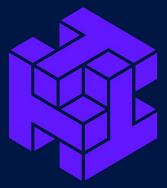
KubeCon | CloudNativeCon

North America 2017

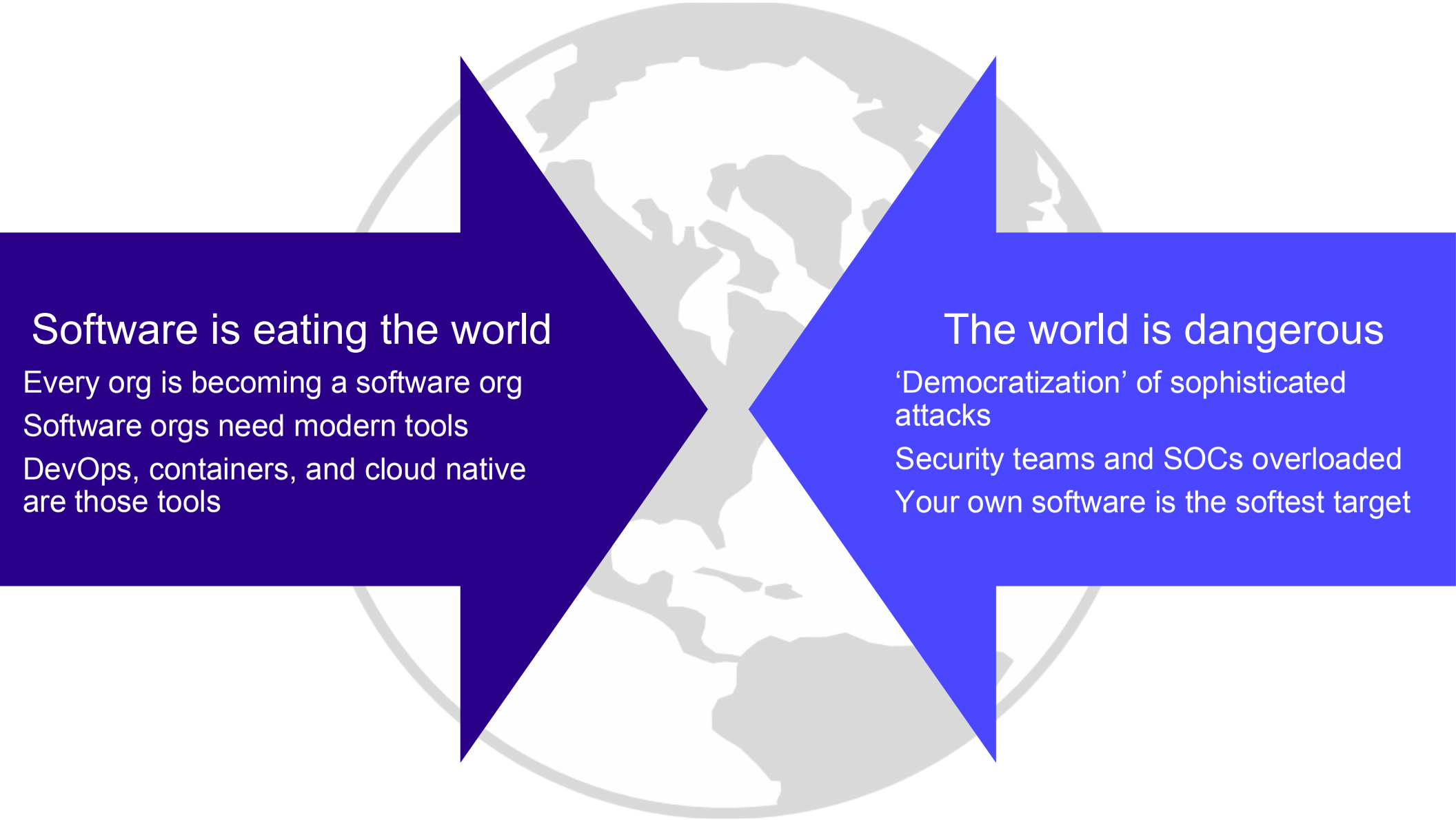


Twistlock™

John Morello

CTO

john@twistlock.com
@morellonet


Software is eating the world
Every org is becoming a software org
Software orgs need modern tools
DevOps, containers, and cloud native are those tools
The world is dangerous
‘Democratization’ of sophisticated attacks
Security teams and SOCs overloaded
Your own software is the softest target

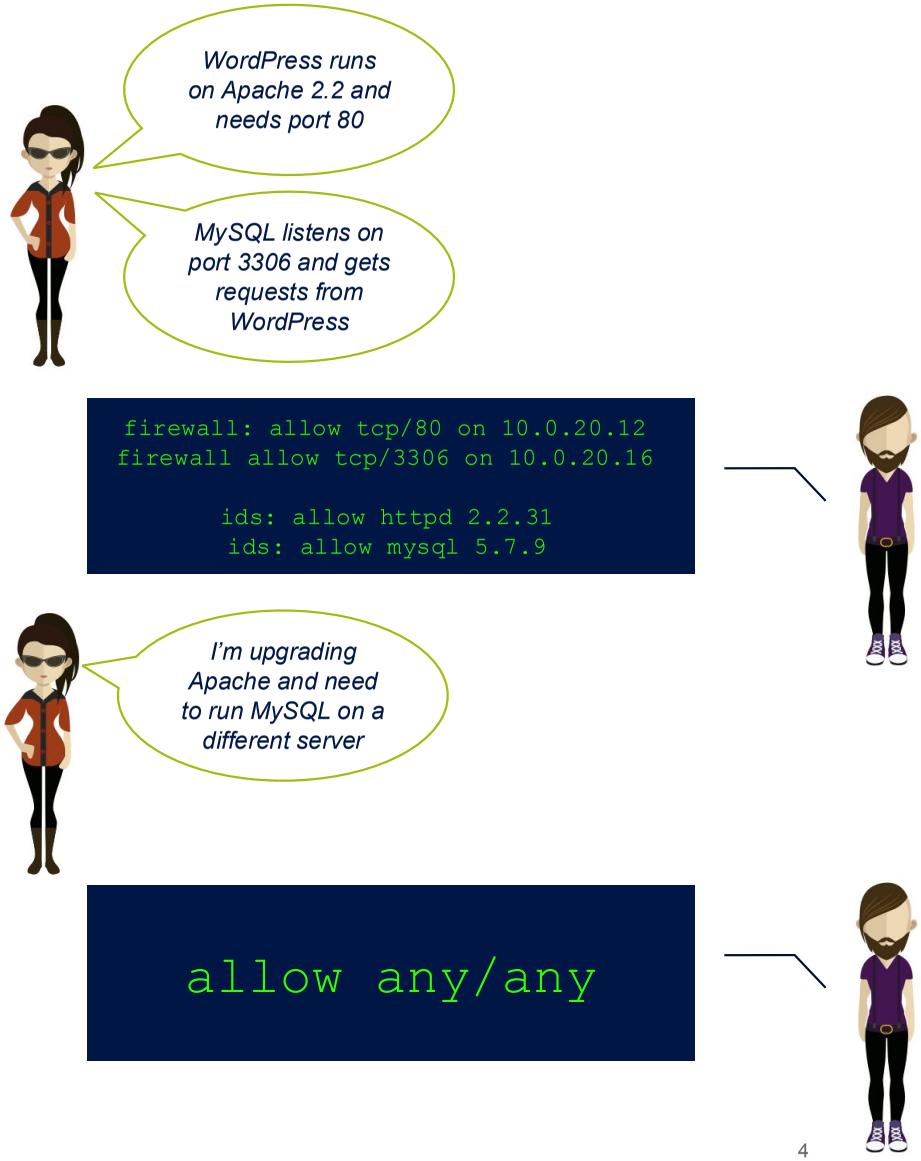
Containers improve security

Old World Security

Developers manually describe their apps to security teams

Security teams manually create policies in multiple tools

As the app evolves, the rules rot



Security Cake

You can have DevOps and containers or you can keep your old world security approach…

But you can't have both

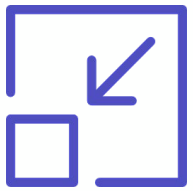
An Opportunity for Better Defense

The nature of containers allows for a new approach to security

Apply machine learning to understand actual runtime behavior

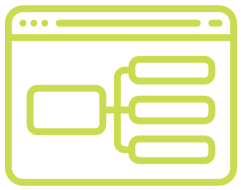
Build models of what containers ***should*** do to detect and prevent what they ***shouldn't***

Container Characteristics



Minimal

Typically single process entities



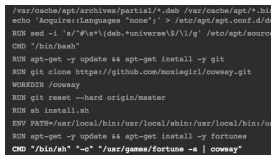
Declarative

Built from images that are machine readable

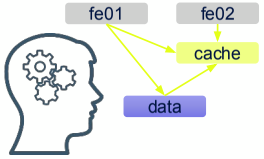
Predictable

Do exactly the same thing from **`run`** to **`kill`**

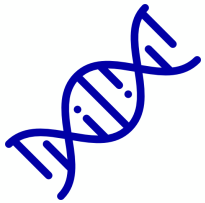
Autonomous Defense



+



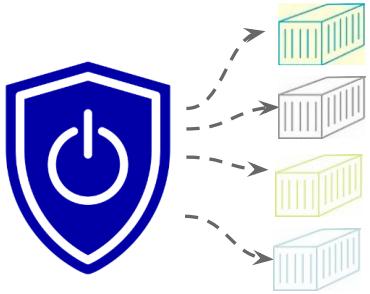
=



+

```
ip, category, score, first_seen,
last_seen, ports
74.88.8.7,31,65,2016-04-16,2016-
04-16,
23.16.9.49,35,125,2016-04-11,201
6-04-20,80
82.16.9.65,35,127,2016-04-09,201
6-04-21,80
```

=



Static analysis

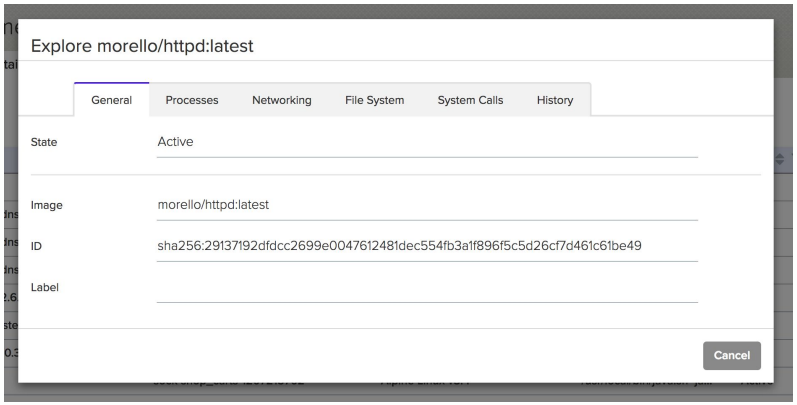
Machine learning

Predictive model

Threat intelligence

Automated defense

What's a Model?



Automatically learned across 4 dimensions

Correlated to unique image digest

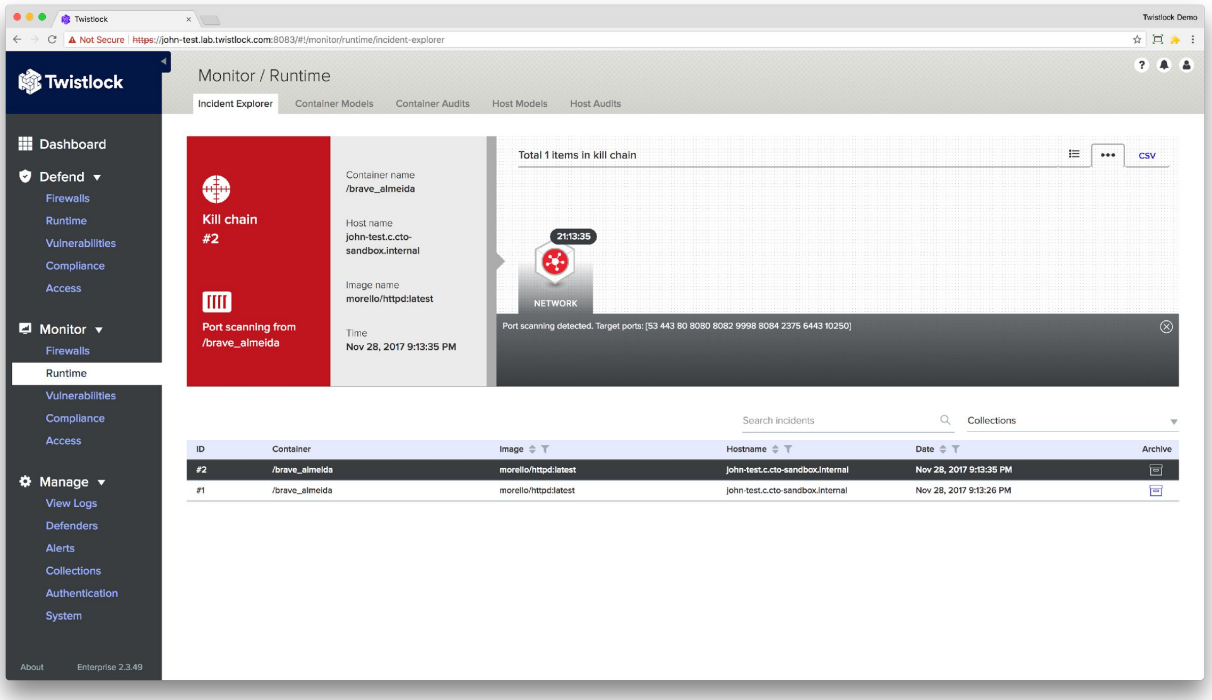
Models are explicit allow lists

```
root@john-test:/home/john# curl -k -u user:pass
"https://localhost:8083/api/v1/profiles/container" | jq . | grep httpd -A 20 -B 5
...
[
  {
    "state": "active",
    "remainingLearningDurationSec": 0,
    "_id": "sha256:29137192dfdcc2699e0047612481dec554fb3a1f896f5c5d26cf7d461c61be49_",
    "image": "morello/httpd:latest",
    "version": "2.3.49",
    "os": "Debian GNU/Linux 8 (jessie)",
    "archived": false,
    "entrypoint": "httpd-foreground",
    "infra": false,
    "processes": {
      "static": [
        {
          "path": "/usr/local/apache2/bin/httpd",
          "ppath": "",
          "md5": "f9ff43be045e42222f08b6dede293af3"
        },
        {
          "path": "/bin/bash",
          "ppath": "",
          "md5": "33135f5a1fb45f5dff915ec1193c0dc7"
        },
      --
    },
    "network": {
      "static": {
        "listeningPorts": [
          {
            "app": "/usr/local/apache2/bin/httpd",
            "ports": [
              80
            ],
            "allPorts": false
          }
        ]
      },
      "behavioral": {
        "outboundPorts": [],
        "listeningPorts": [],
        "dnsQueries": []
```

Automatic Prevention

Models enable automatically detecting and preventing anomalies at scale

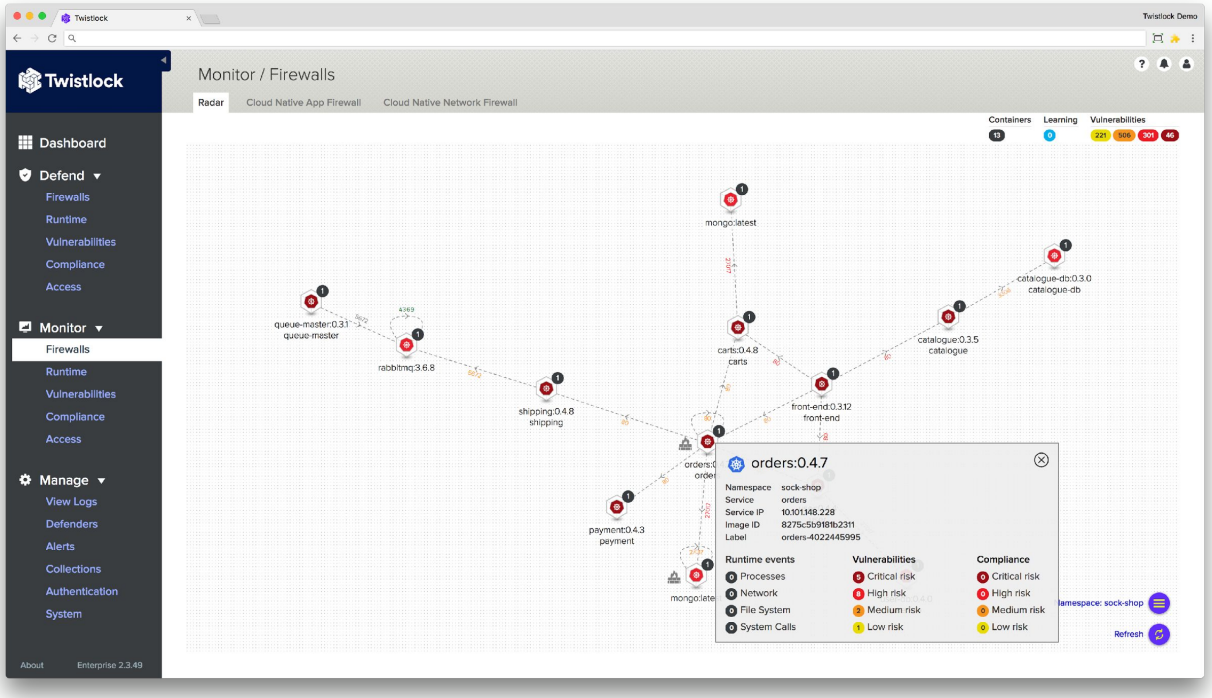
Correlate data from multiple sensors to summarize multilayered attack patterns



Supermodels

Correlate models from multiple microservices to create supermodels

Visualize and compartmentalize intra-namespace traffic flows



New World Security

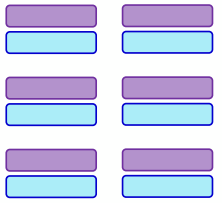
Modeling integrated into development and deployment

Custom tailored policy for each app

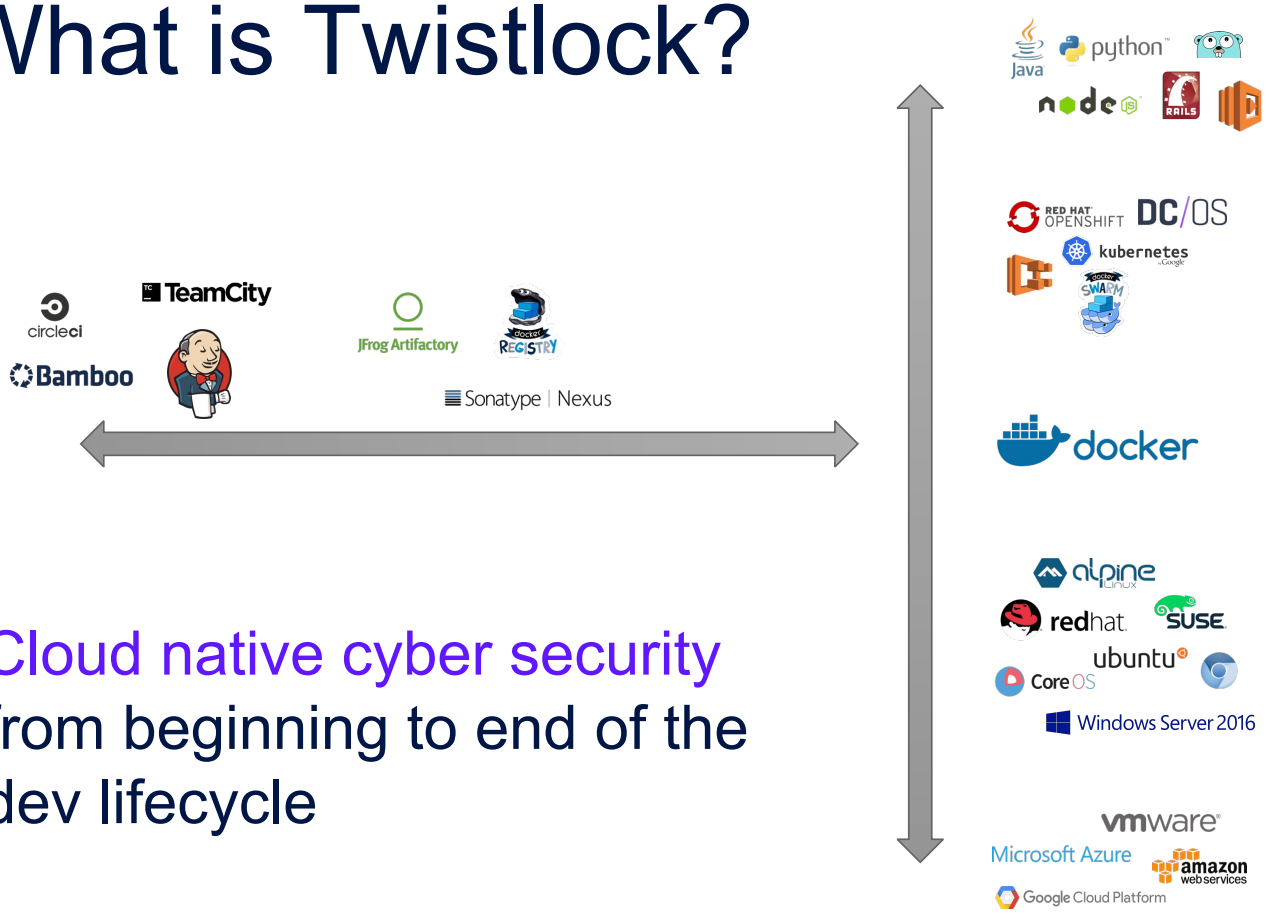
Security scales with the app, everywhere it runs

```
var express =
require('express'); var
app = express();
```

```
app.listen(3000, function () {
  console.log('Example app
listening on port 3000!'); });
```



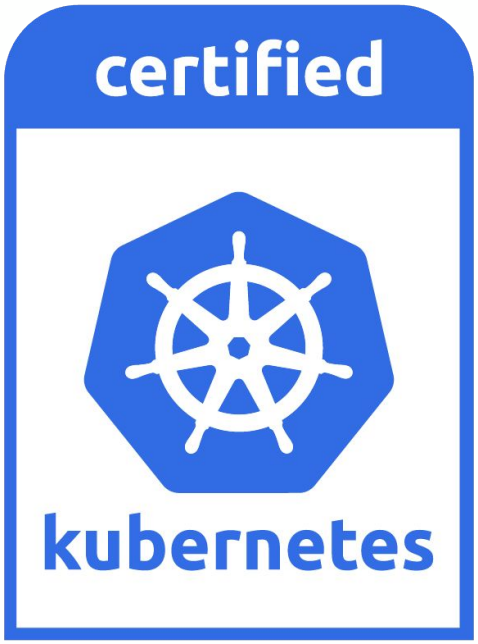
What is Twistlock?



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

Cloud native cyber security
from top to bottom of the stack

Kubernetes Certified



https://github.com/cncf/k8s-conformance/pull/94

Deploy Console as a Replication Controller

Deploy Defender to every node as a Daemon Set

Who Are We?

Technology pioneer and innovator

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

12 major releases shipped, including >250 customer requested features to date

13 patents pending

4 container related 0-days discovered by our research team

Market leader

>100 customers around the world

Enterprise grade global support with 24/7/365 SLA

>$30M raised to date

Ecosystem leader

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

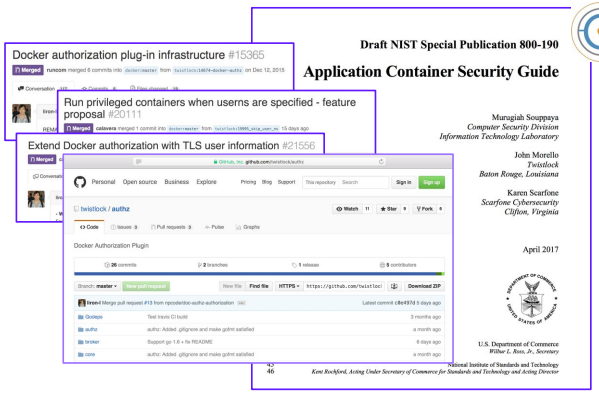
Lead author of NIST SP 800-190, the Container Security Guide

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

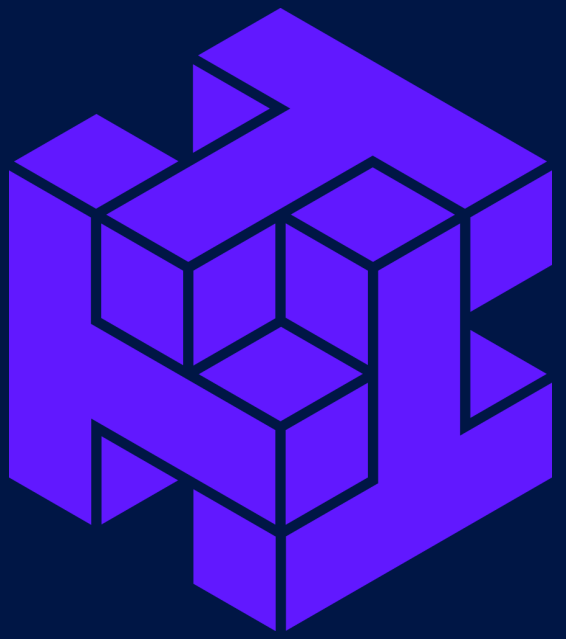
Awards & press

Partnerships

Open source and standards work



twistlock.com



@TwistlockTeam

sales@twistlock.com

Booth G28