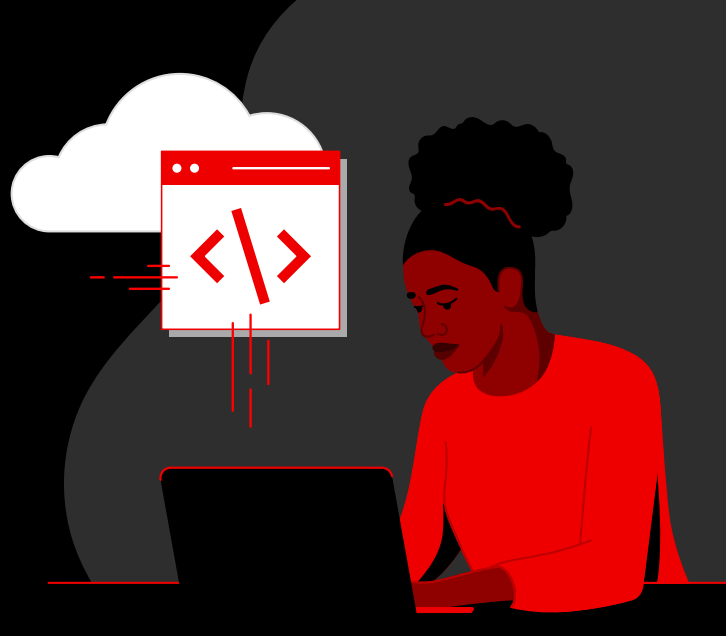
Red Hat

5 ways to boost software supply chain security



Data breaches and software supply chain attacks continue to increase, but many organizations struggle to adopt DevSecOps practices successfully.

742% average annual increase in software supply chain attacks over the past 3 years[2]

19% of data breaches in 2021 were caused by supply chain attacks[1]

Here are 5 ways to integrate guardrails into your software life cycles and supply chain to speed innovation without compromising security.

1 Use trusted images and libraries

Use signed, verified images and libraries for development to prevent vulnerabilities from making it to production and boost user trust.

51% of organizations require developers to use validated images[3]

2 Automate security scans early in the process

91% of organizations say image scanning and vulnerability management are top security use cases[3]

Build automated security scanning and checks into your continuous integration and deployment (CI/CD) pipelines to find vulnerabilities earlier and avoid costly, time-consuming rework when deploying to production.

3 Adopt software bills of materials

Generate software bills of materials (SBOMs) every time you download new open source code to verify the authenticity of software components and make sure they are patched, up-to-date, and in compliance.

91% of codebases contain open source code with no development activity, including security patches, in the past 24 months[4]

4 Apply release policies as code

72% of organizations say security-as-code will be a highly relevant cybersecurity approach within the next 24 months[4]

Implement release policies as code to add security into your CI/CD pipelines and block suspicious build activities without impeding productivity or efficiency.

5 Continuously monitor software behavior

Implement runtime observability tools that monitor software behavior, analyze the risk of changes, and prioritize remediation actions to help security teams respond effectively.

30% of organizations experienced a runtime security incident in the past 12 months[4]

Red Hat Trusted Software Supply Chain

Red Hat Trusted Software Supply Chain, delivered as a cloud service, helps you successfully adopt DevSecOps practices and build security into your software development life cycle. Code, build, and monitor your software with trusted platforms, certified content, and built-in security tools that let you get started quickly and efficiently.

Boost development speed, application security, and business resiliency with a trusted software supply chain.

Learn more

1 IBM Security. "Cost of a Data Breach Report 2022," 2022.
2 Sonatype. "8th Annual State of the Software Supply Chain," October 2022.
3 Red Hat. "2022 State of Kubernetes security report," May 2022.
4 Synopsys. "2023 Open Source Security and Risk Analysis Report," 2023.

Red Hat