



**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



Act 1

# The "Black Box" Problem









**Nutrition**  
**Bollet vana 2'9**

**Yong 29**

**Bitte anfordern**

Component	Weight %
Base Polymer	100.00
Resin	10.00
Hardener	10.00
Filler	10.00
Colorant	10.00
UV Stabilizer	10.00
Flame Retardant	10.00
Antioxidant	10.00
Plasticizer	10.00
Thermal Stabilizer	10.00
Processing Aids	10.00
Other Additives	10.00

### INGREDIENTS

[illegible]

**DINA MOTE ALSTETAL**

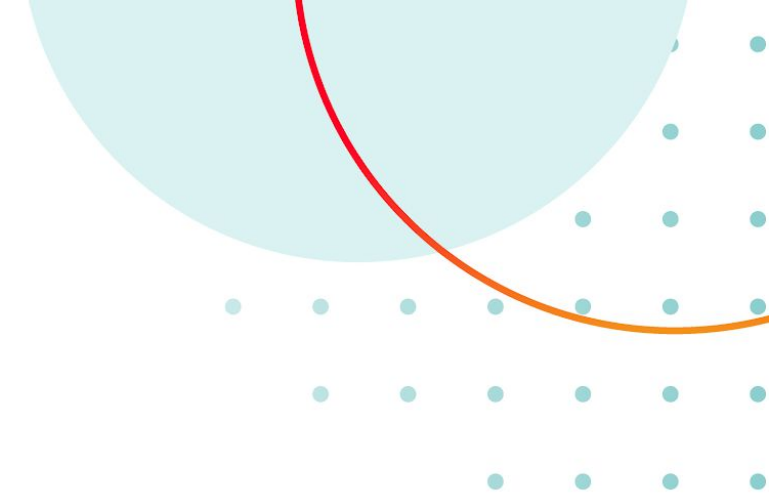
Paragon Performance  
Performance Contrast

**CHIRBIDA RALLABADI**

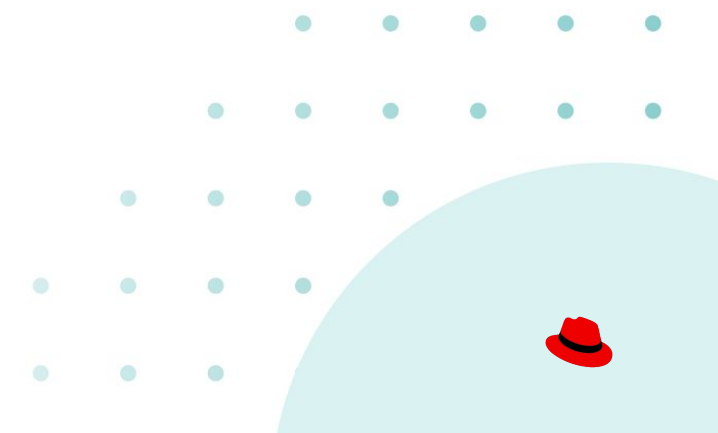
Canada's largest  
Pulse, Soybean, Corn, Wheat, Barley, Oats, Rye, and  
Canola. We are the leading processor of these crops in  
Canada and the United States. We are also a leading  
exporter of these crops to the United States and  
other countries.

The image shows a document page with a large, dark, irregular stain or smudge covering a significant portion of the right side. The visible text on the left is printed in a non-Latin script, likely Cyrillic, and appears to be a list or index of items. The text is arranged in several columns, with some lines appearing to be numbered or bulleted. The overall appearance suggests a historical or archival document that has been damaged by water or other liquid.



