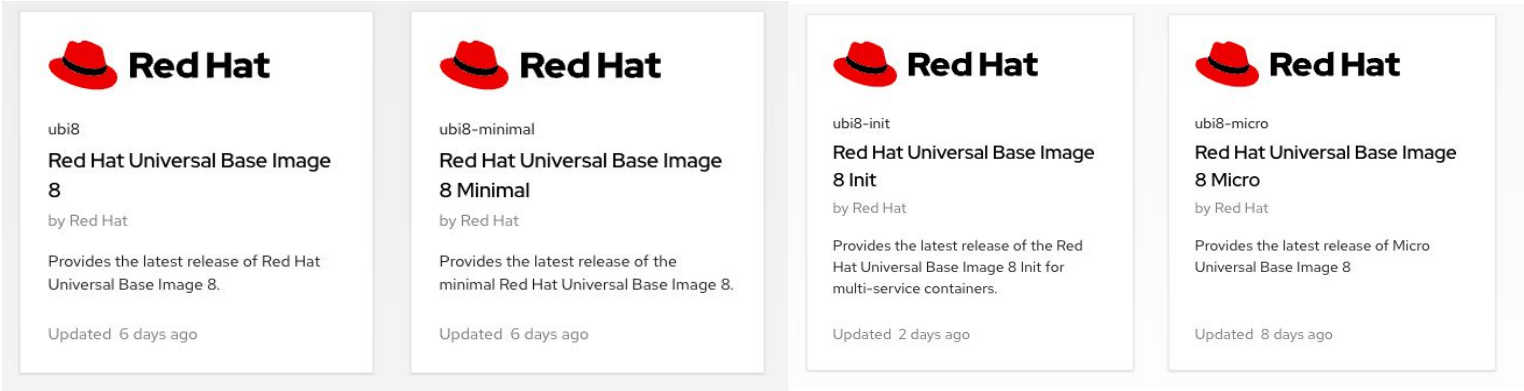
- Podman provides container capabilities

- Security features
  - SELinux, signed images, Linux capabilities, non privileged user
  - Trusted repositories (registry.redhat.io ...)

Red Hat

Running containers on Edge

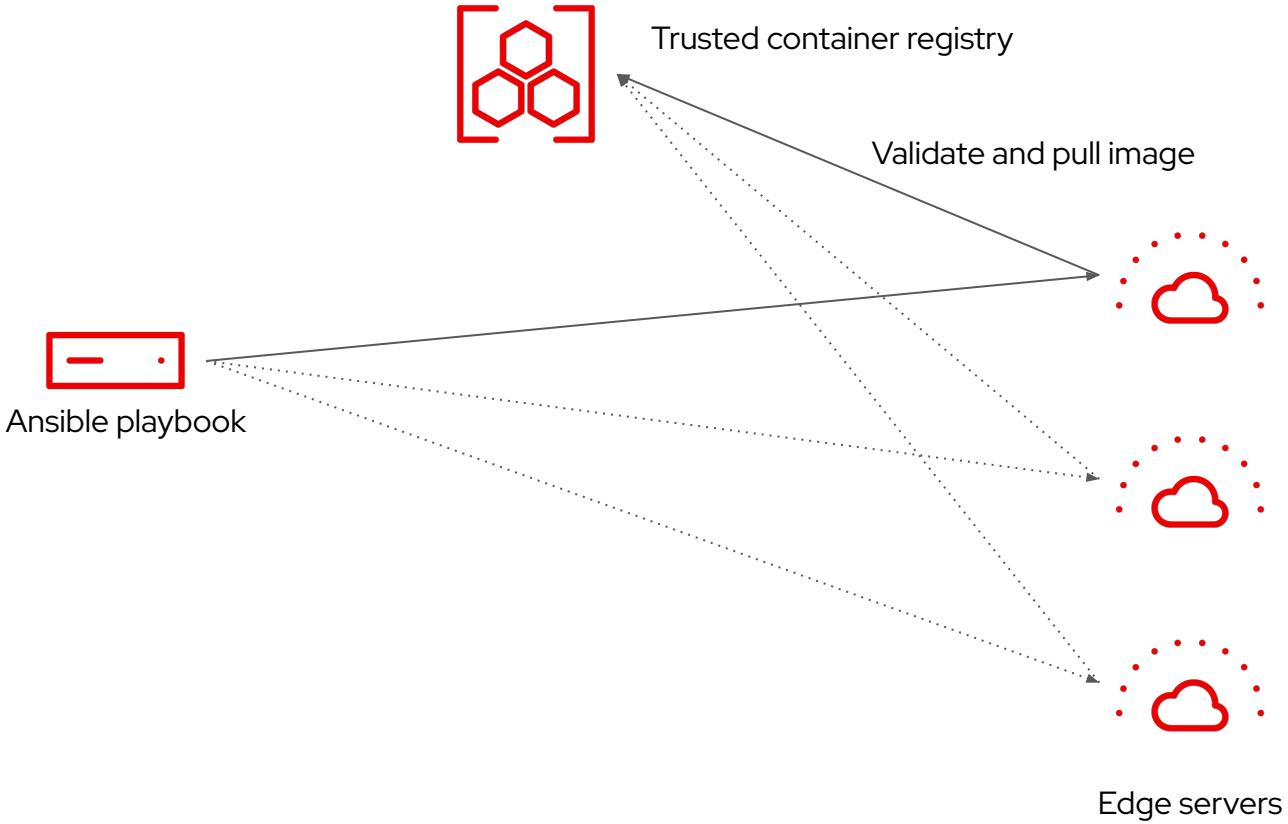
- Universal Base Images (UBI)
  - Uniform
  - Red Hat maintained base images for Podman and OpenShift



