

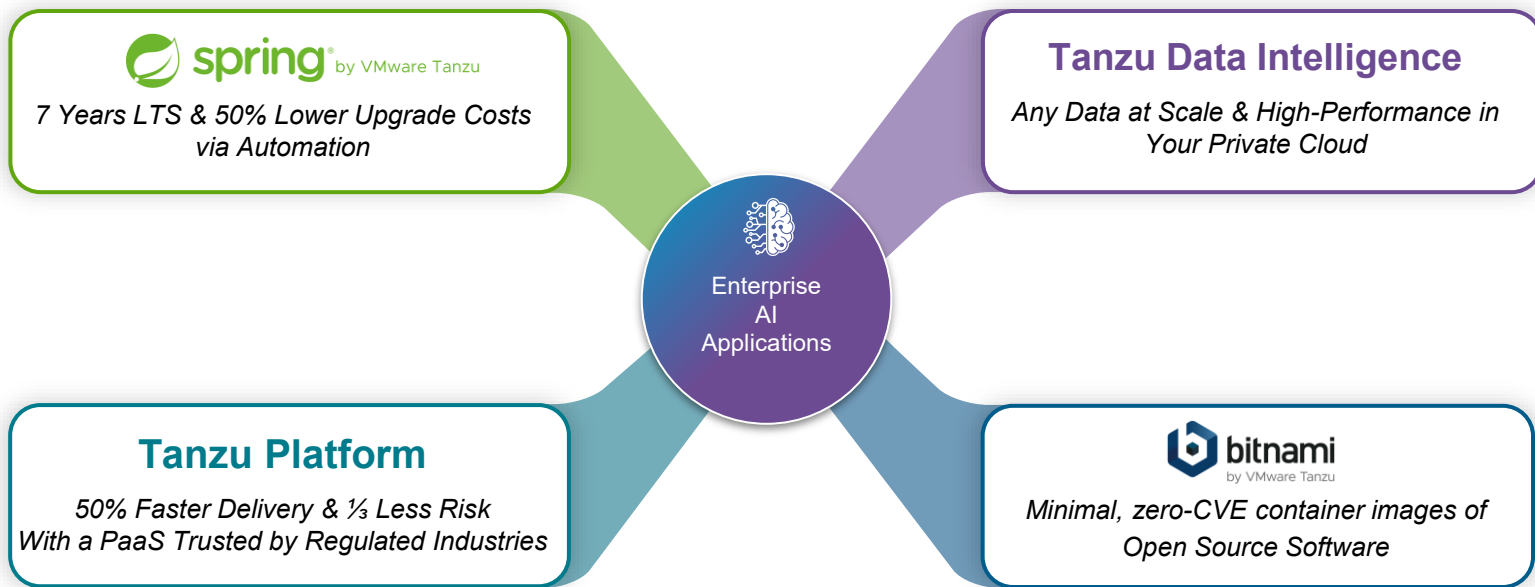
Golden Path to Production

by Broadcom

How to operate, thrive and defend in the era of AI



VMware Tanzu® — Trusted To Drive Business Value in the Enterprise



Your critical digital infrastructure depends on open source

Spring and open source data engines are ubiquitous in the enterprise

97%

of enterprise
applications use
OSS components

75%+

of code in typical
enterprise codebase
is **OSS frameworks
and libraries**

9 in 10

Fortune 500
companies run
**applications built
with Spring**

95%+

of enterprises
deploy at least one
OSS database



TL;DR> New Reality

