VMware Tanzu®

Implement a Secure Software Supply Chain

Deliver software to production quickly and securely with VMware Tanzu

vmware®

A secure path to production is integral to accelerating your DevSecOps capabilities. With threats to software supply chains growing more persistent every day, organizations need to address the risk inherent in application development. Security teams are often at the forefront of this initiative, but may encounter difficulties with implementation. A recent report from Forrester noted that 66.8 percent of security teams struggle to integrate security into the DevOps cycle and 67.6 percent are concerned about securing workloads and containers. Understanding and mitigating vulnerabilities in your path to production helps to de-risk business investments, provides opportunities to deliver more secure software to end users at a rapid pace, and removes friction for developers deploying code.

With VMware Tanzu, you'll improve automated tooling and implement DevSecOps practices so you can ship high-quality code securely and reliably to production and fix security vulnerabilities faster.

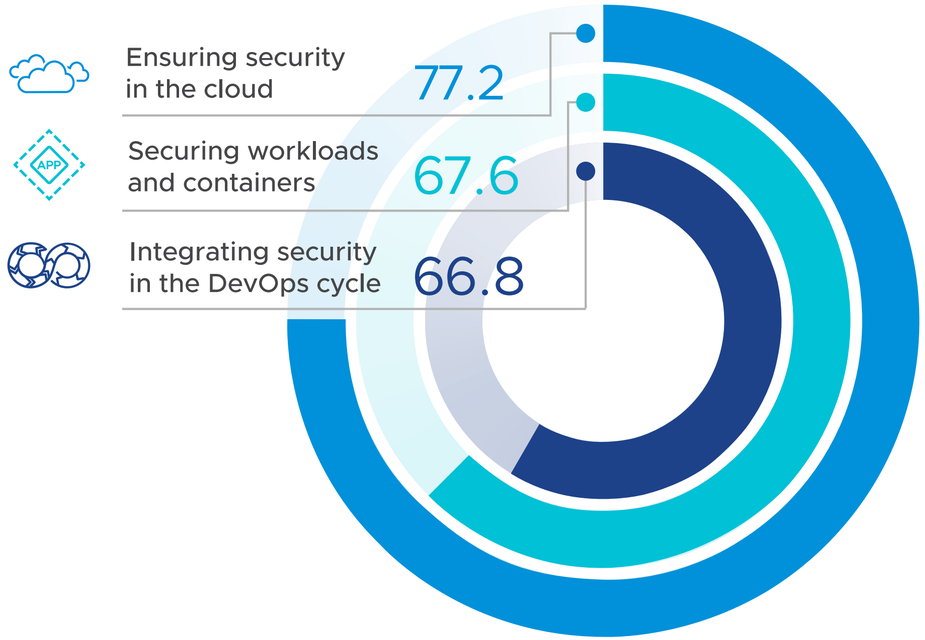

Figure 1: Forrester Consulting study commissioned by VMware, Bridging the Developer and Security Divide, September 2021.

VMware offers solutions in five focus areas of a secure software supply chain. Your secure software supply chain starts with a VMware Tanzu Kubernetes Grid runtime and VMware Tanzu Mission Control, which provide Kuberenetes cluster security. To further develop your secure supply chain capabilities, we provide best-in-class tools like VMware Application Catalog and VMware Tanzu Application Platform, and teach DevSecOps practices that make software secure by design. Our world-class software gives organizations a secure platform on which to build their ideas and tooling that developers will love to use. Consulting services from VMware Tanzu Labs help organizations establish practices that provide greater collaboration between development and security teams. Tanzu Labs engineering consultants can help design and implement a secure software supply chain using the tooling that's best for your teams. By adopting these tools and techniques, you'll chart a course toward a more secure software supply chain.

