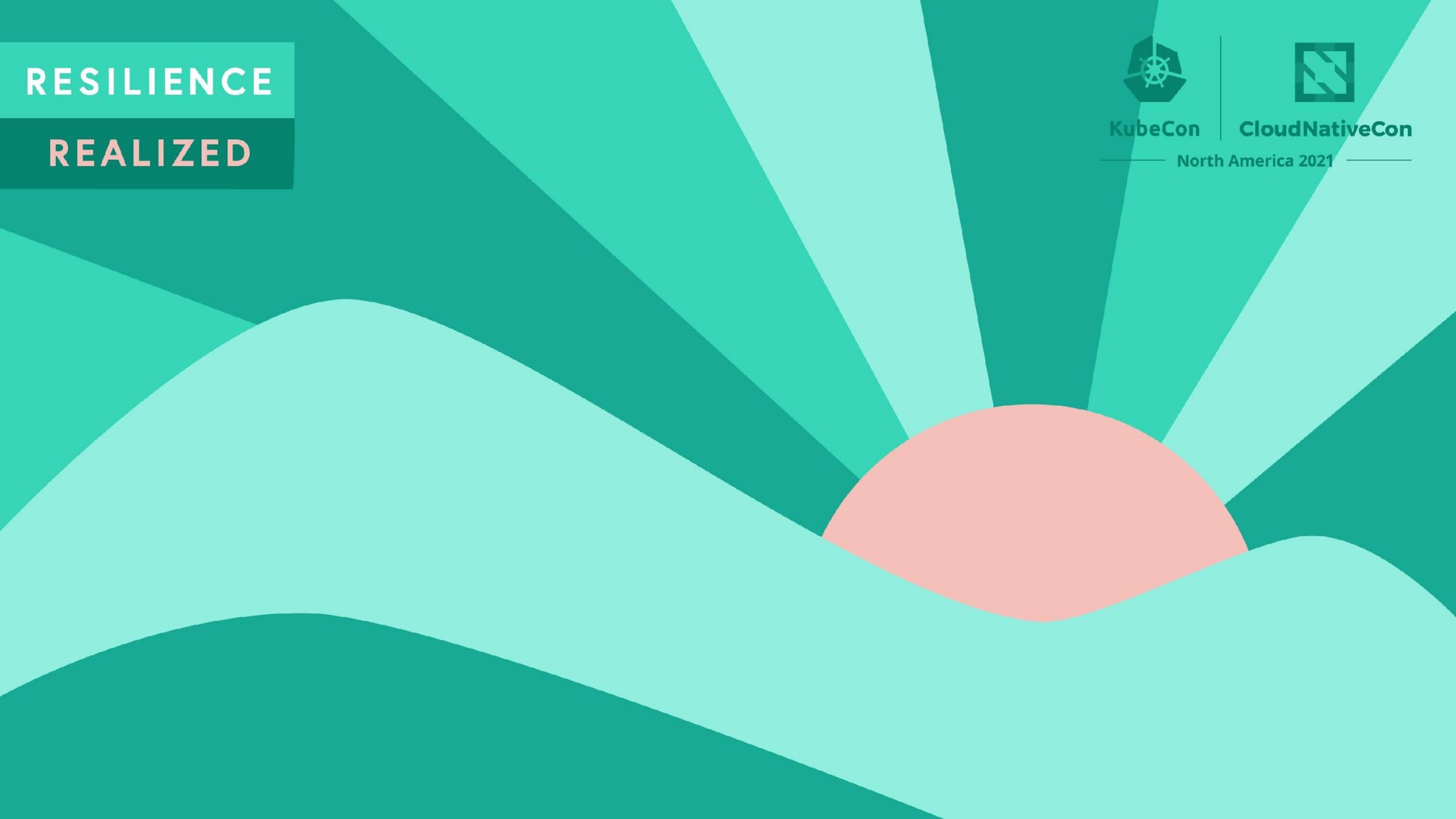


RESILIENCE
REALIZED

KubeCon | CloudNativeCon
North America 2021

KubeCon | CloudNativeCon

North America 2021

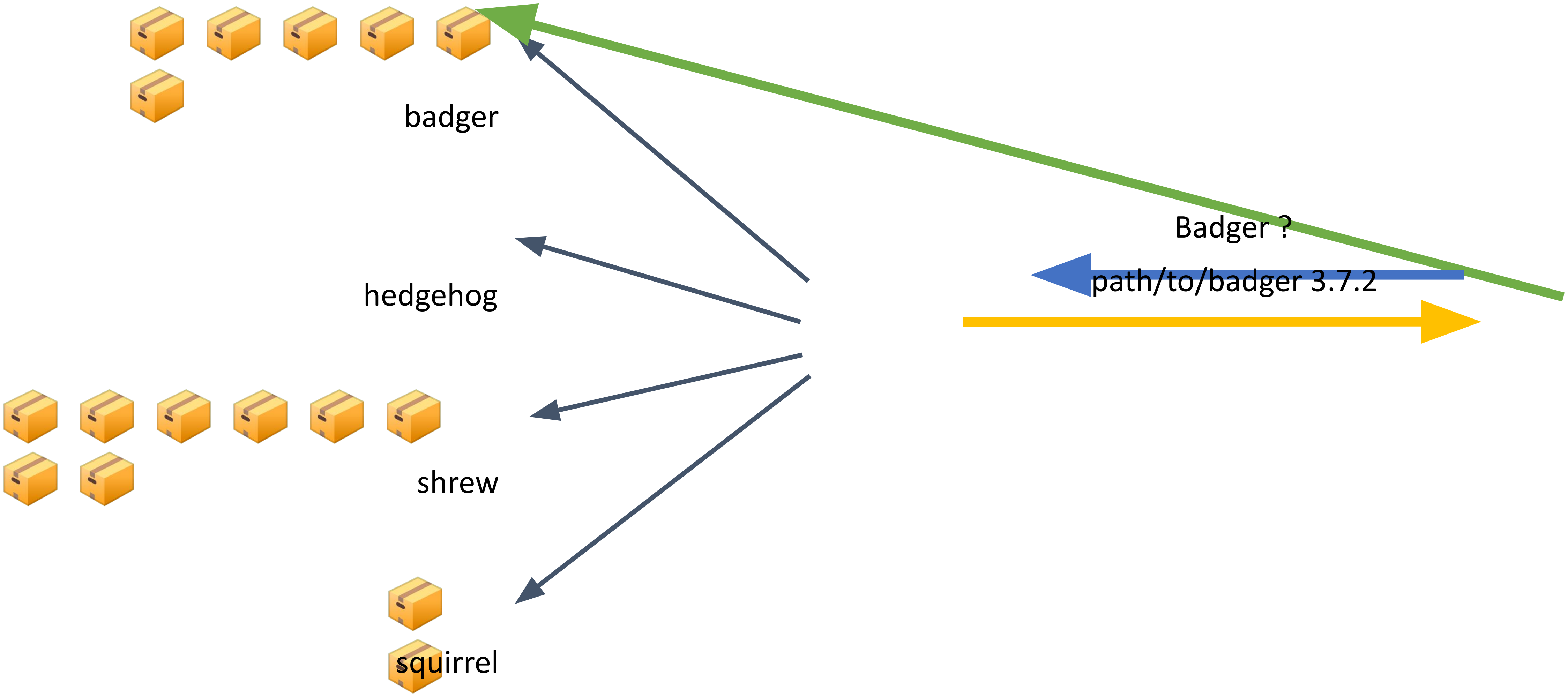
RESILIENCE REALIZED

Securing Content Repositories with The Update Framework (TUF)

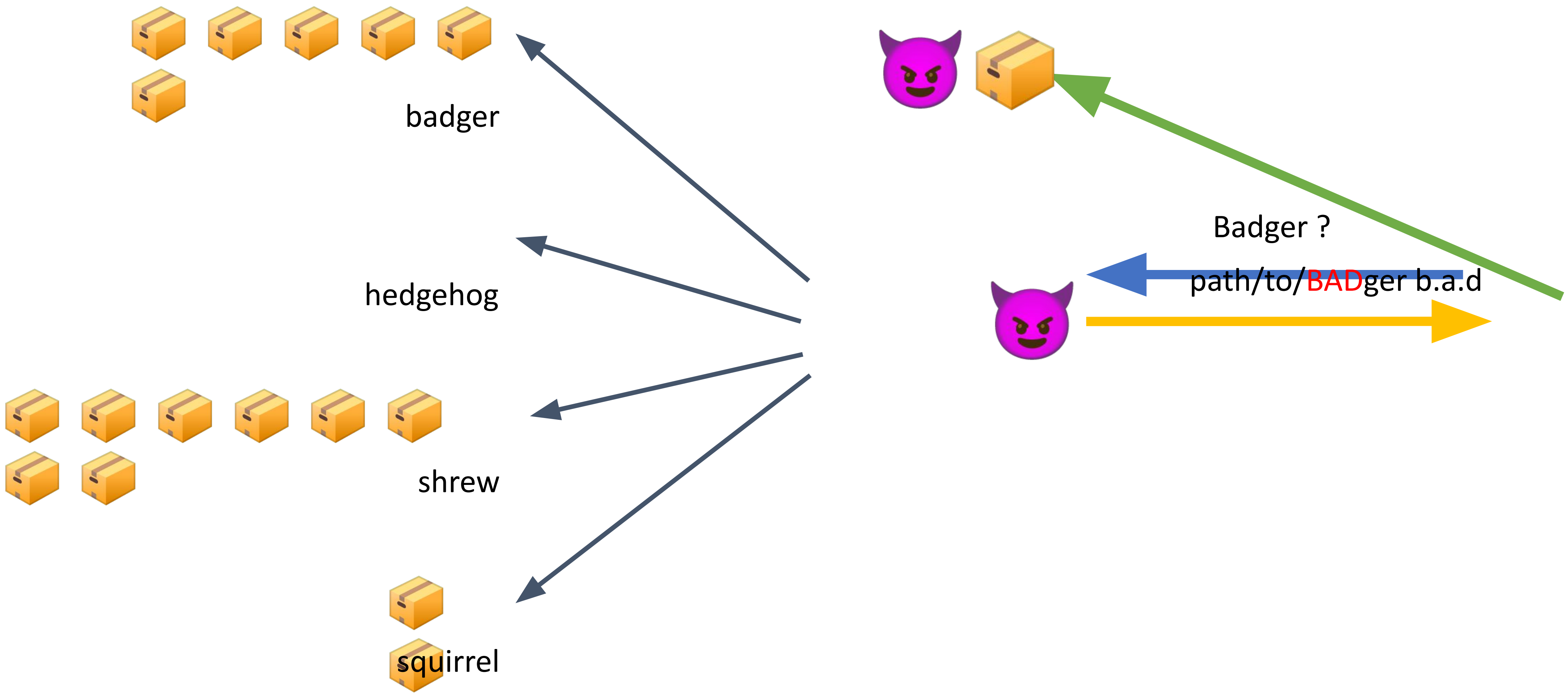
Marina Moore (NYU)
Joshua Lock (VMware)

What are content repositories?

Content repositories



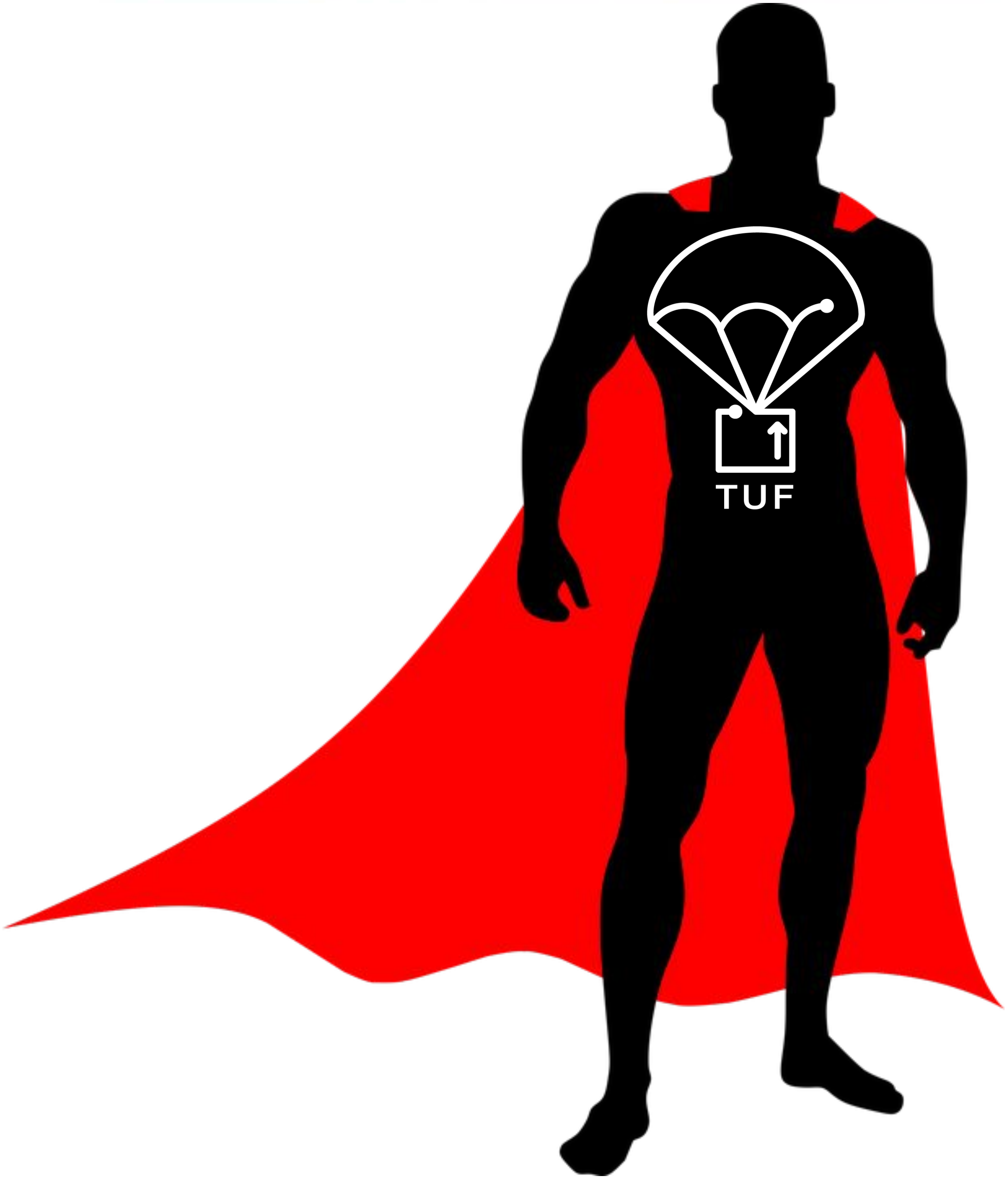
What might go wrong?



It has gone wrong...

Adobe
Opera
APACHE
HTTP SERVER PROJECT
Windows
php
pear
"PHP Extension and Application Repository"
CCleaner
debian
RubyGems
source forge
FreeBSD
Linux Mint
from freedom came elegance
FOSSHUB
Linux

The Update Framework (TUF)



- Protect **freshness**, **consistency**, and **integrity**
- Reduce **impact** of compromise
- Allow **recovery**

TUF Project

📃 Specification – describes the framework including metadata formats and workflows.

🚰 Enhancement process (TAPs) – process for peer-reviewed and tested changes to the specification.

👷‍♀️🏗️ Reference implementation – Python implementation symbiotic with the specification.

TUF Deployments

Adopted	WIP	Derived	Adapted
Bottlerocket OS	PyPI	Uptane / IEEE-ISTO 6100.1.0.0	Conda
DataDog	Drupal (php-tuf)		F-Droid
Fleet DM	TYPO3 (php-tuf)		Guix
Foundries.io	Mamba / CondaForge		Hackage
Fuchsia			OPAM
Sigstore			
Notary			

What’s brewing?

- TUF documentation clarity
  - Additional supplementary documentation
- Notary v2 collaboration
  - TUF on registries
- Sigstore collaborations
  - Fulcio + TUF TAP
  - TUF root of trust in Sigstore
  - Trust delegations
- PyPI integration
- Reference implementation refactor
- Dead Simple Signing Envelope (DSSE)

Developer key management

- New TAP that integrates Sigstore’s Fulcio project into TUF
- Short-lived certificates for developers
  - Do not need to be securely stored for a long time
- TUF delegates to the Fulcio identity
  - Using OIDC

Notary v2 ∩ TUF

- The Notary v2 project’s tuf-notary subproject
- Storing TUF metadata on registries
- Some additions to TUF
  - Scaling snapshot metadata
  - Client-side selection of Targets metadata
  - Signing digests

Integrations

- PyPI: Warehouse integration of PEP 458 almost complete
- Conda Forge/Mamba
- Drupal & TYPO-3: php-tuf
- Sigstore

Implementation Updates

- Python-tuf refactor
- Go-tuf delegations, work toward specification 1.0.0 compliance
- Uptane 1.2 release, working toward 2.0.0
- Fuchsia’s implementation shipped on first-gen Nest Hubs
- Php-tuf initial implementation

Ways to contribute

- Participate in open source integrations and implementations
- Contribute to the specification
  - Improving spec approachability
  - TAPs for new features
- Ask us questions
  - TUF mailing list
  - On the CNCF slack
  - On github

Acknowledgements and Thanks

Thank you to:

- TUF maintainers
- Maintainers, contributors of all subprojects, implementations

Questions

marinamoore@nyu.edu
@mnm678 on Github
@marinanmoore on Twitter

jlock@vmware.com
@joshuagl on GitHub
@hi_joshuagl on Twitter