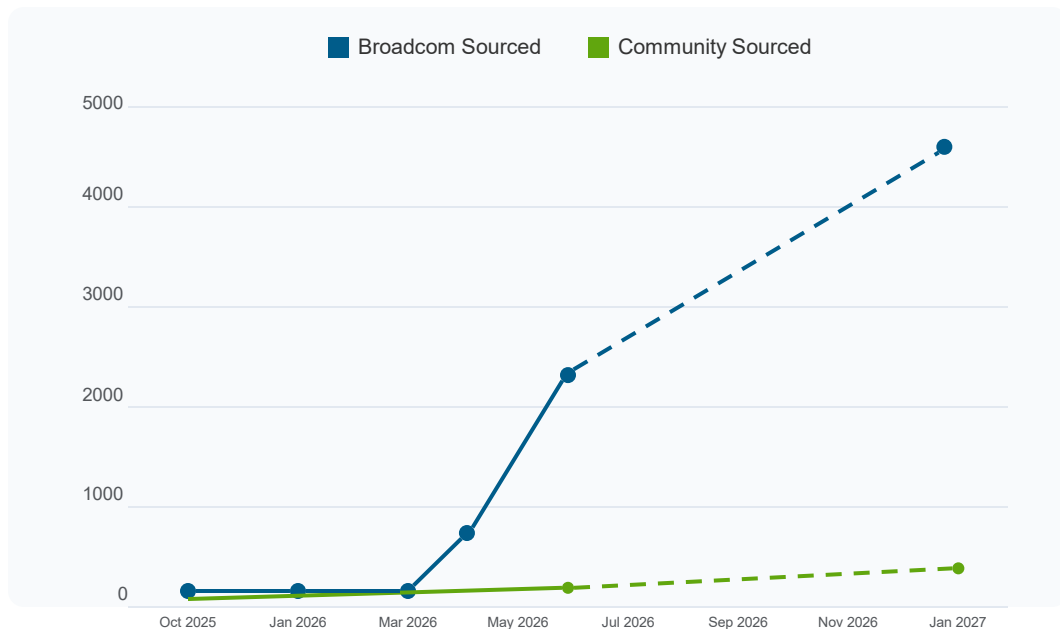
Security threats are evolving, and your current defenses **are not enough**.

Stop waiting for a breach to happen and **secure your workloads and infrastructure now** before you're the next target.



Surge in AI-detected vulnerabilities in open source software

Spring Example: Despite being strong in security, Spring has seen a massive increase



+1700%

Increase in security advisory reports from March to April 2026

12 BILLION

Tokens used by Broadcom to scan Spring with Frontier AI models

OVER 60%

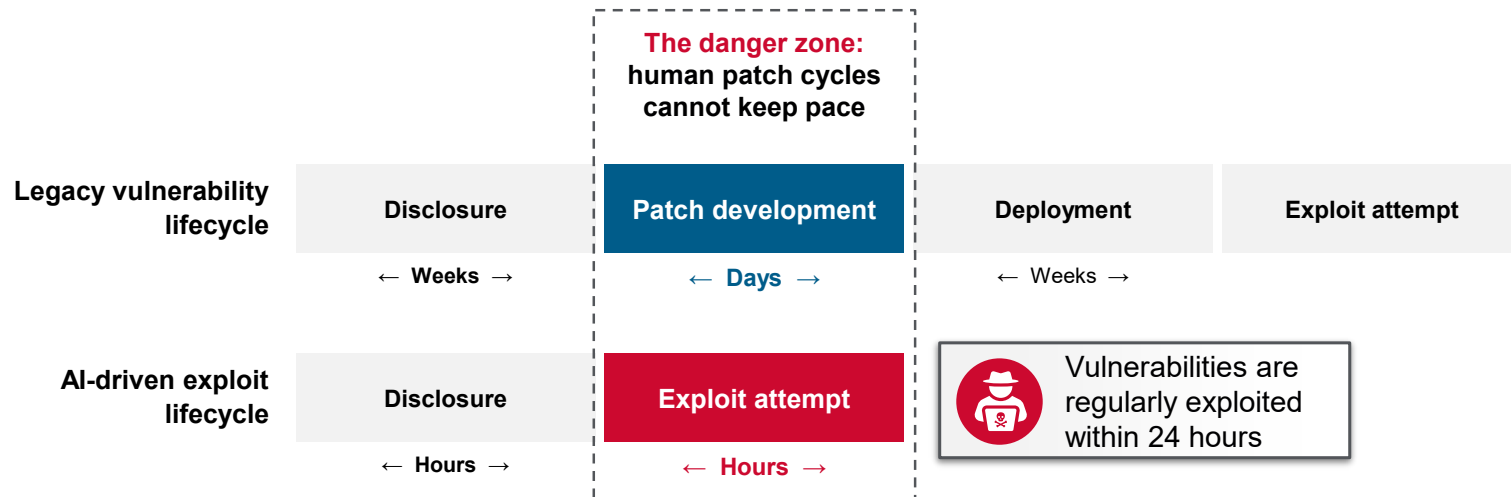
of Spring Boot downloads are out of OSS support window

