Tripwire for DevOps

All-in-One SaaS Security

Tripwire® for DevOps is a comprehensive security SaaS that evaluates container images for vulnerabilities in a sandboxed cloud environment. It equips DevOps teams with a complete security assessment of new application builds as they move through the continuous integration and continuous delivery (CI/CD) toolchain from development to production, providing a quality gate teams can use to fail builds of applications based on customizable security compliance and configuration standards.

"The days are over when we just reviewed application security and the environment at the end of a project. Now we have to integrate that into daily work."

— Gene Kim, Author of *The DevOps Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations*

Dynamic vs. Static Analysis

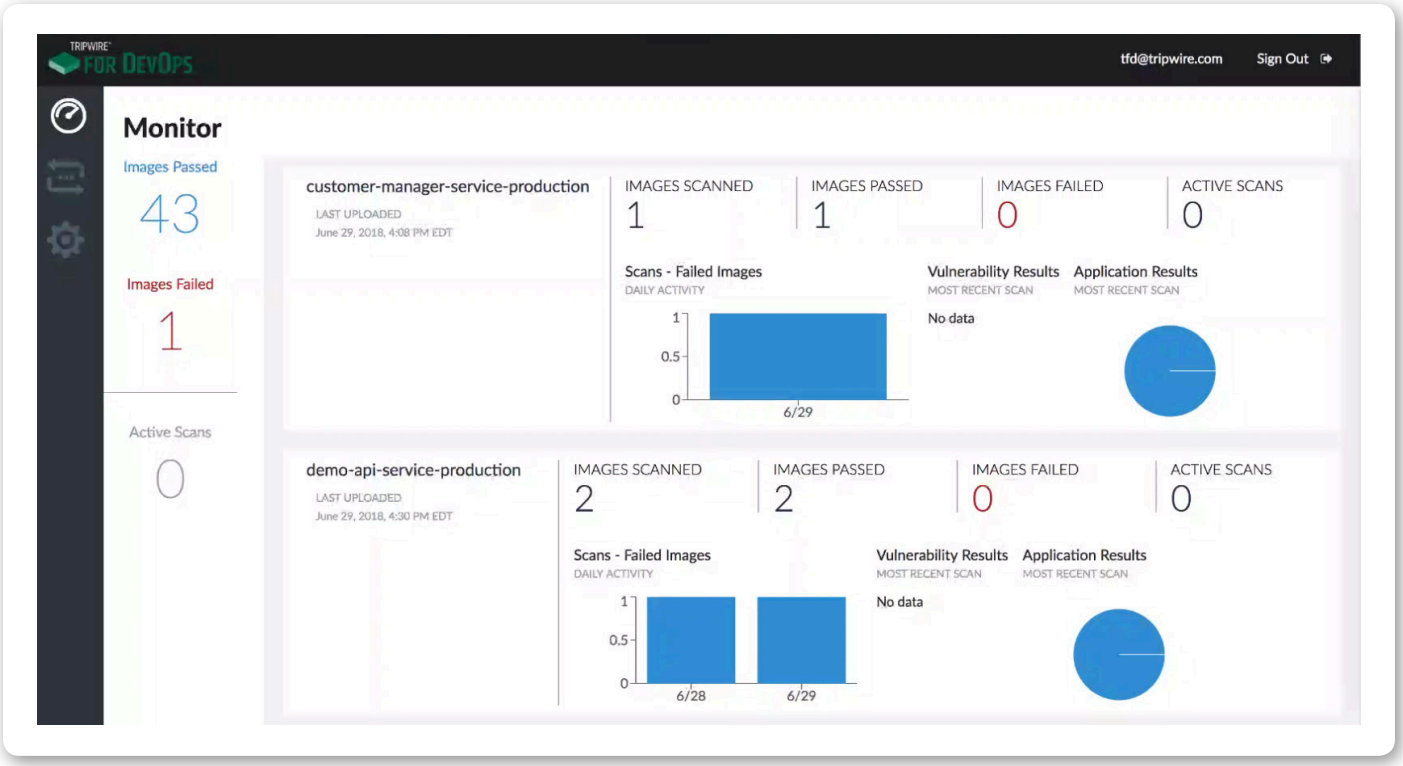
Security breaches like the one Equifax made headlines with in 2017 are avoidable with Tripwire for DevOps. Registries hold the application dependency file list that makes up a container, and some security solutions only scan that file list for known vulnerabilities. Breaches like Equifax's occur when teams only scan their containers for vulnerabilities in this static state, because some vulnerabilities only emerge when a container is running.

The best case scenario for those using static analysis is discovering and remediating vulnerabilities during production. Tripwire for DevOps uses a sandbox environment to spin up containers in the cloud for dynamic analysis with all apps running so you can discover and remediate vulnerabilities before production.

Integrate Compliance

Tripwire for DevOps does more than catch vulnerabilities—it also scans for compliance with industry best practice frameworks like the Center for Internet Security's CIS Controls. Compliance policy alignment is tested through your customizable quality gate, giving you clear visibility into the remediation steps you need to take to return to compliance. Tripwire manages over 130,000 different vulnerability rules and has the broadest set of compliance combinations and policies, which are updated continuously.

When distributing applications using containers, it's common to start with a "base image" created by someone else. But how do you know its configuration is secure and compliant? Tripwire for DevOps lets you compare the security and compliance postures of various base images to not only improve security, but also reduce time spent remediating deficiencies in base images. In addition, it evaluates containers as they're being worked on to make sure they're becoming more compliant over time and configuration issues aren't creeping in—issues that would be costly to fix at the end of the delivery cycle.



The Tripwire for DevOps dashboard provides at-a-glance information on active scans as well as which of your images have passed or failed.

Integration with Your CI/CD Toolchain

Security shouldn't slow down continuous integration and delivery. Tripwire for DevOps provides native capabilities for system vulnerability assessment and security configuration auditing, as well as integrations with the popular CI/CD pipeline tools and REST API availability for custom integrations.

Docker

Push your Docker images to Tripwire for DevOps' hosted Docker registry. Tripwire for DevOps can also periodically scan external image registries like Docker V2 and Amazon ACR. The Tripwire Docker tool has push, status and results commands, and uses Docker Compose containers.

We support CIS benchmarks for these Linux distributions:

- » Amazon Linux
- » Ubuntu
- » Debian
- » CentOS
- » RHEL
- » Oracle Linux
- » SUSE

Supported registries include:

- » Amazon ECR
- » Docker Registry
- » Azure Registry
- » Quay.io Registry
- » Google GCR

AWS

You don't need to worry about Amazon Cognito authorization either, as Tripwire for DevOps is deployed into AWS.

Jenkins

You can use Tripwire for DevOps in your Jenkins build jobs. This way, much of the logic in the background is handled for you within your Jenkins Branch Master and Pull Request environments. Tripwire for DevOps also periodically queries for the status of scans once you've pushed your image, until it arrives at a pass or fail. You can then put the results of your scan in JSON or JUnit format for better visibility in Jenkins.

In addition to these tools, Tripwire for DevOps also integrates with TeamCity, Bamboo, Microsoft Team Foundation Server, Ansible, Puppet, Chef and Salt.

Tripwire for DevOps in Action

Let's run through a simplified example use case for Tripwire for DevOps. When you're ready to test your build, push your Docker images into Tripwire for DevOps through Jenkins. Your images are then spun up within Tripwire for DevOps' secure cloud sandbox for dynamic analysis of vulnerabilities as well as for a configuration compliance check. A pass or fail result is then provided for your build. You can immediately drill down into failed tests to see why they failed and what remediation need to be taken.

That is a basic overview, but you can customize Tripwire for DevOps to meet your internal security policies. For example, you can configure your quality gates to pass or fail builds based on specific risk scores. Tripwire for DevOps can also scan virtual machines such as Amazon Machine Images (AMI).

Summary

It's time to take a smarter approach to DevOps security. Tripwire for DevOps makes it easy to reduce cycle time from coding to deployment while conducting dynamic, comprehensive scans to catch and fix vulnerabilities before they make it into production. Learn more about Tripwire for DevOps by downloading the solution brief "***How to Integrate Security into DevOps Without Losing Momentum***."

Ready for a Demo?

Let us take you through a demo of Tripwire for DevOps. Visit **tripwire.com/contact/request-demo/**

TFDDS3a 1903