Continuously Secure. Continuously Compliant.

How the software factory keeps software secure and defect-free

Get Started

vmware by Broadcom

Building better software faster, forever

Across every industry and location, today's leading businesses and agencies—from Ford to Dell and GE, from Accenture and Allstate to the U.S. military—are increasingly powered by their ability to deliver software quickly and safely. Bringing the same forward-thinking approach to software that they bring to every other aspect of their organization, these innovators have created their own software factories to build exceptional teams and products that fuel success.

What is a software factory?

In essence, a software factory is an organized approach to software development that brings together the right mix of people, processes and technologies to enable the consistent and efficient production of software. Software factories provide design and development teams with a repeatable, well-defined path to create and update software while providing a flexible framework that allows for adaptation and evolution over time. This approach can provide a plethora of benefits to your organization.

- ✓ **Increase quality** – Standardizing app development across projects at scale decreases the defect rate.
- ✓ **Enhance productivity** – Well-understood methods, reusable code, and process automation help increase developer productivity.
- ✓ **Improve app release cadence** – A software factory helps speed up the process of creating and testing new app code.
- ✓ **Ensure consistency** – Standardizing processes helps ensure consistency while lowering training and maintenance costs.
- ✓ **Provide a foundation for DevSecOps** – A software factory helps foster the integration of security into the software development process.
- ✓ **Create a framework for change** – Establishing a software factory helps build more collaborative teams and accelerate the cultural change necessary for digital transformation.

The "assembly line" approach of a software factory can produce a wide range of outputs for your organization, including high-performing teams and upskilled talent pools. In this ebook, we'll focus on one of the most essential software factory outputs: **software that is defect-free, secure, and in compliance with industry regulations**.

Read on to discover some of the ways VMware Tanzu® can help you build the software factory that is right for you regardless of your industry.

Spotlight: The U.S. Army Software Factory

When the Army Futures Command discovered that the U.S. Army needed more responsive software development, they enlisted the help of Tanzu Labs to create the U.S. Army Software Factory. Together, they built a robust, compliant and resilient software development process to deliver apps to production more quickly. Learn more about the Army Software Factory.

Golden Paths: Building process architectures for software

Coordinating the development, operation and optimization of modern app portfolios across disparate teams, programs and infrastructures can be overwhelmingly complex. To simplify software development, many of today's leading organizations are adopting Golden Paths.

In keeping with the streamlined approach of the software factory, a Golden Path is a well-defined, standardized set of processes, tools and technologies that an organization applies as the baseline for creating software. Following the Golden Path allows the development process to proceed more smoothly, enabling your organization to build better software and deliver it to production faster, with higher quality and greater control.

A Golden Path enables your organization to consolidate knowledge and best practices, facilitate onboarding of new team members, and increase sharing and discovery between teams. This leads to increased automation and innovation; faster, more secure software production; and an improved developer experience (DevX).

Here are some of the key components of a Golden Path.

- ✓ **Documentation repository** – Developers can create an app from an automatically configured template, jumpstarting the development process.
- ✓ **Software catalog** – This gives developers some latitude to choose their preferred tools and services securely from a pre-approved catalog of container images and open source software.
- ✓ **Scaffolding and frameworks** – Build your own templates to allow teams to quickly create projects, while ensuring compliance with technical standards and specifications.
- ✓ **Software supply chain** – Many Golden Paths incorporate open source projects, such as Backstage as a developer portal or Tekton for CI/CD pipelines, helping to accelerate the supply chain and streamline the software development lifecycle.

To make it even easier for your app teams to follow a Golden Path, Tanzu has introduced the four golden commands.

Understanding Golden Paths

Watch this video to learn the fundamentals of Golden Paths.

Tanzu Platform's golden commands

Golden Paths are about enabling your developers to easily access the services, tools and environments they need, and giving your platform and security teams peace of mind that dev teams are not running afoul of security and compliance standards. Ultimately, Golden Paths are created by platform engineering or DevOps teams in service of development teams. The power of Golden Paths is more thoroughly realized with Tanzu Platform's golden commands, a set of four simple, one-line commands that help ensure your development teams always do the right thing.