Red Hat

Running containers on Edge

- Ansible:
  - Deploy containers to many edge servers
  - Scalable and consistency across the edge



Ansible is used to orchestrate deployment of containers that are check for valid signing before being run

Example playbooks

```yaml
---
- hosts: localhost
  tasks:

  - name: Check container
    ansible.builtin.shell:
      cmd: cosign verify --key cosign.pub quay.io/mbang1/nginx-test:latest
      chdir: ~/opentour
```

```yaml
- hosts: all
  tasks:
  - name: Login to quay.io
    containers.podman.podman_login:
      authfile: <auth.json>
      registry: quay.io

  - name: Run container
    containers.podman.podman_container:
      name: container
      image: quay.io/mbang1/nginx-test:latest
      state: started
```

DEMO TIME!

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

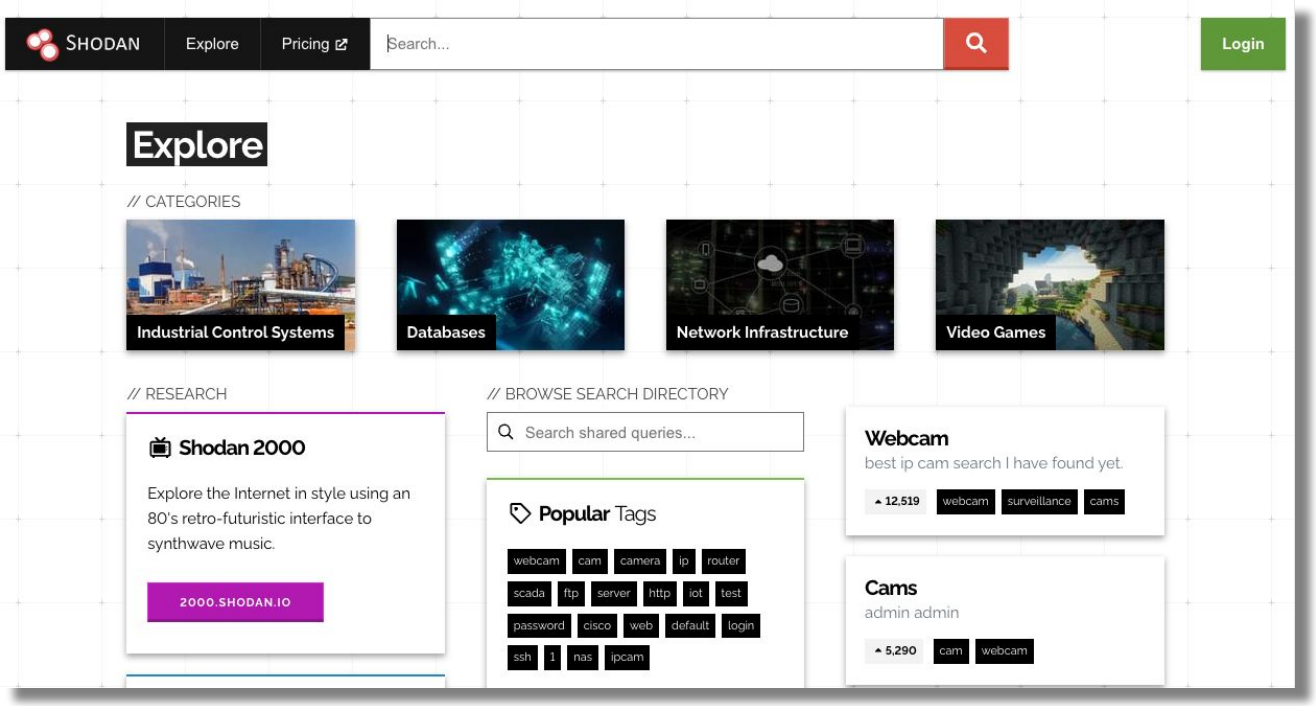

linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Red Hat


SHODAN
Explore
Pricing
Search...
Login
Explore
// CATEGORIES
Industrial Control Systems
Databases
Network Infrastructure
Video Games
// RESEARCH
Shodan 2000
Explore the Internet in style using an 80's retro-futuristic interface to synthwave music.
2000.SHODAN.IO
// BROWSE SEARCH DIRECTORY
Search shared queries...
Popular Tags
webcam cam camera ip router
scada ftp server http iot test
password cisco web default login
ssh 1 nas ipcam
Webcam
best ip cam search I have found yet.
12,519 webcam surveillance cams
Cams
admin admin
5,290 cam webcam


HackMag
Mobile
Security
Malware
Coding
Unix
Devops
Chum Bucket. How I hacked a 20-billion corporation using a free service
Written by Dead Beef
$
As you are likely aware, data breaches occur on a regular basis in this wild world. Each such incident is preceded by painstaking work: information collection and analysis, identification of security holes, selection of attack tools, etc. Today, I will reveal to our readers how I hacked the $20-billion TUI Group using publicly available free tools and my own wits.

Red Hat

USEFUL STUFF

"Reading material"

Installing most open source software today is equivalent to picking up a random thumb-drive off the sidewalk and plugging it into your machine.

3.1 Sigstore

Sigstore is a project with the goal of providing a public good / non-profit service to improve the open source software supply chain by easing the adoption of cryptographic software signing, backed by transparency log technologies. The project seeks to empower software developers to securely sign software artifacts such as release files, container images, binaries, bill of material manifests and more, without the risks and complexity of managing private keys. Instead keys are ephemeral and discarded after use by storing signing materials into a time-stamped tamper resistant public log. The project was founded within OCTO Emerging technologies and is now co-developed alongside Google and many others. Sigtore is planned for productization in OpenShift to sign container images and kubernetes manifests. It is also now hosted under the Linux Foundation with plans to launch a public good service modelled after Let's Encrypt

Q4 Project Updates: sigstore is now an OpenSSF project and the public good service received its first funding round via Red Hat, Google, Cisco, HPE and VMware. The community has continued to see rapid expansion with now over 20 different organisations and just shy of 500 contributors. Productization continues to progress (see graduation trajectory)

Graduation trajectory: sigstore will now be integrated into multiple OpenShift silos.

