Trust is the throttle for adoption

What we learned building software with agents, and what it means for yours

Purnima Padmanabhan, GM, Tanzu Division, Broadcom |

AI in Finance Summit, London, September 2026

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

VMware Tanzu is the leading provider of application and data services

TrueSource by Broadcom, Tanzu Platform and Tanzu Data Intelligence



Stewards of the open source enterprises run on

Home to the core maintainers of Spring and RabbitMQ



10 out of top 10 largest financial institutions

Trust VMware with mission-critical app and data workloads



Millions of apps in production

On Tanzu Platform with near-zero downtime



Trillions of transactions and 1+ Exabyte data

Processed and analyzed by Tanzu Data Intelligence



Leading enterprise framework for AI

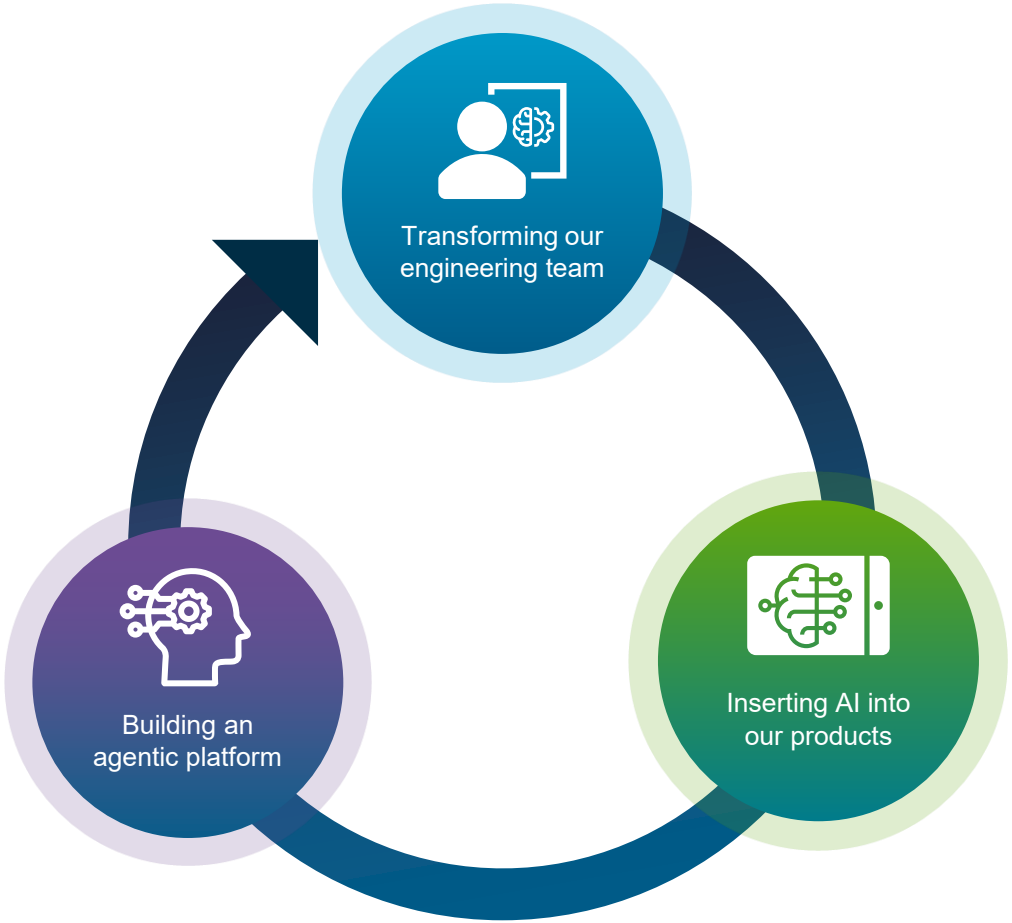
With Spring AI simplifying adoption for millions

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

We sell the platform, and we build our own software on it

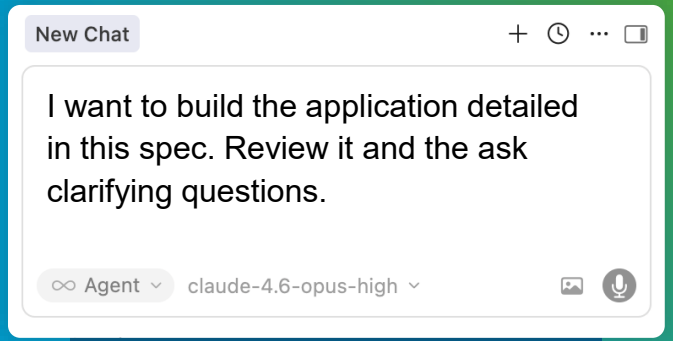
Tanzu Division of Broadcom:
A unique vantage point on AI adoption



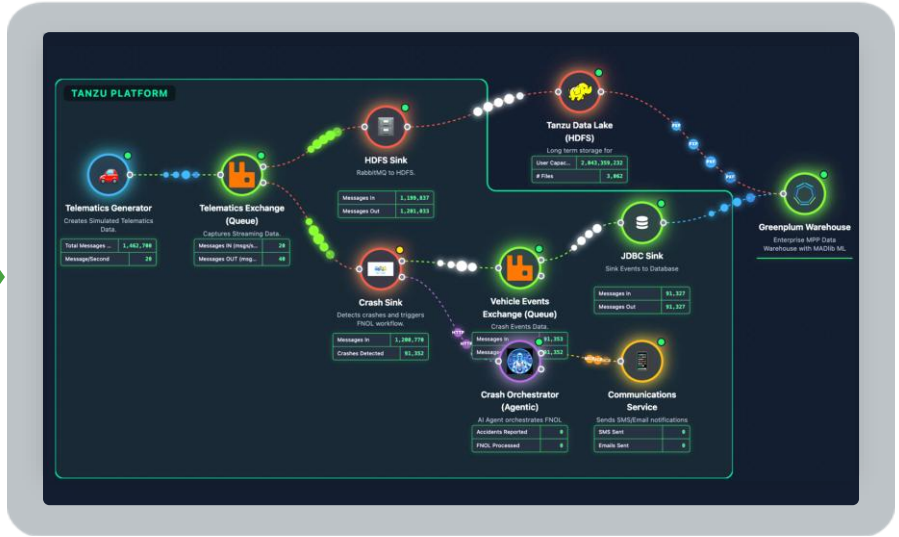
vmware by Broadcom
Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

AI makes software look easy

Example: “vibe coded” greenfield POC software project 1 week from spec to completion



