# How AWS internal teams approach application security

At Amazon Web Services (AWS), security is our top priority. Through experience, we have learned that building secure, innovative applications rapidly and cost-effectively is about three things: people, practices, and technology.

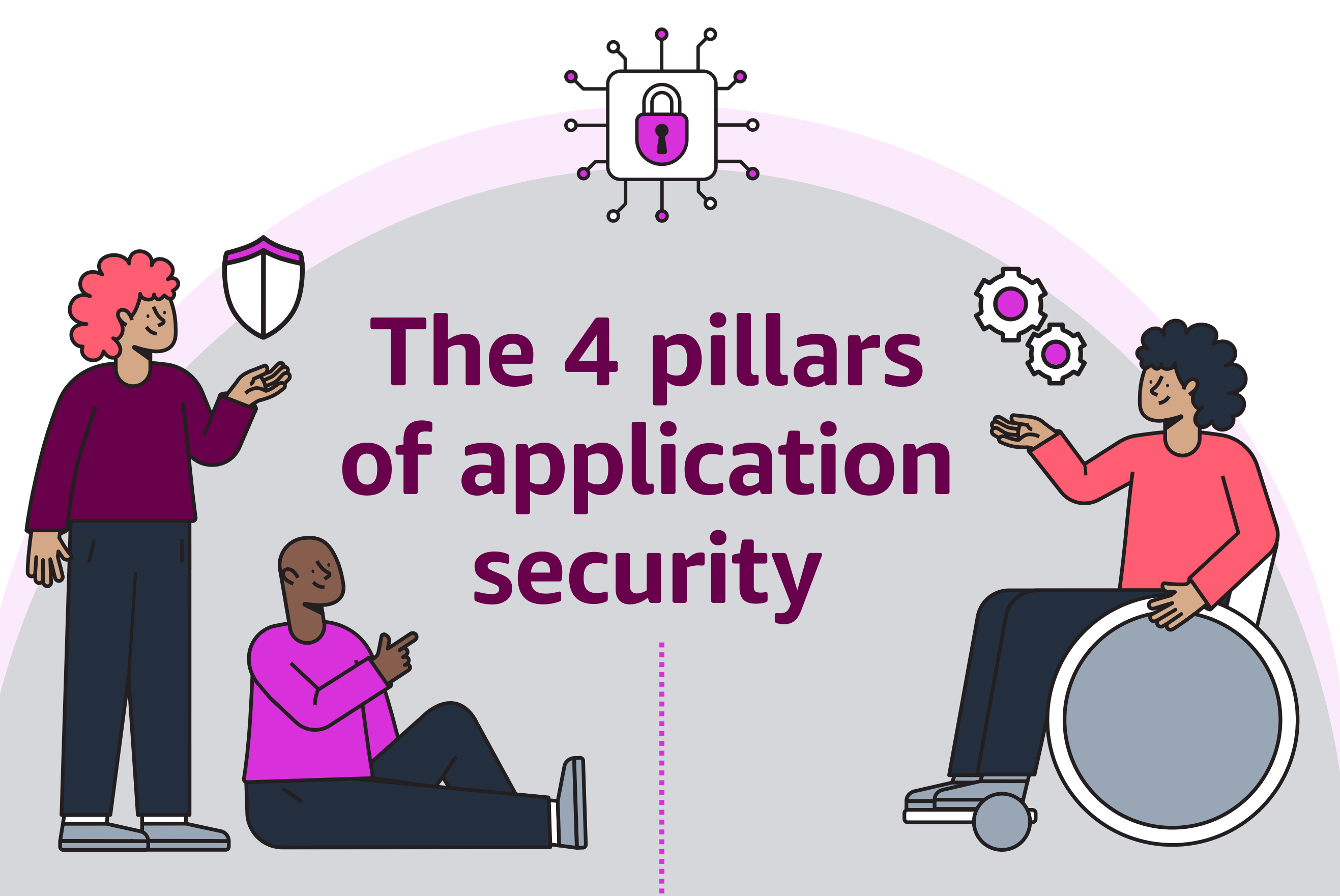
As a result, we've implemented application security (AppSec) approaches that weave these things together for our internal teams to reduce security issues and speed up our pace of innovation. In this infographic, we'll outline some of these approaches that you can replicate.

## What is AppSec—and why is it important?

AppSec is the set of people, practices, and technologies designed to continuously evaluate the security properties of applications during all phases of the software development lifecycle (SDLC).

**You need AppSec to:**

- **Improve software posture**
- **Address vulnerabilities early**
- **Increase delivery speed**



# The 4 pillars of application security

PILLAR 1

## A culture of security

**Integrate security best practices at scale.**

### Distributed security ownership

Because our leadership prioritizes security, it's understood within AWS that security is everyone's job. Security teams and product development teams work together to help ensure that products are built and shipped securely. Despite this collaboration, the development teams own the security of their product. They are responsible for making sure that security controls are built into the product and that customers have the tools they need to use the product securely.

