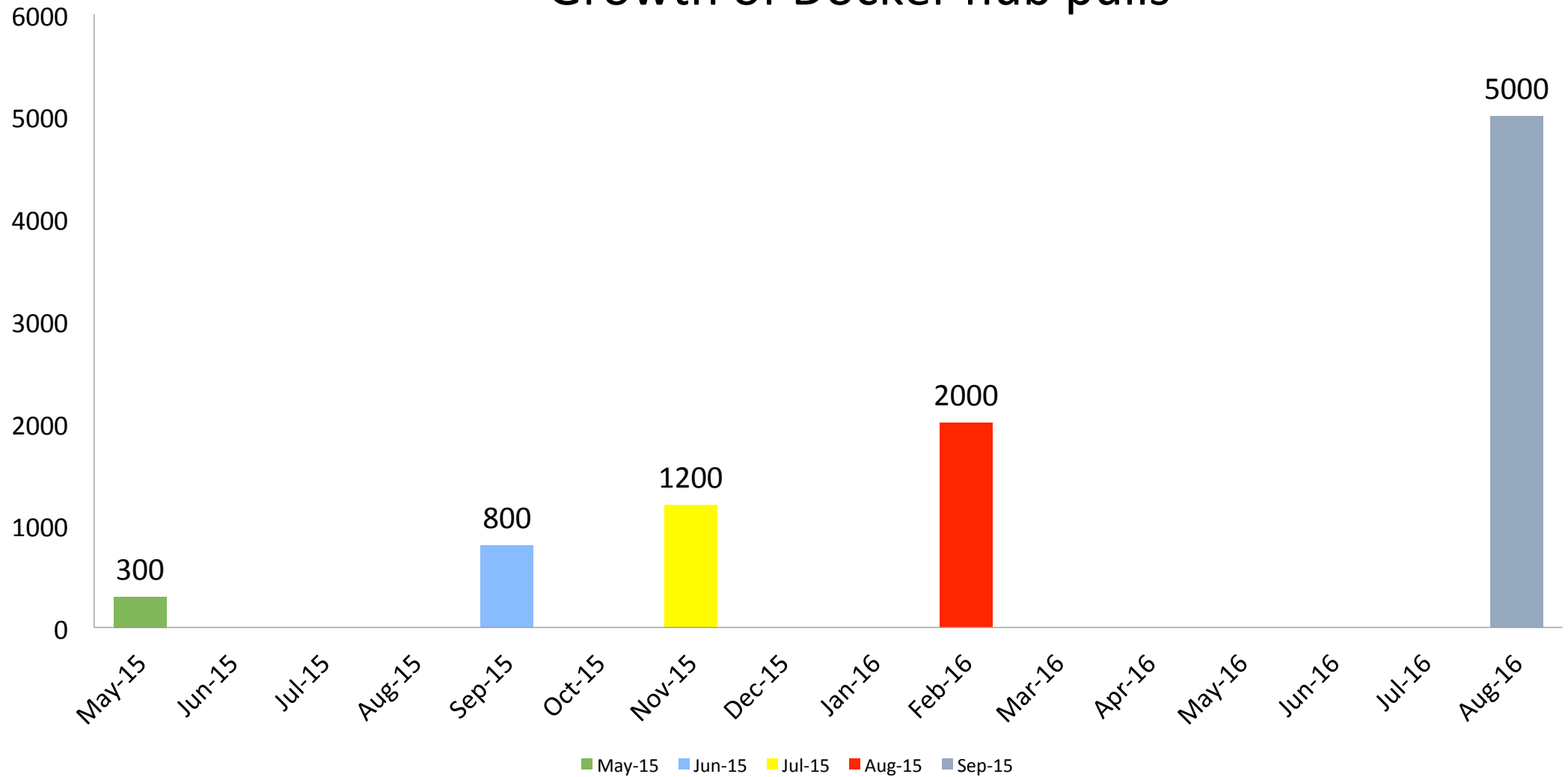




**Twistlock**  
Security, built for containers

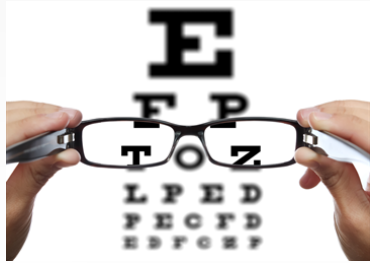
millions

## Growth of Docker hub pulls



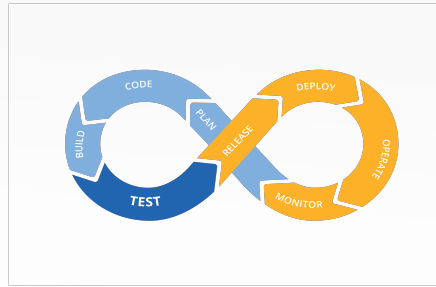
# Security challenges of container operations

## Lack of visibility



Containers are a blind spot to security operations

## Lack of control



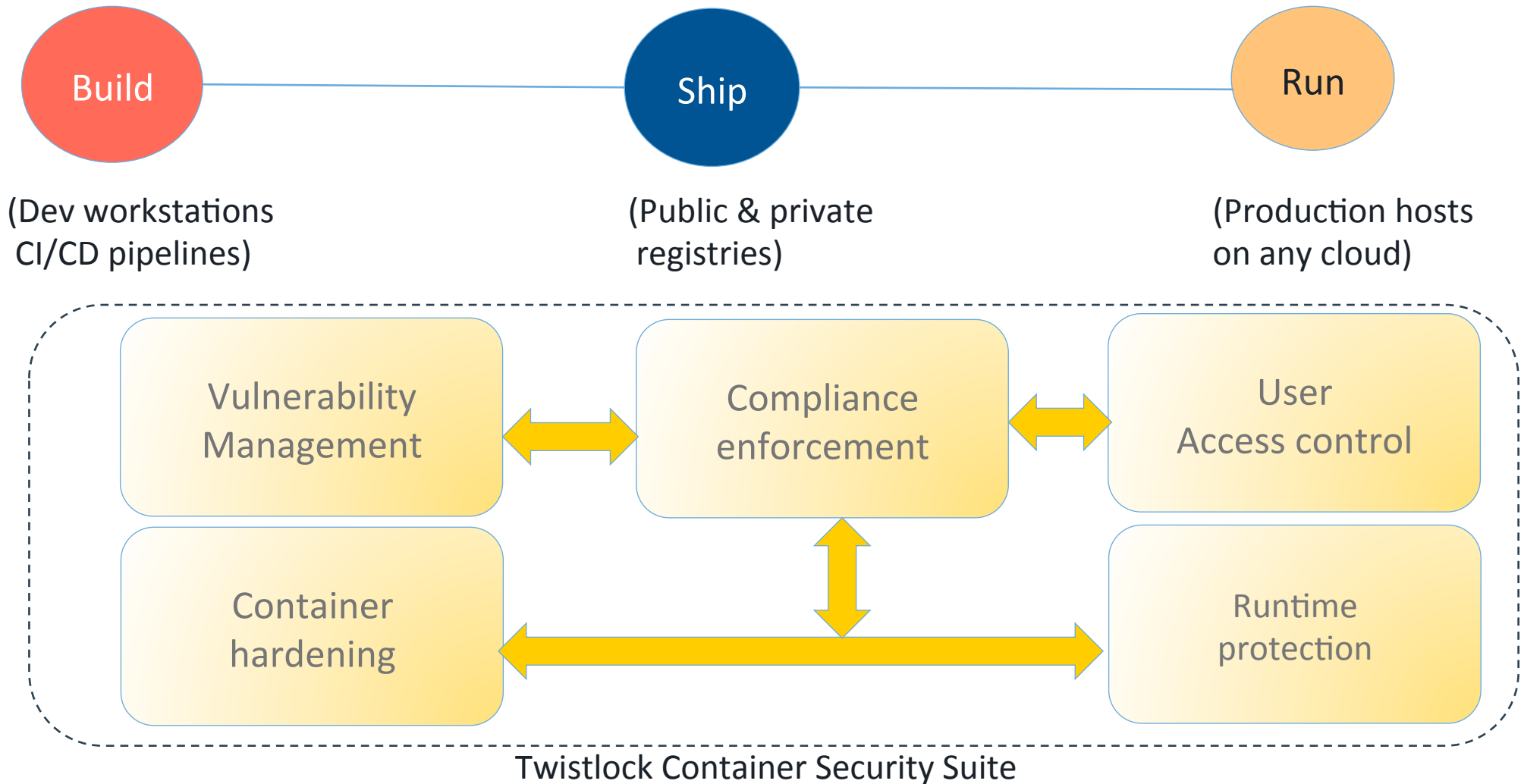
Shared OS, Continuous integration and continuous delivery break traditional security models

