Accelerate Your Development of Secured Microservices in the Cloud with IBM Cloud Hyper Protect Containers

Chris Poole
IBM

Twitter: @chrispoole
LinkedIn: @chrispoole643

November 2018
Session CA

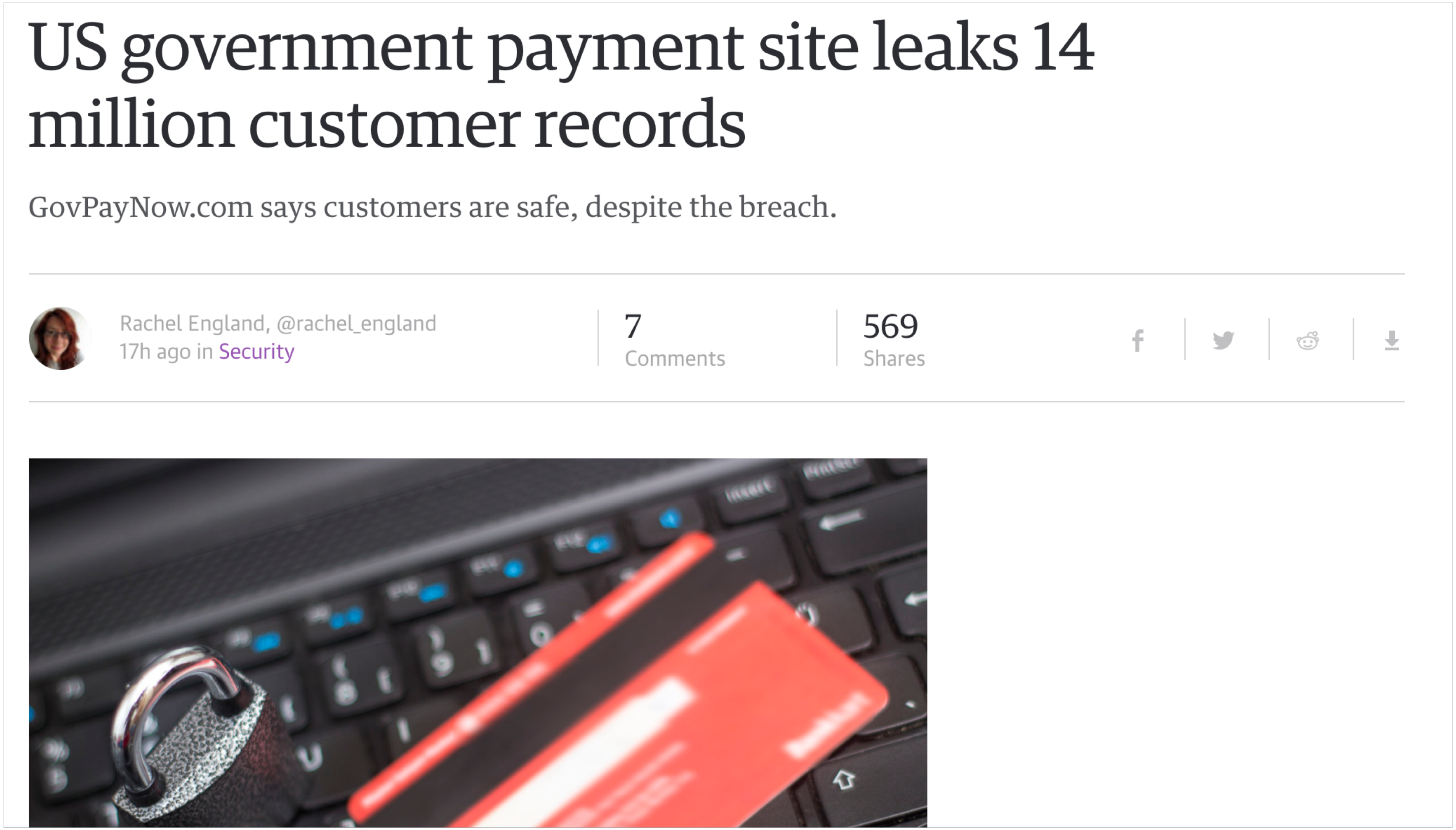
Please note

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user’s job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

“

> Within one Kubernetes pod, access credentials were exposed to Tesla's AWS environment which contained an Amazon S3 bucket that had sensitive data such as telemetry.

https://arstechnica.com/information-technology/2018/02/tesla-cloud-resources-are-hacked-to-run-cryptocurrency-mining-malware/



US government payment site leaks 14 million customer records

GovPayNow.com says customers are safe, despite the breach.

Rachel England, @rachel_england
17h ago in Security

7
Comments

569
Shares

https://www.engadget.com/2018/09/18/us-government-payment-site-leaks-14-million-customer-records-GovPayNow/?platform=hootsuite&guccounter=1

73%
Allow root access

2%
Corporate data encrypted

58%
Threats from insiders

https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-17425&S_PKG=ov59678&
https://www.techrepublic.com/article/tesla-public-cloud-environment-hacked-attackers-accessed-non-public-company-data/
https://healthitsecurity.com/news/58-of-healthcare-phi-data-breaches-caused-by-insiders

“Move to the cloud”?