App Specification



1 person

Expert understanding of architecture

Working understanding of business logic

Not a daily coder

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

…but this is not how enterprise software works

Simply adding tools to the existing process and organization doesn’t work



AI solves every problem like it's the first time

AI doesn’t know how or why something had been tried before and failed

Human teams get smarter about their own system over time, AI doesn’t



Perfect syntax hides semantic failures

Syntactically perfect code removes familiar warning signals

AI cannot understand the runtime performance or infer undocumented standards



Adoption at scale requires organizational change

AI threatens craft and ownership

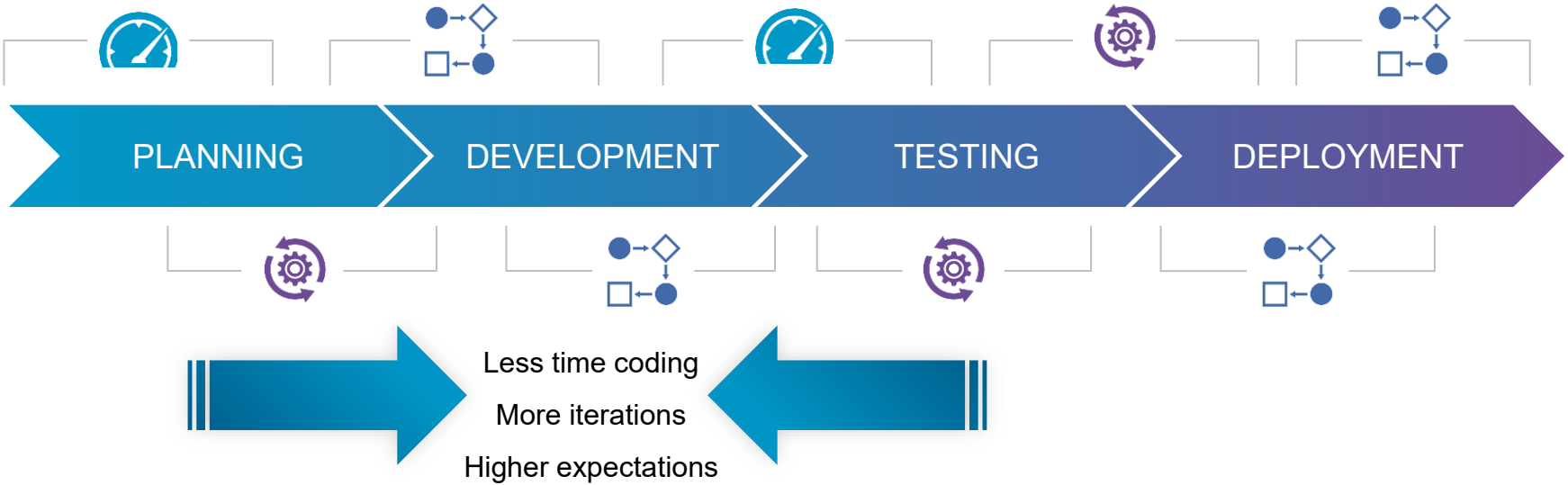
Software expertise doesn't automatically transfer to AI fluency

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Rebalancing the software delivery lifecycle

AI doesn’t remove work, it moves it



Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How we are evolving our approach to software

Rethinking organization with a centaur inspired model



Institutionalize the challenger

ADD A SKEPTIC ROLE

Counter automation bias with a designated rotating role **challenging the outputs**



Encode standards, remove variance

BUILD-IN GUARDRAILS

Frameworks and guardrails replace judgment calls with **deterministic outcomes**



Give agents context like you would a new hire

CURATE CONTEXT

Onboard it with what matters, in the order it matters.



Drive accountability across lifecycle

TRANSFORM ORG

Cross-functional **human-AI pods** own delivery and check each other's work

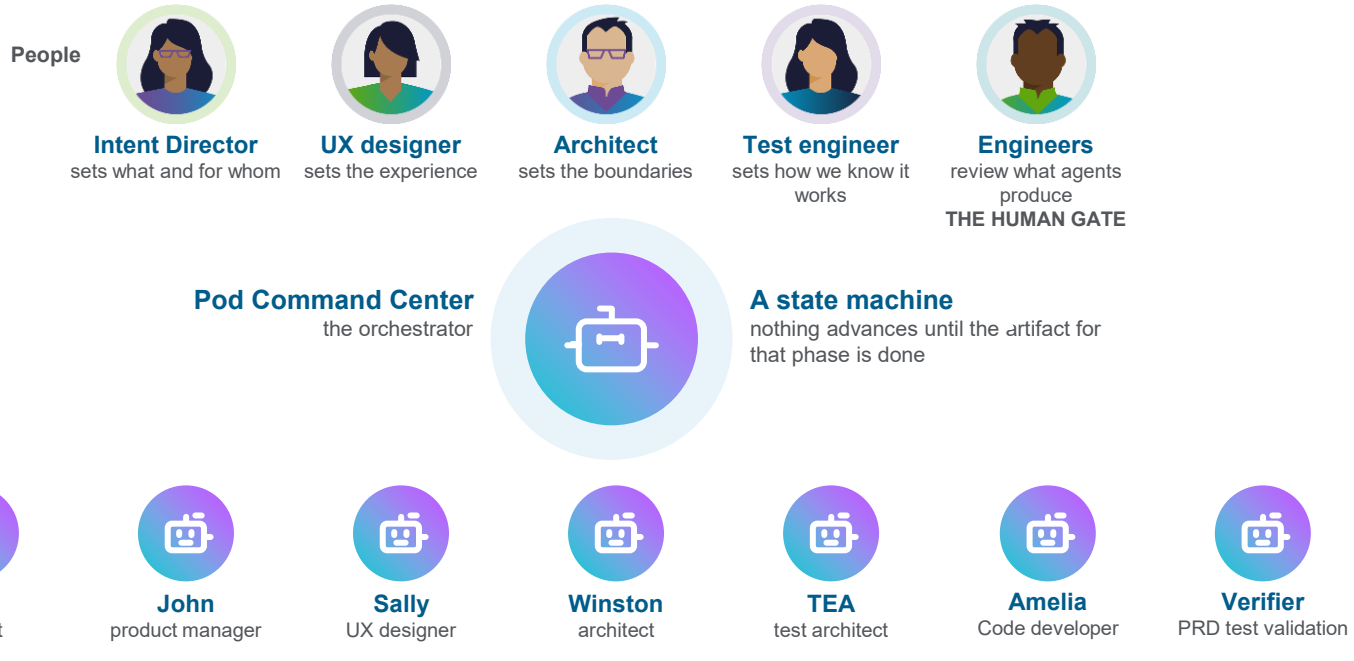
vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Our product team pod: people and agents, one orchestrator

People set intent and review, agents plan, headless agents write the code

Product Pod: people and agents, interactive



Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

A day in the life of a feature

Tanzu Platform agentic software delivery lifecycle

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Our results on running these agents on Tanzu

Results from our own product and engineering teams, six months in



12 to 3

weeks from requirements to task assignment



59%

reduction in mean time to resolve issues



54%

increase in features delivered versus the previous release



48 hours

from a six-month release cycle to a working prototype

Source: internal Broadcom data; Tanzu Talk, July 2026. Prototype throughput figure applies to the Tanzu Platform product organization.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Agentic AI blurs software execution and decision making

Acts before anyone can check

Reaches past what you scoped

Does what you said, not what you meant

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three questions for every agent

1

What is it made of?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context supplied to it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three questions for every agent

1

What are agents made of, and what ingredients does it use

The open source your agent is built from and uses

2

What are the boundaries around it?

Where it can reach and what it can do

3

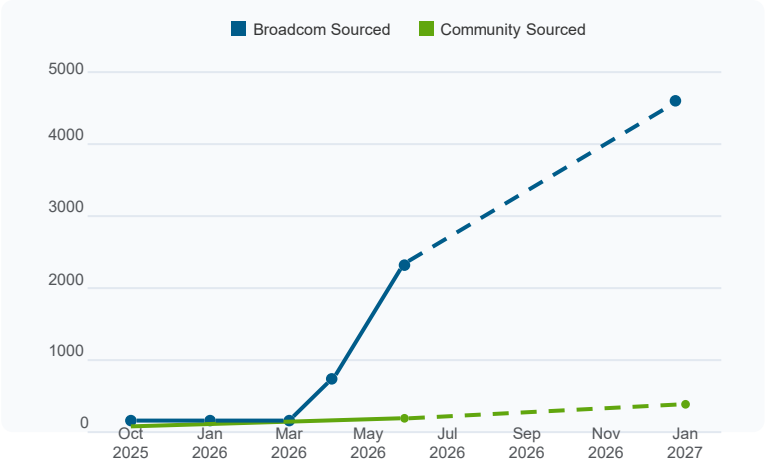
What is the context supplied to it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Most apps and agents are built with open source ingredients

Open Source is under attack



+1700%
increase in security advisory reports from March to April 2026

12 BILLION
tokens used by Broadcom to scan Spring with Frontier AI models

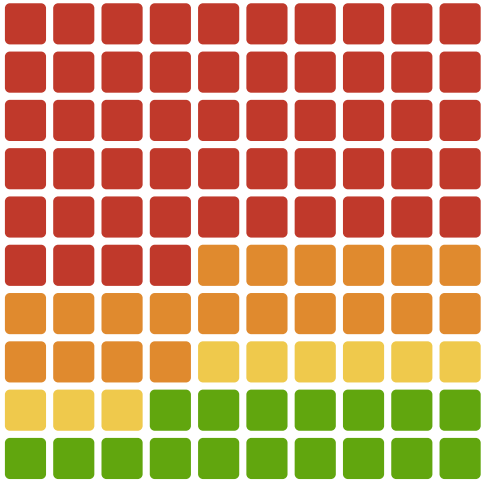
97%
of enterprise applications are built using open source software

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

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

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

54
fail to fix it, add a new flaw, or both

20
fix it, but change app behavior

9
fix it, but fragile

17
fix it robustly

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

Copyright © 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Clean ingredients to build apps and agents: TrueSource by Broadcom

Spring Enterprise

Spring and its full dependency tree

- Day-zero, CVE-only patches across current and LTS lines
- SLSA 3 clean-room builds, direct support from the Spring team

TrueSource Trusted Artifacts

Java, Python, Node.js, Bitnami Secure Images

- Curated language libraries and container images
- Scanned, fixed, and contributed upstream

TrueSource Data Services

Postgres, RabbitMQ, MySQL, Valkey, DSM

- Curated distributions, engines, and extensions
- Deployment expertise and 24x7 support

Curate from deep domain expertise

Work with maintainers

Early access to remediation

Automate fixes and make them visible

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three questions for every agent

1

What are agents made of, and what ingredients does it use?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

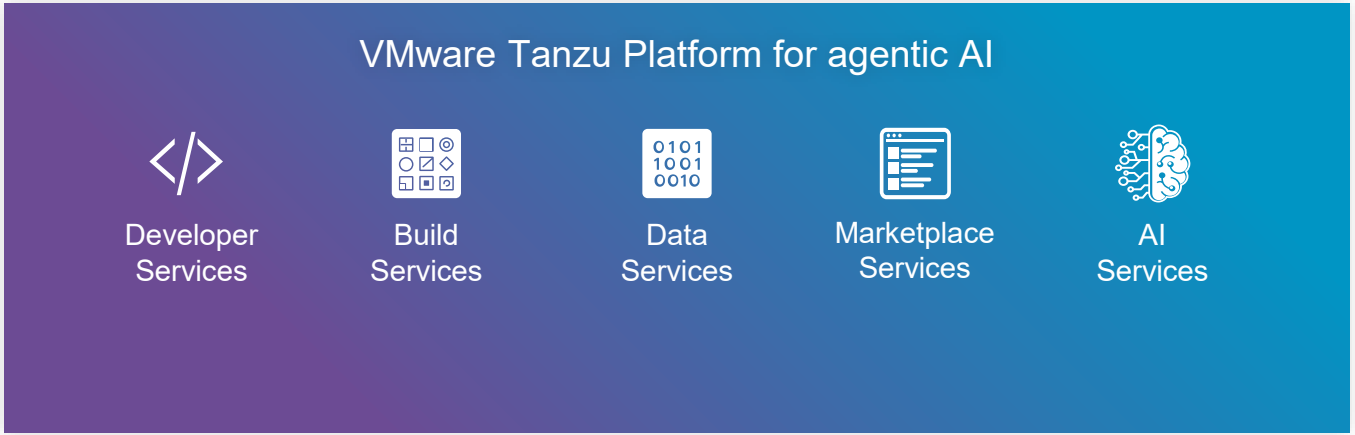
3

What is the context supplied to it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Tanzu Platform: Safe, governed, modular agent services



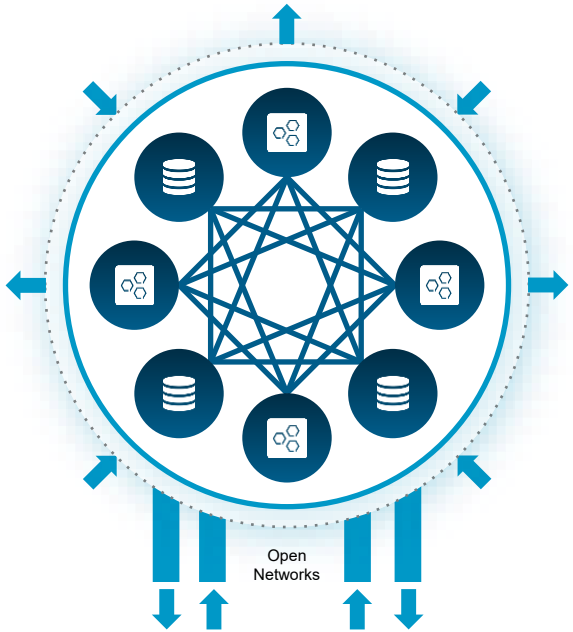
Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The platform assumption changes everything

Open vs. Deny

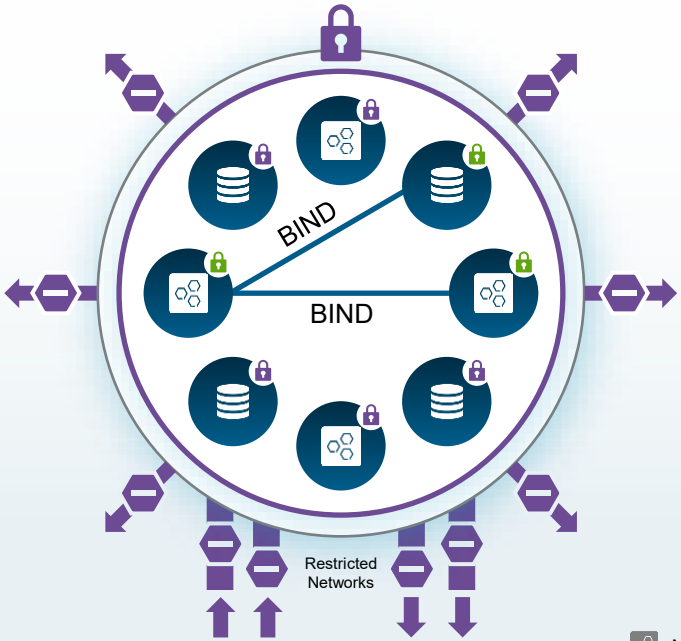
Default cloud-native approach

Microservices discover & connect freely (Cross-namespace)



Our approach: Deny by default

Services isolated explicit grants only



Microservices

Data services

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Safer agent autonomy

Question two: Agent runtime makes it simple to both run and contain agents



The agent sandbox on Tanzu Platform

Reach is declared up front

Explicit routes and service bindings. An agent's connections are known before it runs, not found in an audit afterward.

A runaway agent runs out of room, not budget

Resource guardrails across virtual machines and Kubernetes contain loops, retries, and token spend.

Credentials are shielded from the agent itself

A prompt injection cannot trick an agent into leaking the keys it runs with, because it never holds them.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three questions for every agent

1

What are agents made of, and what ingredients does it use?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context supplied to it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The data for agents has to be just right and no more



BUILD NOTE: Explore 132 treatment on white, original labels; designer to check pill fills and the glow line

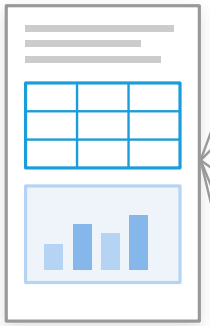
Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

AI-ready data in Tanzu Platform

Sovereign, private data ingestion and governed access for agents

Ingest & Parse — OCR, layout, tables
Structure — typed records
Govern — policy + lineage
Publish — to the marketplace

Complex document

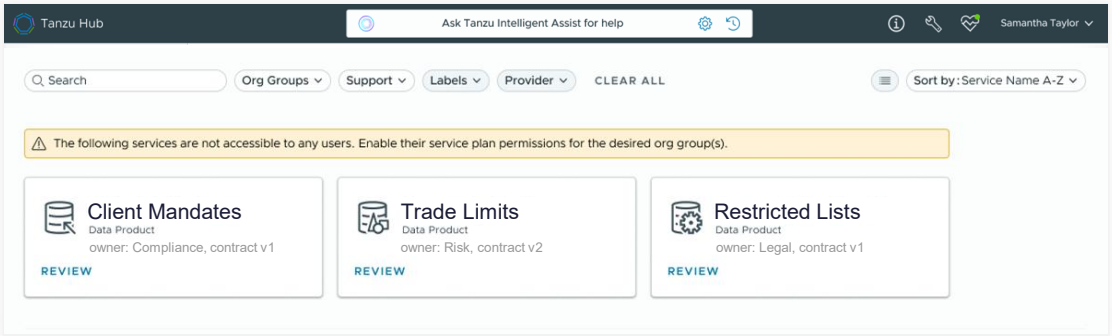


scanned, OCR, or native

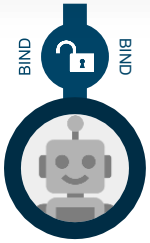
What parsing recovers

- Narrative text + headings
- Tables to rows and columns
- Key values + entities
- Layout, sections, page refs
- Author, date, source, type

Governed data products that agents with explicit access can bind to:



A data product others can find, trust, and bind to an agent



Pre-trade compliance check agent

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Tanzu Platform for agentic AI

The three questions, answered in one platform, on VMware Cloud Foundation

Agent sandbox

Deny by default. Contain before you enable.

Build and harness

Pre-approved skills, tools, and models. Autonomy you control.

Curated marketplace

Everything an agent consumes, from one governed catalog.

Agent governance

Identity, policy, and observability for every action.

AI-ready data

Governed data products with truth, purpose, and provenance.

Millions

of business applications in production

7+ years

continuous uptime for customer business applications

400:1

average app developer to platform engineer ratio

BUILD NOTE: re-skin of Explore 102; the only whole-product slide, deliberately after the argument

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How we can help your teams

Common initiatives we are helping customers with today

Optimized, Secure Coding & SDLC

- Seamless assistant access
- Enhanced code compliance
- Accelerated SDLC
- Optimized prompts and configurations
- Higher quality via parallel coding

AI-assisted App Modernization

- AI-assisted app analysis and guided modernization journey
- Standardized automated upgrades
- Continuous patching

Rapid AI / Agent App Development

- Unified multi-agent platform
- Secured service connections
- Governed tool and model usage
- Enhanced observability for optimization

Come talk to us about your projects

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Thank you

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Appendix: source slides for the designer

Original light-background slides referenced in the build notes. Not for presentation.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How Tanzu is evolving our approach to software

Update

Rethinking organization with a centaur inspired model

Equivalent with security?

PRINCIPLE 01



Institutionalize the Challenger

THE SKEPTIC ROLE

Counter automation bias with a designated rotating role **challenging the outputs**

PRINCIPLE 02



Encode Standards, Remove Variance

BUILD-IN GUARDRAILS

Frameworks and guardrails replace judgment calls with **deterministic outcomes**

PRINCIPLE 03



Leverage Curated Building Blocks

CONSTRAIN DEPENDENCIES

Leverage curated systems and data to constain deployment dependencies

PRINCIPLE 04



Drive Accountability Across Lifecycle

TRANSFORMED SDLC

Cross-functional human-AI pods own delivery and check each other's work



Structure prevents the “confident wrong answer” from reaching production.

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The benefits we're already seeing at Update

Lifecycle Acceleration:

Requirements-to-task assignment phase reduced from **12 weeks to 3 weeks**.

Team coordination efficiency:

Auto-breaking scenarios into Epics and Tasks & auto-assign **Reduced meetings by 30%**

Faster coding:

24m lines of code created or refactored in **6 weeks**

Efficient documentation:

100% AI-generated documentation process

Speed bug analysis and fixes:

Reduced MTTR by **59%**



SUPPORTED BY OUR OWN AGENTIC PLATFORM AS A SERVICE

Remote coding assistants running secure MCP services

Secured, governed agents driving SDLC processes

Test environments with production dependencies and curated data

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Agentic AI blurs software execution and decision making

What makes agents powerful also introduces risk



AI Agent

(Executes Actions)



Acts without being asked twice



Reaches across systems **simultaneously**



Presents uncertainty **as confidence**



Makes commitments on your behalf



Optimizes for **what you said**, not what you meant

The trust and safety gap

Unpredictable agents are difficult to lock down and govern

The AI silo trap

Agents built on isolated stacks restrict innovation on enterprise apps

Agentic system complexity

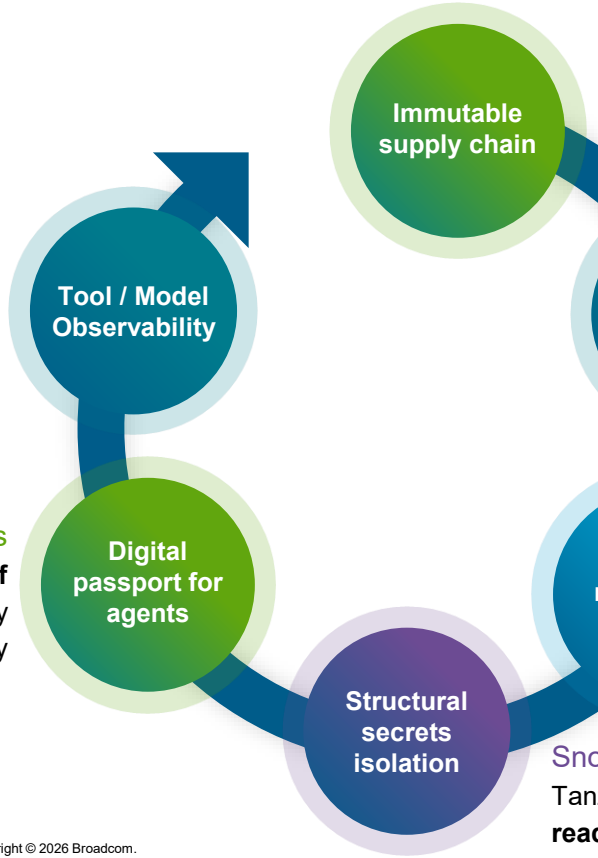
Agent adoption creates operational risk and inconsistency

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

New Agent runtime combats risk of autonomous agents

Agent Runtime



Prompt injection

Protects agents from security threats using trusted Buildpacks instead of arbitrary Dockerfiles.

Runaway loops

Curated resources limit **CPU and memory** to contain runaway agents

Lateral movement

Explicitly grants network access via service bindings so **agents cannot access unauthorized systems**

Snooped secrets

Tanzu Platform structurally **prevents agents from reading another's credentials at runtime.**

Traceability

Every agent tool call and model interaction is **logged and audited** meeting compliance requirements

System level access

Eliminates the **anonymity of autonomous actions** ensuring every tool call is tied to a verifiable identity

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Sovereign data pipelines for agents in Tanzu Platform

Controlled, private data ingestion and access for agents

Sovereign Data Pipelines

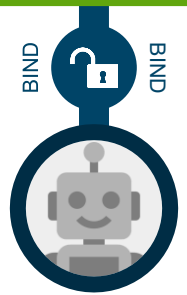
Automated data pipelines and orchestration

Document ingestion	Generate embedding vectors with AI model	Store, index and cluster embeddings
Event-driven process to convert to raw text	Loading & streaming services Embedding service	In DB Analytics Vector store real-time

"What asset classes is this client approved to invest in?"

"What is the single trade authorization limit for this client?"

"Are there any restricted securities or issuers listed?"



Pre-trade compliance check agent

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Alternates for slides 6 and 7

Three options. Pick one pairing and the rest go.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

Three pilot pods. Three weeks of a clogged pipe with a trickle of water coming out.

Everyone expected magic in a couple of hours. What came out was wrong, slow, and not about our platform at all.

BUILD NOTE: simple pipe visual, one line of copy, nothing else

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The airplane and the wheelbarrow

An agent is only as good as the context in front of it.

We asked for an airplane. We got a wheelbarrow. It holds people, and it will get you from Los Angeles to New York in six hours if you run fast enough.

BUILD NOTE: one illustration, airplane vs wheelbarrow; this analogy pays off again at slide 17

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

Three pilot pods, and what fixed them was not a smarter model

Day 1



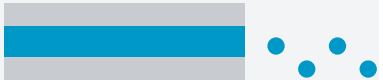
Three pilot pods, high hopes

Weeks 1 to 3



A clogged pipe, a trickle of water

Week 6



The pipe is flowing

Today



Can we make the pipe bigger?

BUILD NOTE: OPTION B, slide 6: the arc from disaster to flow on one strip; pairs with the comparison slide that follows

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The airplane and the wheelbarrow

An agent is only as good as the context in front of it

What we asked for

An airplane.

Carries 40 people.

Los Angeles to New York.

Six hours.

What we got

A wheelbarrow.

Carries people.

Los Angeles to New York.

Six hours, if you run fast enough.

It knew nothing about our platform, our customers, or ten years of history.

BUILD NOTE: OPTION B, slide 7: comparison; the joke lands on the slide, she only has to read it

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

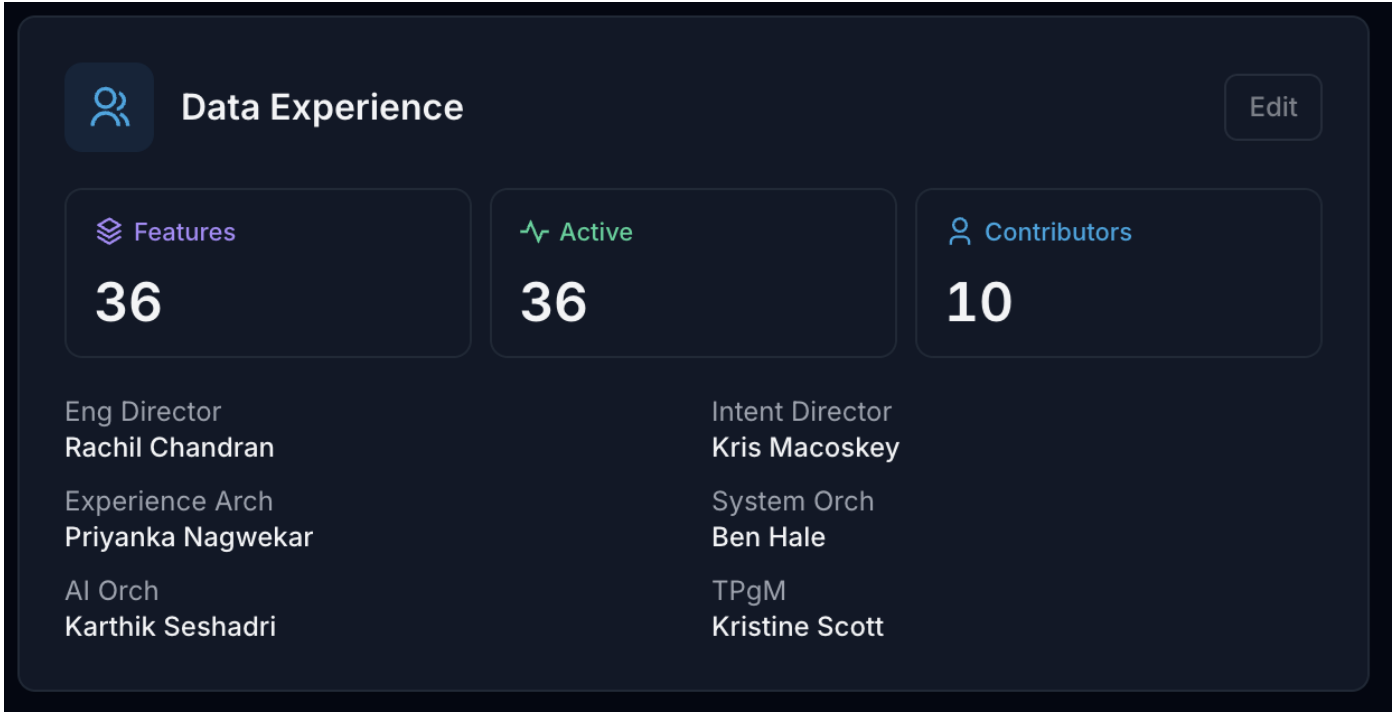
3 weeks **of a clogged pipe with a trickle of water coming out**



Three pilot pods. Everyone expected magic in a couple of hours. What fixed it was not a smarter model.

BUILD NOTE: OPTION C, slide 6: big number form, so it reads differently from the statement slide that follows

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Trust is the throttle for adoption

What we learned building software with agents, and what it means for yours

Purnima Padmanabhan, GM, Tanzu Division, Broadcom |

AI in Finance Summit, London, September 2026

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

VMware Tanzu is the leading provider of Application PaaS and Data Intelligence Services on Private Cloud



Optimized for VMware Cloud Foundation

Tanzu runs best on VMware Cloud Foundation



10 out of top 10 largest financial institutions

Trust VMware with mission-critical workloads



Millions of apps in production

On Tanzu Platform leveraging Cloud Foundry



Trillions of transactions and 1+ Exabyte data

Processed and analyzed by Tanzu Data Intelligence



Leading enterprise framework for AI

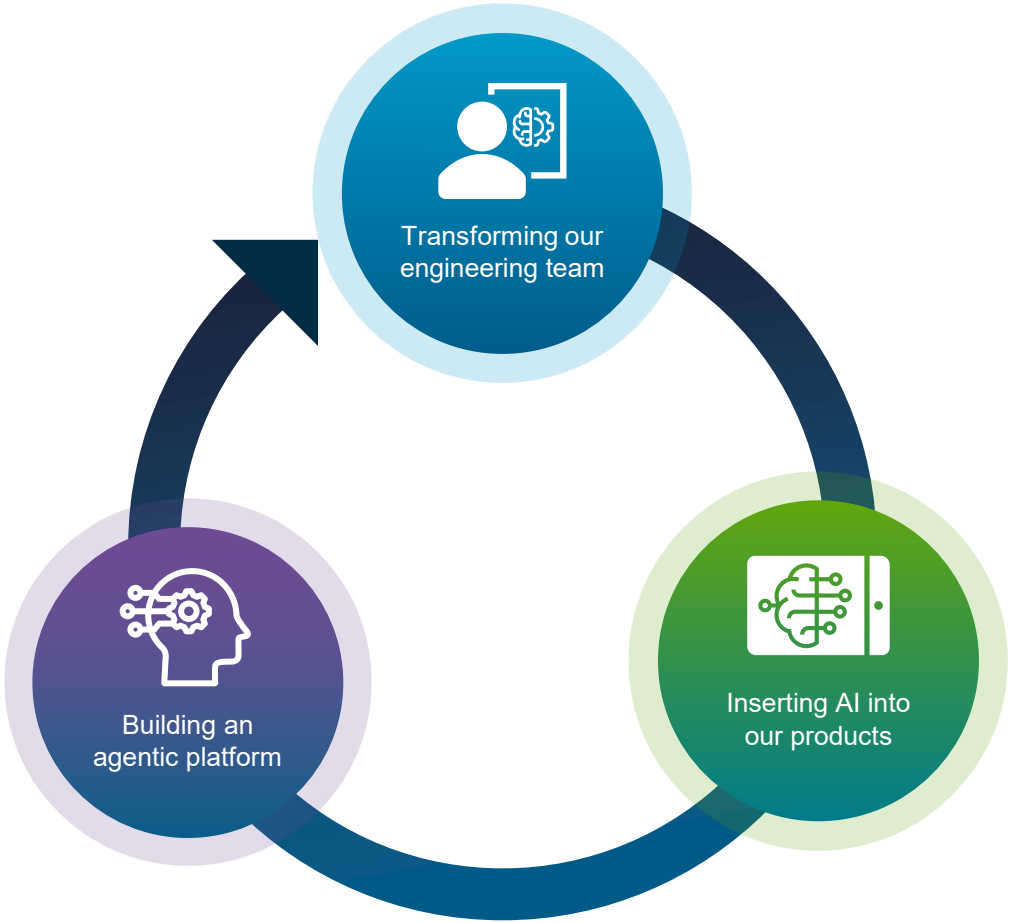
With Spring AI simplifying adoption for millions

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

We sell the platform, and we build our own software on it

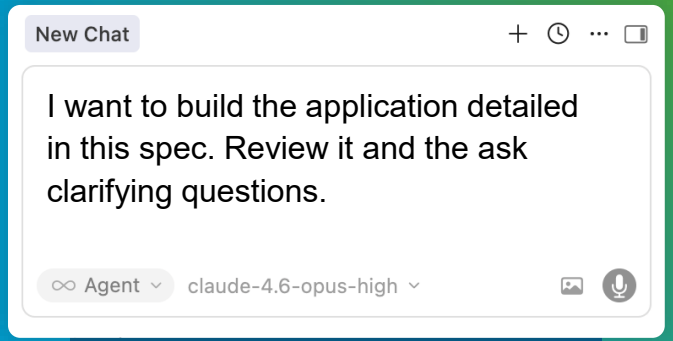
Tanzu Division of Broadcom:
A unique vantage point on AI adoption



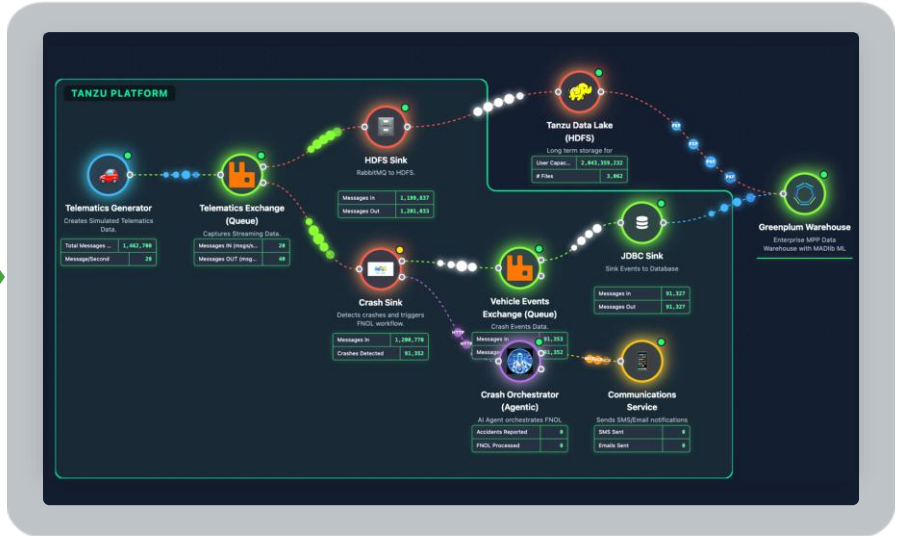
vmware by Broadcom
Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

AI makes software look easy

Example: “vibe coded” greenfield POC software project 1 week from spec to completion



App Specification



1 person

Expert understanding of architecture

Working understanding of business logic

Not a daily coder

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

…but this is not how enterprise software works

Simply adding tools to the existing process and organization doesn’t work

AI solves every problem like it's the first time



AI doesn’t know how or why something had been tried before and failed

Human teams get smarter about their own system over time, AI doesn’t

Perfect syntax hides semantic failures



Syntactically perfect code removes familiar warning signals

AI cannot understand the runtime performance or infer undocumented standards

Adoption is a change management problem



AI threatens craft and ownership

Software expertise doesn't automatically transfer to AI fluency

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

Three pilot pods. Three weeks of a clogged pipe with a trickle of water coming out.

Everyone expected magic in a couple of hours. What came out was wrong, slow, and not about our platform at all.

BUILD NOTE: simple pipe visual, one line of copy, nothing else

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The airplane and the wheelbarrow

An agent is only as good as the context in front of it.

We asked for an airplane. We got a wheelbarrow. It holds people, and it will get you from Los Angeles to New York in six hours if you run fast enough.

BUILD NOTE: one illustration, airplane vs wheelbarrow; this analogy pays off again at slide 17

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three things that fixed it

None of them was a better model

1

Onboard the AI like a new hire

We fed it our history in order of authority: product documentation first, then the knowledge base, then how customers actually use the platform, then years of blogs. Now it starts every feature with that memory.

2

Give it boundaries, not instructions

Four paragraphs of intent produced seventy pages. Prototypes ignored our brand until we handed over the style guide and the approved components. The fix for a bad result is now a written rule, not a code change.

3

Institutionalize the challenger

AI will make mistakes, and beautiful output invites rubber stamps. A designated skeptic reviews what ships, decides which problems are risky enough to go deep, and rotates, because the role fatigues like any other.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

What it produced

Results from our own product and engineering teams, six months in

12 to 3

weeks from requirements to task assignment

59%

reduction in mean time to resolve issues

54%

increase in features delivered versus the previous release

48 hours

from a six-month release cycle to a working prototype

Source: internal Broadcom data; Tanzu Talk, July 2026. Prototype throughput figure applies to the Tanzu Platform product organization.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

A day in the life of a feature

Tanzu Platform agentic software delivery lifecycle

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It runs on the platform we sell

Applications on Tanzu Platform, pushed the same way as millions before them

Secure coding assistants

Running behind governed MCP services, with the tools and models they are allowed to call declared up front.

Governed agents driving the SDLC

Intent, design, build, review, and test agents, each pushed to the platform the same way we have shipped millions of applications.

Test environments with curated data

Production dependencies and governed data products, so what the agent sees in test is what it will see in production.

BUILD NOTE: executive version of Explore 130 and the LD 17 footer; no architecture diagram

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Agentic AI blurs software execution and decision making

Acts before anyone can check

Reaches past what you scoped

Does what you said, not what you meant

BUILD NOTE: Explore 100 re-skinned: scaled to 16:9 at 10in, scheme colors pinned to Explore hues, text set dark; designer to check glow rings on white

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Three questions for every agent

1

What is it made of?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context in front of it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Question 1

1

What is it made of?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context in front of it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Most of your applications are not code you wrote

Question one: what is the agent made of?

You inherit open source, every layer of it

The framework, the libraries under it, the runtime, the container image, and the database your agent queries. Your developers pick one library and inherit hundreds.

Frontier AI now finds flaws faster than communities can fix them

Monthly Spring security advisories are up 1,700 percent. This year we shipped the largest set of security patches in Spring's 23-year history. This is the new normal, not a spike.

BUILD NOTE: merge of TrueSource deck slides 3 and 4; keep the advisory surge chart if it survives simplification

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

AI alone cannot fix your vulnerabilities

Finding is a machine problem. Fixing is a maintainer problem.

1

AI is superb at finding

We use frontier models ourselves to scan and validate at a scale no human team could match.

2

A machine-generated patch is a new risk, not a fix

Patches with no maintainer behind them break compatibility, and the breakage surfaces later, in production. Independent research on AI patching found exactly this pattern.

3

The standard: maintainers author and verify every fix

Curated building blocks with an accountable human behind them. The same lesson as our own pods: boundaries, and a challenger.

BUILD NOTE: from TrueSource deck slide 6; cite the 1Password Off-by-1 Labs study in notes, not on slide

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

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, Node.js, 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

- 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.

Copyright © 2026 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Question 2

1

What is it made of?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context in front of it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

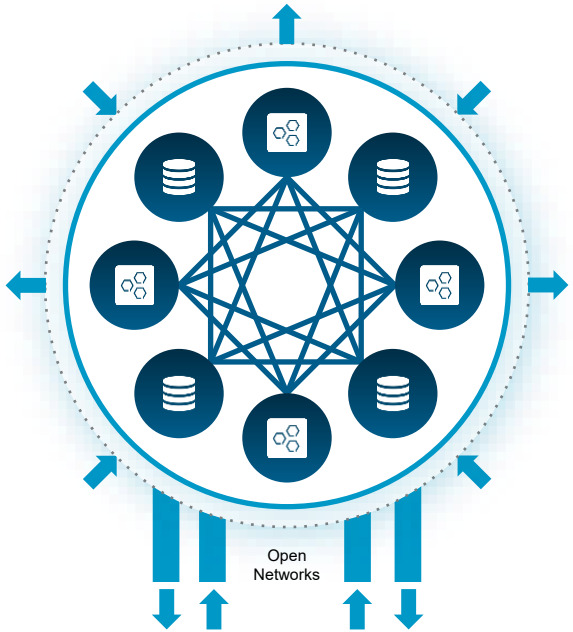
The platform assumption changes everything

Open vs. Deny

Agent Runtime

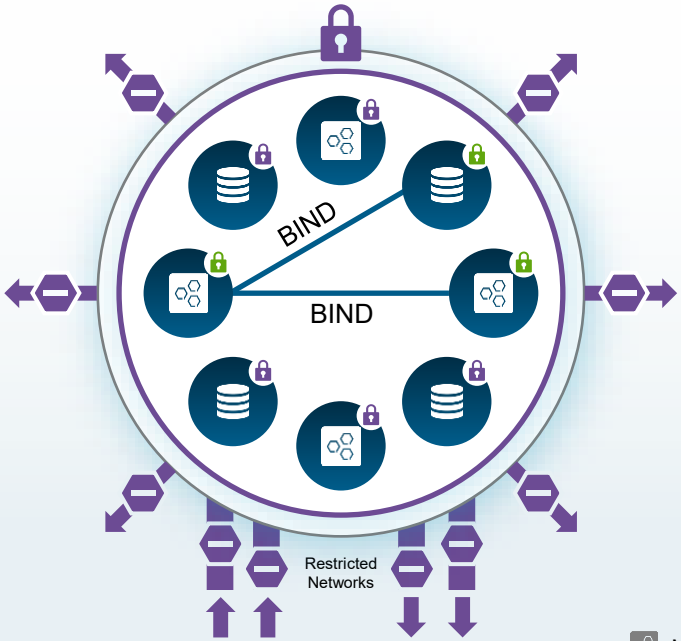
Default cloud-native approach

Microservices discover & connect freely (Cross-namespace)



Our approach: Deny by default

Services isolated explicit grants only



Microservices

Data services

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Safer agent autonomy

Question two: boundaries are declared, not discovered, and no agent is anonymous

1

Reach is declared up front

Explicit routes and service bindings. An agent's connections are known before it runs, not found in an audit afterward.

2

A runaway agent runs out of room, not budget

Resource guardrails across virtual machines and Kubernetes contain loops, retries, and token spend.

3

Credentials are shielded from the agent itself

A prompt injection cannot trick an agent into leaking the keys it runs with, because it never holds them.

BUILD NOTE: executive trim of Explore 104; AgentMinder mentioned verbally as the identity layer, no slide

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Question 3

1

What is it made of?

The open source your agent is built from

2

What are the boundaries around it?

Where it can reach and what it can do

3

What is the context in front of it?

The data it reads and acts on

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Agents read all of your data, and they act on it

Question three: not more data in front of the agent, but data the agent can trust

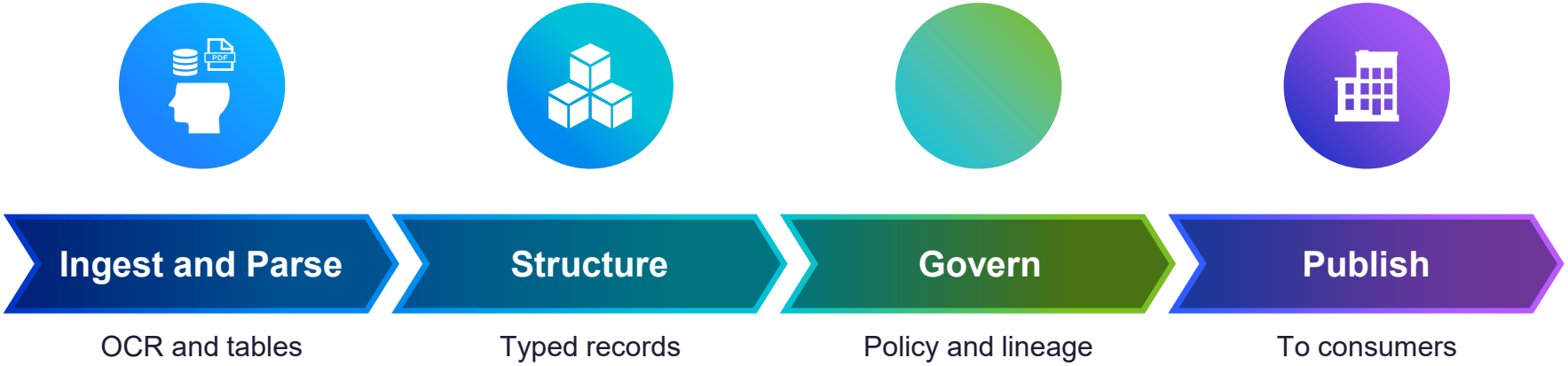


BUILD NOTE: Explore 132 treatment on white, original labels; designer to check pill fills and the glow line

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

AI-ready data in Tanzu Platform

Question three: governed data products, published to agents



BUILD NOTE: Explore 134 treatment on white; Explore title replaced by Broadcom title and subhead

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Tanzu Platform for agentic AI

The three questions, answered in one platform, on VMware Cloud Foundation

Agent sandbox

Deny by default. Contain before you enable.

Build and harness

Pre-approved skills, tools, and models. Autonomy you control.

Curated marketplace

Everything an agent consumes, from one governed catalog.

Agent governance

Identity, policy, and observability for every action.

AI-ready data

Governed data products with truth, purpose, and provenance.

Millions

of business applications in production

7+ years

continuous uptime for customer business applications

400:1

average app developer to platform engineer ratio

BUILD NOTE: re-skin of Explore 102; the only whole-product slide, deliberately after the argument

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How we can help your teams

Common initiatives we are helping customers with today

Optimized, Secure Coding

- Seamless assistant access
- Enhanced code compliance
- Accelerated SDLC
- Optimized prompts and configurations
- Higher quality via parallel coding

AI-assisted App Modernization

- AI-assisted app analysis and guided modernization journey
- Standardized automated upgrades
- Continuous patching

AI / Agent App Development

- Unified multi-agent platform
- Secured service connections
- Governed tool and model usage
- Enhanced observability for optimization

Come talk to us about your projects

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Thank you

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Appendix: source slides for the designer

Original light-background slides referenced in the build notes. Not for presentation.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How Tanzu is evolving our approach to software

Rethinking organization with a centaur inspired model

Update

Equivalent with security?

PRINCIPLE 01



Institutionalize the Challenger

THE SKEPTIC ROLE

Counter automation bias with a designated rotating role **challenging the outputs**

PRINCIPLE 02



Encode Standards, Remove Variance

BUILD-IN GUARDRAILS

Frameworks and guardrails replace judgment calls with **deterministic outcomes**

PRINCIPLE 03



Leverage Curated Building Blocks

CONSTRAIN DEPENDENCIES

Leverage curated systems and data to constain deployment dependencies

PRINCIPLE 04



Drive Accountability Across Lifecycle

TRANSFORMED SDLC

Cross-functional human-AI pods own delivery and check each other's work



Structure prevents the “confident wrong answer” from reaching production.

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The benefits we're already seeing at Update

Lifecycle Acceleration:

Requirements-to-task assignment phase reduced from **12 weeks to 3 weeks**.

Team coordination efficiency:

Auto-breaking scenarios into Epics and Tasks & auto-assign **Reduced meetings by 30%**

Faster coding:

24m lines of code created or refactored in **6 weeks**

Efficient documentation:

100% AI-generated documentation process

Speed bug analysis and fixes:

Reduced MTTR by **59%**



SUPPORTED BY OUR OWN AGENTIC PLATFORM AS A SERVICE

Remote coding assistants running secure MCP services

Secured, governed agents driving SDLC processes

Test environments with production dependencies and curated data

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Agentic AI blurs software execution and decision making

What makes agents powerful also introduces risk



AI Agent

(Executes Actions)