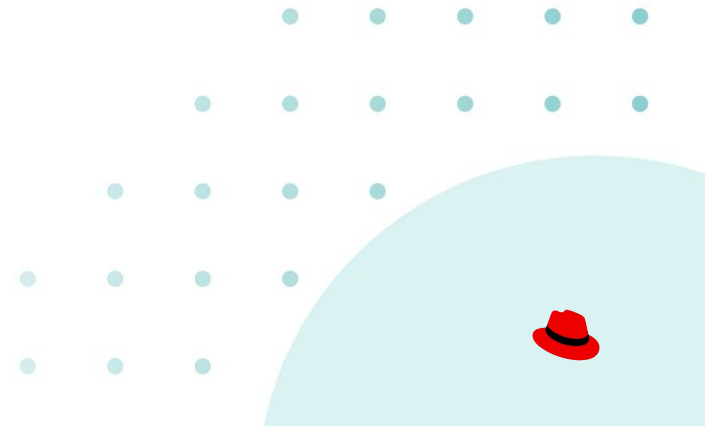


Software is assembled,  
not written

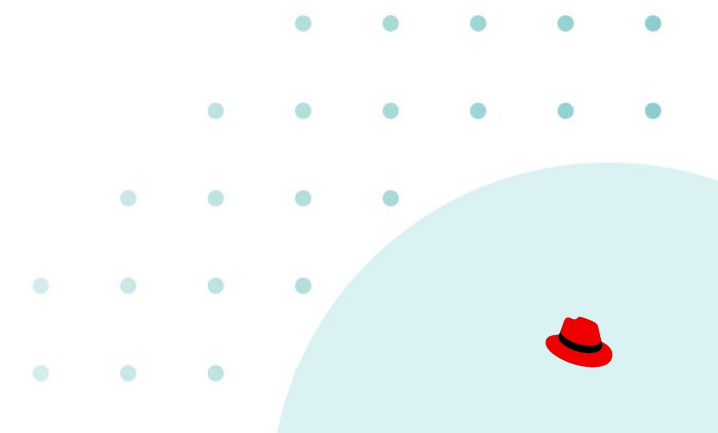




Log4j



# SolarWinds







Do you know what is running in  
your infrastructure?





We need the digital equivalent  
of a nutrition label



Act 2

# The Three Pillars





The image shows three large, weathered stone pillars standing in a grassy field under a clear blue sky. Each pillar has a Latin word inscribed on its front face. The pillars are made of light-colored stone with visible cracks and some discoloration. The background features a flat landscape with scattered rocks and a distant horizon line.

TRANSPARENTIA

IDENTITAS

CLAUSTRA

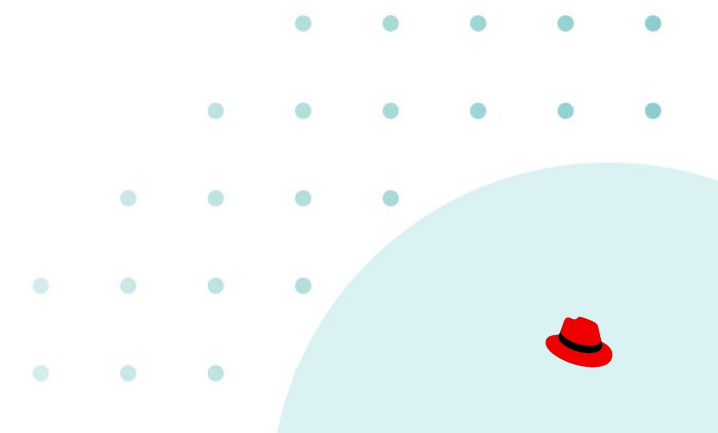




# Transparency, Identity, and Guardrails



# 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>



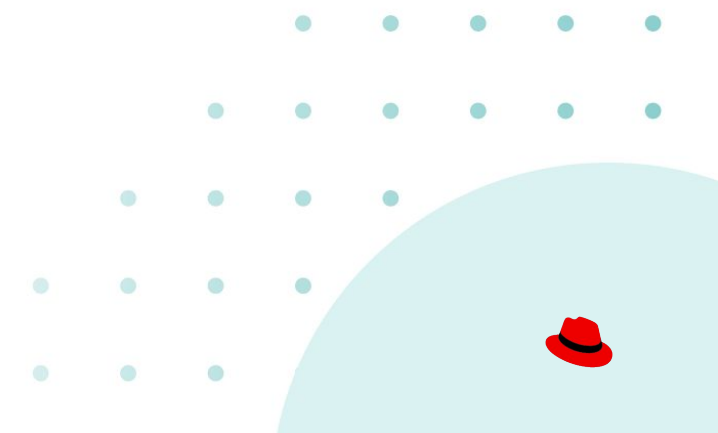
```

},
"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"
      }
    ]
  }
]

```



## 2. Identity











UNSIGNED

ERROR 404!