- The container engineering team under Daniel Walsh are implementing sigstore container signing into podman.
- Sigstore is available as a tech preview feature in ACM 2.3 via collaboration with the ACM governance security team.
- Quay 3.6 now supports sigstore container annotations as of 3.6 release.
- Ansible is working with IBM research to introduce sigstore signed playbooks, roles.

https://www.youtube.com/watch?v=3LKHKpcH2x8
https://security.googleblog.com/2021/03/introducing-sigstore-easy-code-signing.html
https://docs.google.com/presentation/d/1s5v4fxIjGOSaPsZT4CYx3fxcmpdhqH_-LmYHu9Y4YpQ/edit?usp=sharing

https://github.com/sigstore/cosign/releases/tag/v1.8.0
https://www.youtube.com/watch?v=gCi9_4NYyR0
https://docs.sigstore.dev/cosign/openid_signing

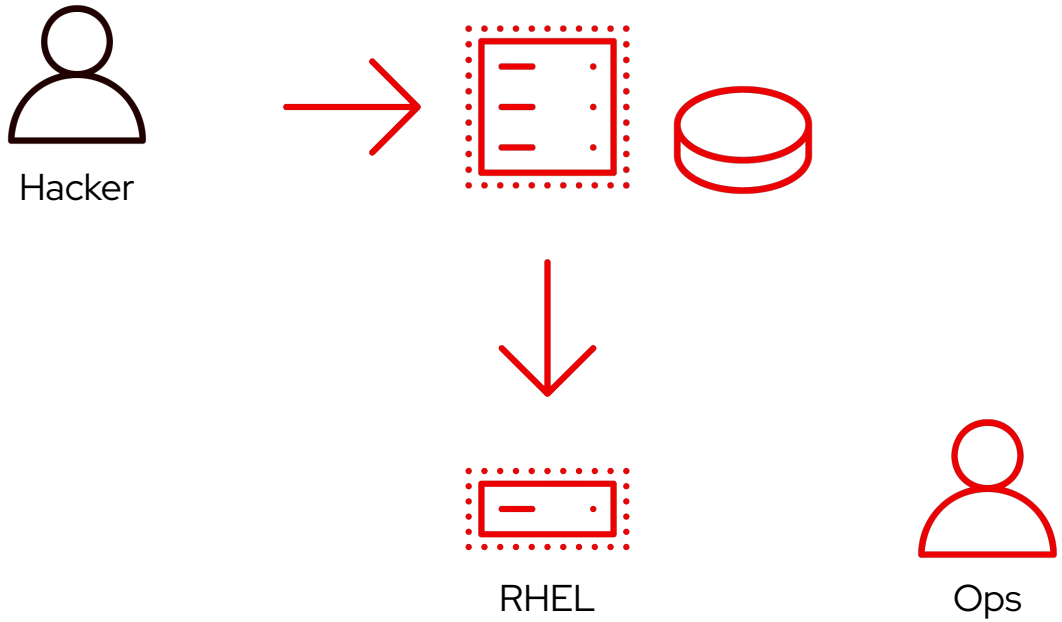
```
export COSIGN_PASSWORD=redhat
cosign generate-key-pair
cosign sign --key cosign.key quay.io/jwesterl/ansible-execution-env:1.0
cosign verify --key cosign.pub quay.io/jwesterl/ansible-execution-env:1.0

Clean up
cosign clean quay.io/jwesterl/ansible-execution-env:1.0
<go to quay.io and remove tag>

EXPERIMENTAL
export COSIGN_EXPERIMENTAL=1
cosign sign quay.io/jwesterl/ansible-execution-env:1.0
<browser window opens, sign in with your oidc>
cosign verify quay.io/jwesterl/ansible-execution-env:1.0
```

Demo ideas, vulnerable supply chain
Run vulnerable container as root.
Run exploit and show selinux protection, mitigating host take over.

Red Hat


Hacker
RHEL
Ops

Red Hat