High Level Description

As software development complexity grows, **developers face increasing cognitive load, security risks, and inefficiencies** that slow down innovation. This proposal focuses on **enhancing developer efficiency and security** by implementing a **Trusted Application Pipeline**, which provides **automation, security guardrails, and self-service capabilities**.

Key Challenges Addressed

- **Onboarding Chaos & Standardization Issues** – Developers struggle with too many choices, lack of clear processes, and difficulty accessing necessary tools.
- **Cognitive Overload** – 76% of organizations report that high cognitive load negatively impacts developer productivity.
- **Software Supply Chain Risks** – With **742% increase in software supply chain attacks** over three years, securing the development lifecycle is critical.

Proposed Solution: Trusted Application Pipeline

A **developer self-service hub** with pre-integrated security features, enabling:

- **Standardized Best Practices** – Automating common tasks with **Golden Path Templates** to simplify workflows.
- **Security by Design** – Integrating **artifact signing, attestation, SBOM generation, and policy enforcement** across CI/CD pipelines.
- **Supply Chain Security** – Ensuring code originates from **trusted sources**, reducing vulnerabilities and compliance risks.

Key Benefits

- **Faster, Secure Software Delivery** – Automating security checks and standardizing workflows.
- **Reduced Risk & Compliance Burden** – Meeting regulatory requirements like **US EO 14017 & EU NIS 2**.
- **Improved Developer Experience** – Reducing overhead and enabling teams to focus on innovation.

Vision

By integrating **trusted security practices into every phase of software development**, organizations can **accelerate innovation while safeguarding user trust**.

EU-LISA Industry Roundtable: Building Better Government Software at Scale

Continuous Delivery with Security and Efficiency

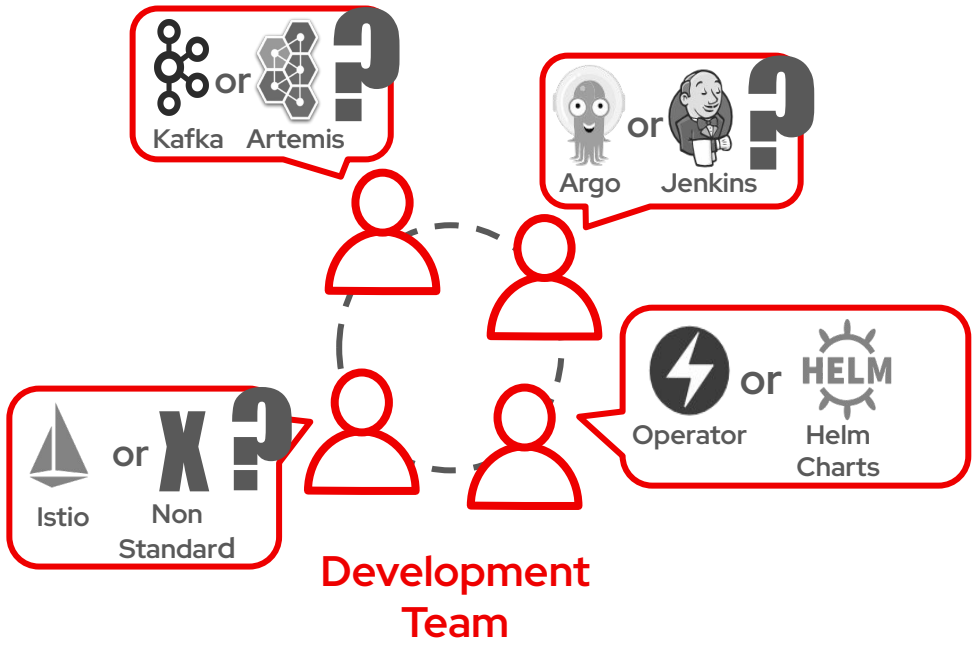
Mustafa Musaji
Principal Solution Architect - EMEA Enterprise Strategy - Public Sector