## Lack of tooling



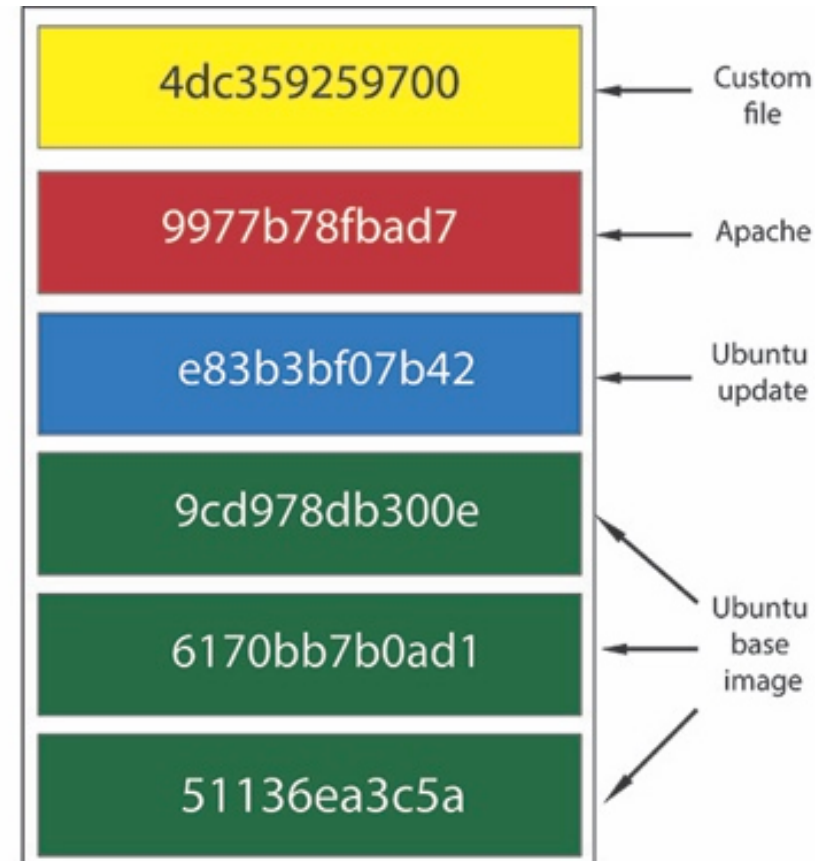
Existing security mechanisms do not work on containers

# Twistlock delivers security built for containers



# Vulnerability Management

- Vulnerability & malware scanning of image layers
  - Linux distro, Java, Node, PHP, Python, Ruby Gem, etc.
- Enforce vulnerability-based policies
  - Prevent vulnerable containers from deploying
- Real-time threat & vuln intelligence
- Built-in CI support: Jenkins, TeamCity
- Any registry, anywhere
  - Docker Hub, GCR, AWS ECR, Artifactory, ...



# Compliance & hardening

- 90+ built-in checks
- Verify settings for
  - Container
  - Docker daemon
  - Host
  - Docker files & directory
  - Hardware
- Trust control
  - Deploy only scanned, approved images

<input type="checkbox"/>	52	container	Verify SELinux security options, if applicable (CIS 5.2)
<input type="checkbox"/>	53	container	Verify that containers are running only a single main process (CIS 5.3)
<input type="checkbox"/>	11	host_config	Create a separate partition for containers (CIS 1.1)
<input type="checkbox"/>	12	host_config	Use the updated Linux Kernel (CIS 1.2)
<input type="checkbox"/>	47	image	Image contains vulnerable jar versions
<input type="checkbox"/>	48	image	Image contains vulnerable ruby gem versions

← **Container policies**

← **Host policies**

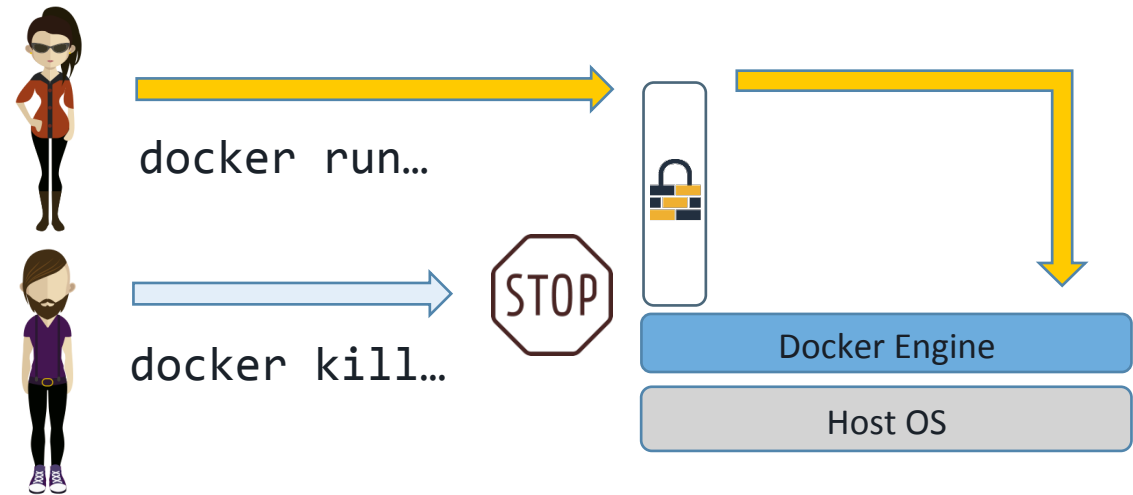
← **Image policies**

# Access control

Fine-grained access control to Docker, Docker Swarm, and Kubernetes management plane

Active Directory, Kerberos, OpenLDAP, and SAML integration

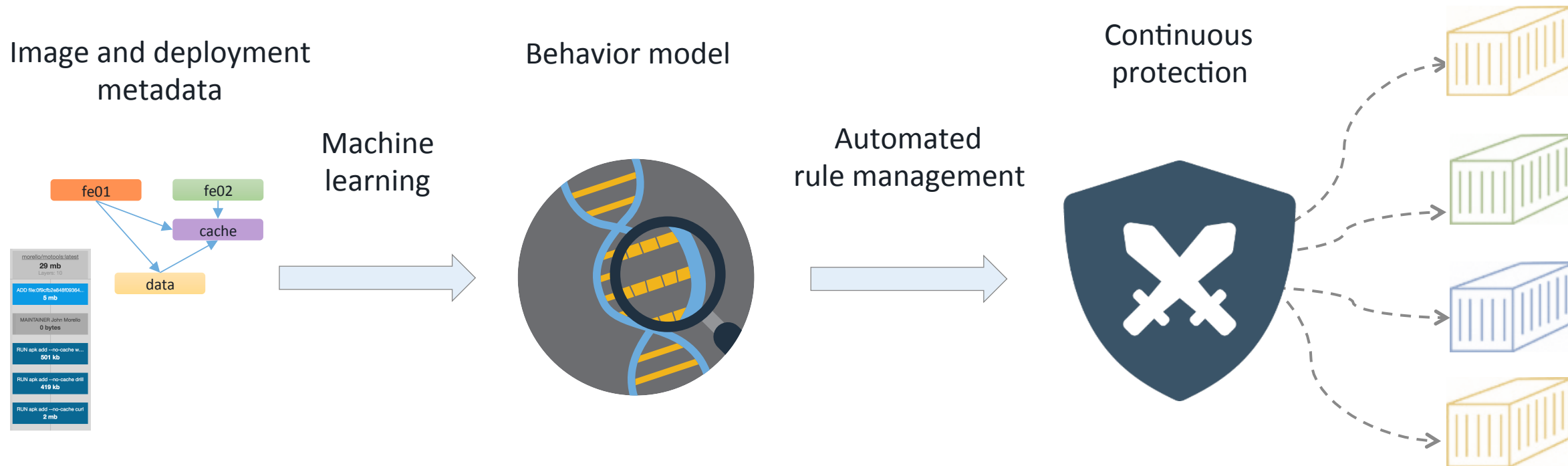
Granular control down to individual APIs with central auditing



```
user@host ~ $ docker kill a83
Error response: [Twistlock] The command 'container_kill'
denied for user 'jake' by rule 'Default - Deny all'
```

jake	container_create	john-access-rule	cto-stable-coreos.c.cto-s...	✓	Feb 19, 2016 2:49:11 PM	✕
jake	container_kill	Default - Deny all	cto-stable-coreos.c.cto-s...	⚠	Feb 19, 2016 2:44:56 PM	✕
jake	container_inspect	john-access-rule	cto-stable-coreos.c.cto-s...	✓	Feb 19, 2016 2:44:51 PM	✕

# Runtime protection

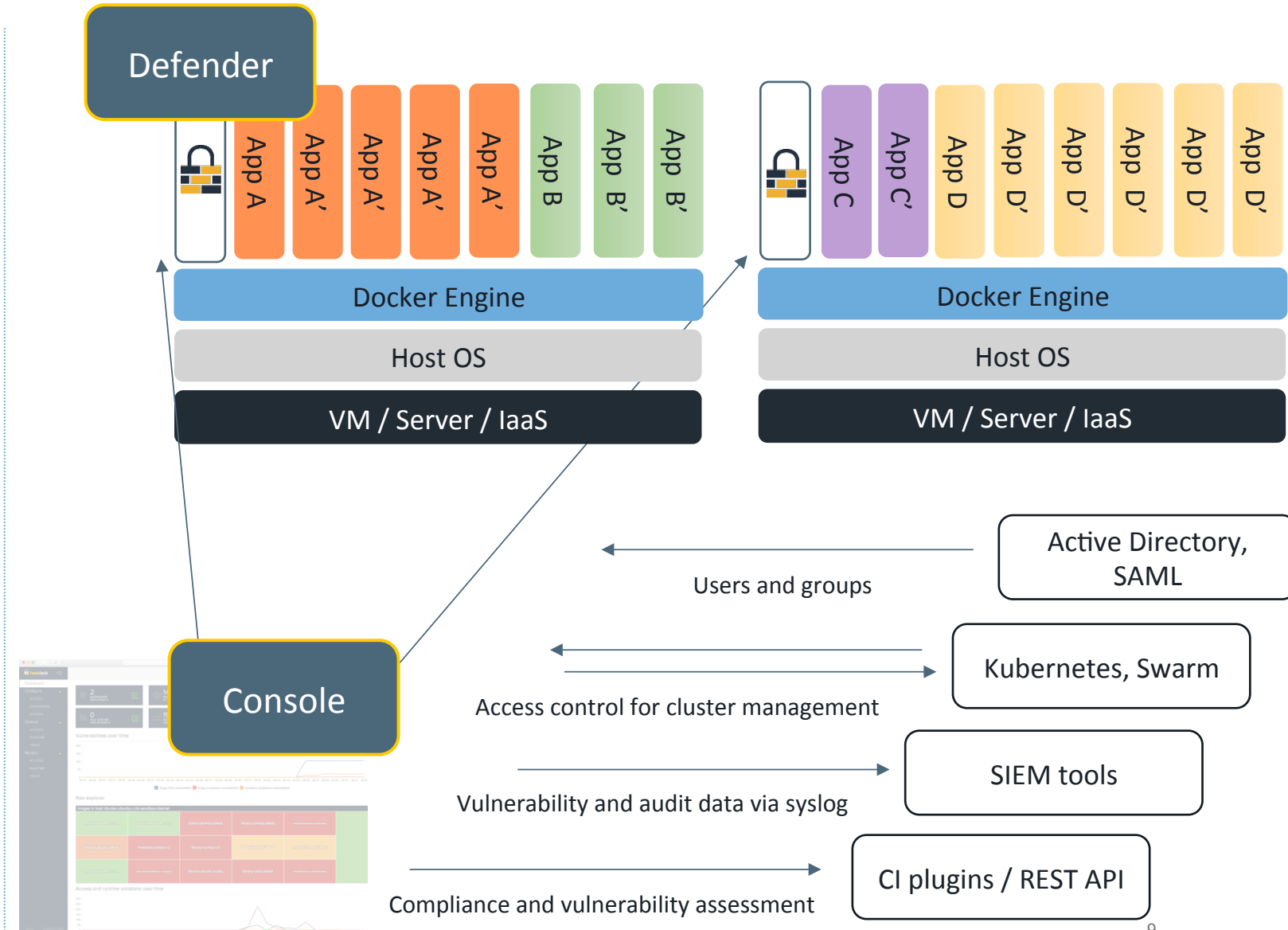