Cryptofail!

Cryptofail! .....

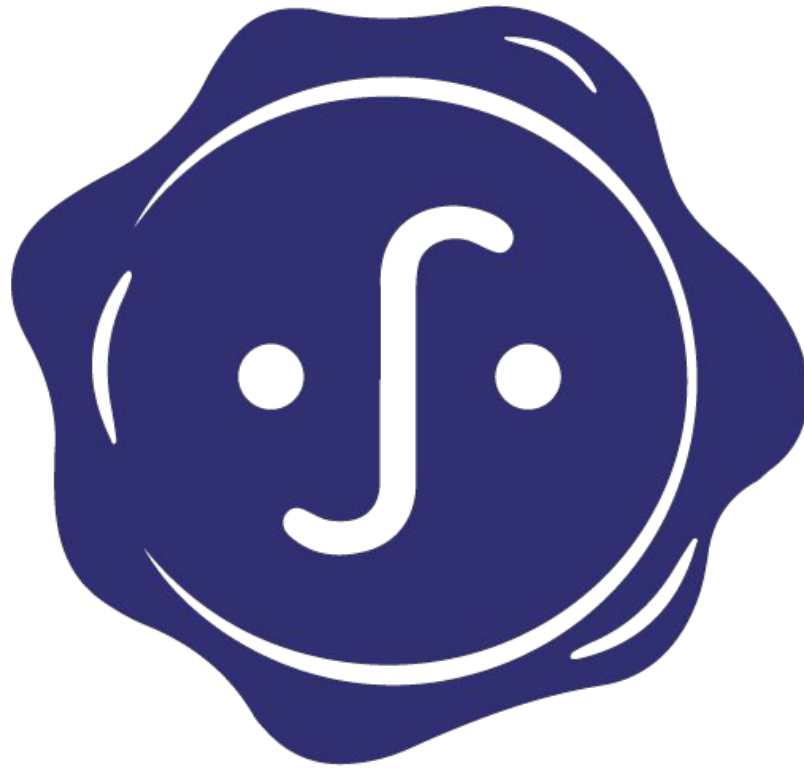
//s\\

Signature not found!

///o/\\

#/1//





<https://www.sigstore.dev/>



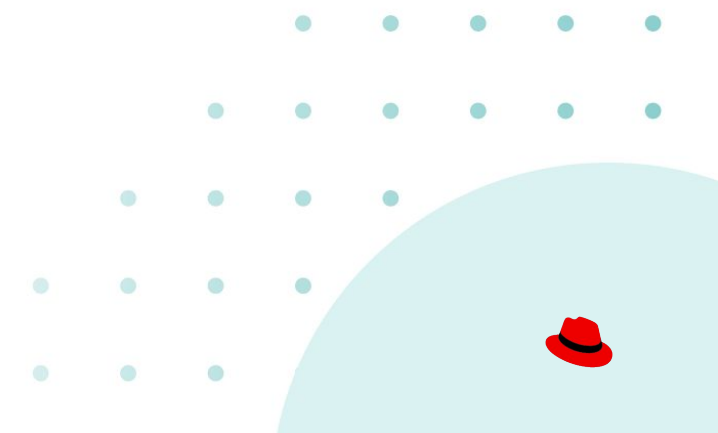


# Red Hat Trusted Artifact Signer

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



# 3. Guardrails





[Home](#) > [Products](#) > [Red Hat OpenShift](#) > [Red Hat Advanced Cl...](#)

# Red Hat Advanced Cluster Security for Kubernetes

Try it

Buy it

## Quick links



[See product documentation](#)



[Start learning](#)



[Get hands-on training](#)

---

## E-book

[A practical guide to software supply chain security](#)

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





Container built on developer  
laptop?



