5 ways to boost software supply chain security

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

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.

81% of organizations require developers to use validated images.

2. Automate security scans early in the process

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.

91% of organizations say image scanning and vulnerability management are top security use cases.

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. Apply release policies as code

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

72% of organizations say security-as-code will be a high-relevance cybersecurity approach within the next 24 months.

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.

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

Learn more