Connect

What's in your Container?

Securing the Software Supply Chain without Slowing Down

Adrian Kosmaczewski
Senior Architect
Red Hat

Adrian Kosmaczewski

Senior Architect
Red Hat

The "Black Box" Problem


SALE


Nutrition Facts
INGREDIENTS
LASAGNA

Software is assembled,
not written

Log4j

SolarWinds

Do you know what is running in your infrastructure?

We need the digital equivalent of a nutrition label

The Three Pillars


TRANSPARENTIA
IDENTITAS
CLAUSTRA

Transparency, Identity, and Guardrails

1. Transparency

SBOM

(Software Bill of Materials)

syft

https://github.com/anchore/syft

Red Hat Trusted Profile Analyzer

https://developers.redhat.com/products/trusted-profile-analyzer

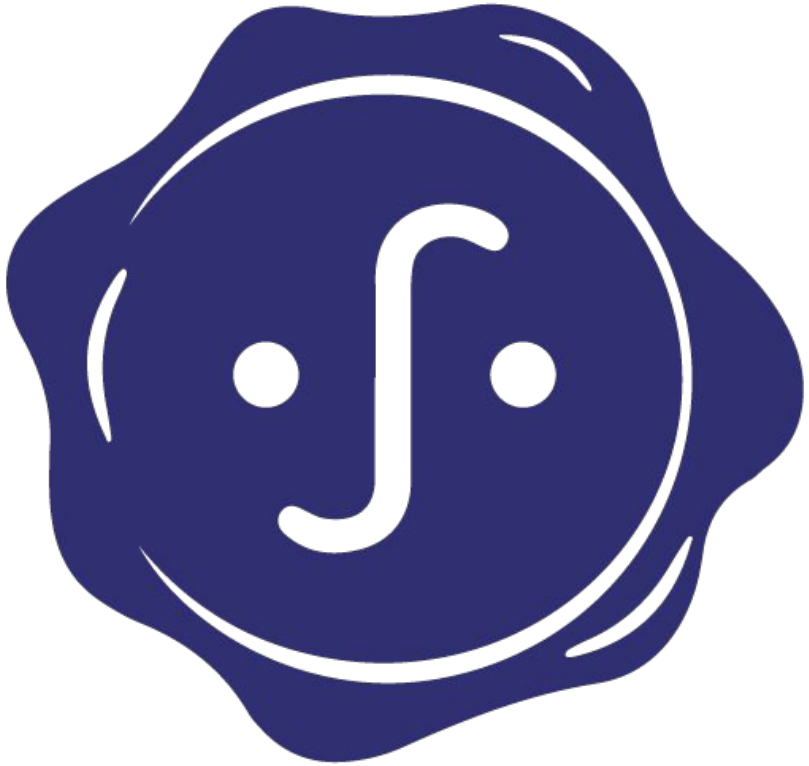
```
  },
  "components": [
    {
      "type": "library",
      "bom-ref": "pkg:maven/org.bouncycastle/bcprov-jdk15on@1.62?type=jar",
      "group": "org.bouncycastle",
      "name": "bcprov-jdk15on",
      "version": "1.62",
      "description": "The Bouncy Castle Crypto package is a Java implementation of cryptographic algorithms. This jar
contains JCE provider and lightweight API for the Bouncy Castle Cryptography APIs for JDK 1.5 to JDK 1.8.",
      "hashes": [
        {
          "alg": "MD5",
          "content": "01b1a8cff910fdb9328cef5c437ff2f9"
        },
        {
          "alg": "SHA-1",
          "content": "633b6739ef8f07f2e71f8eebd1c6f25b17a4ec7d"
        },
        {
          "alg": "SHA-256",
          "content": "2fa0ab71b154da29ac134097bc6bbacd90987dd4c4005516159e6494d1d52ea2"
        },
        {
          "alg": "SHA-384",
          "content": "3c68bbe3e699f6896ef924dd3b580e3173117d48165fb4da3c4c287b7b59e4748151d574e16a8b8ddc6c8f24a8768d33"
        }
```


https://github.com/CycloneDX/bom-examples/blob/master/SBOM/keycloak-10.0.2/bom.json

2. Identity


EOS
MICHELIN


UNSIGNED
ERROR 404!
Cryptofail!
Cryptofail! .....
//s\\
Signature not found!
//o/\\
#!/1://