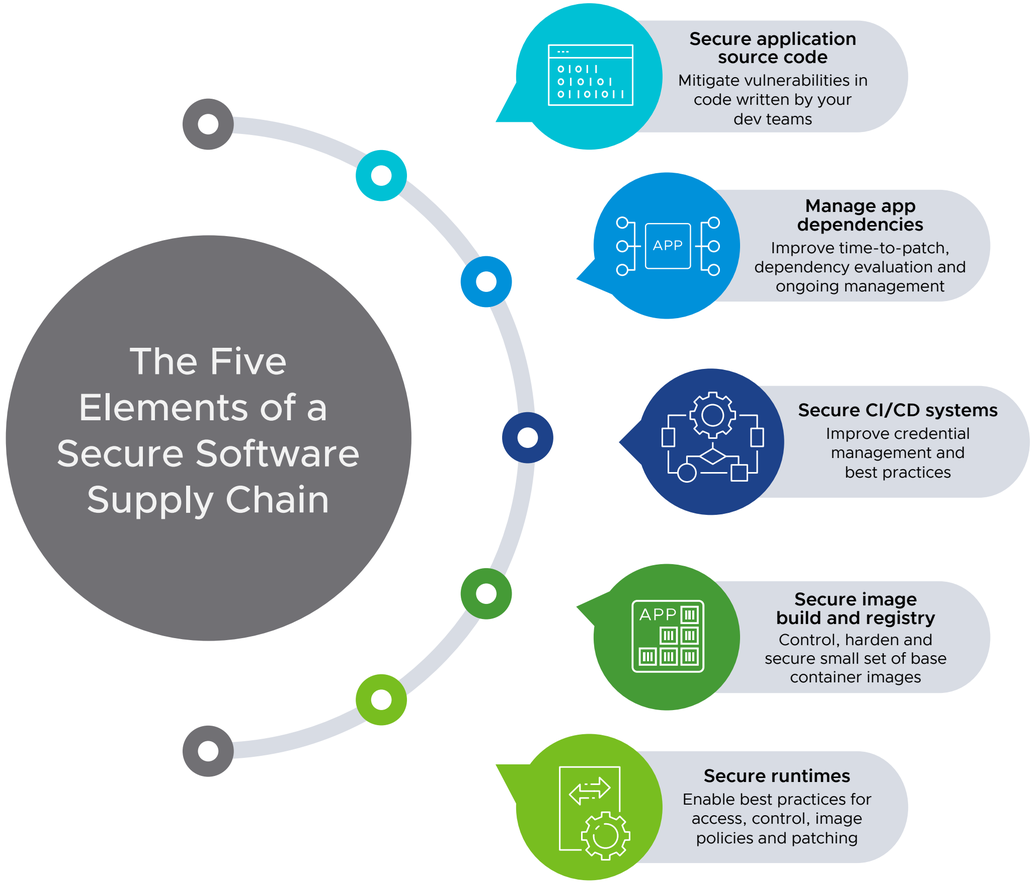

Figure 2: The five elements of a secure software supply chain.

Secure application source code

The part of the supply chain that you have the most control over is the code you write. A secure supply chain doesn't matter if it's shipping insecure code. By implementing strategies to ensure upstream code is secure, you can help mitigate supply chain attacks.

A Tanzu Labs service engagement helps your team implement strategies to ensure code is secure. Our expert engineers show you how to mitigate supply chain attacks using techniques such as secret management, pair programming, or peer review to detect errors and malicious code, along with test-driven development, all while enabling teams to utilize frequent releases in short development cycles.

App accelerators, included with Tanzu Application Platform, provide guardrails for developers that ensure security and compliance.

Manage app dependencies

To ensure secure software design and development, your teams need to be able to clearly visualize their application dependencies. Regular scans to ensure all dependent libraries are patched and free of Common Vulnerabilities and Exposures (CVEs) will reduce the chances that a dependency will be exploited.

Secure CI/CD systems

Governance is an important part of controlling your continuous integration and continuous delivery (CI/CD) pipeline. Making sure permissions for system use are in place and correctly configured can help to secure your software supply chain. This includes least required privileges.

Tanzu Application Platform provides a deploy time policy to allow app operators to introduce policy in their Tanzu Application Platform supply chain (CI/CD) that blocks any unsigned images.

Secure image build and registry

The goal of making container images more secure is to reduce the number of high CVEs in the image registry and shorten the target time required to fix CVEs. We can achieve this by ensuring base images are trusted and signed and that control policies are enforced for the image repository.

Tanzu Build Service as part of Tanzu Application Platform builds images and automatically patches them when their dependencies fall out of date. This feature drastically reduces time to remediate CVEs at scale.

Secure runtimes

Implementing zero-trust architectures and security information and event management (SIEM), along with advanced threat detection tools, creates a more secure environment for your applications and application development platform.

With Tanzu Kubernetes Grid and Tanzu Mission Control, developers get easy access to preconfigured clusters that meet compliance and security requirements. Tanzu Mission Control provides security policies for multitenancy strategies and VMware Carbon Black helps secure containers in multitenant instances. Tanzu Mission Control also enables consistent policy enforcement. VMware Tanzu Service Mesh helps secure workloads, microservices, APIs, and data in transit, preventing attackers from sniffing network traffic.

“One way that security can empower developers is giving them tools that can scan containers and Kubernetes configuration files early in the development lifecycle, automate the application of security policies, discover image vulnerabilities, and provide secure registries, Kubernetes access, and app/container catalogs that enable developers to build secure applications but are tools for which security and operations are able to set policies.”

Forrester Consulting study commissioned by VMware, Bridging the Developer and Security Divide, September 2021

Resources

https://tanzu.vmware.com/content/secure-software-supply-chain