### Security Guardians program

Developer teams own the security of what they're building. To ensure this at AWS, we train a subset of developers on security standards and best practices, so they can act as **security ambassadors** within development teams, promoting best practices and embedding security at earlier stages of the SDLC.

### Results compared to good intentions

This process provides faster security reviews and a scalable way to spread good security practices without significantly increasing headcount. For AWS, this resulted in **over 20 percent fewer security issues and almost 30 percent less time spent during review**.

### A look inside

Amazon's Games, Media, and Entertainment (GME) division is constantly innovating to provide access to world-class entertainment through Amazon Originals, Prime Video, Audible, Amazon Games, Twitch, Amazon Music, Prime Gaming, and more. Amazon's digital entertainment products enable millions of customers to access the latest apps and games; stream or download movies, TV shows, and music; and access their own files anywhere in the world.

amazon

> *"The Amazon GME Security team is focused on creating a customer driven security culture by making security a business enabler. We collaborate with engineering teams to create a friction free experience for security to be applied across the development lifecycle, and aligned with the development team's top business objectives. This approach allows Amazon to scale security, without slowing down development, in order for development teams to continue to drive innovation on behalf of our customers."*
>
> **Brian Lozada, Security Director for Amazon GME**

PILLAR 2

## Security in your pipeline

**Apply security checks at every stage—from the moment your teams start writing code through to deployment—so you can resolve security concerns as they arise.**

At AWS, we deploy over 150 million times per year. To maintain our high security bar, we define relevant controls using threat modeling, then use automation to enforce best practices through the pipeline. Here are some of our best practices that you can replicate:

- Identify key threats and associated mitigations by threat modeling in the design phase before code development even begins
- Reduce mean time to detection on code security issues by identifying vulnerabilities during the authoring process
- Automate pipeline governance to include both preventative and detective controls—including controlled artifact repositories and SAST and DAST scans
- Define secure pipeline flow control mechanisms, such as branch protection rules and automerge limitations, to protect production deployments

For a more complete list, review the **Deployment Pipeline Reference Architecture**.

### AWS services that can help increase security in your pipeline

**Amazon Inspector**
Scan for insecure third-party packages in AWS and for security vulnerabilities in Amazon Elastic Compute Cloud (Amazon EC2) instances, containers, and serverless functions

**Amazon CodeGuru Security**
Conduct static code analysis to identify security flaws in first-party software source code

**Amazon Q**
Help remediate the identified issues with an IDE plugin that offers generative artificial intelligence (AI)-powered code suggestions

**AWS Secrets Manager**
Store, manage, and secure secrets

PILLAR 3

## Security of your pipeline

**Understand the potential threats that your continuous integration and delivery (CI/CD) pipelines and code repositories face, so you can implement effective security measures.**

**Threats and significant security risks** include unauthorized code changes, insecure dependencies, compromised build environments, inadequate access controls, unencrypted communication, and weak authentication mechanisms.

AWS assesses and prioritizes threats to develop a resilient security strategy. Key security controls for CI/CD pipelines in cloud workloads include:

### Pipeline configuration management

Manage configurations as code under version control, and include rigorous reviews for any changes.

### Restricted access control

Limit access to the CI/CD pipeline infrastructure to authorized personnel only. Use Zero Trust and identity-based least privilege access controls.

### Pipeline security scanning

Periodically scan the infrastructure hosting the CI/CD pipeline for vulnerabilities. This includes servers, containers, and other components used in the pipeline process.

### AWS services that can help increase the security of your pipeline

**Amazon CodeCatalyst**
Centralized and secure access management to help organizations collaborate and scale fluidly across teams

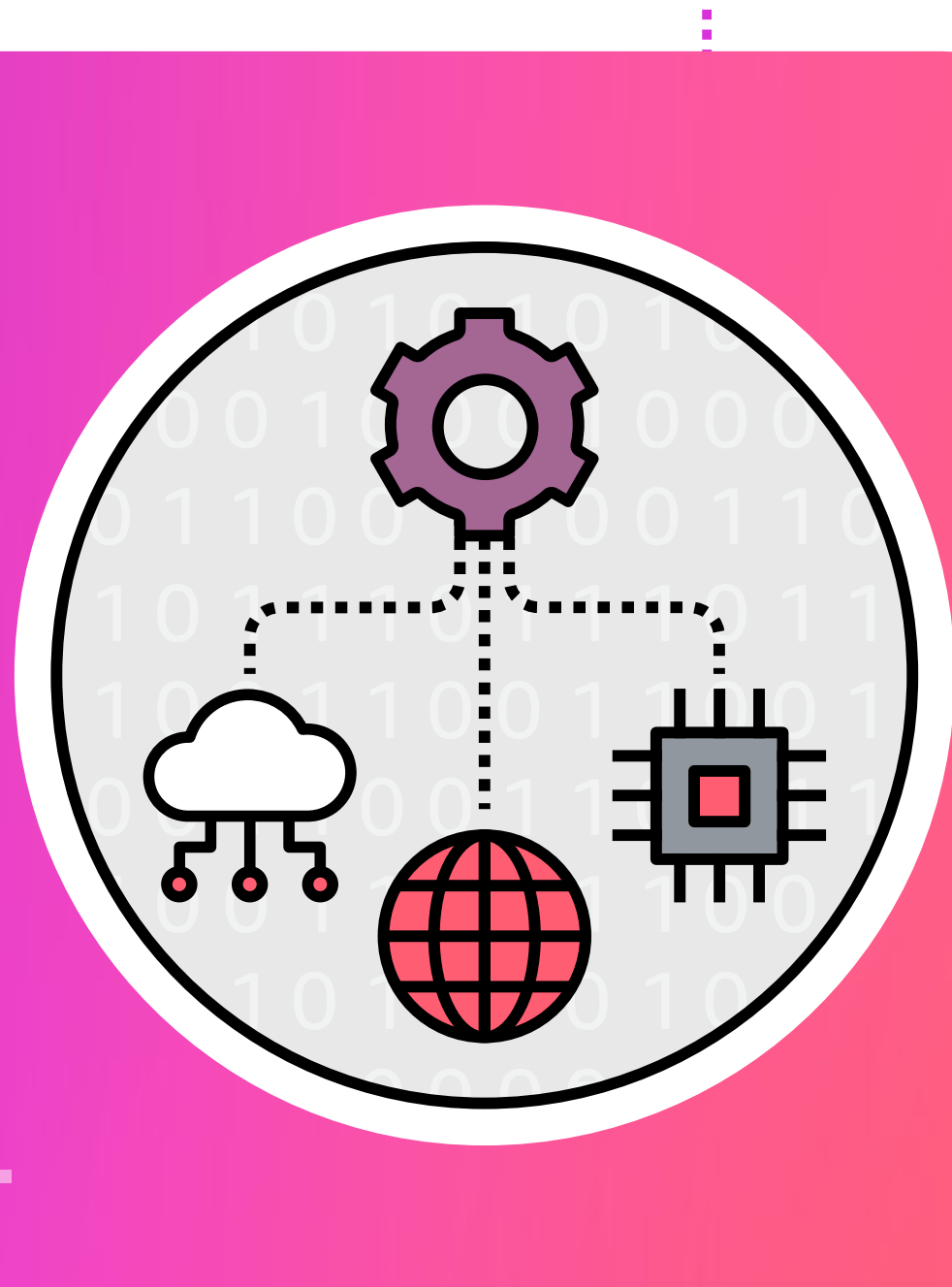
**AWS Signer**
Code validation against a digital signature to confirm that the code is unaltered and from a trusted publisher

**AWS CodeBuild**
Fully managed build service used to perform security testing

**AWS CodePipeline**
Continuous delivery service that integrates CodeBuild, alerts key stakeholders of security issues, and helps manage code releases

PILLAR 4

## Supply chain management



**Monitor and review each component in your software supply chain that's part of an application or interacts with it during the SDLC.**

At AWS, we monitor and review every third-party component in our supply chain to reduce risk.

AWS uses and contributes to multiple industry-wide supply chain frameworks and risk assessment tools. We recommend the following:

### SLSA

Industry-agreed guidelines for supply chain security

### NIST SSDF

Industry-vetted security best practices that span the SDLC

### OSSF Scorecard

An AWS-backed project to help open-source maintainers and open-source consumers improve their security

### Take a proactive stance on application security

A software bill of materials (SBOM) is a nested inventory of all the open-source and third-party software components of your codebase. An SBOM can be a useful tool for software development teams to identify vulnerabilities and ensure software integrity because it underpins your supply chain management. If you don't yet know everything that will go into your application, then you likely don't know what needs to be secure.

Amazon Inspector aids in automating the detection of software vulnerabilities to secure the software supply chain. A combination of Amazon Inspector and SBOMs equips organizations to effectively manage supply chain risks, help ensure compliance with industry and organizational standards, and protect against threats.

Southwest®

> *"If our security system is not running, we're not flying. So having the robust security posture and capabilities we achieve on AWS is critical for us."*
>
> **Jon Barcellona, Former Cybersecurity Engineering Director, Southwest Airlines**

# Get started

**Discover how to incorporate AppSec throughout the SDLC.**

**Learn more about security, identity, and compliance on AWS.**

**Learn more about threat modeling best practices on AWS.**