+478% YTD increase in identified security advisories for Spring in 2026



Frontier AI shrinks the window from CVE discovery to exploit

Open source software components are prime targets for exploitation



Shortened patching window

CVE remediation windows shrink from days to hours, requiring faster patching

Increased chaining speed

AI significantly increases the potential for identifying and exploiting combinations of low severity CVEs

Out-of-support risk

Significant amounts of unpatched vulnerabilities will remain in unsupported open source data engines

1. Hacker News: [LMDeploy CVE-2026-33626 Flaw Exploited Within 13 Hours of Disclosure](#)
2. [AI Speed Exploitation Changes Everything Leaders Thought](#)
3. Broadcom customer anecdotes



The attacker's clock changed. The patch process did not.

Disclosure to exploit fell from weeks to hours. Patching still waits on a release train.

The world your patch process was built for



The world it runs in now



12h 31m

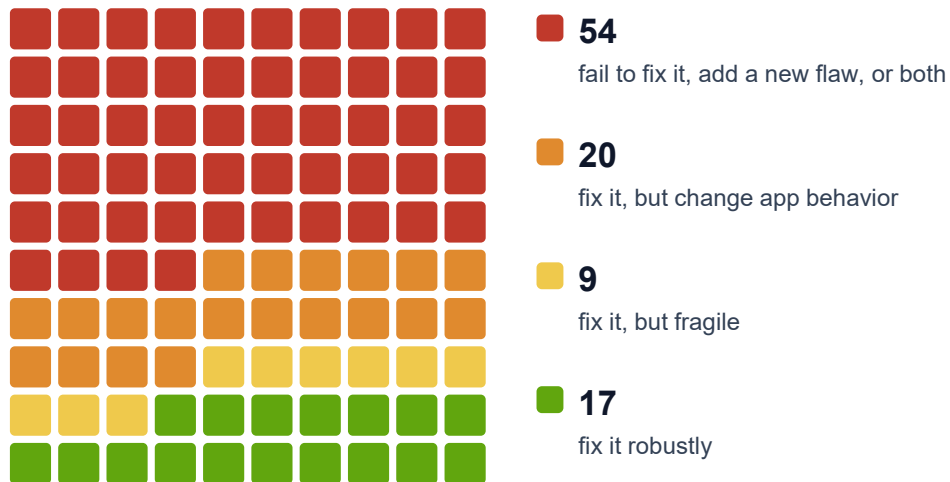
LMDeploy CVE-2026-33626: from advisory publication to the first observed exploitation attempt. The attacker built from the advisory, not a public proof of concept.

Source: Sysdig Threat Research Team, CVE-2026-33626 analysis, April 22, 2026. Upper-track timings illustrate the historical pattern and are not a measured average.



AI alone cannot fix your vulnerabilities

Independent research finds autonomous AI patching is net-negative without expert review



Every square is one AI-generated patch

Only 17 in 100 AI-produced patches are clean, durable fixes

Building a patch is more than just a code change

Safe fixes take knowing what the code is meant to do. That knowledge lives with the engineers who maintain it.