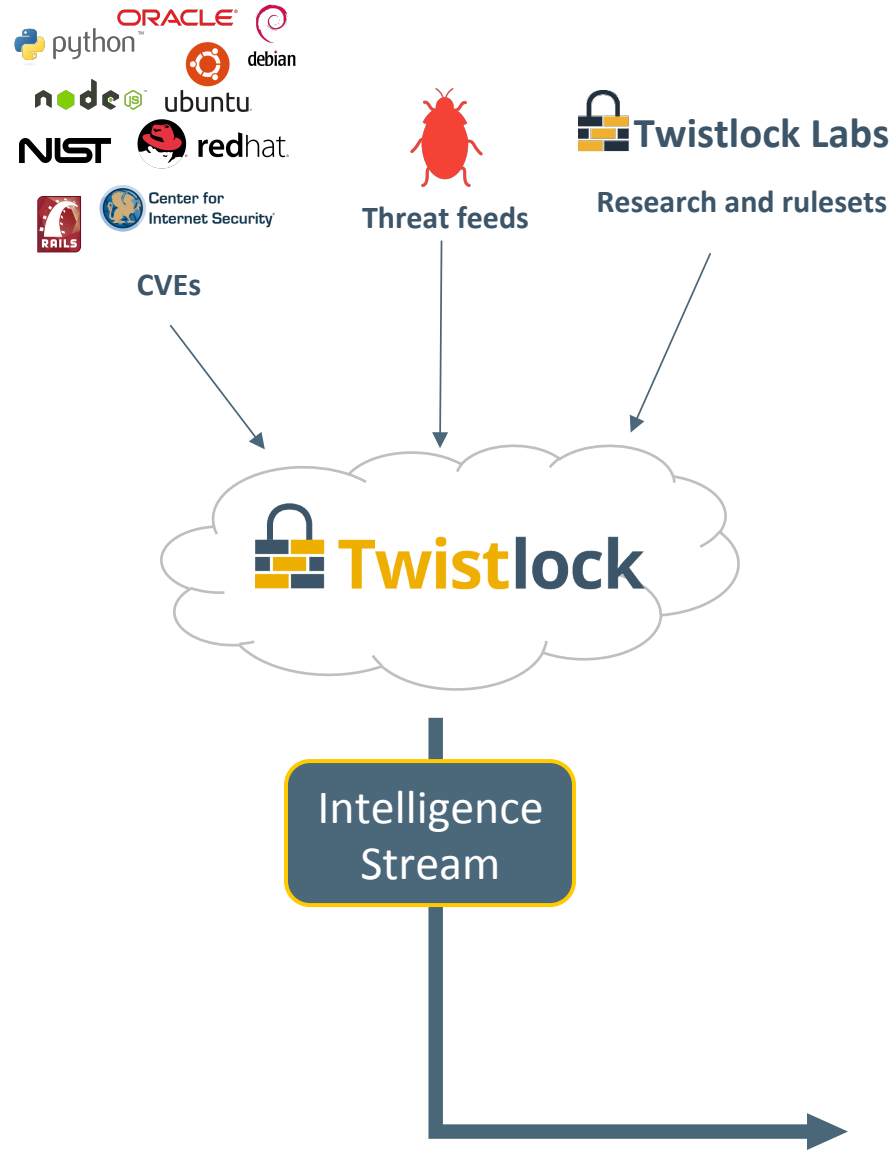