Adopting golden commands enables your organization to unlock a variety of capabilities:

- Use standardized and secure components and services at scale.
- Deploy any code to any environment with one command.
- Scale and automatically heal CVEs with no downtime.
- Provide self-service data services and curated OSS with no tickets.
- Leverage a shared understanding of code, containers, clusters and underlying infrastructure for faster troubleshooting and remediation.

Today, the Tanzu Platform offers four golden commands: build, bind, deploy and scale.

Build – Easily create deployable artifacts from local machines or by using existing pipelines. Tanzu Platform offers preconfigured app accelerators and templates that allow your teams to adopt a repeatable process to ensure quality software and security.

Bind – Turn governance into a superpower. The bind command connects the app to services (data, messaging queues, caches, etc.) in a curated manner to ensure that your developers can only access the services you allow them to use. This enables platform teams to easily enforce role-based policies through RBAC and secrets and credentials management, while eliminating the need for developers to toil with configurations because they're already baked in.

Deploy – Say goodbye to the need to manually curate how things are run. Deploy the application artifact to an application runtime with a single command to run an artifact or source to app.

Scale – Up, down, across, you name it. Scale anyway you want with a simple command.

Creating a culture of continuous compliance

Historically, software maintenance was something that was done every six months or so, maybe even just once a year. As long as the software was working, there was no pressure to upgrade it. Like many things that used to be, this is no longer the case. Today, bad actors are working faster and with more sophistication than ever, and they're not slowing down anytime soon. Keeping your software secure requires constant vigilance—and maintenance. Source code upgrades need to be done continuously to stay a step ahead of bad actors and keep your organization secure.

Creating a culture of continuous improvement means keeping up with the latest releases and fixes. This is a critical element of a successful software factory model—software that's always up to date should inherently be more stable and secure, giving your organization the confidence to continue moving forward at the speed of business.

Building your upgrade muscle

For organizations that haven't been performing upgrades on a regular basis, this is not always an easy muscle to activate. There's no cheat code to turn it on at scale. All organizations have patterns that are difficult to disrupt, and all organizations are unique—they can't simply be plugged into an existing recipe. This is where the Tanzu Labs team can make all the difference, by providing hands-on support to establish a culture of continuous upgrades within your organization.

Here's a glimpse of what we'll do.

- **Create portfolio visibility** – We'll take time to understand what's running in production (apps, dependencies, libraries) within your portfolio and identify where the biggest risks are.
- **Prioritize and plan** – Our experts will assess and bucket apps into groups with common patterns, ranging from apps that are relatively easy to upgrade to ones that require a more hands-on approach.
- **Leverage tools and automation** – We'll implement tooling and migration recipes for common frameworks and security fixes to begin automating the refactoring and remediation of apps.
- **Tackle complex upgrades** – Our team will develop custom migration recipes for complex applications that can be applied at scale and establish a framework for continuous upgrades going forward.

By establishing a culture of continuous upgrades with the help of Tanzu Labs, your organization can reduce the frequency and time to resolution of vulnerabilities and rest assured that what you ship into market today will stand the test of time, remaining safe and secure for years to come.

Learn more

What is a "continuous upgrade" culture and why is it important? Read the latest blog.

Staying compliant and up-to-date with Tanzu Platform

Wanting your software to always be up to date is one thing. Actually making it happen is another. That’s where Tanzu Platform can help. This modern app platform enables your organization to continuously deliver and run microservices securely at scale both on-premises and across clouds.

- **Accelerate upgrade cadence** – Release new features and updates to production daily.
- **Reliably run apps at cloud scale** – Efficiently manage Day 2 operations across clouds.
- **Reduce risk and protect your systems** – Apply security patches and platform updates with near-zero downtime.

Data security, compliance and process automation

Secure by default, Tanzu Platform is highly automated and improves the security posture across your app portfolio, dramatically lowering risks posed by manual processes. It uses cloud native security principles to automate compliance tasks, saving you time and money, and enables you to build automated systems that log every activity. In addition, it allows you to create an operational toolchain that can rapidly patch and update components as new bits become available.

With Tanzu Platform, you can keep your software continuously secure and compliant, and keep your organization one step ahead of cybercriminals.