Acts without being asked twice



Reaches across systems **simultaneously**



Presents uncertainty **as confidence**



Makes commitments on your behalf



Optimizes for **what you said**, not what you meant

The trust and safety gap

Unpredictable agents are difficult to lock down and govern

The AI silo trap

Agents built on isolated stacks restrict innovation on enterprise apps

Agentic system complexity

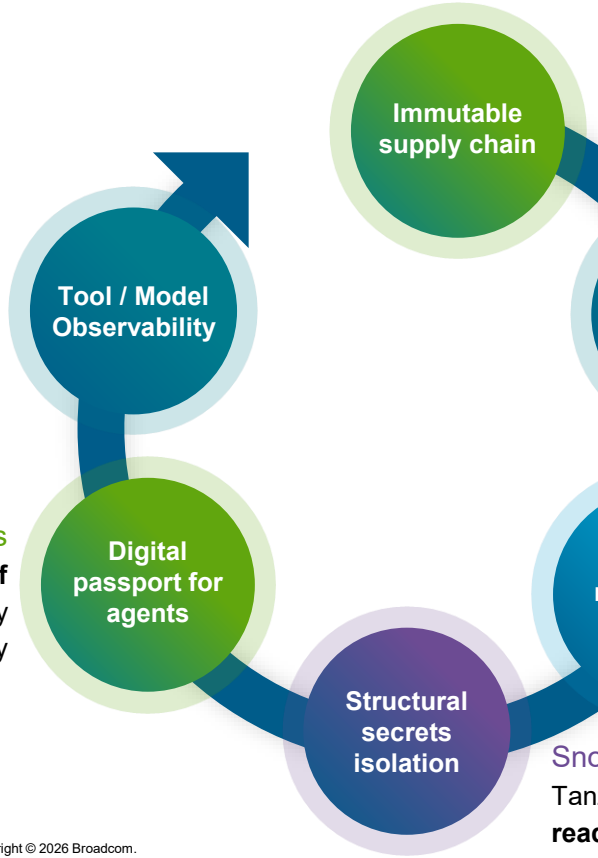
Agent adoption creates operational risk and inconsistency

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

New Agent runtime combats risk of autonomous agents

Agent Runtime



Prompt injection

Protects agents from security threats using trusted Buildpacks instead of arbitrary Dockerfiles.

Runaway loops

Curated resources limit **CPU and memory** to contain runaway agents

Lateral movement

Explicitly grants network access via service bindings so **agents cannot access unauthorized systems**

Snooped secrets

Tanzu Platform structurally **prevents agents from reading another's credentials at runtime.**

Traceability

Every agent tool call and model interaction is **logged and audited** meeting compliance requirements

System level access

Eliminates the **anonymity of autonomous actions** ensuring every tool call is tied to a verifiable identity

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Sovereign data pipelines for agents in Tanzu Platform

Controlled, private data ingestion and access for agents

Sovereign Data Pipelines

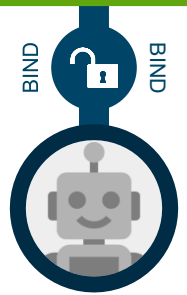
Automated data pipelines and orchestration

Document ingestion	Generate embedding vectors with AI model	Store, index and cluster embeddings
Event-driven process to convert to raw text	Loading & streaming services Embedding service	In DB Analytics Vector store real-time

"What asset classes is this client approved to invest in?"

"What is the single trade authorization limit for this client?"

"Are there any restricted securities or issuers listed?"



Pre-trade compliance check agent

vmware by Broadcom

Broadcom Proprietary and Confidential. Copyright © 2026 Broadcom.
All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Alternates for slides 6 and 7

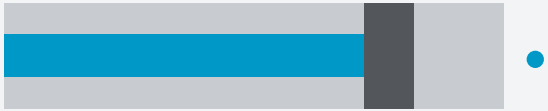
Three options. Pick one pairing and the rest go.

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

An agent is only as good as the context in front of it

Three weeks of a clogged pipe



Three pilot pods. Everyone expected magic in a couple of hours. What came out was a trickle, and it was wrong.

We asked for an airplane. We got a wheelbarrow.

What we asked for

Carries 40 people, Los Angeles to New York in six hours.

What we got

Carries people. Gets you there in six hours if you run fast enough. Knows nothing about our platform.

BUILD NOTE: OPTION A: one slide replaces 6 and 7; illustrations for pipe and wheelbarrow to come from design

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

Three pilot pods, and what fixed them was not a smarter model

Day 1



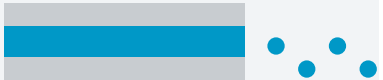
Three pilot pods, high hopes

Weeks 1 to 3



A clogged pipe, a trickle of water

Week 6



The pipe is flowing

Today



Can we make the pipe bigger?

BUILD NOTE: OPTION B, slide 6: the arc from disaster to flow on one strip; pairs with the comparison slide that follows

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

The airplane and the wheelbarrow

An agent is only as good as the context in front of it

What we asked for

An airplane.

Carries 40 people.

Los Angeles to New York.

Six hours.

What we got

A wheelbarrow.

Carries people.

Los Angeles to New York.

Six hours, if you run fast enough.

It knew nothing about our platform, our customers, or ten years of history.

BUILD NOTE: OPTION B, slide 7: comparison; the joke lands on the slide, she only has to read it

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

It started as a disaster

3 weeks

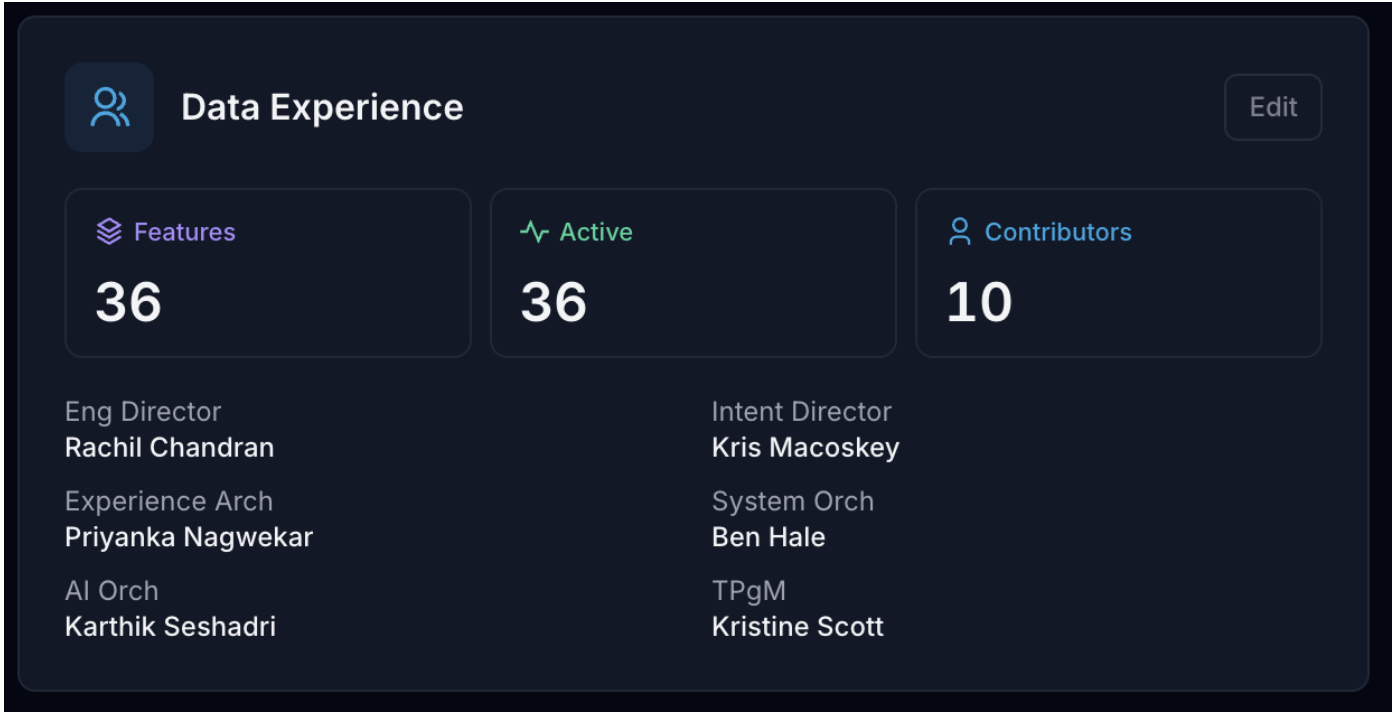
of a clogged pipe with a trickle of water coming out



Three pilot pods. Everyone expected magic in a couple of hours. What fixed it was not a smarter model.

BUILD NOTE: OPTION C, slide 6: big number form, so it reads differently from the statement slide that follows

Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.



Copyright © 2026 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.