

Software delivery now spans more teams, repositories, pipelines, artifacts, and CI/CD tools. As those environments scale, signing controls, approval processes, security findings, and release evidence can become inconsistent across teams.

That creates risk at two points in the software release lifecycle.

At release: Different teams may follow different signing, approval, and security processes, making it harder to ensure every release meets the same security standards.

After release: New vulnerabilities can affect software that previously passed its security checks. Teams then need to determine which releases and versions are affected, understand the relevant dependency and security context, and prioritize remediation.

A software release requires more than a signature

Code signing establishes the authenticity and integrity of software. A broader release-governance process also needs to answer what security context is associated with a release, whether required controls were followed, and what happens if risk changes later.

Before release



More teams
and tools



Different signing and
release processes



Inconsistent
controls



Greater
release risk

After release



Software
released



New vulnerability
disclosed



Identify affected
releases and versions



Evaluate and
prioritize remediation

A software release requires more than a signature

Code signing establishes the authenticity and integrity of software. A broader release-governance process also needs to answer what security context is associated with a release, whether required controls were followed, and what happens if risk changes later.



Signed

Control how software receives trust.

Protect signing keys and certificates, control who or what is authorized to sign, and apply consistent policies and approvals across development teams.



Secured

Understand the release and its known risk.

Connect each release with SBOM-derived dependency information, known vulnerabilities, CVSS severity, and security-scan status to determine what may require attention.



Deployed

Maintain context after release.

Monitor how release risk changes over time and retain the information needed to identify affected releases, support investigation, and prioritize remediation.



Result

Code Signing establishes authenticity and integrity, while release visibility shows what a release contains, the known risk associated with it, and how that risk changes over time.

What effective release governance requires



1. Consistent signing processes

Centralize control over signing authority, protected credentials, access, policies, and approvals so releases can follow the same security standards across development teams.



2. Automation within existing workflows

Integrate signing into CI/CD and development processes so governance can scale without creating separate manual steps or disrupting established workflows.



3. Release-level security context

Connect vulnerabilities, SBOM-derived dependency information, severity, and scan status to the specific releases they affect.



4. Ongoing visibility into changing risk

Identify when newly disclosed vulnerabilities affect released software and determine which releases and versions require investigation or remediation.



5. Traceable release evidence

Maintain clear records of what was signed, approved, and released—and under which controls—so teams can support customer reviews, audits, investigations, and incident response without manually reconstructing the release process.

How DigiCert® Software Trust Manager supports the release lifecycle

Software Trust Manager provides the foundation for governed software signing, including protected signing credentials, centralized certificate and key management, access controls, policy enforcement, CI/CD automation, and audit evidence.

Software Trust Manager extends that foundation with deeper release-risk visibility, monitoring, and remediation support through Secure Releases functionality, helping teams:



Connect GitHub releases with SBOM-derived dependency information, known vulnerabilities, CVSS severity, and security-scan status



Monitor release risk as vulnerability information changes over time



Identify releases and dependencies that may require investigation



Use supported fix-version suggestions to help evaluate remediation options



Define vulnerability- and SBOM-based requirements within supported signing and release workflows

The organization determines the policies, conditions, and thresholds appropriate for its environment.

Secure Releases does not replace dedicated vulnerability scanners. It connects supported security information to the releases it affects, so teams can use that context in signing, release, investigation, and remediation decisions.

Questions to ask about your software release process

A strong software release process should be able to answer:



Do we apply consistent signing controls across development teams?



Do we connect security information to the releases it affects?



If a new vulnerability appears tomorrow, can we quickly identify which released versions are affected?



Can we show what controls and security contexts were associated with a release when it was approved?



Do we turn our vulnerability and SBOM requirements into repeatable release controls?

Put your process to the test

Use the Software Release Trust Readiness Checklist to identify where signing, release security, monitoring, or evidence may need stronger controls.



[Check your release readiness](#)

About DigiCert

DigiCert is a global leader in intelligent trust. We protect the digital world by ensuring the security, privacy, and authenticity of every interaction. Our AI-powered DigiCert ONE platform unifies PKI, DNS, and certificate lifecycle management, to secure infrastructure, software, devices, messages, AI content and agents. Learn why more than 100,000 organizations, including 90% of the Fortune 500, choose DigiCert to stop today's threats and prepare for a quantum-safe future at www.digicert.com.

© 2026 DigiCert, Inc. All rights reserved. DigiCert is a registered trademark of DigiCert, Inc. in the USA and elsewhere. All other trademarks and registered trademarks are the property of their respective owners.