Turning compliance into a superpower

Cloud native computing and software as a service (SaaS), along with other modern IT constructs like microservices and distributed edge, have helped today's organizations operate with more efficiency and agility than ever before. However, these modern systems can make compliance a significant challenge, especially for organizations in highly regulated industries. This is where the Modern Compliance Architect (MCA) can make a huge difference.

Fostering a Modern Compliance Architect discipline

Tanzu Labs has a team of Modern Compliance Architects that helps our customers adopt and deploy the best tools and practices for their organization to adhere to regulatory and industry requirements. An MCA can help supercharge your software development and delivery process while enforcing governance and policy at the right place and time for minimal disruption.

By fostering a modern compliance mindset or practice, security becomes an integral part of the app delivery process rather than a hindrance, and your developers can focus on development rather than policy enforcement.

Here are some of the aspects that fall within the MCA's purview.

- **Risk Management Frameworks (RMFs)** including NIST, FISMA and FedRAMP.
- **Identifying and prioritizing risks** where security bottlenecks may exist in the software development lifecycle.
- **Writing security and access policies** and identifying the best ways to enforce them.
- **Understanding industry-specific guidelines**, requirements and modern architectural paradigms.

The building blocks of a secure software supply chain

Once upon a time, your organization's apps were built almost exclusively from internal codebases. This is no longer the case. Today's sophisticated apps are powered by a variety of third-party services, open source software (OSS) stacks, and internal codebases. Using OSS components as building blocks brings an unprecedented level of flexibility and efficiency to the software development process. It also brings the possibility of increased supply chain vulnerabilities.

To best mitigate the supply chain risks posed by OSS, the software factory looks at four main sources.

- Software bill of materials (SBoM)
- Common vulnerabilities and exposures (CVE) scan report
- Vulnerability Exploitability eXchange (VEX) document
- Risk Management Framework (RMF)

Let's take a closer look at these elements.

Demystifying the software bill of materials (SBoM)

Watch Tanzu Developer Advocate, Whitney Lee, and Tanzu Solutions Architect, Alex Barbato, unpack the Software Bill of Materials (SBoM) in this video.

What is a software bill of materials (SBoM)?

A software bill of materials is a comprehensive inventory of an application's dependencies, including third-party services, software packages, OSS stacks and codebases. More than just a list, the SBoM manages software dependencies in an automated, machine-readable manner, enabling your organization to easily track application changes and identify and remediate vulnerabilities.

Because every individual, department and partner has access to the SBoM, it makes patching and remediating software vulnerabilities much simpler. When a vulnerability is identified, all you need to do is locate the specific third-party service, software package, OSS stack, or codebase listed in the SBoM and make the proper remediations.

However, as helpful as they can be, SBoMs alone aren't enough to efficiently manage supply chain vulnerabilities. This is where CVEs and VEX documents come in.