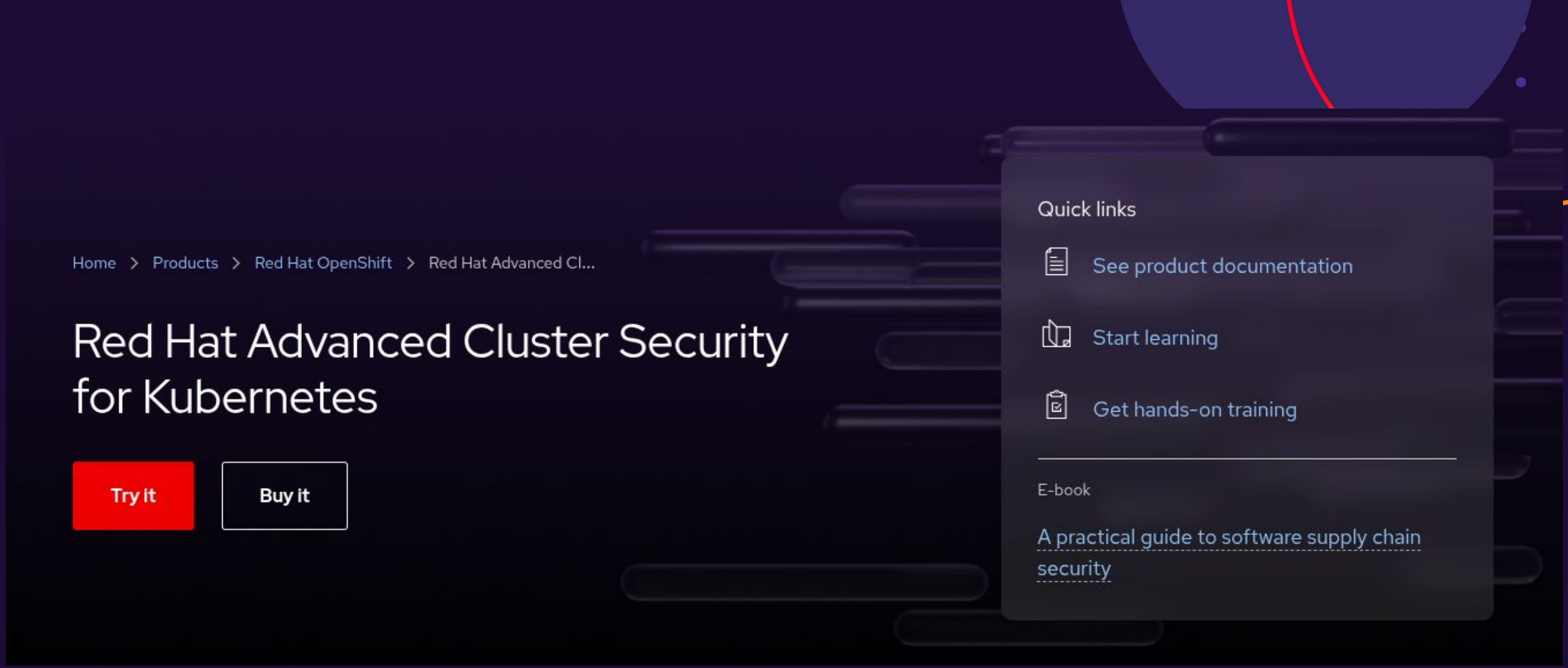


https://www.sigstore.dev/

Red Hat Trusted Artifact Signer

https://developers.redhat.com/products/trusted-artifact-signer

3. Guardrails



https://www.redhat.com/en/technologies/cloud-computing/openshift/advanced-cluster-security-kubernetes

Container built on developer laptop?


DEPLOYMENT
DENIED

Container signed with the key of another department?


DEPLOYMENT
DENIED

Container image built and signed by the trusted application pipeline?


DEPLOYMENT
APPROVED

Fundamental Shift on our Security

Trust
but Verify

Verify,
then
Trust


TRANSPARENTIA
IDENTITAS
CLAUSTRA

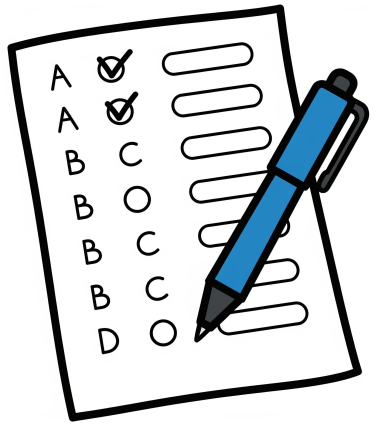
Act 3

The Architecture of the Factory Floor

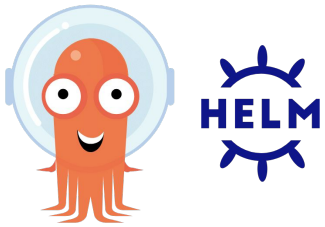

SOFTWARE BILL OF MATERIALS
CRYPPTORAPIC SIGNING
TESTING
BUILD
SHIPPED
SHIPPED

git

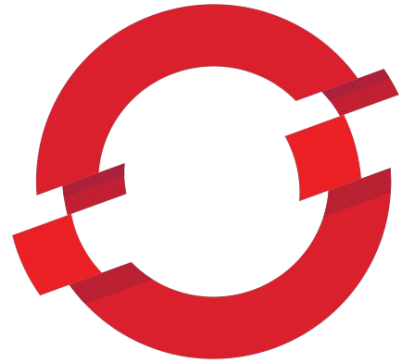
TEKTON



Red Hat
Trusted
Artifact Signer



HELM



OPENSHIFT

```
$ podman build -t quay.io/developer/some-image .
$ podman push quay.io/developer/some-image

$ oc new-app quay.io/developer/some-image
```

Conclusion

Trust.