EU-LISA

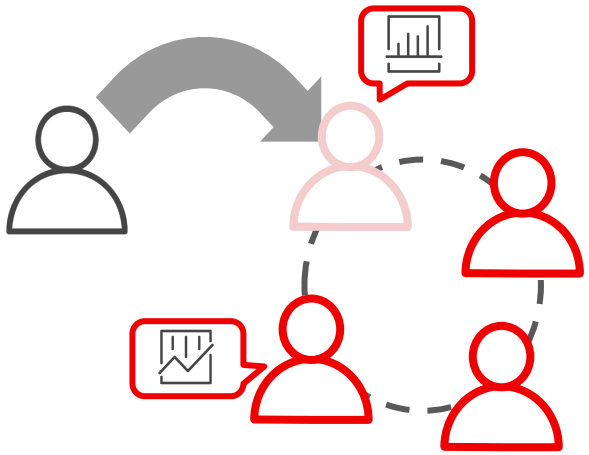
Red Hat

Development teams are under pressure

Analysis Paralysis - too many choices

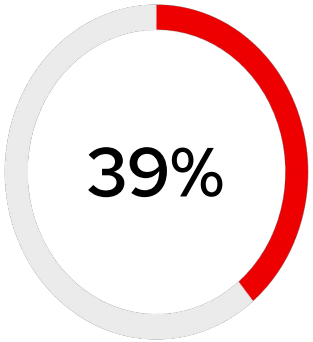


Onboarding Chaos

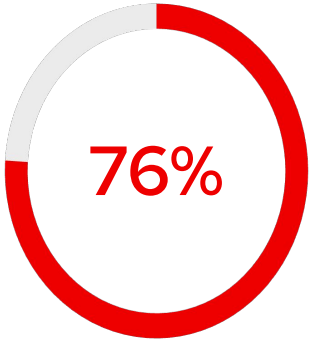


Lack of Standardization

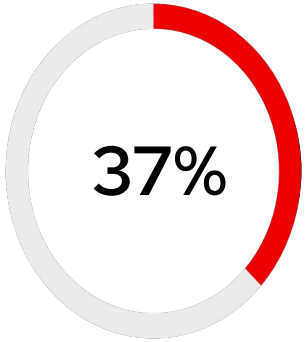
Impact of cognitive overload on productivity



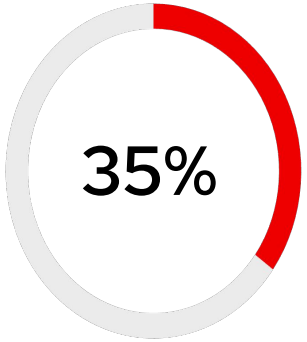
Increasing workload / demand from other teams leads to increased overhead.



More than three-quarters of organizations say the **cognitive load is high enough to negatively impact productivity.**[1]



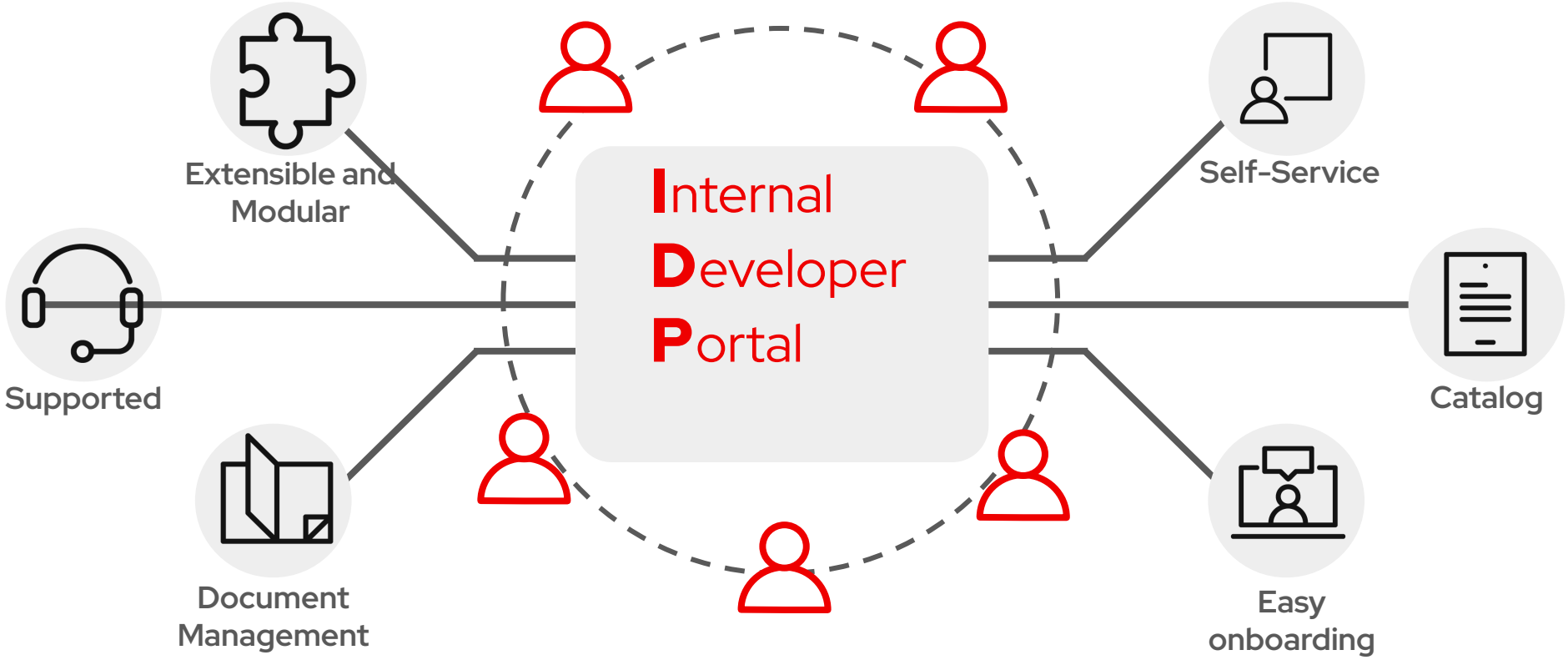
Adapting to the pressures of digital transformation is third biggest challenge.[1]



Learning skills to adapt to new technologies and approaches.[1]

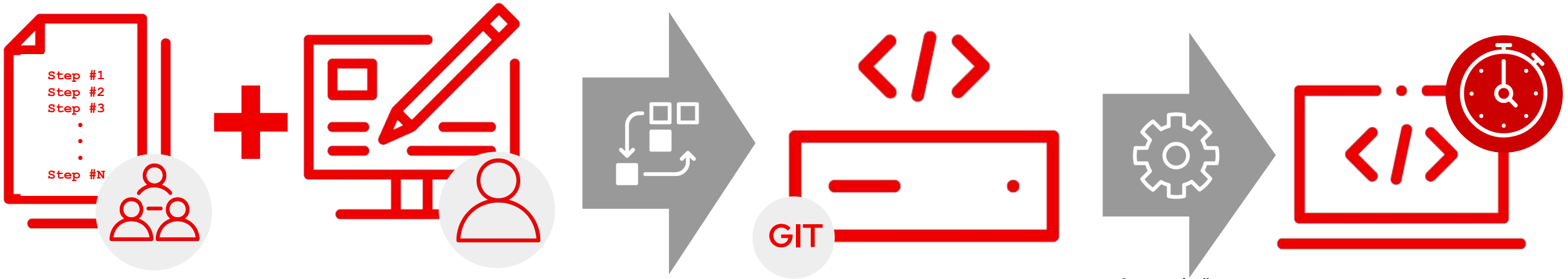
[1] Salesforce productivity survey

The solution is an Internal Developer Portal



Standardization with Golden Path Templates

Quickly spin up new projects with your organization's best **(security!)** practices



Development Team Best Practices

Leverages on existing practices and uses company's guidelines to automate the most common tasks

User fills out a form

Inputs all the necessary data related to this task in order to generate the desired outcome

Automatically created a new Git repository

Everything goes to a Git Repository the development team can working on

Everything done in a matter of minutes

Automatically created and provisioned following organization's guidelines

Securing the Software Supply Chain - **Why**?

That's why - if we don't build it right,

it will come back to haunt us!

Securing the Software Supply Chain - **Why**?

Software supply chain attacks: a matter of when, not if

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years [1]

45%

of organizations worldwide will experience supply chain attacks by 2025 [2]

1 in 5

data breaches are due to a software supply chain compromise [3]

71%

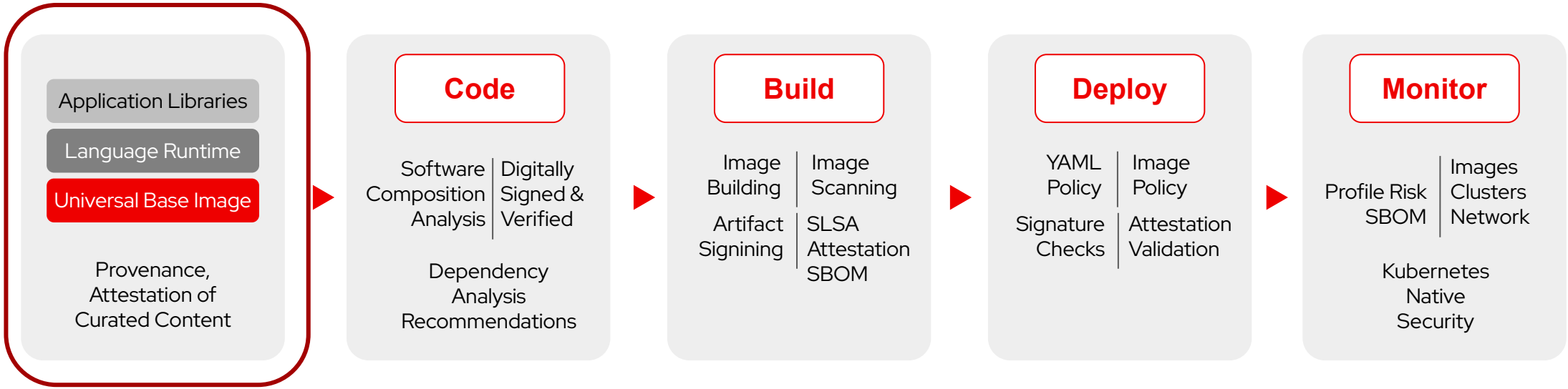
YoY increase in cost of average ransom payment [4]

[1] State of the Software Supply Chain | [2] Cost of a Data Breach 2022 - IBM Report | [3]State of Kubernetes Security Report 2022 - Red Hat Report | [4]State of Enterprise Open Source 2022 - Red Hat Report

Securing the Software Supply Chain - **Why**?

- US Executive Order on Improving the Nation's Cybersecurity
- US Executive Order 14017 - America's Supply Chains
- US Executive order 14018 Improving the Nation's Cybersecurity
- EU Network and Information Security 2 Directive
- Government willingness to enforce and fine executives ignoring SSC
  - SEC fines SolarWinds and CISO for concealing vulnerabilities
  - Log4J vulnerability

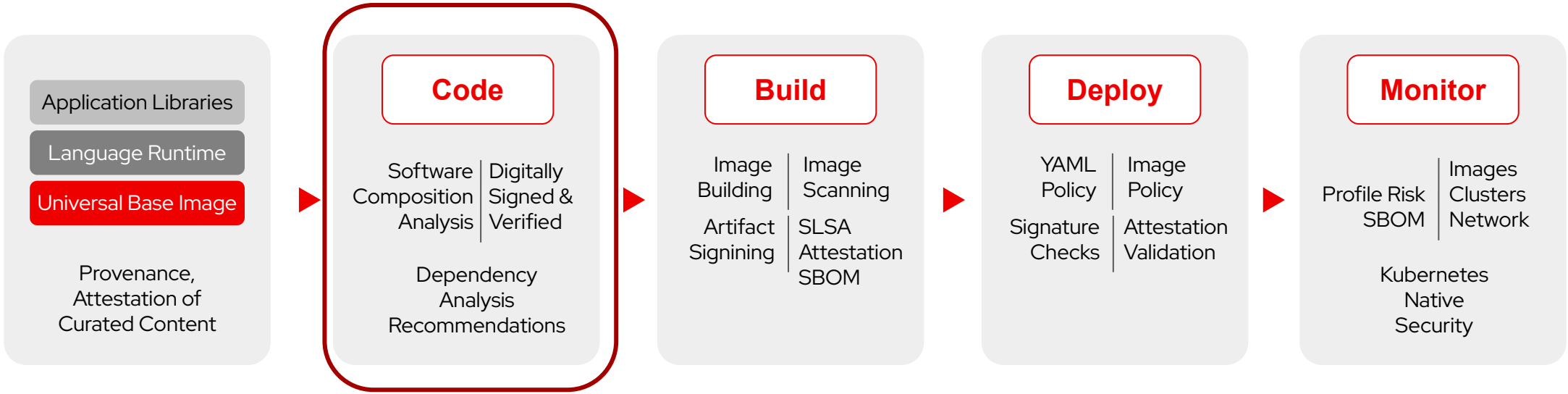
Securing the Software Supply Chain - **How**?



Start by using Trusted Content

- Your code should be based on trusted images, libraries and runtimes.

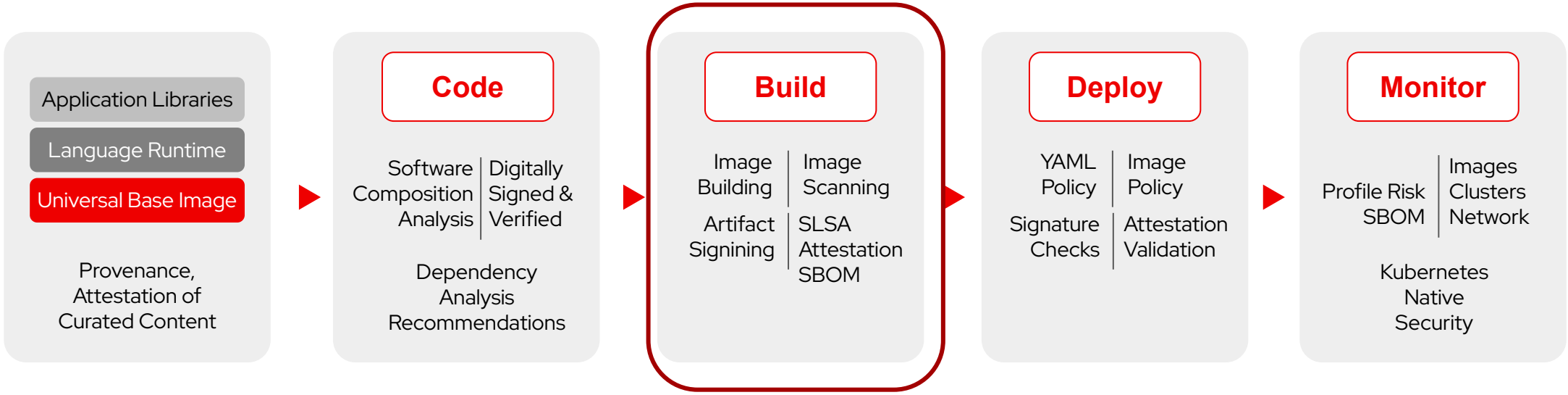
Securing the Software Supply Chain - **How**?



Give your developers the right tools

- Provide automated composition and dependency analysis.
- Make signing any component simple, without cumbersome additional steps.
- Provide developers with curated templates (based on trusted content) to create new components.