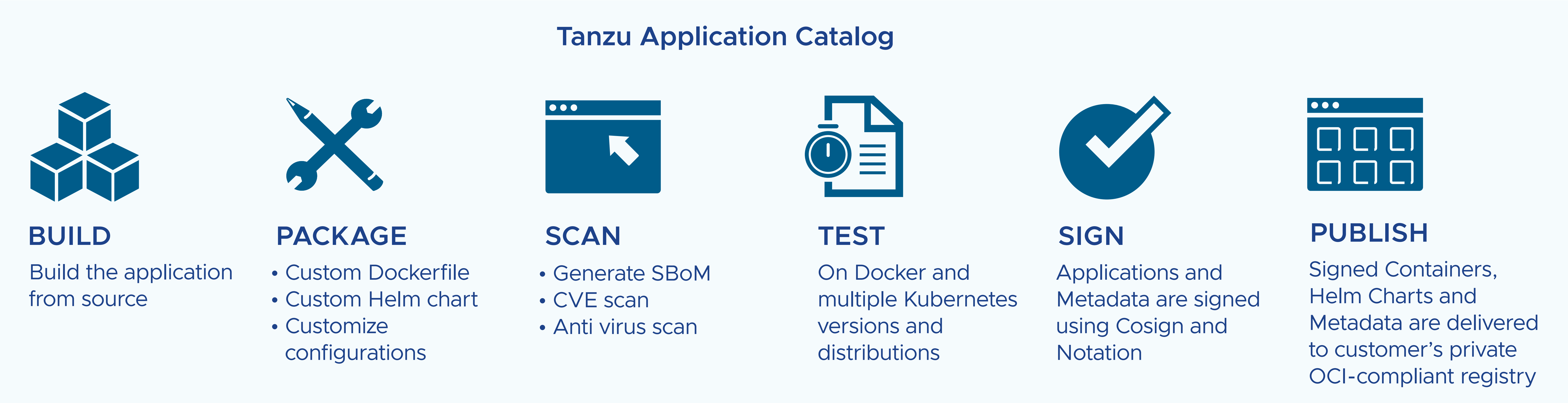
CVE and VEX documents

As the name suggests, common vulnerabilities and exposures (CVE) scan reports provide your organization with a list of vulnerabilities that could potentially expose your software to known risks. This is a very good thing. The only drawback is that scanning an OSS application usually generates a long list of vulnerabilities, many of which are no longer exploitable, or only exploitable under very specific configurations or circumstances. In other words, finding a vulnerability in your CVE scan report doesn't automatically mean your software is at risk.

This is where the Vulnerability Exploitability eXchange (VEX) document comes into play. A machine-readable type of security advisory developed by the National Telecommunications and Information Administration (NTIA), the VEX document is designed to help you understand the exploitability of the vulnerabilities found in your CVE scan reports, providing context and potential remediating measures. It is extremely useful in boosting the efficiency of security teams by reducing the time spent investigating non-exploitable vulnerabilities that don't actually affect a given software product.

So, how do you get a VEX document?

Based on the open source Bitnami catalog, Tanzu Application Catalog enables you to build a catalog of custom-packaged open source application components. Tanzu Application Catalog also builds VEX documents for your security teams with all the information they need to efficiently filter out false positives and focus on vulnerabilities that require immediate remediation.



Tanzu Application Catalog

BUILD

Build the application from source

PACKAGE

- Custom Dockerfile
- Custom Helm chart
- Customize configurations

SCAN

- Generate SBoM
- CVE scan
- Anti virus scan

TEST

On Docker and multiple Kubernetes versions and distributions

SIGN

Applications and Metadata are signed using Cosign and Notation

PUBLISH

Signed Containers, Helm Charts and Metadata are delivered to customer's private OCI-compliant registry

Figure 1: How Tanzu Application Catalog works.

The Risk Management Framework (RMF)

Originally developed by the National Institute of Standards and Technology (NIST), the RMF provides a process that integrates security, privacy and software supply chain risk management activities into the system development lifecycle. Tanzu supports the RMF process by providing artifacts and information for the Implement, Assess and Monitor steps, helping your organization identify and minimize risks.

By leveraging SBoMs, CVE scan reports, VEX documents, and the RMF, you can start producing secure, compliant and defect-free software with factory-like efficiency.

Vulnerability management white paper

Discover how Tanzu Application Catalog provides SBoMs, CVE scan reports, and VEX documentation to help you accurately assess risks in this white paper.

Get started with Tanzu Platform and Tanzu Labs

The engine that powers the software factory is Tanzu Platform, a single solution that enables your organization to deliver high-value software faster by simplifying and integrating the processes and tools used by developers and IT operations. Here are some highlights of what Tanzu Platform can help you do.

- Empower app teams with the four golden commands (build, bind, deploy and scale) to jumpstart app development, eliminate tickets, and reduce onboarding time.
- Harness the power of the three Rs (repave, repair and rotate) to build security and resiliency into operations.
- Get the speed and simplicity of a cloud-based managed service with the governance and cost-efficiency you need for your most critical apps.
- Supercharge the runtimes of your preferred apps.
- Leverage cloud native consulting services from the experts at Tanzu Labs.

Get Started Today

See how Tanzu Platform and Tanzu Labs can help your organization build a software factory that enables continuous security and compliance.

LEARN MORE

vmware® by Broadcom

7540-SOFTWARE-FACTORY-EB-20240715 7/24