Every private fix is a fork you must maintain

Fixes that never land upstream get re-applied every release, accumulating drift and breaking upgrade paths.

You can only verify fixes if you have the advisory

The full picture of a flaw is shared privately with the maintainers. Everyone else works backward from the CVE disclosure.

Scan for the study



Source: Axel Mierczuk, Spencer Michaels, and Keith Hoodlet, Off-by-1 Labs (1Password), "Frontier Models' Vulnerability Patches are Often F.L.A.W.E.D.", 2026. 6,080 patch attempts, two frontier models, six recent high-impact CVEs. 1password.com/files/resources/frontier-models-vulnerability-patches-flawed.pdf



Our commitment and investment in open source



Billions

Tokens used for
continuous
scanning of OSS



100%

OSS Spring and
RabbitMQ
contributions are
reviewed by
Broadcom



>300

Bitnami images,
charts, and
operators across
OSS



75%

Apache Tomcat
fixes are from
Broadcom



The TrueSource approach

1

Curate from deep domain expertise

Stewards of Spring and RabbitMQ, Bitnami maintainers, a decade on Postgres, MySQL and Valkey

Artifacts selected for enterprise application architectures, built and verified by Broadcom

2

Work with maintainers

Broadcom contributes fixes upstream rather than forking

Backs community maintainers with engineering time and support

3

Collaborate in a private clearinghouse

Licensed customers and Broadcom engineers work findings together before public disclosure

Outcome: early access to fixes, with a dedicated path for critical infrastructure organizations

4

Automate fixes and make them visible

Tooling to analyze repositories and automate fixes

Coming soon: visibility across your repositories and pipelines, so verified artifacts reach production

One standard, guided by our experience as OSS stewards and maintainers, applied to every offering



TrueSource by Broadcom: one standard, three offerings

Every offering shares the same build discipline. Depth follows the reach of Broadcom's stewardship

Spring Enterprise

Spring and its full dependency tree

- Simultaneous access to patches for current and LTS versions
- CVE-only patches for faster deployment
- SLSA Level 3 Builds of Spring and its Java dependency tree, including Apache Tomcat, Kotlin
- Direct support from Spring engineering team
- Patch automation tooling

TrueSource Trusted Artifacts

Java, Python, NPM Node/JavaScript, secure images (subset of Bitnami Secure Images)

- Secure, curated language libraries
- Hundreds of container images, Helm charts
- Scanned, fixed, and contributed upstream
- SLSA Level 3 builds

TrueSource Data Services

Postgres, RabbitMQ, MySQL, Valkey, DSM, secure data images (subset of data-related Bitnami Secure Images)

- Curated, enterprise-grade distributions, including engines and extensions
- Helm charts and operators
- DBaaS automation and integration
- Deployment expertise and 24x7 support
- SLSA Level 3 builds

The standard on every offering

Clean room builds · CVE scanning · Selective patching, upstream · early access available · end-to-end dashboards (*coming soon*)

Separate offerings, each available with simple, tiered site licensing. One standard, set by the Spring team, applied across all three.



The Fast Lane: Golden Path to Production



golden path



◆ AI Overview



A "golden path" is **an opinionated, supported, and templated way of building and deploying software within an organization, ensuring consistency and efficiency**. It's a pre-defined set of tools, processes, and best practices for common tasks, allowing developers to build software more quickly by providing a self-service option that meets organizational standards. The term is also used in science fiction, most famously in Frank Herbert's Dune series to describe a long-term survival plan for humanity. [🔗](#)



Highway to Production: Built for Developers & Coding Agents

Enabling developers and AI coding agents to rapidly deploy, bind services, test, and iterate

Traditional DevOps Route

Weeks to Months • Complex & Manual

1. Find available hosts & configure pods
2. Install middleware & retrieve libraries
3. Create application packages
4. Configure load balancers & firewalls
5. Update monitoring & log collectors
6. Wait for manual ticket approvals
7. Repeat for every environment...