Security

≠

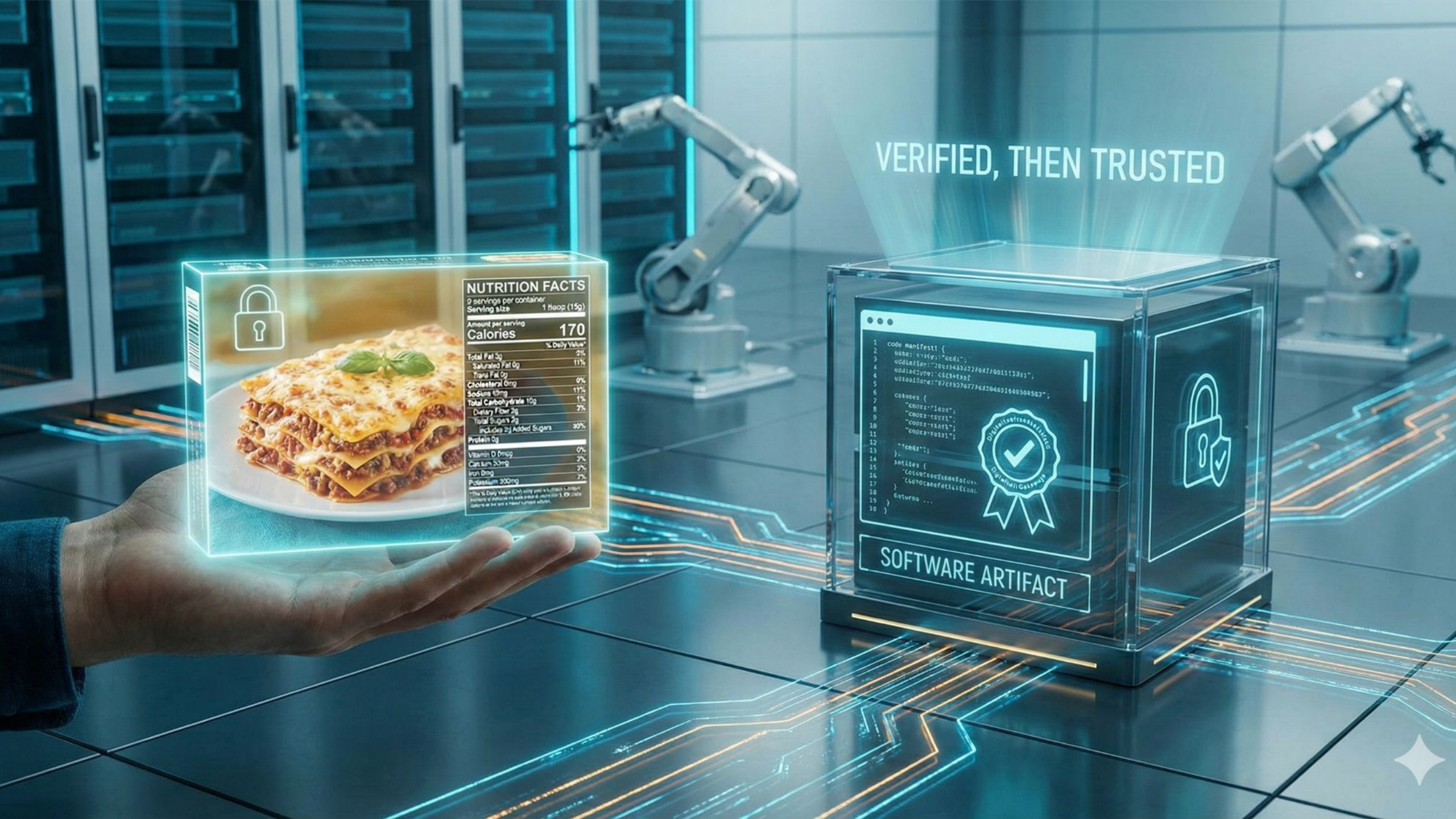
"Department of No"

Trusted Software Supply Chain


TRANSPARENTIA
IDENTITAS
CLAUSTRA

Secure way == Easiest way

Sovereignty


VERIFIED, THEN TRUSTED
NUTRITION FACTS
2 servings per container
Serving size 1 Heap (15g)
Amount per serving
Calories 170
% Daily Value*
Total Fat 3g 2%
Saturated Fat 0g 11%
Trans Fat 0g
Cholesterol 0mg 0%
Sodium 43mg 11%
Total Carbohydrate 10g 1%
Dietary Fiber 2g 5%
Total Sugars 2g
Includes 2g Added Sugars 30%
Protein 0g
Vitamin D 0mcg 0%
Calcium 30mg 3%
Iron 0mg 3%
Potassium 300mg 2%
SOFTWARE ARTIFACT

Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat