Twistlock™

What is Twistlock?

Cloud native cyber security from beginning to end of the dev lifecycle

Cloud native cyber security from top to bottom of the stack

Why Twistlock?

Technology pioneer and innovator

Started in early 2015 as the first ever purpose-built solution for containers and cloud native security

13 patents pending

3 container related 0-days discovered by our research team

Market leader

>60 customers across US, EMEA, APAC and many verticals

Enterprise grade global support with 24/7/365 SLA

Ecosystem leader

We built the authorization framework in Docker and OpenShift and secrets management in Docker Swarm

Lead author of NIST SP 800-190, the Container Security Guide

The launch partners for Amazon, Google, and Microsoft's container services

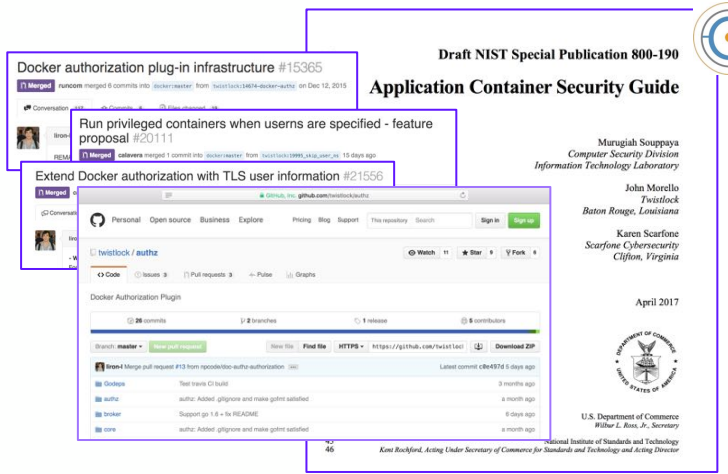
Native integration with CI/CD platforms like Jenkins

Security for the whole stack with deep support for Kubernetes, Swarm, AWS ECS, and DC/OS

Recent awards & press

Partnerships

Open source and standards work



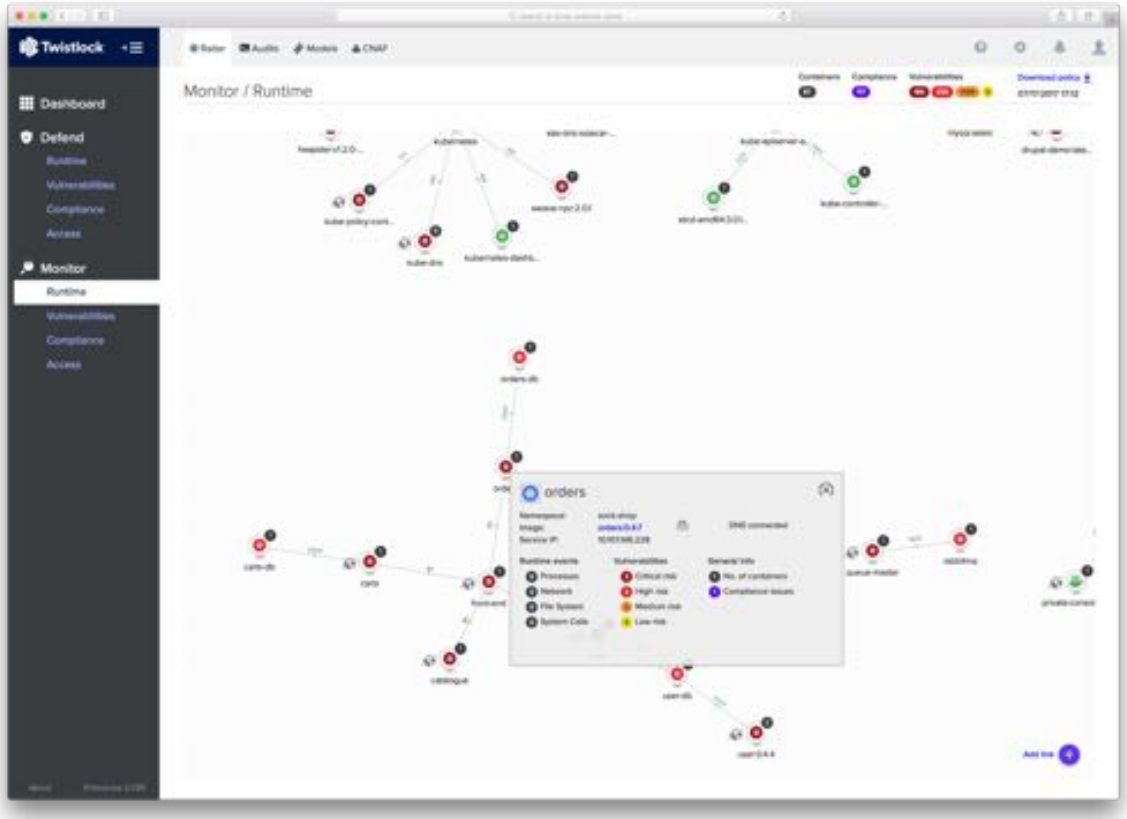
Automatically prevent next gen attacks against containers and cloud native apps

Twistlock uses machine learning to automatically build whitelist behavioral models for every app in your environment, helping you shift from trying to prevent the bad to only allowing the good

Twistlock correlates knowledge of the container with how you've deployed it to provide automatic micro-segmentation and a Cloud Native App Firewall that filters layer 7 traffic before it reaches your app, without requiring any additional network devices

Twistlock combines data from multiple sensors focused on process, network, and file system activity across the host and every container to create actionable, visual knowledge about attack patterns

Twistlock is purpose built for cloud native and doesn't require changes to your images or containers, doesn't rely on a legacy kernel mode architecture, and can be instantly deployed across thousands of nodes using native capabilities in Kubernetes, Swarm, and DC/OS



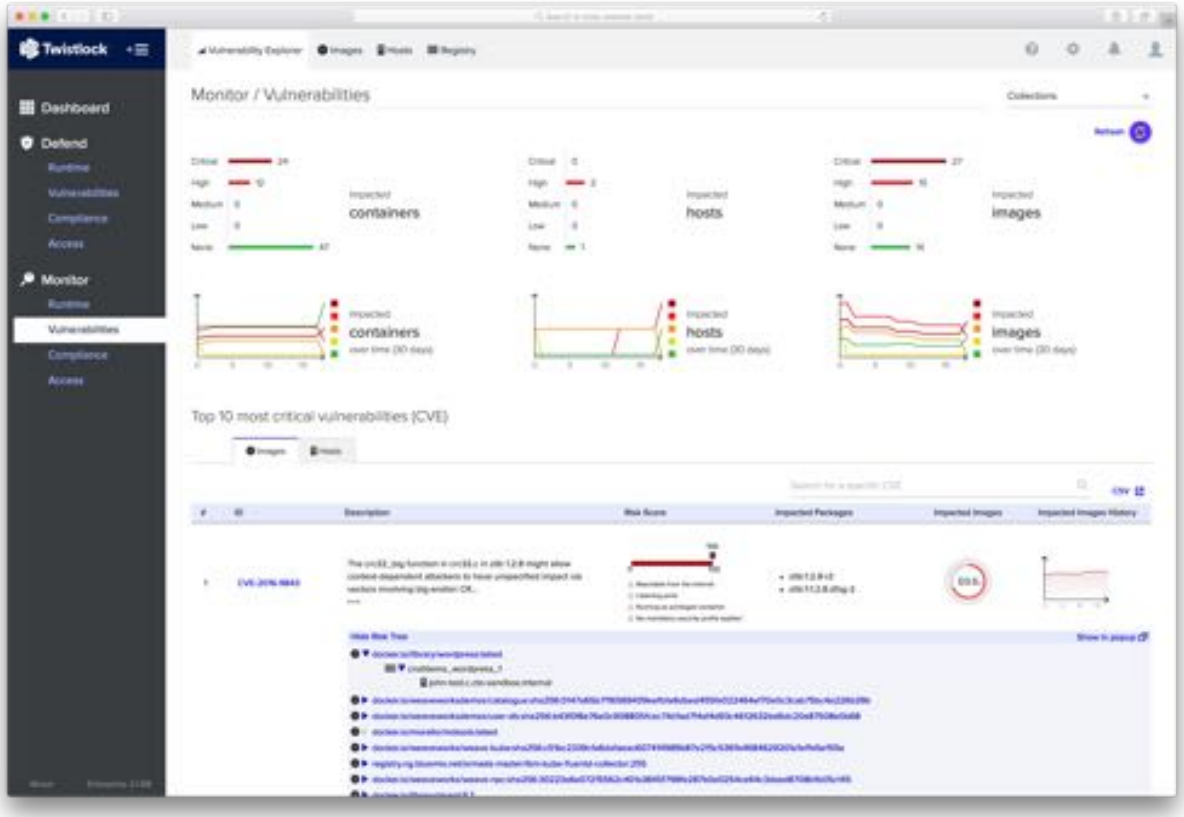
Detect and prevent vulnerabilities before they make it to production

Twistlock collects and curates vulnerability data from over 20 open source and commercial providers to provide the lowest false positive rate

Twistlock detects vulnerabilities at every stage of the lifecycle, from developer to registry to production and across all layers of the stack, from host to container to image

Twistlock prioritizes vulnerabilities based on your specific use cases, factoring in deployment size, network exposure, and privilege level, so you can focus on the most important risks to you

Twistlock allows you to create granular policies to prevent vulnerabilities by severity level, component, and specific CVE from the build process to production



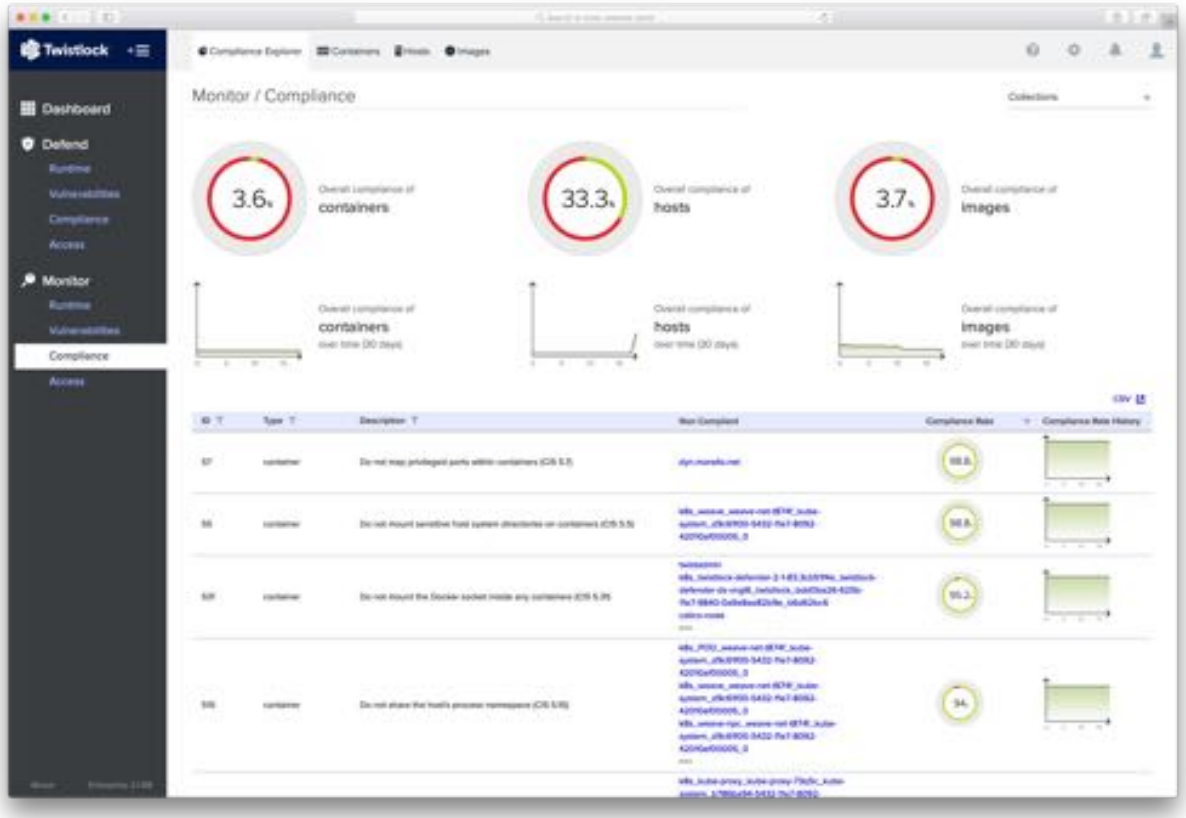
Extend corporate compliance into your containers and cloud native environments

We were the primary authors of NIST's SP800-190, the Container Security Guide, contributors to the Center for Internet Security's Kubernetes Benchmark, and have deployment templates for PCI and HIPAA as well

Twistlock monitors and enforces compliance using a built in library of >100 industry standards and support open standards for adding your own

Twistlock covers all layers of your stack from the host to the daemon, to the container, across all phases of the lifecycle from build to production

Compliance Explorer gives you a real time, auditor centric, dashboard tracking compliance for the specific settings and regulations relevant to your industry and business needs



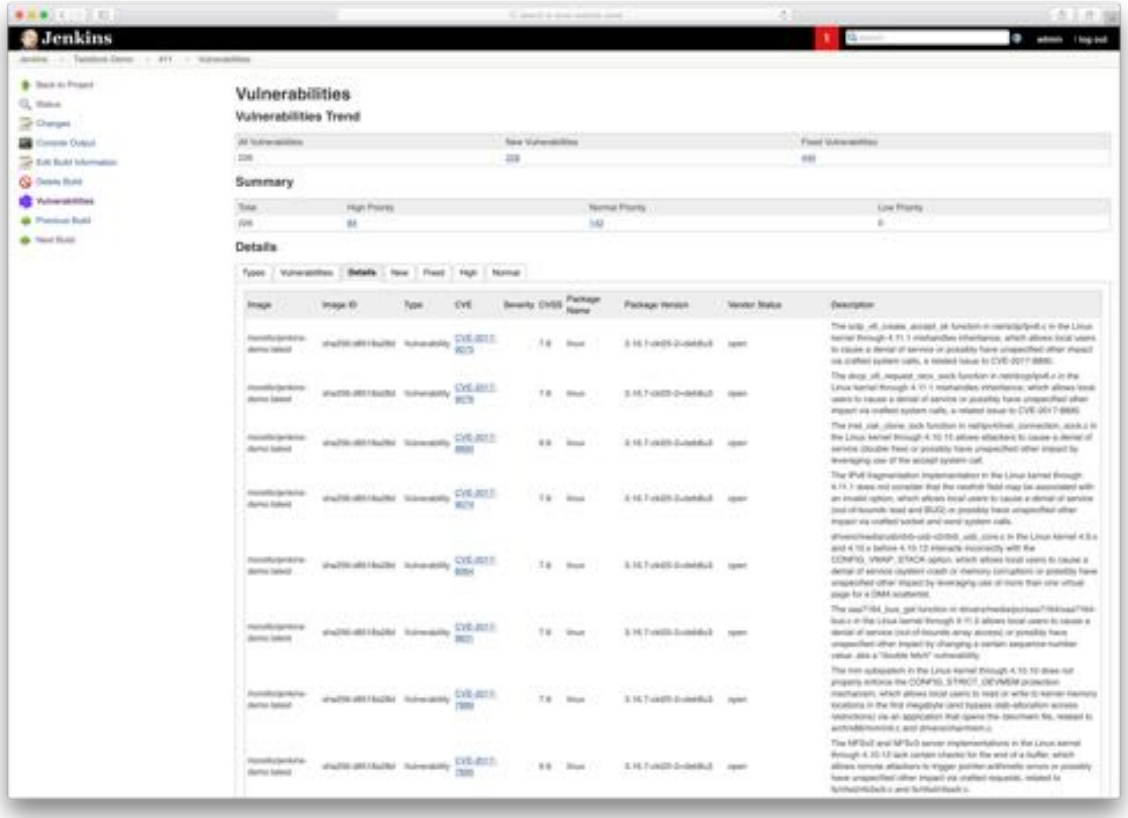
Help you deliver DevOps speed with CISO control

Twistlock has native plugins for platforms like Jenkins that integrate directly into the developer workflow, providing visibility and enforcement for every build

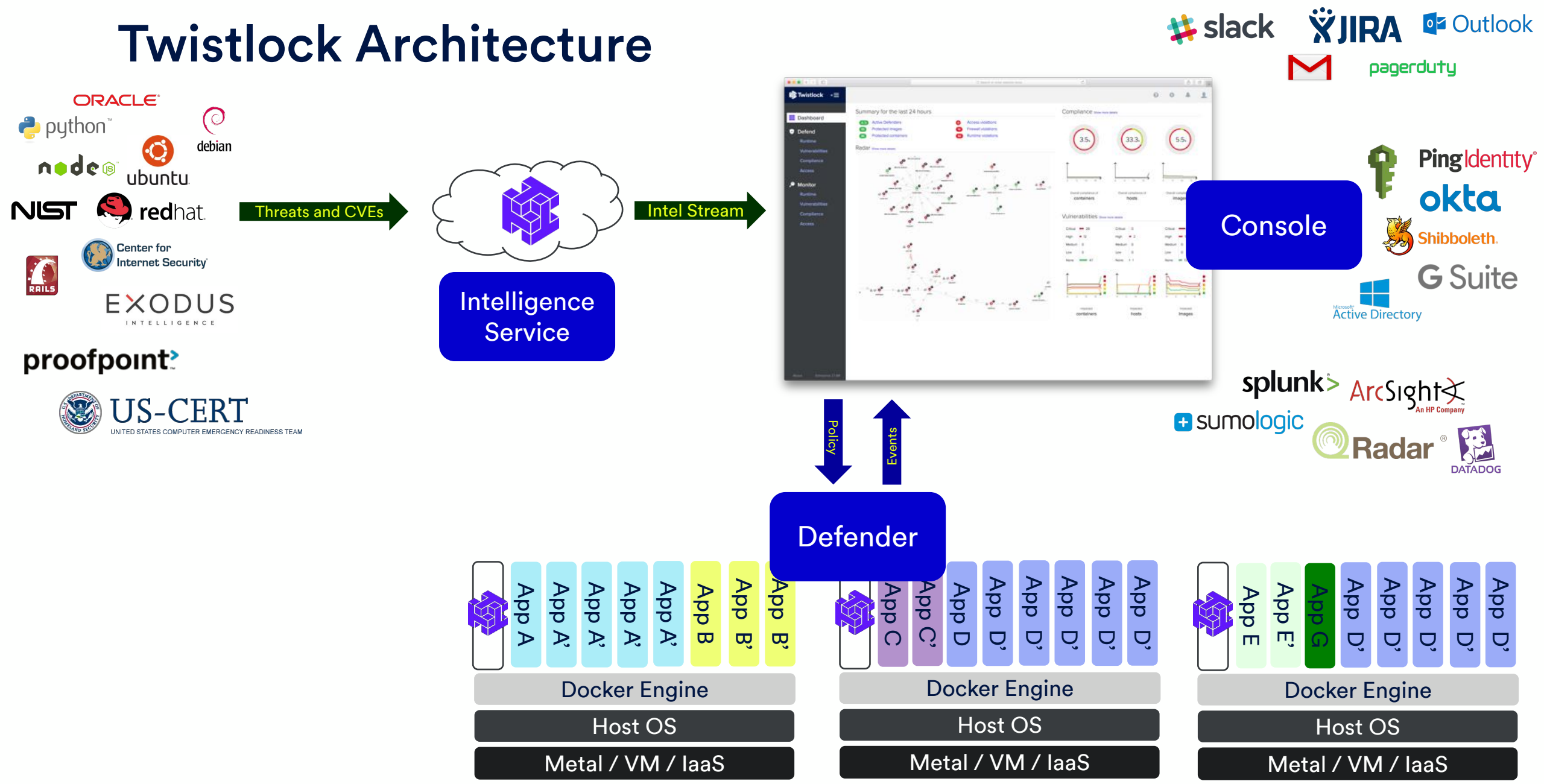
Twistlock has a standalone scanner, designed for interactive use by every dev and easy automation and integration into any CI/CD workflow

Twistlock begins learning app behavior and building a runtime model from the very first time we see an image, whether in the CI process or in production

Every click in our UI is backed by a fully documented REST API, making it simple to integrate with other tools and processes



Twistlock Architecture



Product Demo

Next Release (2.2) Roadmap

Cloud Native Firewall (layer 3)

Automated deployment on Swarm and DC/OS

Comprehensive host protection

3rd party integrations: JIRA, Slack, AWS IAM

Compliance for Kubernetes

twistcli scanner and configuration tool

US CERT threat feeds

Native log generation, viewing, exporting, and uploading from Console

Twistlock Enterprise Edition

Licensed as an annual subscription, per host, which includes:

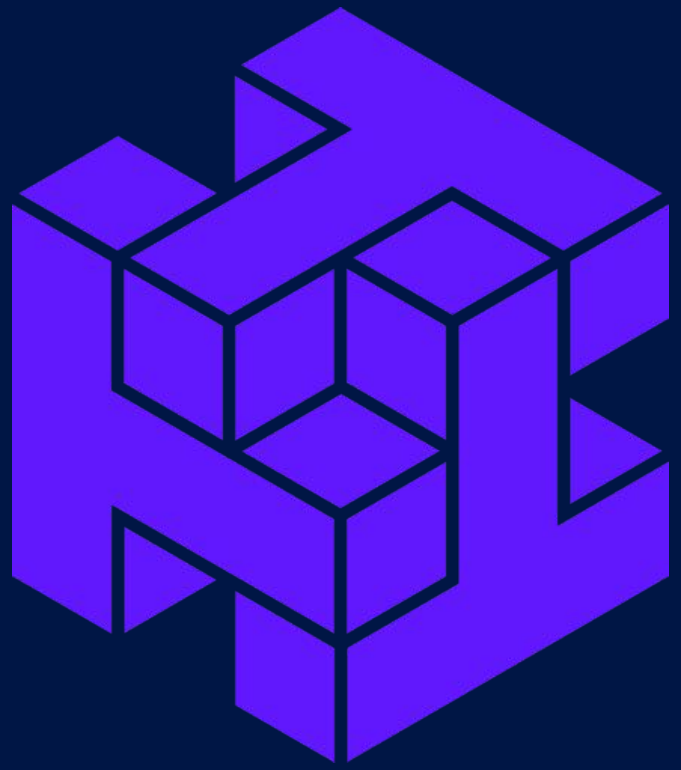
- Product updates (~2 month release cycle)
- 24/7/365 SLA backed global support
- Commercial vulnerability and threat feeds

A host is a Docker Engine that's protected, whether physical, virtual, or in a cloud provider

- No additional costs per container or image
- No additional costs per management console

twistlock.com

sales@twistlock.com



What Makes Us Different?

Battle tested, automated, machine learning driven, runtime defense

The broadest and deepest vulnerability management available

The most comprehensive compliance enforcement

We built the authorization and secrets management framework in Docker

Portable security: every cloud, every orchestrator

Every click in the UI is API driven and easy to integrate

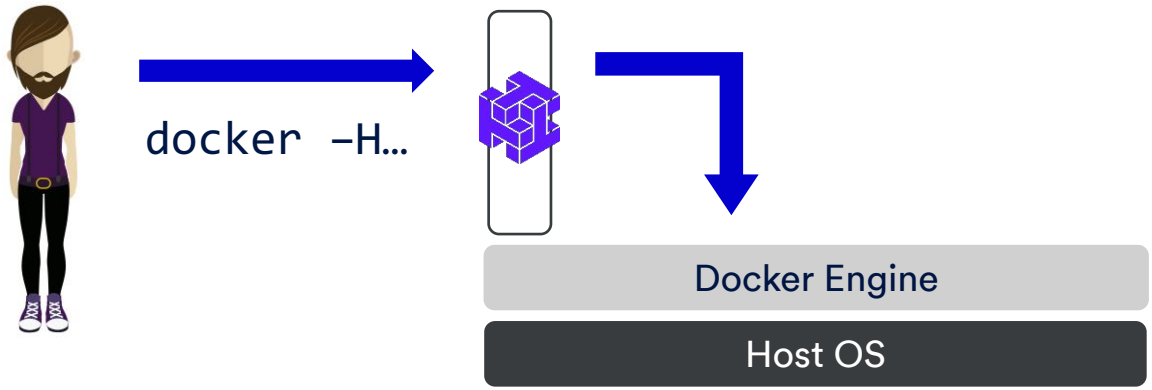
All of your data is 100% under your control at all times

Passion for our customers

Defender Architecture

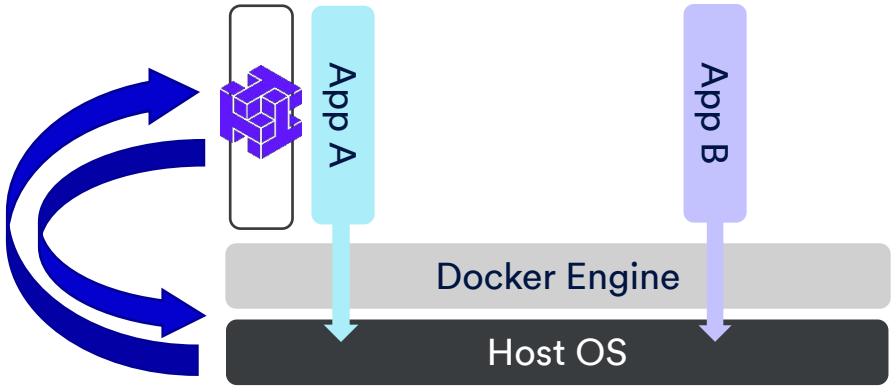
Only management plane traffic passes through

- e.g. **`docker run nginx`**
- Rules applied and allowed commands forwarded to Docker Engine

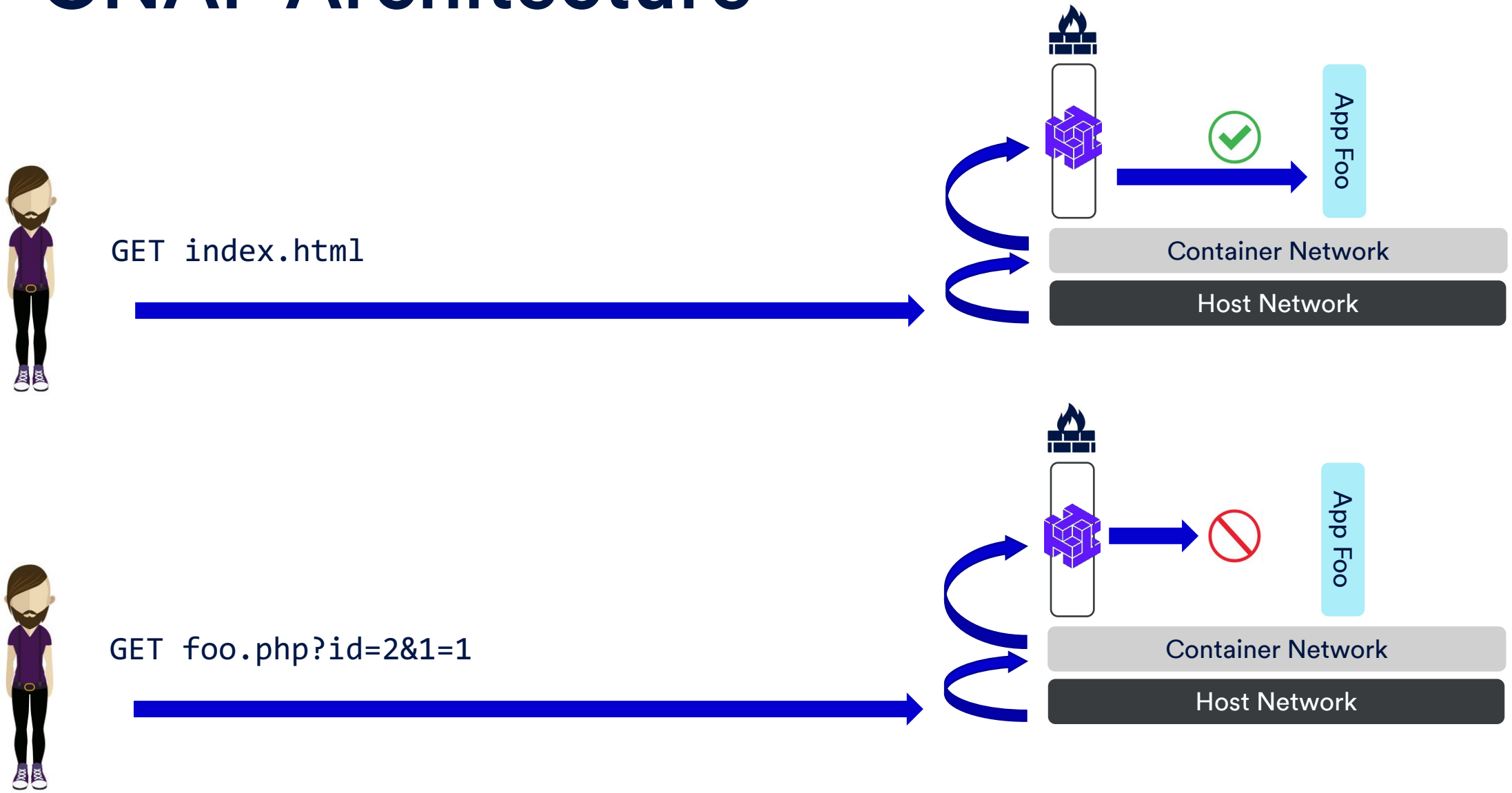


Runtime defense via sideband host layer sensors

- Notifications via kernel interfaces
- Actions via kernel and Docker APIs



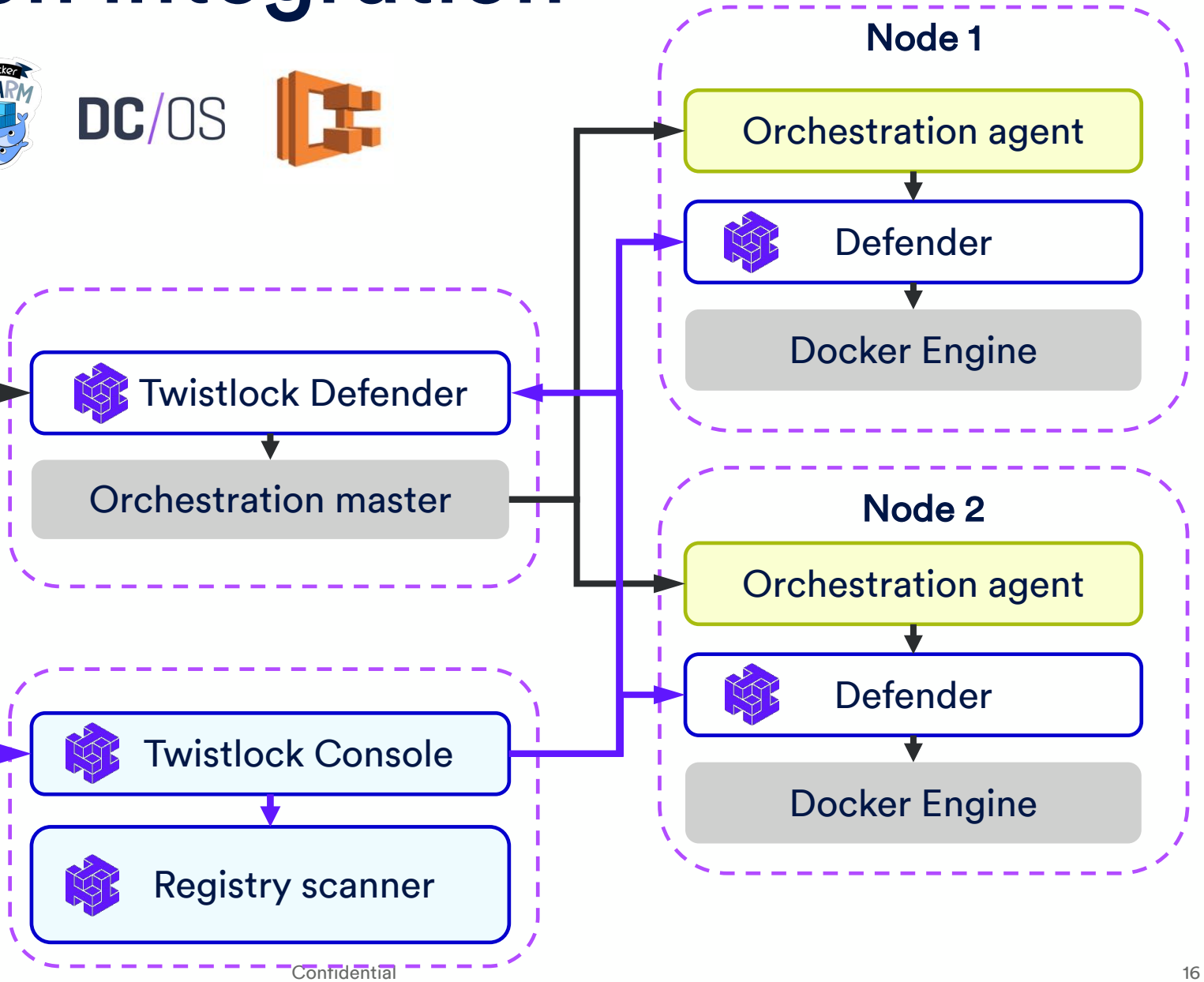
CNAF Architecture



Orchestration integration

Orchestration admin

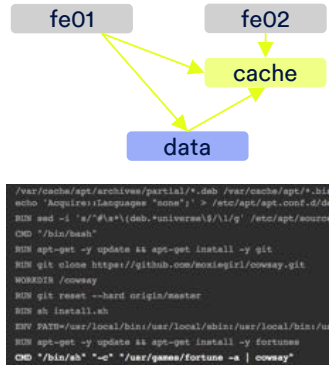
Twistlock admin



Runtime Defense

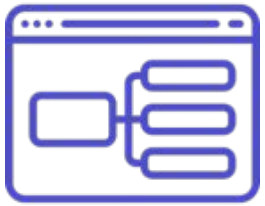
Use machine learning to model what each image is intended to do

Automatically look for anomalies between the model and runtime behavior



+

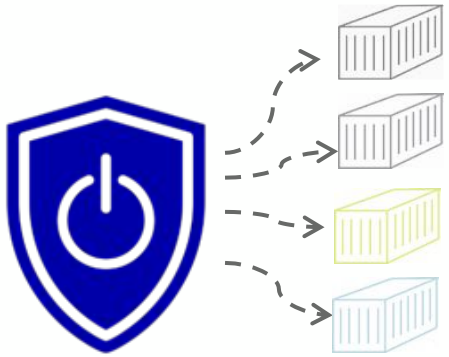
=



+

```
ip, category, score, first_seen,
last_seen, ports
74.88.8.7,31,65,2016-04-16,2016-04-
16,
233.16.9.49,35,125,2016-04-11,2016-
04-20,80
82.16.9.65,35,127,2016-04-09,2016-
04-21,80
```

=



Static analysis

Machine learning

Predictive model

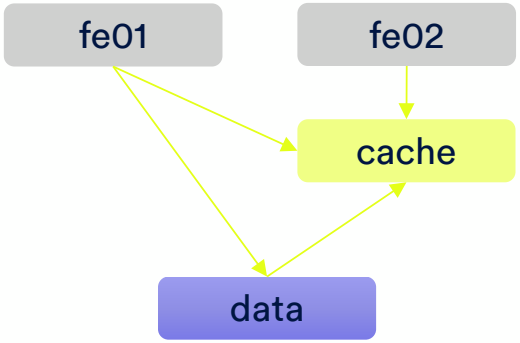
Twistlock Advanced Threat Protection

Runtime Defense

Building The Model

```
/var/cache/apt/archives/partial/*.deb /var/cache/apt/*.bi
echo 'Acquire::Languages "none";' > /etc/apt/apt.conf.d/d
RUN sed -i 's/^#\s*\(deb.*universe\$/\1/g' /etc/apt/sourc
CMD "/bin/bash"
RUN apt-get -y update && apt-get install -y git
RUN git clone https://github.com/moxiegirl/cowsay.git
WORKDIR /cowsay
RUN git reset --hard origin/master
RUN sh install.sh
ENV PATH=/usr/local/bin:/usr/local/sbin:/usr/local/bin:/u
RUN apt-get -y update && apt-get install -y fortunes
CMD "/bin/sh" "-c" "/usr/games/fortune -a | cowsay"
```

+



+

Static analysis

Binary checksums

Twistlock Labs app intel

System calls

Launch time metadata

Mounted volumes

Connected networks

Published sockets

Machine learning

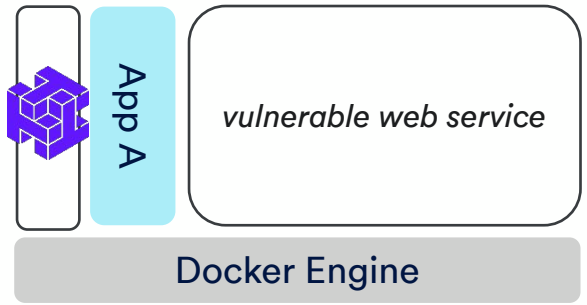
Actual observed runtime behaviors

Process activity

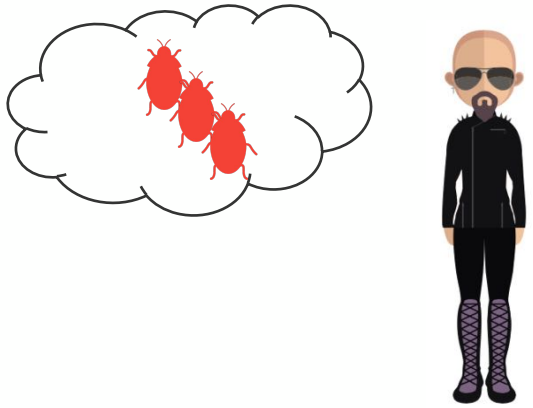
East / west and north / south IP flows

Stopping The Kill Chain

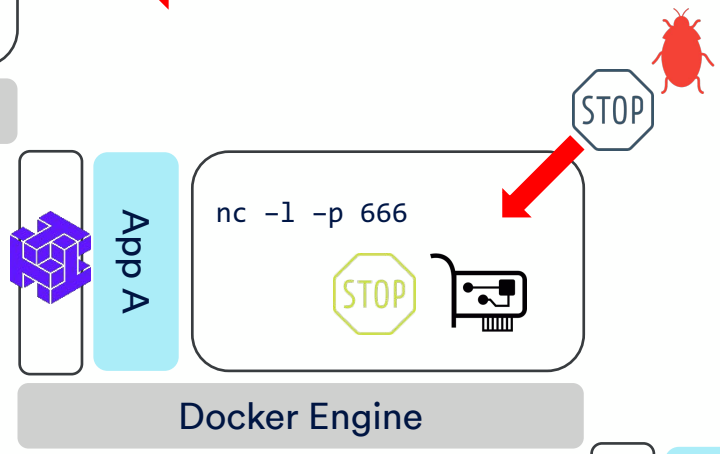
syscall sensors detect anomalous kernel calls



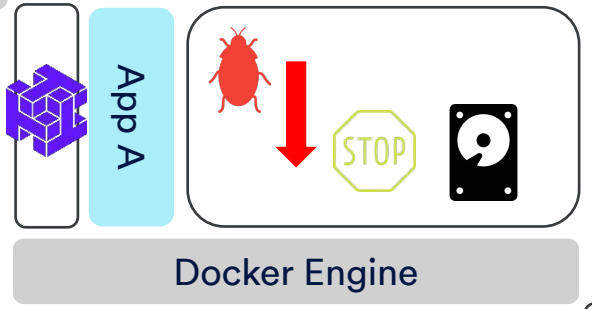

```
buffer = OPENSSL_malloc(1 + 2 +
payload + padding);bp = buffer;
```



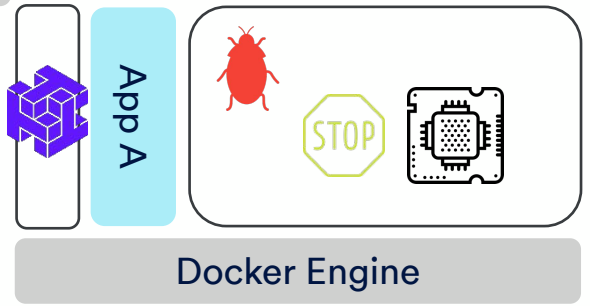
network sensors detect abnormal traffic flows and dangerous endpoints



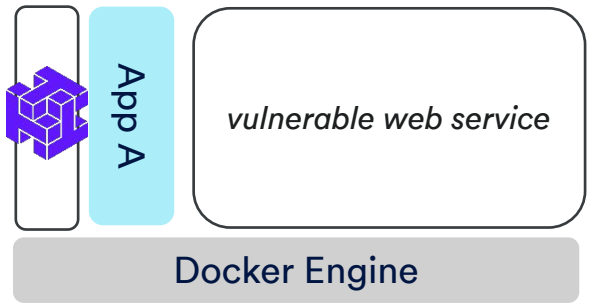
storage sensors looks for malware and suspicious file access patterns

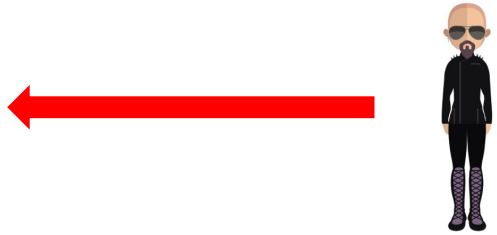


process sensors see a process not in the authentic image and stop it from spawning



Real World Runtime Example





```
root@54cc524f9f37:/usr/local/apache2# nc -l -p 80
data being stolen!!!
```

Attempts to exfiltrate data

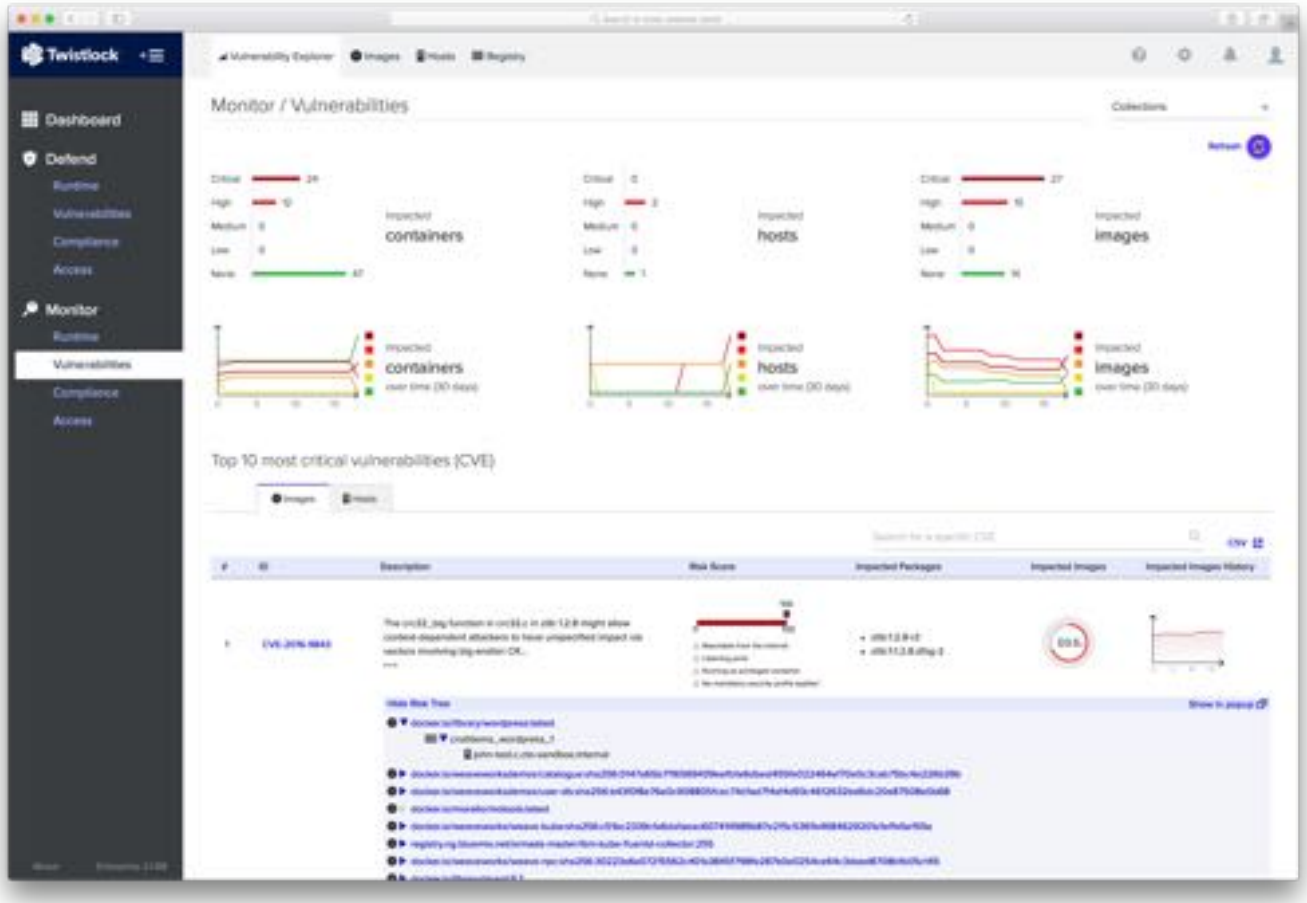
```
DEBU 2016-09-02T18:18:52:24.828 (*scanner).Subscribe scanner.go:165 Received event '54cc524f9f374e65a386163ee089210f24c4b0269de85e630557c76028c9c603' 'httpd' 'top'
DEBU 2016-09-02T18:18:52:25.113 (*procMonitor).Handle proc_monitor.go:264 Found child process "/usr/local/apache2/bin/httpd" 21105 "/nostalgic_mcnulty httpd"
DEBU 2016-09-02T18:18:52:25.116 (*scanner).Subscribe scanner.go:165 Received event '54cc524f9f374e65a386163ee089210f24c4b0269de85e630557c76028c9c603' 'httpd' 'archive-p
ath'
DEBU 2016-09-02T18:18:52:25.140 (*procMonitor).newProcViolation proc_monitor.go:3[illegible] Searching for binaries in container: "/nostalgic_mcnulty httpd" based on cmd: "/bin/
bash" total: 988
DEBU 2016-09-02T18:18:52:25.140 (*procMonitor).newProcViolation proc_monitor.go:[illegible] found binary "bash" "/nostalgic_mcnulty httpd" based on cmd: "/bin/bash"
DEBU 2016-09-02T18:18:52:25.140 (*procMonitor).newProcViolation proc_monitor.go:[illegible] Startup processes for container: "/nostalgic_mcnulty httpd" [{bash /bin/bash 578[illegible]
014ef2f7fbcfa95802afc9002 } {rm /bin/rm 2314b8d72ef05e807b99a0963a117602 } {httpd /usr/local/apache2/bin/httpd 4cbaefc0f1c921248c187832843455e }]
DEBU 2016-09-02T18:18:52:50.538 (*scanner).Subscribe.func1 scanner.go:190 Running delayed scan to detect networking and processes "54cc524f9f374e65a386163ee089210f24c4b
0269de85e630557c76028c9c603"
```

But Twistlock learned what processes are genuine and how they connect to networks

And can stop the attack when it sees an invalid process listening on a normal port

Completely automatically, with no human creating rules or editing profiles

Vulnerability Management



Protect all your images, everywhere they are, throughout their lifecycle

- Integrated with the CI process
- Scan any registry, anywhere
- Protection on every compute node

Vulnerability Explorer ranks risks based on your unique deployment

From the base layer, to app frameworks, to your own code

- Java, Node, PHP, Python, Ruby
- >20 CVE data providers

Detect CVEs, 0-days, and malware

Granular policies to prevent vulnerable images from running

Continuously Integrated Security

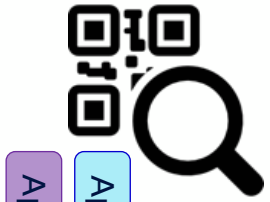
Dev builds new images via existing CI pipeline

App C App D

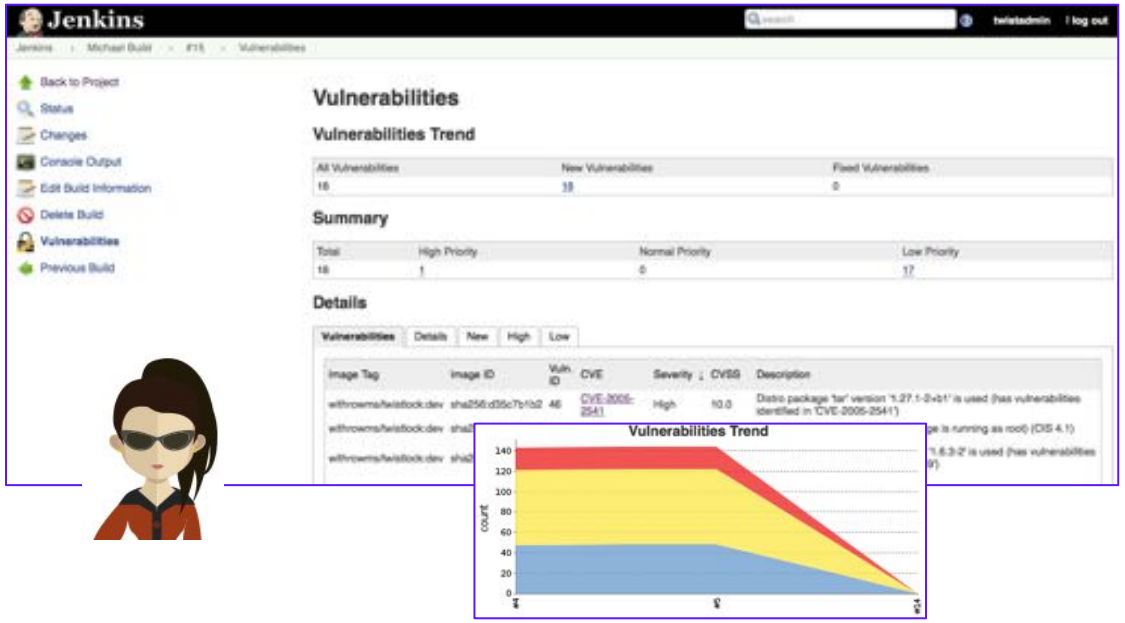
CI tool calls Twistlock plugin

`{imageC, imageD}`

Twistlock scans the images



App C App D



Twistlock puts the results back into the same tools she's already using

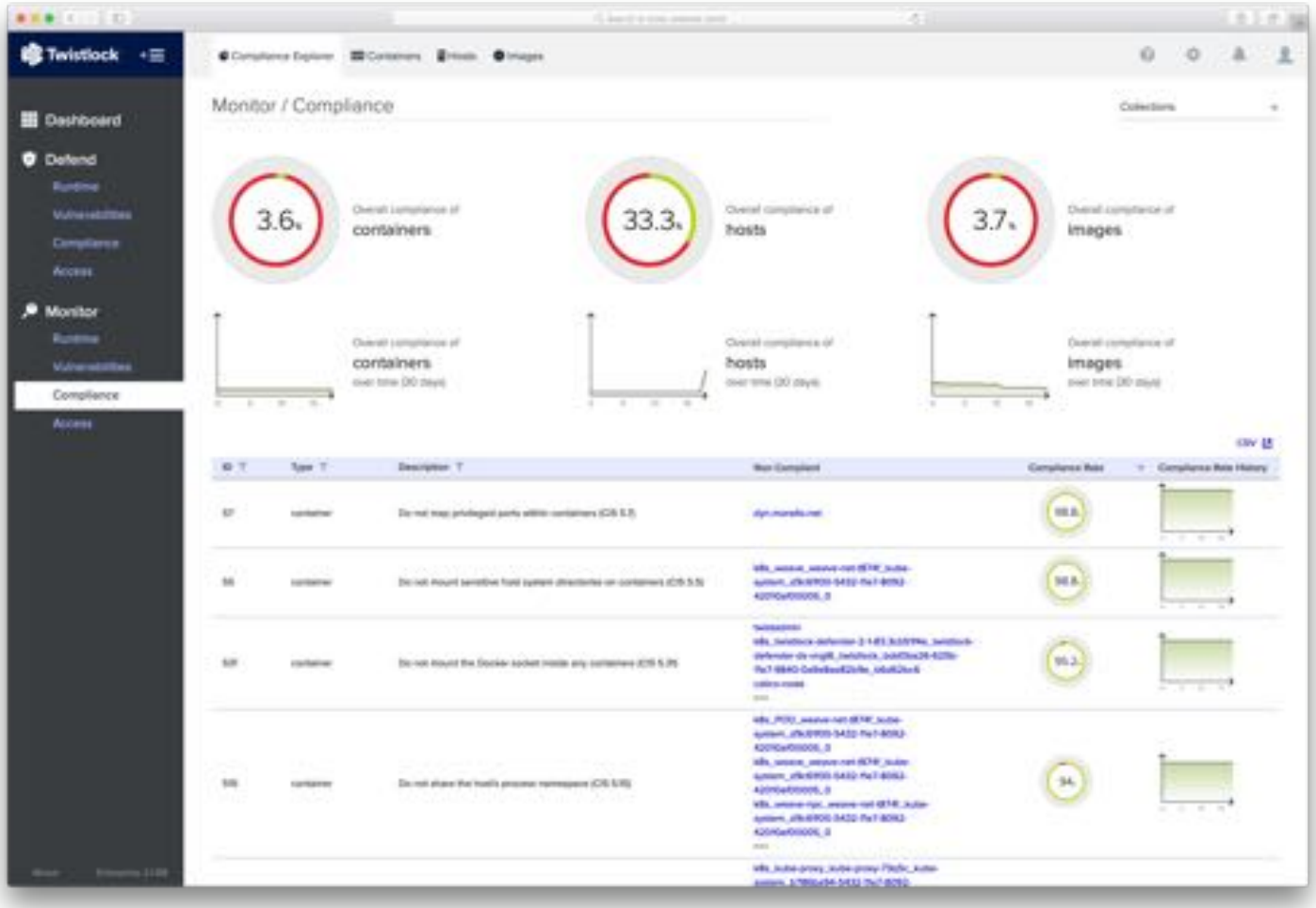
`{imageC:0, imageD:2}`

Compliance

>90 out of the box checks for covering the Docker and Kubernetes CIS Benchmarks, customizable via OpenSCAP

Trusted Images for precise control over what images are allowed to run where

Compliance Explorer dashboard tracks what's important to you



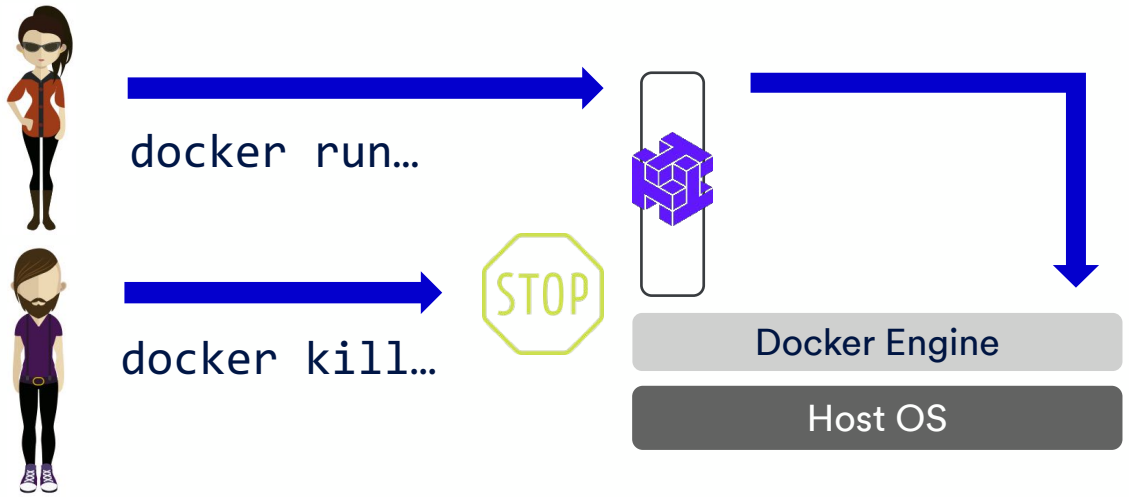
Access Control

Built on Twistlock's authorization plugin framework that ships in Docker and OpenShift

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

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'
```

Twistlock API

REST APIs providing access to all functionality

- Deploy, create rules, pull audit and vulnerability data

Auto-scale Twistlock protection alongside your app

Easy integration with orchestration and CI tools

- Mesos, Kubernetes, Jenkins, TeamCity, Chef, Puppet