Symantec

DevOps + InfoSec
The New Dynamic Duo

The current strategic divide between DevOps and InfoSec is rooted in competing objectives. Developers are driven to rapidly deliver new applications, while cyber security teams are tasked with methodically ensuring the applications cannot be compromised. DevOps and InfoSec need to integrate their processes (a function called DevSecOps) and work collaboratively to secure organizations as their reliance on public cloud infrastructure grows.

DevSecOps inserts the Information Security function into the Continuous Integration (CI)/Continuous Development (CD) agile framework.

Villains in the Cloud

Security events in the cloud are increasing exponentially and becoming more dangerous. Threat monitoring and policies aren't enough, which only raises the tension between agility and security.

8500%
increase in coin miner detections, creating new vectors for cloud breaches[1]

1 in 13
web requests lead to malware (+3%)[2]

Only 37%
of security managers say they can adequately analyze threat data[3]

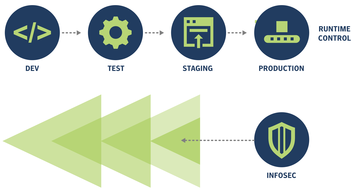
24%
of successful cloud exploits happen at the app layer[2]

[1] Symantec Internet Security Threat Report, Volume 23, March, 2018.
[2] Symantec 2018 Shadow Data Report
[3] Oracle and KPMG 2018 Cloud Threat Report, February 2018.

Shifting Security Left

Traditionally, security has been bolted on at the end. With continuous integration and continuous delivery (CI/CD), there is an opportunity to insert security into pre-deployment earlier on, as well as the development, testing and production environments.

CI/CD PIPELINE



Wonder Powers Unite

Simply put, DevOps and InfoSec are better together.
With integration at each stage, better compliance and enhanced collaboration, threats don't stand a chance.

How companies are planning to deploy DevSecOps[4]
(Percent of respondents, N=303, multiple responses accepted)

46%
will identify workload configuration vulnerabilities before deployment to production

42%
will identify software vulnerabilities before deployment to production

41%
will identify workload configurations that are out of compliance with a regulation before deployment to production

[4] ESG Master Survey Results, Trends in Hybrid Cloud Security, March 2018.

5 STEPS TO BETTER SECURITY

The Dynamic Duo Action Plan

1 **Embrace the shared responsibility model.**
Approach for the relationship between the DevOps team and the security team—both teams need to work collaboratively to secure public cloud infrastructure.

2 **Apply security at all layers in the CI/CD pipeline.**
Shift left for planning, shift right for runtime. This moves security management to a continuous validation mode. The cloud allows you to change things or move things really rapidly and in a software-driven way.

3 **Implement a "least privilege" approach.**
Adopt a "least privilege" approach upfront and if you are just starting down the DevSecOps path, focus on the users and apps that have the most risk for your business.

4 **Protect data in transit and at rest.**
Leverage the agile software development processes to write cyber security-related use cases with data protection foremost in mind.

5 **Embed a security professional or engineer within DevOps.**
Ensure security is a regular discipline in CI/CD pipeline by having developers and InfoSec professionals working elbow-to-elbow.

Learn how Symantec Cloud Workload Protection (CWP) can help you automate security into the development workflows:

Try Symantec Workload Protection free of charge!*

Symantec.

* 20,000 hours of free usage, valid for 89 days. Details.