Red Hat Summit

Connect

Productive by default, secure by design

OpenShift's latest innovations

Torbjörn Dahlén Martin Östmark Magnus Eklund

Key challenges

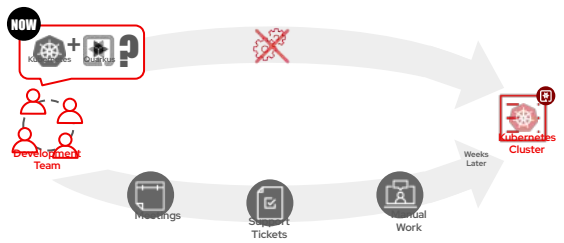
Developer productivity is negatively impacted by “technology overload” and lack of a Self-Service experience

Applying **security** best practices is perceived as complex and is applied, if at all, in the end

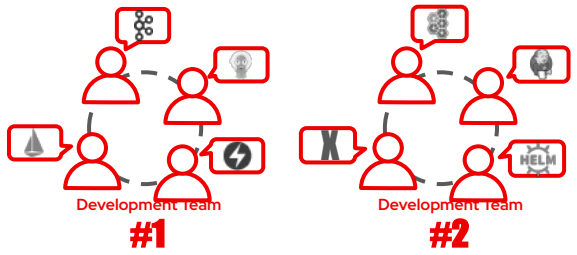
Providing **identity** and trust for workloads across **hybrid** and **multi-cloud** environments

#1 Developer productivity

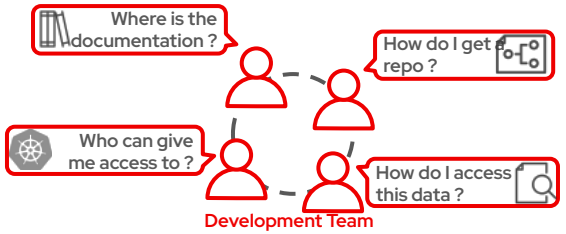
Challenges in the Software Development Lifecycle



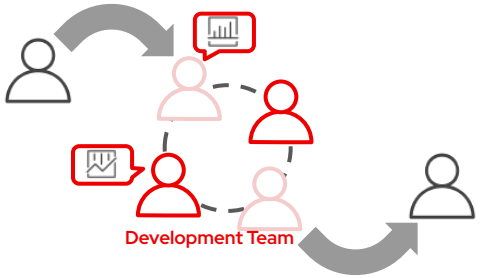
Lack of Self-Service



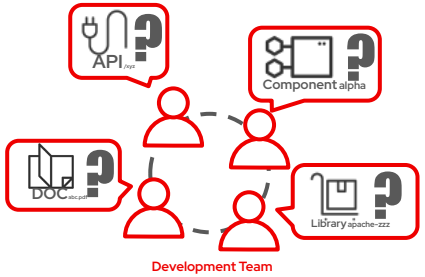
Lack of Standardization



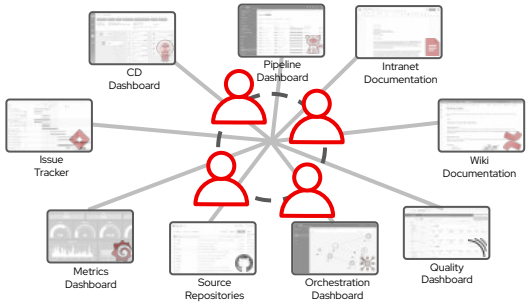
Siloed Knowledge



Onboarding/Departure Chaos



Difficulty Discovery of Development Resources



Too Many Dashboards

52m

Average time spent by developers coding each day

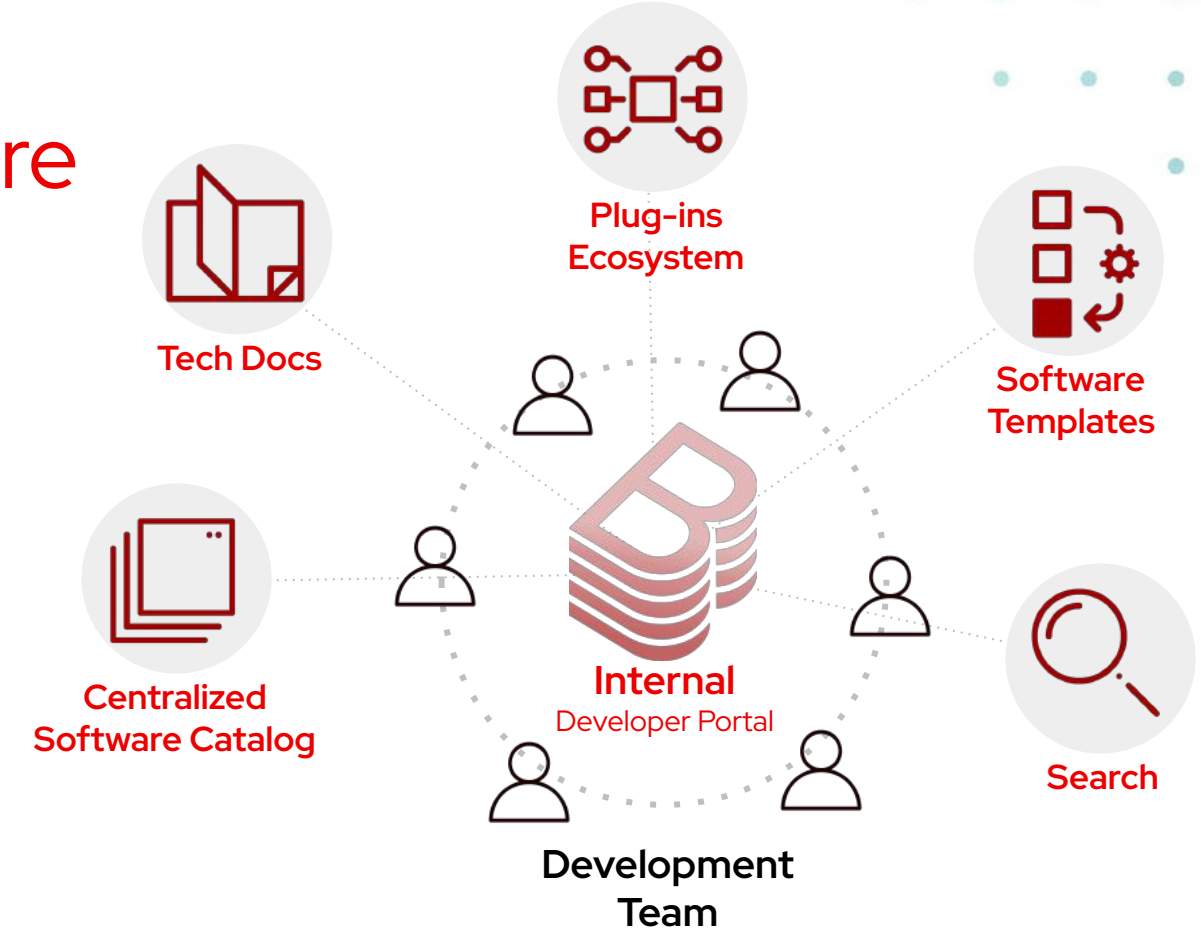
76%

of organizations say the cognitive load is so high that it is a source of low productivity

Source: Salesforce

Internal Developer Portal = one frontend for your entire infrastructure

Unifies all your tooling, services, apps, data, and docs with **a single and consistent UI**



Red Hat Developer Hub

Red Hat Plug-ins for Backstage

Includes **supported plugin bundle**

- Authentication and Authorization with Keycloak
- GitOps with Argo CD
- Pipelines with Tekton
- Application Topology for Kubernetes
- Container Image Registry for Quay
- Multi Cluster View with Open Cluster Manager (OCM)

Integrates with industry standards and technologies through a broad ecosystem of community plugins.

GitLab, git, Jenkins, sonarqube, argo, MANY MORE

Based on Backstage, an open source platform for building developer portals.

Backstage

Red Hat Developer Hub - **supported when deployed on**

Customer-managed Red Hat OpenShift	Managed Red Hat OpenShift services	Managed Kubernetes Services
Red Hat OpenShift Platform Plus Red Hat OpenShift Container Platform Red Hat OpenShift Kubernetes Engine	IBM Cloud, aws, Azure, Google Cloud	EKS, AKS, GKE

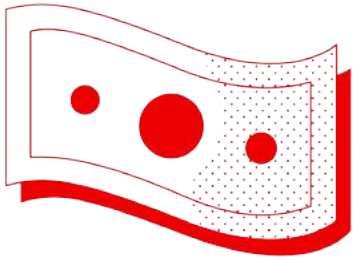
Single pane of glass to increase engineering productivity.

Self-service with guardrails for cloud-native development.

Best practices with GitOps and automation.

Customer Success Story

Red Hat worked with a financial services company to build an IDP to simplify application development



Reduced application onboarding time from **2 weeks → 10 minutes**

Challenge

The current onboarding of users, applications and infrastructure as a service is slow and inefficient.

Solution

Engaged Red Hat to build an IDP in order to simplify the application development experience for faster innovation.

Results

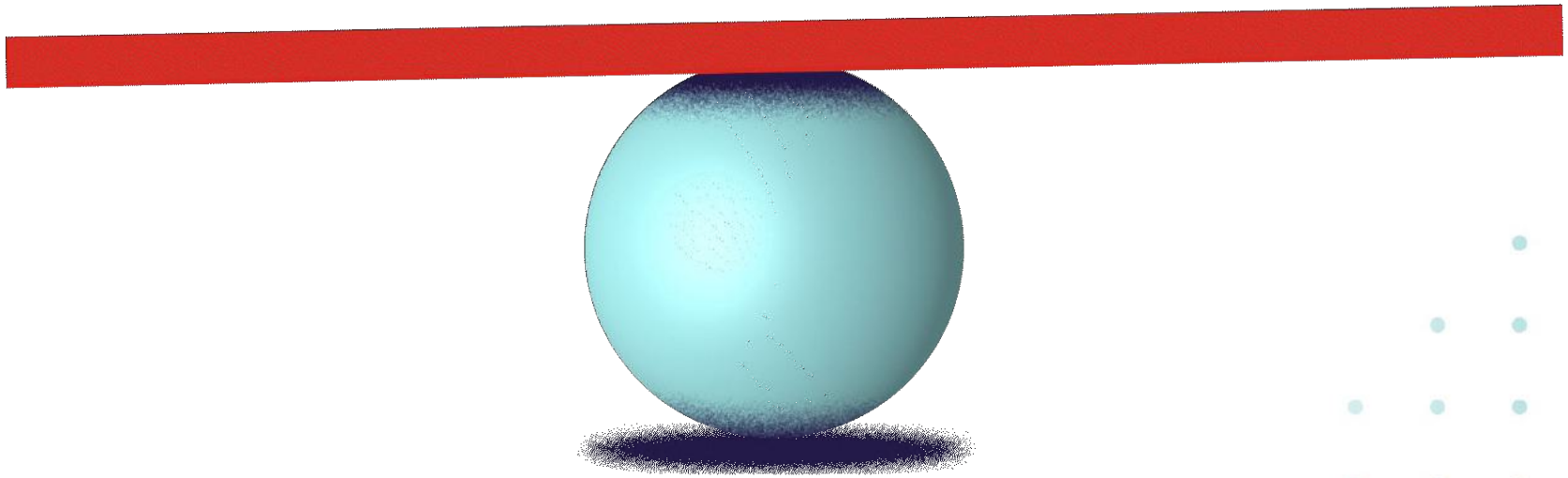
- Reduced application onboarding time from **2 weeks to 10 minutes**
- Average time to release went from **51 days down to 12.5 days**
- **Better compliance** with organizational governance models

#2 Security

The Challenge: Balancing Productivity & Security

Productivity & Innovation

Security



Software Supply Chain Security

Software Supply Chain Security

6 out of 7

project vulnerabilities come from transitive dependencies

742%

Average **annual increase in software supply chain attacks** over the past three years. **45%** of organizations will experience attacks. **Is a matter of when, not if.**

90%

of components in modern applications utilize open source software

Source: Sonatype

The Supply Chain Security space is relatively young

Leading to Increased regulations, frameworks and directives

"The Cyber Resilience Act is the first ever EU-wide legislation of its kind. It introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software/.../throughout its lifecycle"

Government Cybersecurity Regulations
Cybersecurity Agency Frameworks and Directives
DevSecOps movement

2019
ENISA

2022
DORA

2023
NIS2

2024
CRA

2024
AI Act

[1] SEC Final Rule - Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

Trusted Software Supply Chain

Platform engineer for security and compliance

Provenance

Understanding the composition, vulnerabilities and origin of software content

Integrity

Apply and verify digital signatures to container images and software artifacts

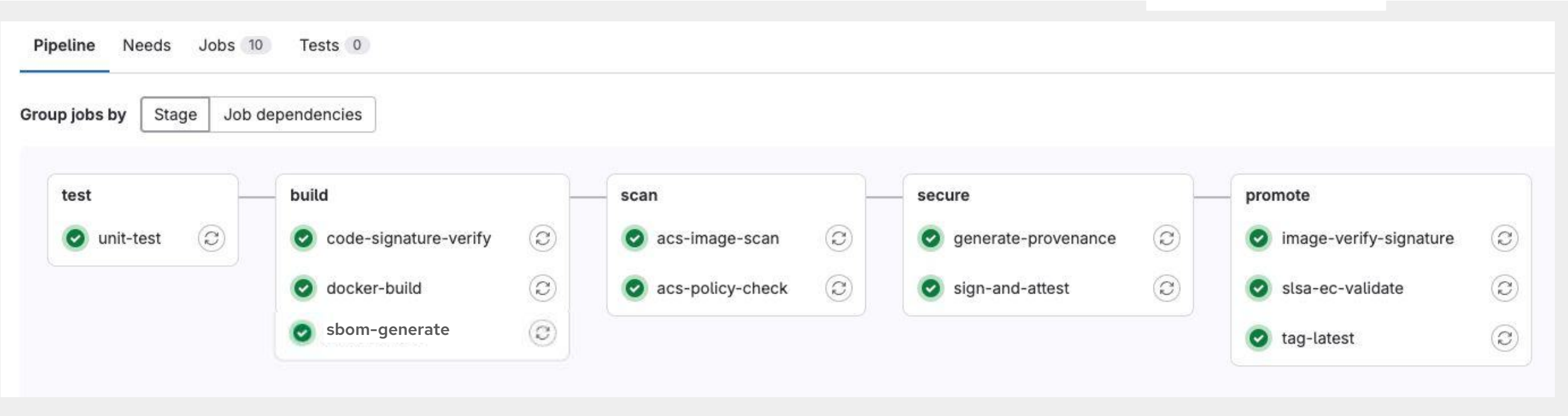
Controls

Restriction of software usage that does not meet defined compliance levels

From Code Commit to Runtime Enforcement - integrating all the moving parts

Stitching it together

Code app	Build app	Deploy app	Run app
Identify dependencies, vulnerabilities, recommend actions Sign code on git commit. Signing events stored in tamper-proof ledger for verification	Only build from signed and verified source code Sign the built artifact Run vulnerability scanning Create SBOMs during build Sign test results from automated testing frameworks	Validate compliance - Policy-based image scanning (no log4j), Policy-based deployment scanning (limits) Verification of artifact promotion across environments Signature checks before deploy	Ensure policy compliance across clusters Detect and respond to runtime threats with risk assessments Analyze CVE impact through SBOM:s Identify suspicious behaviour



Developer Hub

OpenShift

Trusted Profile Analyzer

Trusted Artifact Signer

Advanced Cluster Security

Red Hat Summit

Red Hat Advanced Developer Suite

INCLUDED PRODUCTS

IDP: Internal Developer Portal

Red Hat Developer Hub

Trusted Software Supply Chain

Red Hat Trusted Artifact Signer

Red Hat Trusted Profile Analyzer

COMPLEMENTARY TECHNOLOGIES

AI/Kube Developer Desktop Experience : **Podman Desktop**

Development Tools

IDE Plugins

Red Hat OpenShift Dev Spaces

Migration Toolkits

AI Enablement

Developer Lightspeed

Podman Desktop AI Lab

Red Hat Developer Hub AI Integration

Products and related technologies that allow developers to **quickly and securely deliver applications to production**

Enabling platform engineers to more easily enforce operational controls and compliance across hybrid multi-cloud environments

#3 Multi-Cloud Workload Identity

Challenge

Scaling workload identities across heterogeneous environments

Container orchestrators, and cloud computing have led to production environments that are **increasingly dynamic and heterogeneous**.

Conventional security practices (e.g. Kubernetes Service Accounts, Long lived API tokens) **struggle to scale under this complexity**.

Goal

Enable defense in depth

Provide strongly attested identities to reduce the likelihood of breach through credential comprise.

Reduce operational complexity

Consistent, automated management of identity reduces the burden of devops teams.

Simplify Interoperability

Simplify the technical aspects of full interoperability across multiple stacks.

CLOUD NATIVE COMPUTING FOUNDATION

spiffe

- Common identity format
- Specification on how workloads securely obtain identity

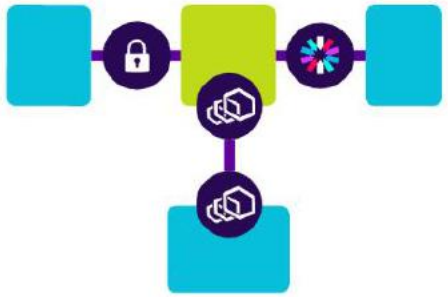
SPIRE

- Implementation of SPIFFE
- Organization-wide management of SPIFFEE identities and identity attestation
- Issuance/rotation of identity tokens
- Single point of federation with OIDC discovery

tornjak

- Control plane for SPIRE
- Visibility & management for workload identities
- Together with Kubernetes registrar, provides Universal Workload Identity

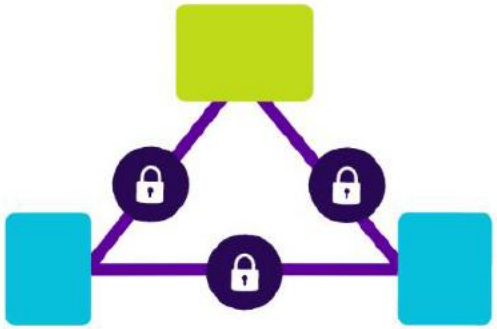
Key Use Cases



Secure microservices communication automatically with Envoy, X.509 PKI, or JWT

Authenticate securely to common databases or platforms without passwords or API keys

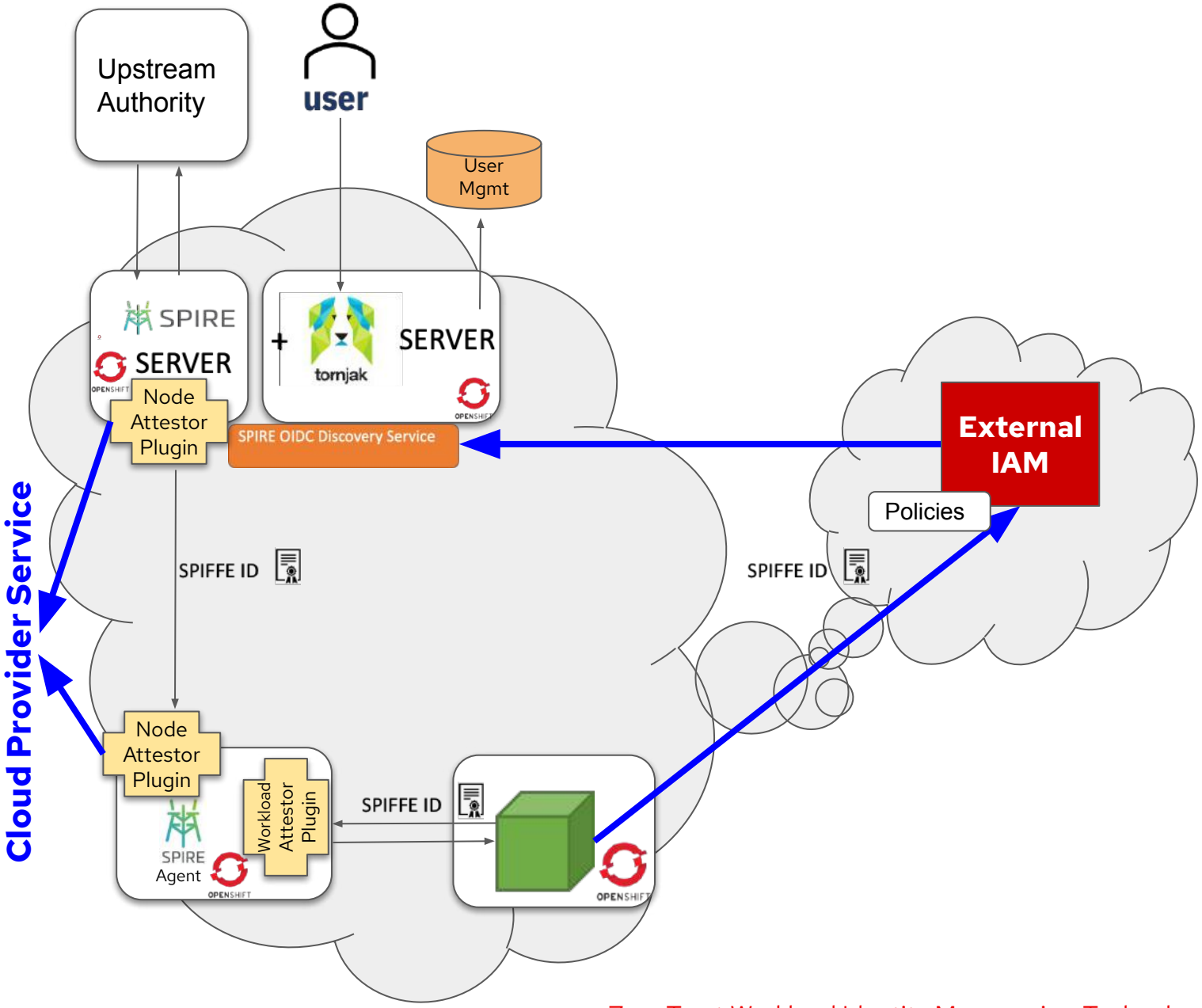
Build, bridge, and extend service mesh across organizations without sharing keys



Cross-service authentication for zero trust security model

Bridging the gap between Kubernetes and other platforms

Red Hat Zero Trust Workload Identity Manager



Multi-factor authentication for workloads - identities provided after node and workload attestation.

- Operator Lifecycle Management for ease of deploying SPIFFE/SPIRE on OpenShift as a Day-2 Operator.
- Includes OIDC plugin that federates with OIDC Identity Providers.
- Validated against HashiCorp Vault and Microsoft Entra ID OIDC
- SPIRE Controller Manager for automatic workload registration on OpenShift clusters.
- Metrics support for SPIRE Server and Agent
- Custom Resources for
  - SpireServer
  - SpireAgent
  - SpireCSIDriver
  - SpireOIDCDiscoveryProvider

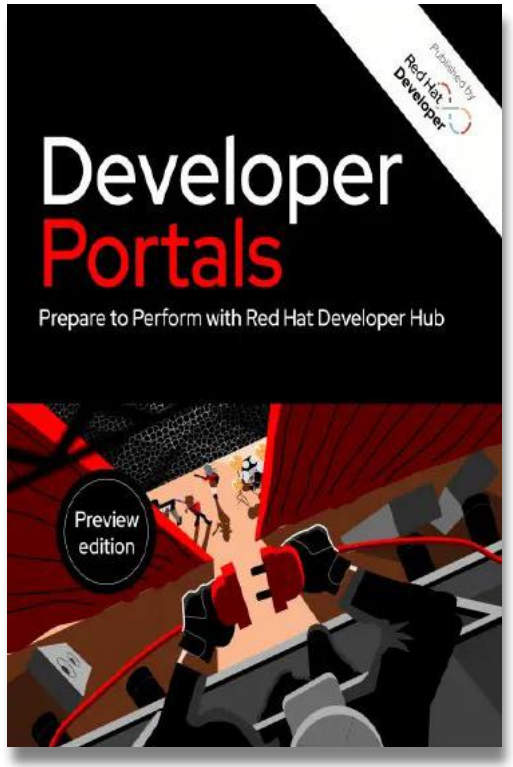
Zero Trust Workload Identity Manager is a Technology Preview feature only

Key takeaways

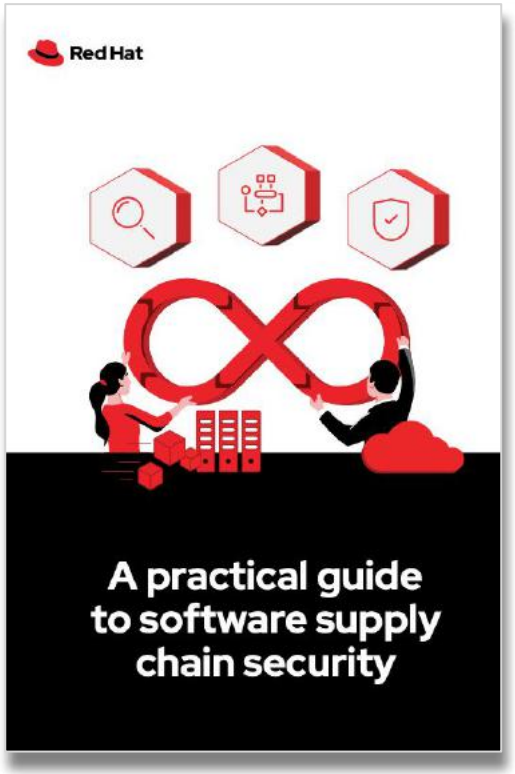
Key Takeaways

- Cognitive overload is affecting developer productivity negatively - Can be mitigated by templating, automation and information centralization
- An Internal Developer Portal enhances the Developer Experience and boost productivity - It unifies all your tooling, services, apps, data, and docs with a single and consistent UI
- Red Hat Developer Hub is an enterprise grade distribution of Backstage - an open source platform for building developer portals
- Software supply chain security is about trust -You need to know where software comes from, what's inside it, and whether it has been tampered with.
- Shift security left -Integrate scanning, signature & policy checks and signing directly into CI/CD to catch issues early.
- Security is continuous -Red Hat Trusted Artifact Signer, Trusted Profile Analyzer and Advanced Cluster Security can help secure your whole software delivery lifecycle
- Conventional security practices struggle to scale under the complexity of cloud and container production environments
- SPIFFE/SPIRE provide a uniform identity control plane across modern and heterogeneous infrastructure
- Red Hat Zero Trust Workload Identity Manager leverages SPIFFE and the SPIFFE Runtime Environment (SPIRE) to provide a comprehensive identity management solution for distributed systems

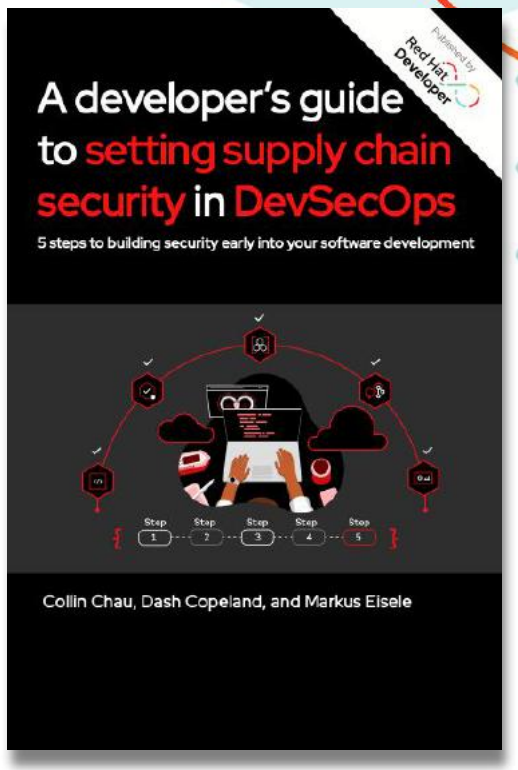
Free ebooks



https://red.ht/developer-hub-ebook



https://red.ht/supplychainsecurity-ebook



https://red.ht/devsecops-ebook

Zero trust workload identity manager now available in tech preview

May 19, 2025 | Anjali Telang | 3-minute read

Security Security automation

< Back to all posts

Non-human identities—also known as machine or workload identities—are becoming increasingly critical as organizations adopt cloud-native ecosystems and advanced AI workflows. For workloads spanning multiple cloud platforms, adhering to zero trust principles becomes challenging as they cross identity domains. A unified identity framework provides consistency in automating identity issuance and enforcing access control policies across diverse environments. SPIFFE/SPIRE, an open source identity issuance framework, enables organizations to implement centralized, scalable identity management on par with cloud platforms. This article will introduce the zero trust workload identity manager, an operator designed to bring SPIFFE/SPIRE capabilities to Red Hat OpenShift, empowering customers with security capabilities to manage workload identities across various cloud infrastructures.

See you at

Red Hat

Meet the Experts!

Red Hat Summit

Connect

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat