Red Hat Trusted Software Supply Chain

Accelerate application delivery with integrated security guardrails

Benefits of DevSecOps

- **Scale development while adding security.** With short feedback loops, developers find security issues sooner in the software development life cycle so that they can swiftly make corrections before applications go to production.
- **Automated continuous security.** Fully automated security guardrails and auditing across the software development life cycle helps businesses reduce risk and improve compliance.
- **Operational excellence.** Software is built on a foundation of resilience, including trusted code repositories, security-focused pipeline orchestration and site reliability engineering (SRE).

Deploy at the speed of operations

Deploying new software at the "speed of operations" requires trust that the software is compliant, high-quality, built with automated security guardrails, and observable.

Practices like test driven development (TDD) and continuous integration/continuous deployment (CI/CD) promote a DevSecOps culture and build trust. But introducing these practices is one thing and enforcing them is another. Even when teams have the best intentions, making sure they do the right things is difficult without development guardrails.

Implementing DevSecOps starts with a "shift-left" approach to security that introduces security checks and guardrails in every step of the software development life cycle (SDLC) to protect the software supply chain. Reduce your security concerns and adopt practices that allow integrating security more straightforward.

The value of a trusted software supply chain

A trusted software supply chain gives organizations DevSecOps practices and tools that provide security for the software components early in the SDLC and automates security practices at every phase of the software development life cycle.

With a security-focused software supply chain, customers and users can have greater trust in the software they are using. This builds customer loyalty and brand reputation all while reducing the risk of vulnerabilities and threats being introduced after the software is running in production. Organizations can release new software features and updates more quickly, to keep pace with changing customer preferences.

Compliance with industry regulations and standards can be improved through the implementation of a software supply chain security solution. Organizations can avoid costly fines and penalties for noncompliance, and at the same time improve the overall quality of software. This can result in more stable and reliable software, where security issues are identified before affecting users.

Software engineering leaders need help to mitigate risks of using open source software components in the software development life cycle. Their teams need to consistently code, build, and monitor a trusted supply chain in their software factory—without holding back development productivity and efficiency.

Elements of the trusted software supply chain

For 30 years, more than 90% of Fortune 500 companies rely on Red Hat to deliver tried, tested, and trusted enterprise open source software. Curated images and application libraries that have been signed and verified with provenance checks. We have since made our own software supply chain available with just a few clicks.

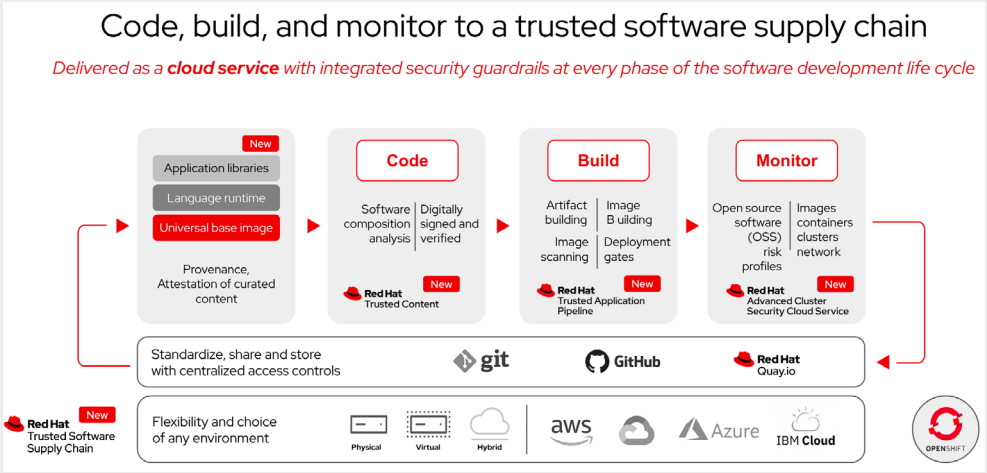

Figure 1. Code, build, and monitor to a trusted software supply chain

Available as a cloud service, Red Hat® Trusted Software Supply Chain helps enterprises successfully adopt DevSecOps practices, consume open source code and third party dependencies safely, and build security into the software development life cycle. We integrate security guardrails at every phase of a DevSecOps framework to offer teams accelerated time to value for a trusted software supply chain that:

- Prevent and identify malicious code: Red Hat Trusted Content helps identify transient dependencies and security vulnerabilities during application code to eliminate risks and exposures early in the development process by running software composition analysis and using trusted content. Developers can now avoid deploying applications that contain security vulnerabilities.
- Safeguard build systems: Red Hat Trusted Application Pipeline allows teams to build applications using automated, security-focused CI/CD workflows with continuous images scanning, provenance checks, attestations and auto-generation of SBOMs that comply with industry standards and regulations. IT organizations now have an accurate inventory of their software components, while improving their development efficiency and productivity.
- Continuously monitor security at runtime: Red Hat Advanced Cluster Security Cloud Service makes certain that organizations can detect, alert and respond to security issues proactively by continuously monitoring the behavior of software components at runtime and drill down with analytics-driven contextual insights. Teams reduce alert noise and fatigue to respond to issues in less time.

Powered by Red Hat OpenShift®, Red Hat Trusted Software Supply Chain brings together, trusted cloud services and prescriptive workflows. AppDev leaders can now release applications in less time while meeting security requirements. This means businesses improve their supply chain resiliency to keep pace with their innovation cycles. Where they keep and grow their user trust to avoid reputational damage, customer churn and revenue loss.

By enforcing best practices with opinionated gates and security controls, we provide a high degree of confidence in continuous deployments. This helps operations teams adopt efficiency-boosting SRE practices.

Learn more about Red Hat Trusted Software Supply Chain

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#338333_0523