High Friction Route

Infrastructure management slows down velocity and distracts developers.

Tanzu Highway to Production

45 Seconds to Production • Automated & Standardized



1

1. Deploy

Code or AI agents deploy directly to running apps with zero friction.

2

2. Bind

Self-service DB, MQ, and AI platform services bound on demand.

3

3. Test & Observe

Instant telemetry & logs enable agents to quickly test and iterate.

4

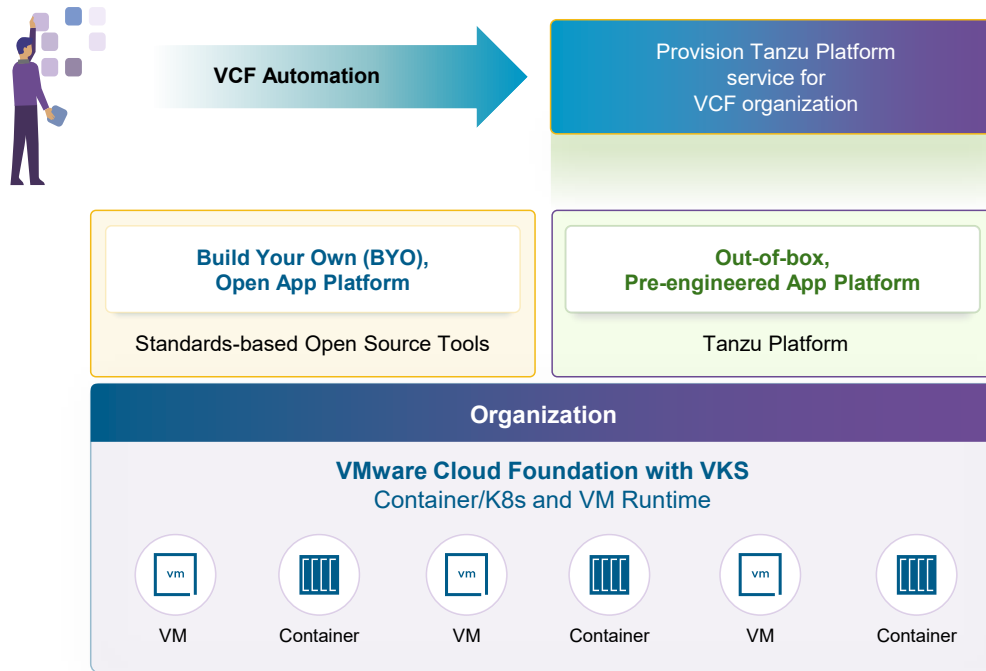
4. Govern

Policy by default with automated guardrails for autonomous code.



Click and go PaaS with Tanzu Platform + VCF 9 integration

Easy-to-operate, single destination for all application types and runtimes



One-click provisioning

Seamless, automated provisioning of PaaS for fast, simple experience. Option to schedule containers on attached VKS cluster*.



Consistent AppOps experience

Tanzu Platform abstracts the runtime complexity, ensuring the developer experience remains consistent.



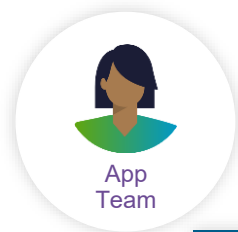
Common cloud operations

Leverage the VCF Supervisor services for integrated networking, storage and security.

**services only support for VKS*



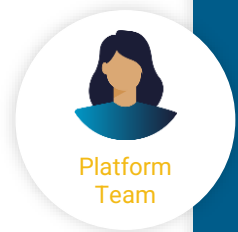
Tanzu Platform delivers modern and AI apps with PaaS



Modern applications

GenAI applications

Agentic workflows



VMware Tanzu Platform



Build Services



Spring Services



Data Services



AI Services



Marketplace Services



Elastic App Runtime Service



VMware Cloud Foundation

Public Cloud



Thank you!