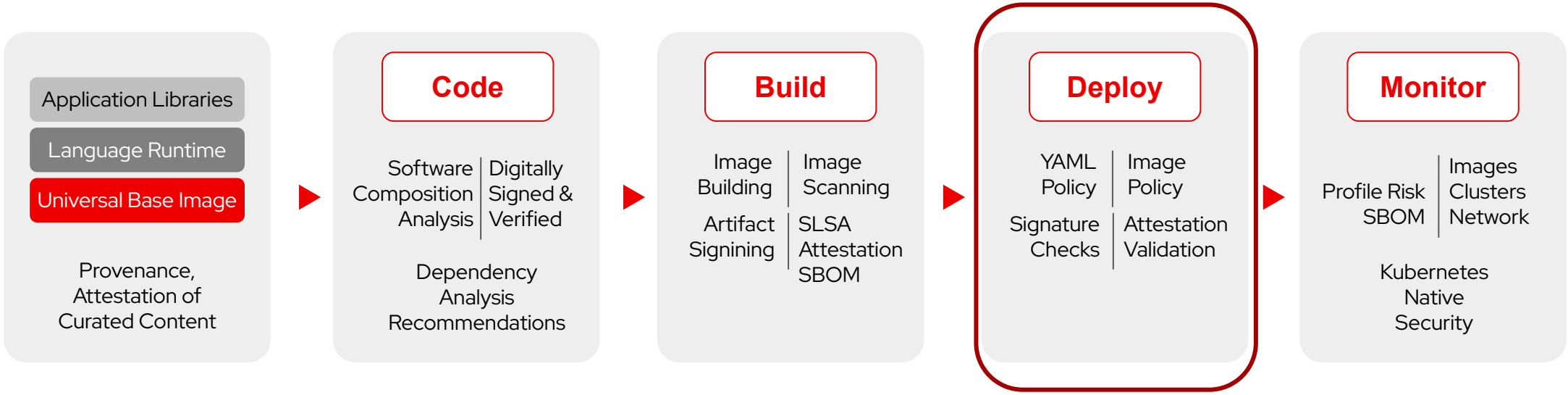
Securing the Software Supply Chain - **How**?



Augment and secure your build process (CI)

- Only build from signed and verified source code.
- Only use signed and verified images.
- Include vulnerability scanning and policy enforcement.
- Create SBOMs in the build process so you know what is used.
- Attest the integrity of your artifacts and build pipelines Supply Chain Levels for Software Artifacts (SLSA)

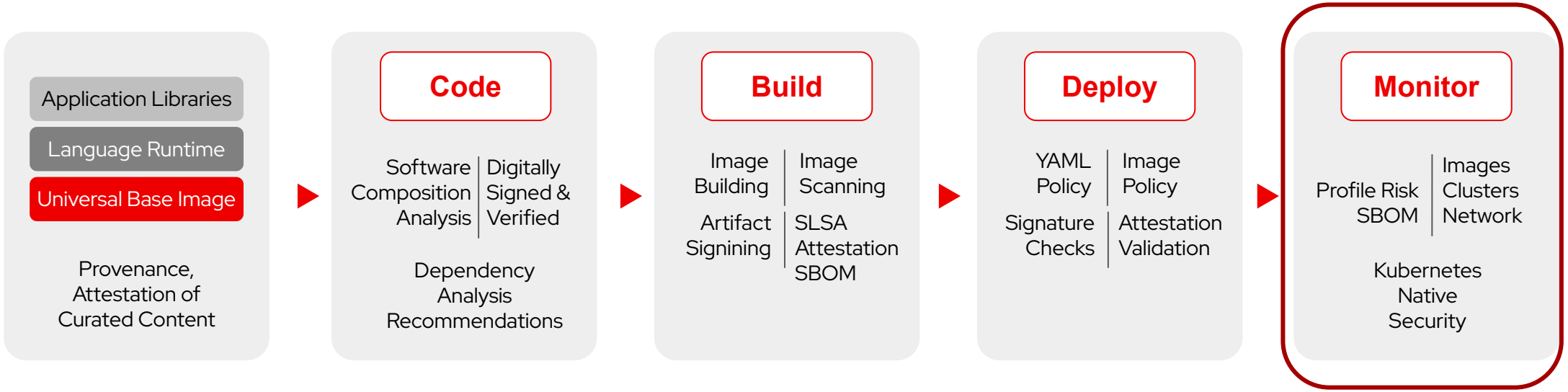
Securing the Software Supply Chain - **How**?