**DEPLOYMENT  
DENIED**





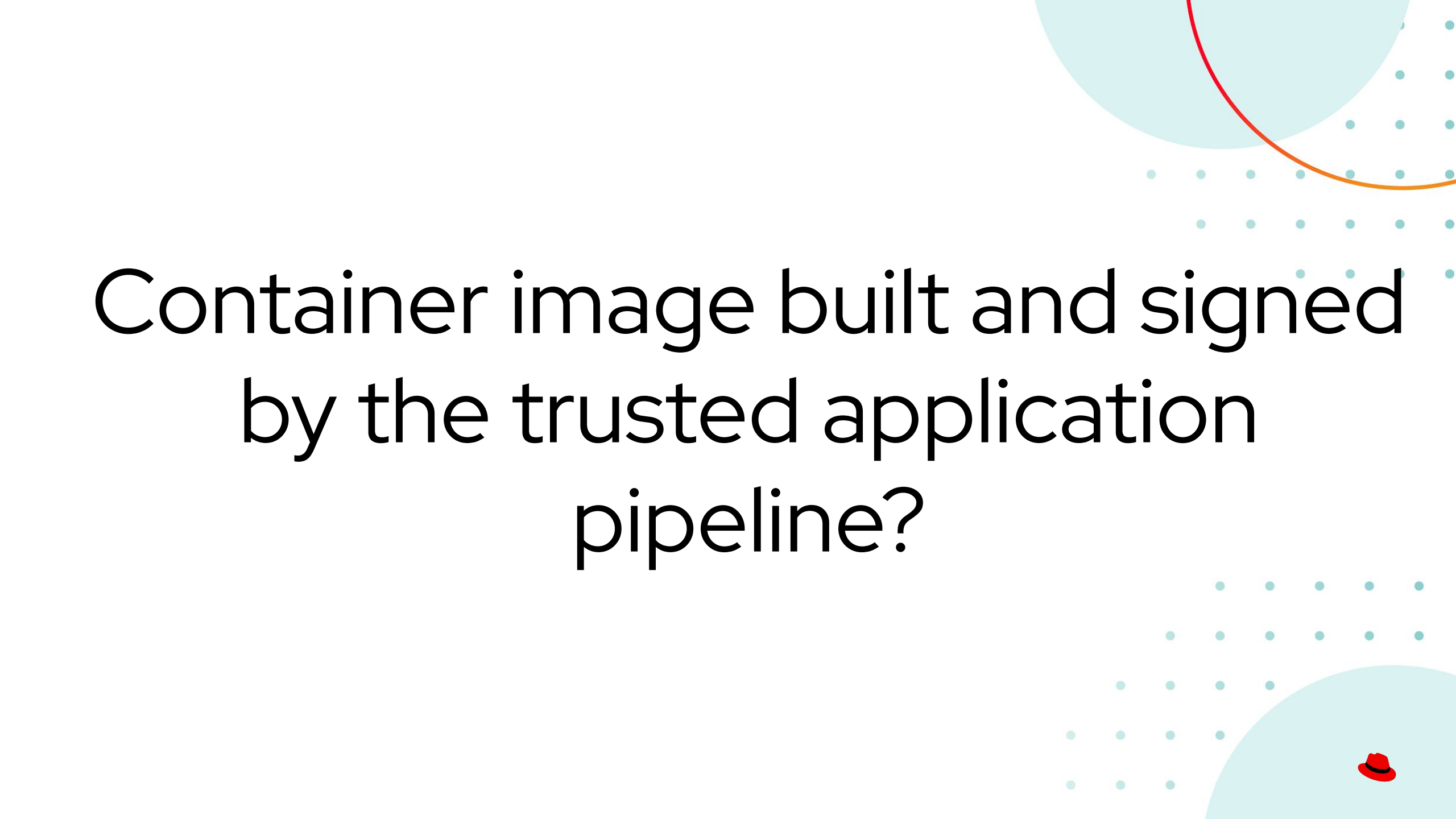
Container signed with the key of  
another department?



