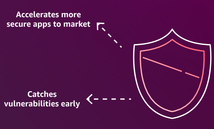
How to infuse security into DevOps

Security remains a top priority—as more organizations migrate, build, and scale applications in the cloud. And, as more organizations integrate security into the DevOps process, they are finding new opportunities to accelerate innovation. Learn why many security leaders are embracing the efficiency and automation of DevSecOps.

A culture of DevSecOps drives value across the app lifecycle



4 steps to make security a business enabler

1 Cultivate a security culture

Moving successfully to a DevSecOps model goes beyond the adoption of new cloud technologies and best practices. It means embracing a fresh mindset—and a culture that delivers smarter, safer applications by integrating security at every stage of the software development process.

CORE COMPONENTS OF A SECURITY CULTURE:

Communication
Promoting cultural change from the top

People
Security and DevOps teams excel by working together

Technology
Automate security to accelerate delivery at scale

Process
Security is fully integrated at every stage

"In order for us to remain trusted partners for our everyday entrepreneurs, security has to be part of our DNA."

Bindi Davé, Former Director of InfoSec, GoDaddy

2 Shift security left

"Shifting left" is the modern process of analyzing applications for vulnerabilities from the earliest stages of the build. Software teams that actively shift left can integrate secure code into the DevSecOps process, which helps prevent potential breaches from infecting apps during or following development.

SHIFT LEFT WITH AMAZON WEB SERVICES (AWS):

- Analyze, develop, and secure code with **AWS CodeCommit**
- Externalize and scale authorizations with **Amazon Verified Permissions**
- Centralize your security with **Amazon Security Lake** data
- Implement frictionless authentication with **Amazon Cognito**

"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, Cybersecurity Engineering Director, Southwest Airlines

3 Shift security right

Ready to make security a business enabler post-launch? Focus on security after the application is deployed. Some vulnerabilities may escape earlier checks and become apparent only when customers use your software. "Shifting right" helps continuously protect both application and customer data.

RUN RIGHT WITH AWS:

- Secure apps from vulnerabilities with **AWS Shield**
- Protect access to corporate apps with **Amazon Verified Access**
- Automate vulnerability management at scale with **Amazon Inspector**
- Centralize security checks and alerts with **AWS Security Hub**

"We've taken a disciplined approach to refining and redefining processes in the AWS Cloud, which provides a clearer picture to manage issues and understand the implications of change."

Sten Christensen, Former DPIE Senior Team Leader, SEED

4 Automate security everywhere

Automation liberates your security teams to focus on high-value tasks. Start reducing human error and scaling security best practices across your business. Learn how the DevSecOps model empowers scanning tools that keep security evaluations from disrupting your business momentum.

AUTOMATE WITH AWS:

- Protect against distributed denial-of-service (DDoS) attacks with **AWS Shield Advanced**
- Scan cloud and containers continually with **Amazon Inspector**
- Provide secure, frictionless authentication with **Amazon Cognito**
- Build Infrastructure as Code (IaC) with **AWS CloudFormation**

"...(Amazon Inspector) allows us to focus on vulnerability remediation, rather than managing multiple discovery tools and configurations."

Paul Clarke, Head of Security, Canva

Take the direct route to DevSecOps with AWS

Rapid development and secure applications are no longer mutually exclusive. Experience fewer obstacles on the road to DevSecOps with AWS.

Learn about our cloud services for modern apps.

Learn more

Explore AWS Cloud security solutions.

Explore