Augment and secure your deployment process (CD)

- Automatically check and verify artifacts and attestations as part of your pipeline.
- Only deploy signed and verified artifacts.
- Attest the same signature (the same artifact) has been promoted across environments.

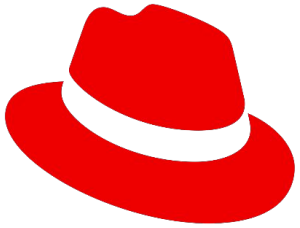
Securing the Software Supply Chain - **How**?



Manage your Security Posture and Monitor your Platform

- Manage your own and 3rd party SBOMs and VEX-Files.
- Know your security posture and manage your risk profile.
- Monitor your platform security
  - Manage platform policies.
  - Identify suspicious behaviour.

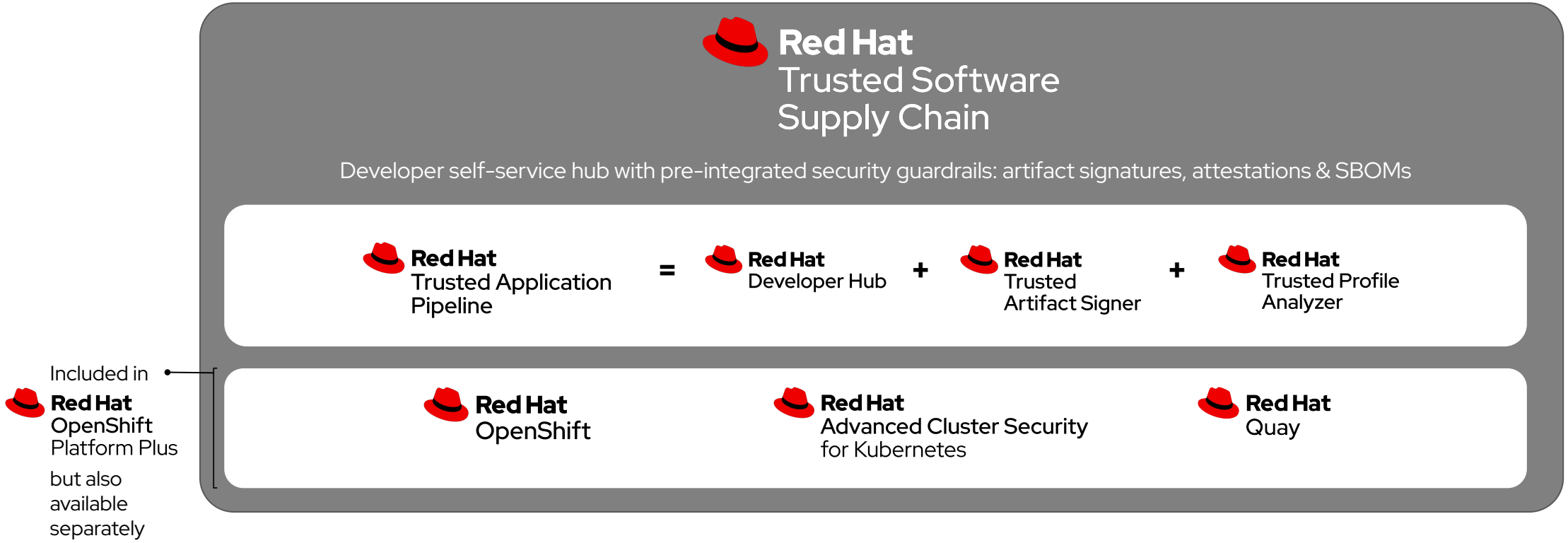
With that said...



Red Hat
Advanced
Developer Suite

Accelerate Innovation that Safeguards User Trust

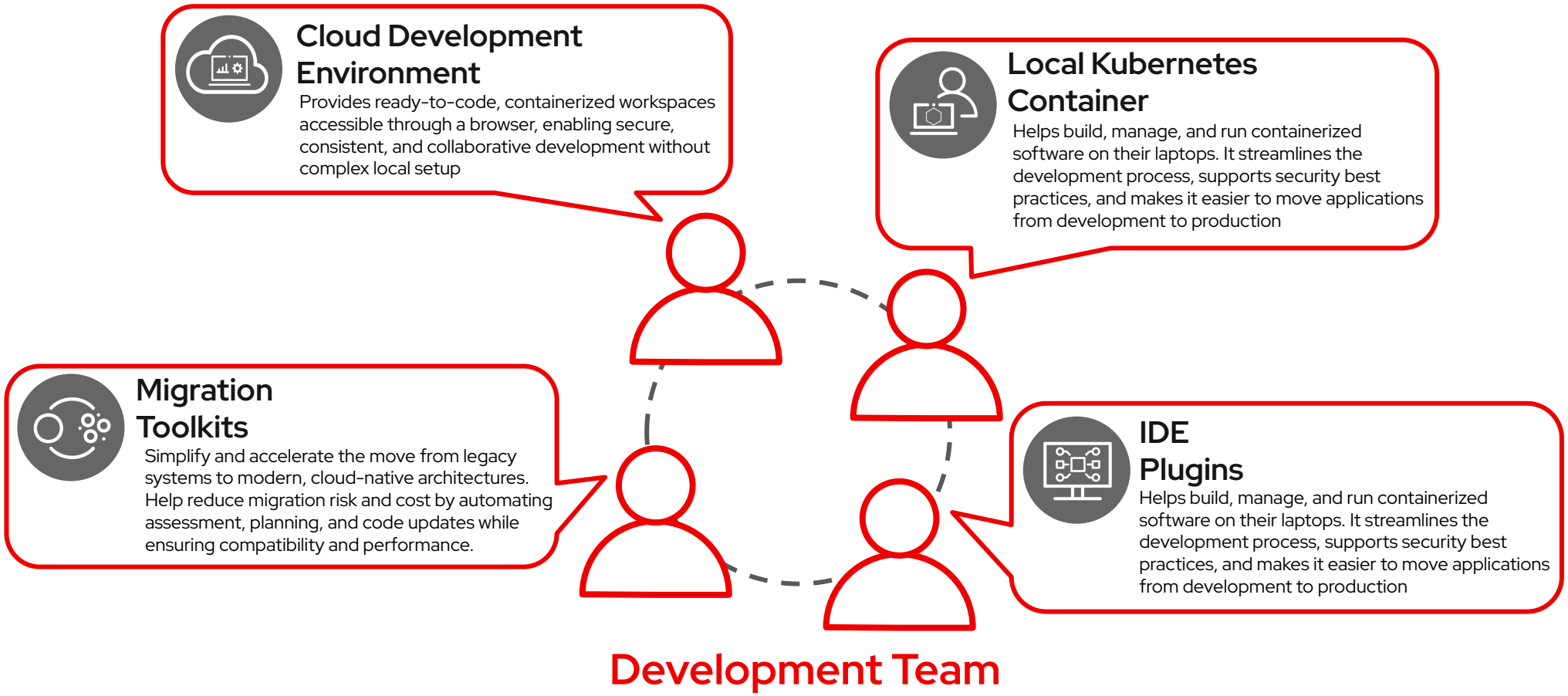
Delivered with integrated security guardrails at every phase of the software development lifecycle



**Red Hat Trusted Application Pipeline is a single product SKU.*
Includes Red Hat Developer Hub, Red Hat Trusted Artifact Signer, Red Hat Trusted Profile Analyzer capabilities with its own installer

Modernizing and Adapting Effortless

Providing the tools and resources to build better software at scale



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

x.com/RedHat

Red Hat