**DEPLOYMENT  
DENIED**





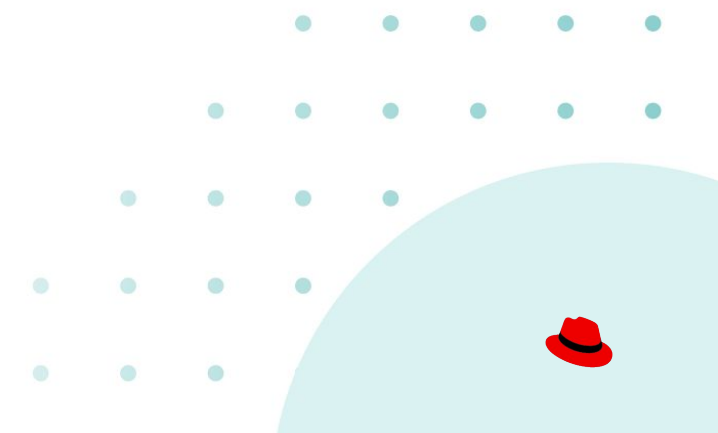


Container image built and signed  
by the trusted application  
pipeline?

**DEPLOYMENT  
APPROVED**



# Fundamental Shift on our Security



Trust  
but Verify

Verify,  
then  
Trust







TRANSPARENTIA

The image shows three large, weathered stone pillars standing in a grassy field under a sunset sky. Each pillar has a Latin word carved into its face. The pillars are made of light-colored stone with visible cracks and textures. The background features a horizon line with distant hills and scattered rocks in the field.

IDENTITAS

CLAUSTRA



# The Architecture of the Factory Floor





BUILD



CRYPTTORAPIC  
SIGNING  
TESTING

SOFTWARE BILL  
OF MATERIALS

SHIPPED





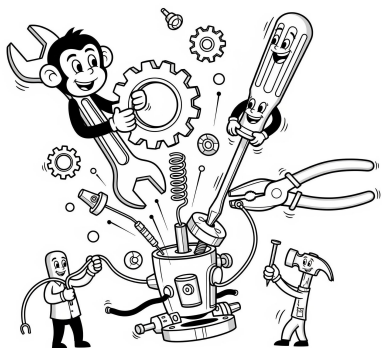
git



**TEKTON**

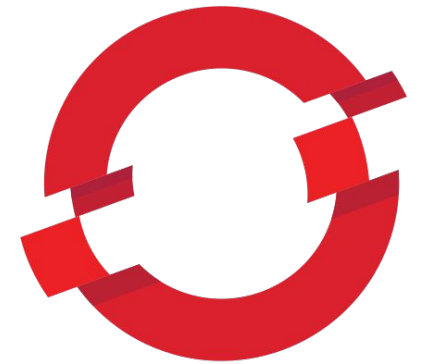
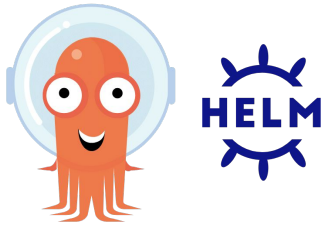






 **Red Hat**  
Trusted  
Artifact Signer

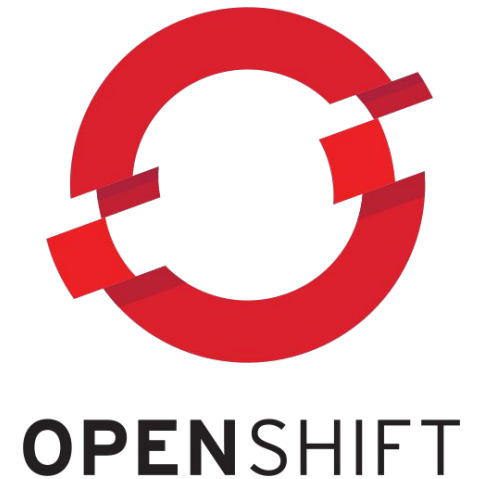




**OPENSIFT**



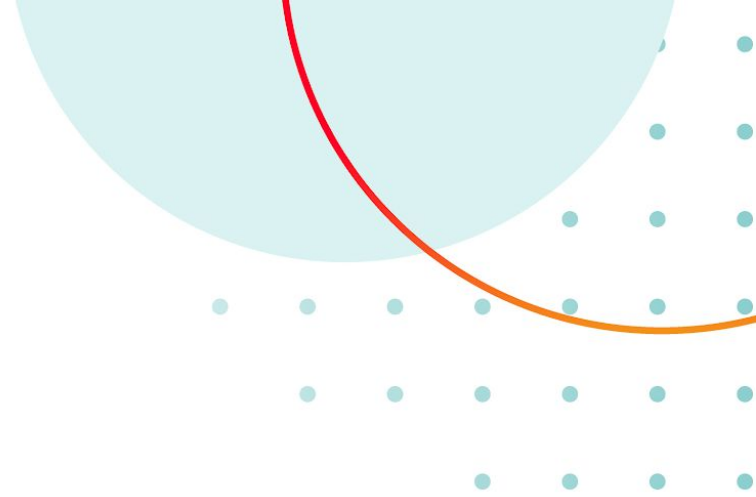
\$ podman build -t quay.io/developer/some-image .  
\$ podman push quay.io/developer/some-image  
\$ oc new-app quay.io/developer/some-image



# Conclusion



Trust.







Security

≠

“Department of No”





# Trusted Software Supply Chain





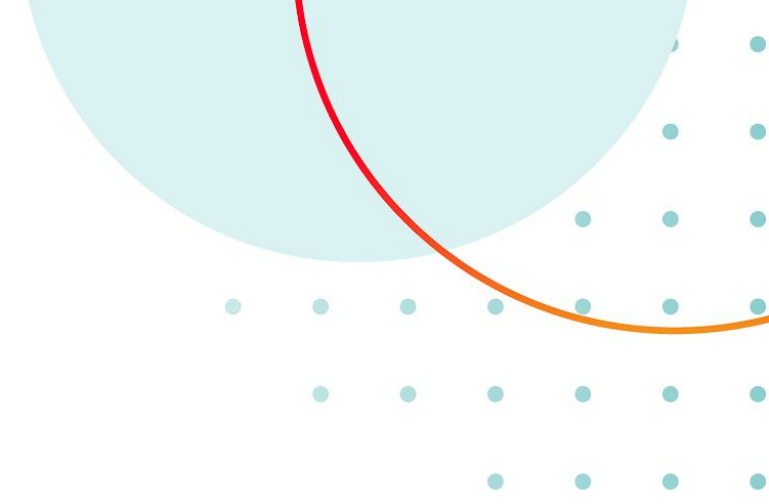
The image shows three large, weathered stone pillars standing in a grassy field under a sunset sky. Each pillar has a Latin word carved into its face. The pillars are made of light-colored stone with visible cracks and textures. The background features a horizon line with distant hills and scattered rocks.

TRANSPARENTIA

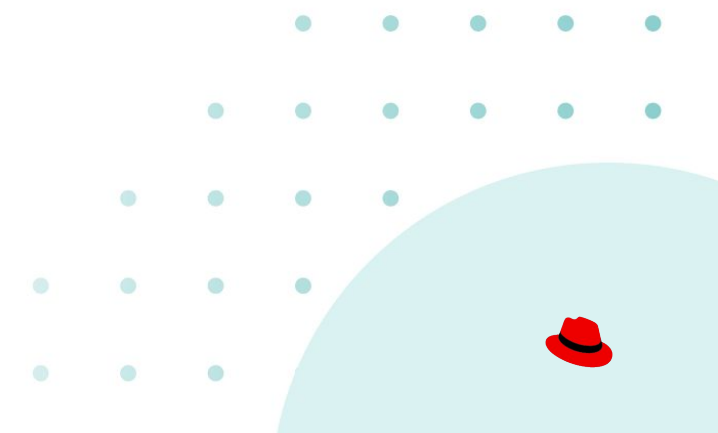
IDENTITAS

CLAUSTRA





Secure way == Easiest way



# Sovereignty





## VERIFIED, THEN TRUSTED





Connect

# Thank you



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[twitter.com/RedHat](https://twitter.com/RedHat)