Combine knowledge of the image and how it's deployed to understand the app's 'DNA': what it ***should*** do

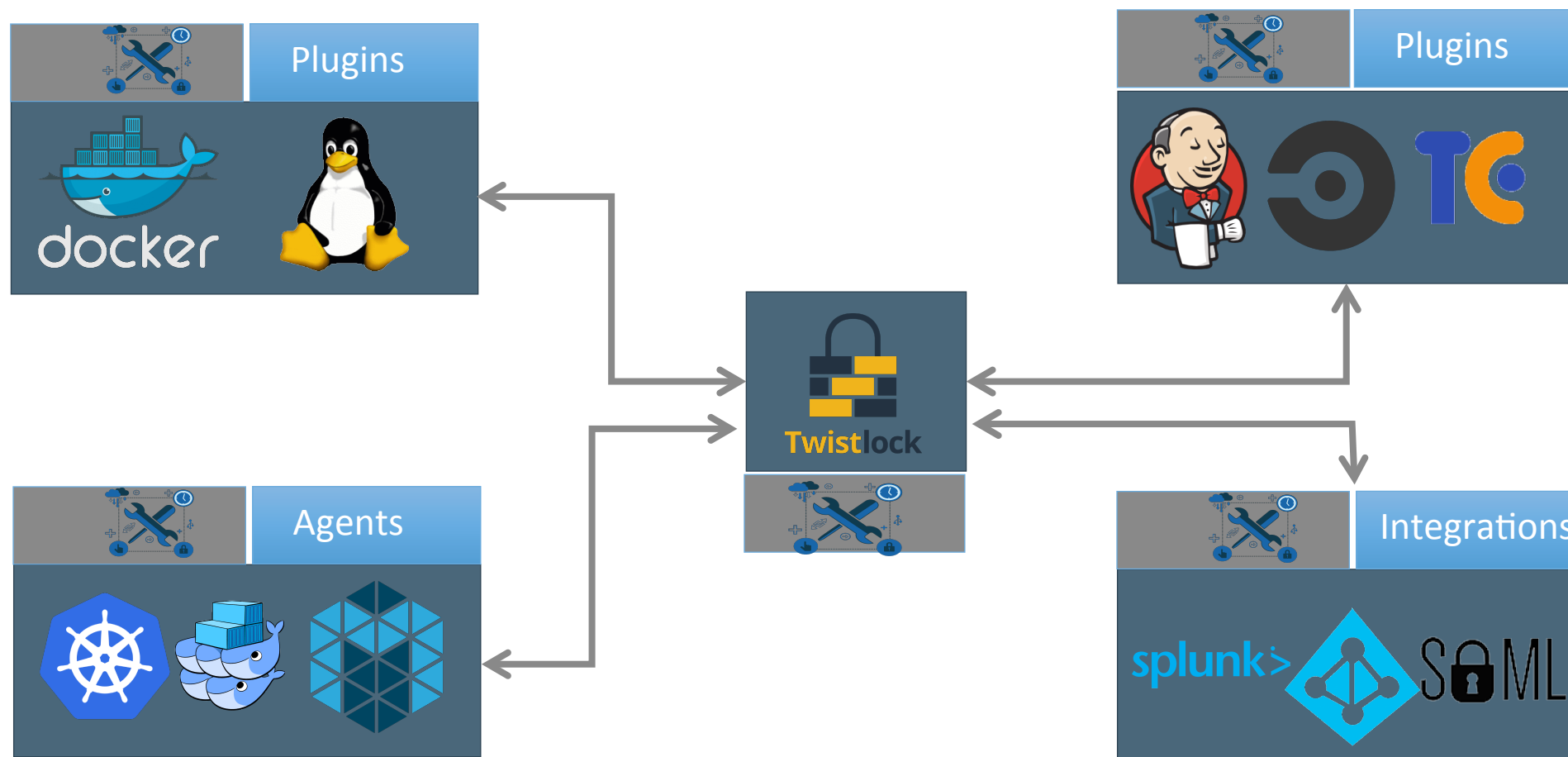
Automatically build rules to compare the DNA to what containers are ***actually*** doing



# Twistlock's architecture



# Twistlock is purpose-built for containers



# Hyperscale security



AWS EC2 Container Service and Registry launched December 2015

Twistlock selected as the only security launch partner

<https://aws.amazon.com/blogs/aws/ec2-container-registry-now-generally-available/>



Google Cloud Platform

GCP Container Service and Registry launched November 2015

Twistlock selected as the only security launch partner

<https://cloudplatform.googleblog.com/2015/11/enhancements-to-Container-Engine-and-Container-Registry.html>

## Microsoft Azure

Azure Container Service launched in April 2016

Twistlock the only featured security partner

<https://blogs.msdn.microsoft.com/azuresecurity/2016/05/26/insights-on-container-security-with-azure-container-service-acs/>



# Why Twistlock?

## Technology pioneer and innovator

- First purpose-built solution for container and micro-services
- 15 patents pending, with innovation in runtime defense and dev-to-production security

## Market leader

- >30 customers across US, EMEA, APAC and nearly all verticals
- Enterprise grade global support with 24/7/365 SLA

## Ecosystem leader

- Sole security launch partners for AWS and Google container registries
- Active Docker open source project contributor
- Extensive integration with CI/CD and existing enterprise security technologies
- Integration with Kubernetes, Docker Swarm, and Mesos for orchestration

[www.twistlock.com](http://www.twistlock.com)

[sales@twistlock.com](mailto:sales@twistlock.com)

[@TwistlockTeam](https://twitter.com/TwistlockTeam)

1.844.TWISTLOCK

156 2nd St.  
San Francisco, CA 94105



# Security advantages of containerized architectures

