DevSecOps
SOLUTION GUIDE

In the early days of application development, production teams were siloed; coders focused on coding; quality assurance (QA) focused on their testing; and system administrators focused ongoing maintenance. This segmented approach led to many inefficiencies in the build process, but in the last decade, the Development and Operations (**DevOps**) model has restructured the design process, integrating these teams into close collaborative units. While there are benefits to DevOps—developer teams are more **agile**, product goes to market quicker, teams innovate faster—security is still segmented and siloed away from core development functions. But as the rate of cyberattacks increase, security cannot remain separate from the DevOps process. **Security** must be integrated early and throughout development. Many commercial and federal organizations, however, struggle to bring security under the DevOps umbrella.

ECS helps organizations unite IT operations, security, and development into a seamless product pipeline with our development, security, and operations (**DevSecOps**) solutions. Through fast, flexible, and responsive application development, ECS protects your code from concept to implementation and operation, resulting in a stronger and more effective product every time.

CONTINUOUS INTEGRATION/CONTINUOUS DEVELOPMENT (CI/CD)

CHALLENGE: Your changes take too long to get into users' hands, delaying user feedback and subsequent development.

SOLUTION: Based on your project's size, complexity, and specific technical requirements, ECS establishes a DevSecOps pipeline with an automated CI/CD model. By automating aspects of the integration and delivery processes, ECS ensures a unified state of product between your developers and enables your organization to increase their iteration and testing rate, resulting in more frequent releases and smaller code changes. Code can go live within minutes of writing it, making it much easier to continuously receive and incorporate user feedback.

TESTING

CHALLENGE: Manual testing is very time intensive and error prone. Fixing errors late in development is costly.

SOLUTION: With our CI/CD solution, ECS ensures error testing at each stage of the pipeline from development and integration to staging and beyond. ECS automates the testing of repetitive tasks and processes helping to minimize delays and bottlenecks in development. After the tests pass, ECS applies release policies for final deployment approval. ECS conducts safe Green/Blue deployment to minimize risks and reduce errors from making into production, improving quality and reducing the cost to fix errors. Similarly, ECS also applies A/B testing and Canary testing methods once a release is deployed.

ACCESS CONTROL

CHALLENGE: You worry that malicious actors will use root or admin access to deploy payloads during development.

SOLUTION: ECS secures your development processes through privilege control, rotating access keys, and strong password policies, which allow organizations to expedite workflows without providing unrestricted access to multiple individuals. By leveraging these tightened access controls, ECS tracks users and changes through every stage of the development process, ensuring a clean audit trail when it comes time for compliance.

ECS also consolidates identities at a single point of entry, so users can access what they need from a variety of applications without having to go into each account separately, cutting down on the number of entry points while reducing the attack surface.

AUTOMATED DESIGN

CHALLENGE: Implementing compliance and security policies is difficult and time-consuming for your developers.

SOLUTION: With automated security tools for code analysis, configuration management, patching, and vulnerability management, ECS designs scalable security processes for the entire DevSecOps pipeline. By leveraging automation, ECS minimizes the risk of human error and associated vulnerabilities while reducing the overhead that comes with managing software and infrastructure. ECS also builds compliance and security controls into the release pipeline, increasing efficiency and consistency while mitigating security flaws.

ACTIVE MONITORING

CHALLENGE: The development process is daunting, and your organization lacks the time, budget, and operational manpower to monitor the build.

SOLUTION: ECS tests security at every stage of a build, ensuring security is a constant part of the product lifecycle. If a build fails, ECS' cross-functional teams of developers and testers quickly deliver new iterations in an upwardly evolving and collaborative programming environment. Our experts continually monitor events and metrics for abnormal behavior, capturing and remediating vulnerabilities before they become post-production issues. Once the product has been released, ECS continues to monitor 24/7/365, ensuring your application remains secure even post-development.

Interested in learning more about ECS' DevSecOps solutions?
Reach out and **talk to an expert** at **cloud@ecstech.com**

ECS is a leading information technology provider delivering solutions in cloud, cybersecurity, software development, IT modernization, and science and engineering. The company's highly skilled teams approach and solve critical, complex challenges for customers across the U.S. public sector, defense, and commercial industries. ECS maintains partnerships with leading cloud and cybersecurity technology providers and holds specialized certifications in their technologies.