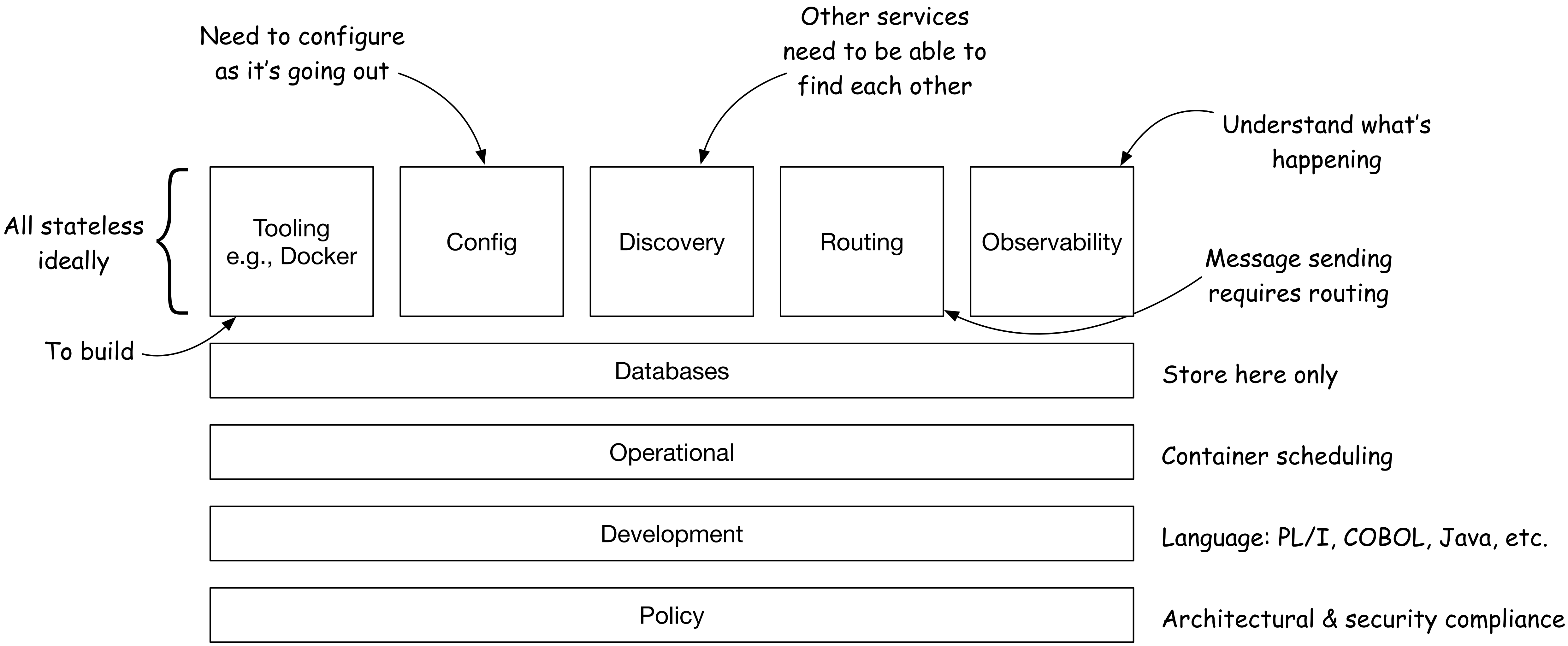
“Move to the cloud”?

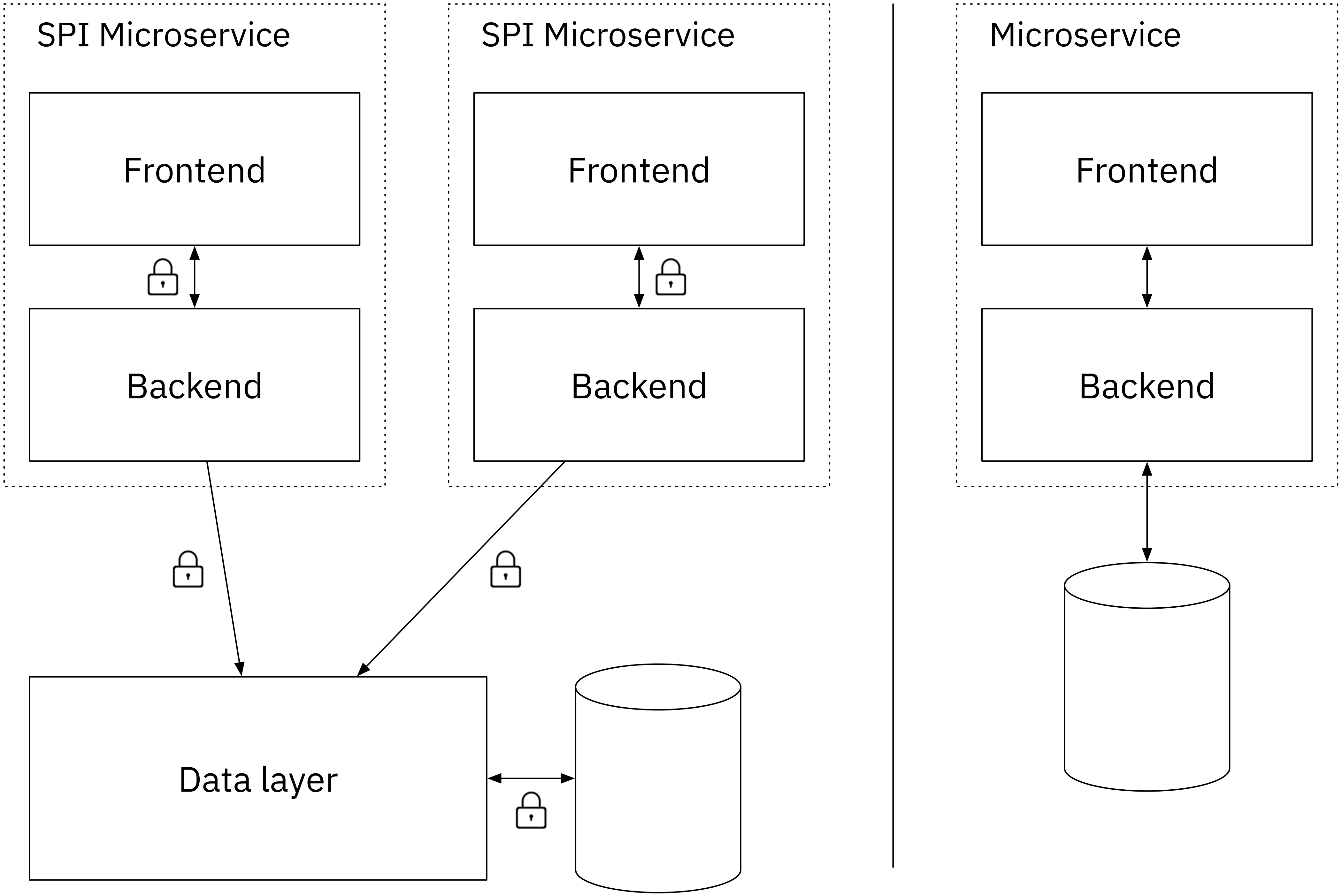
GDPR

EU General Data Protection Regulation

HIPAA

PCI DSS COMPLIANT

Need to configure as it's going out
Other services need to be able to find each other
Understand what's happening
All stateless ideally
Tooling e.g., Docker
Config
Discovery
Routing
Observability
Message sending requires routing
To build
Databases
Store here only
Operational
Container scheduling
Development
Language: PL/I, COBOL, Java, etc.
Policy
Architectural & security compliance



SPI Microservice

Frontend

Backend

SPI Microservice

Frontend

Backend

Data layer

Microservice

Frontend

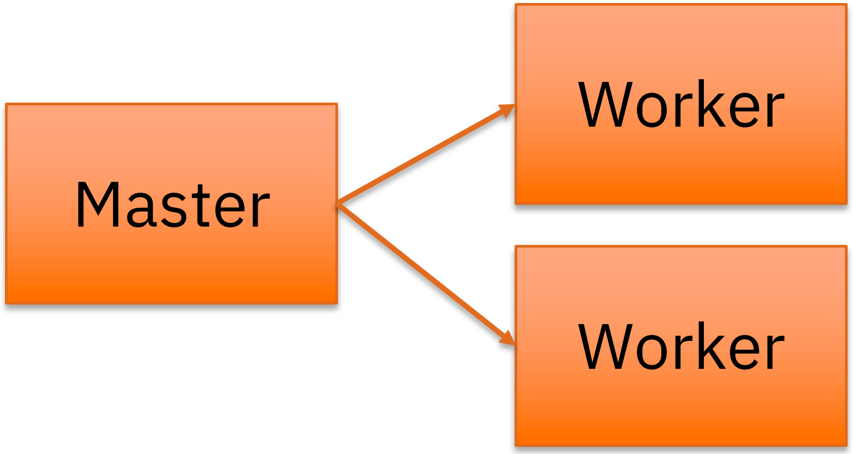
Backend

Improving application development

- Recognition that an app isn’t just the source code: libraries etc.
- DevOps encourages ownership by the dev team
- Test, lift, drop, deploy
- Containers as lightweight alternative to VMs

Orchestrate your containers

- Kubernetes
- HA
- Load balancing
- Master, worker nodes

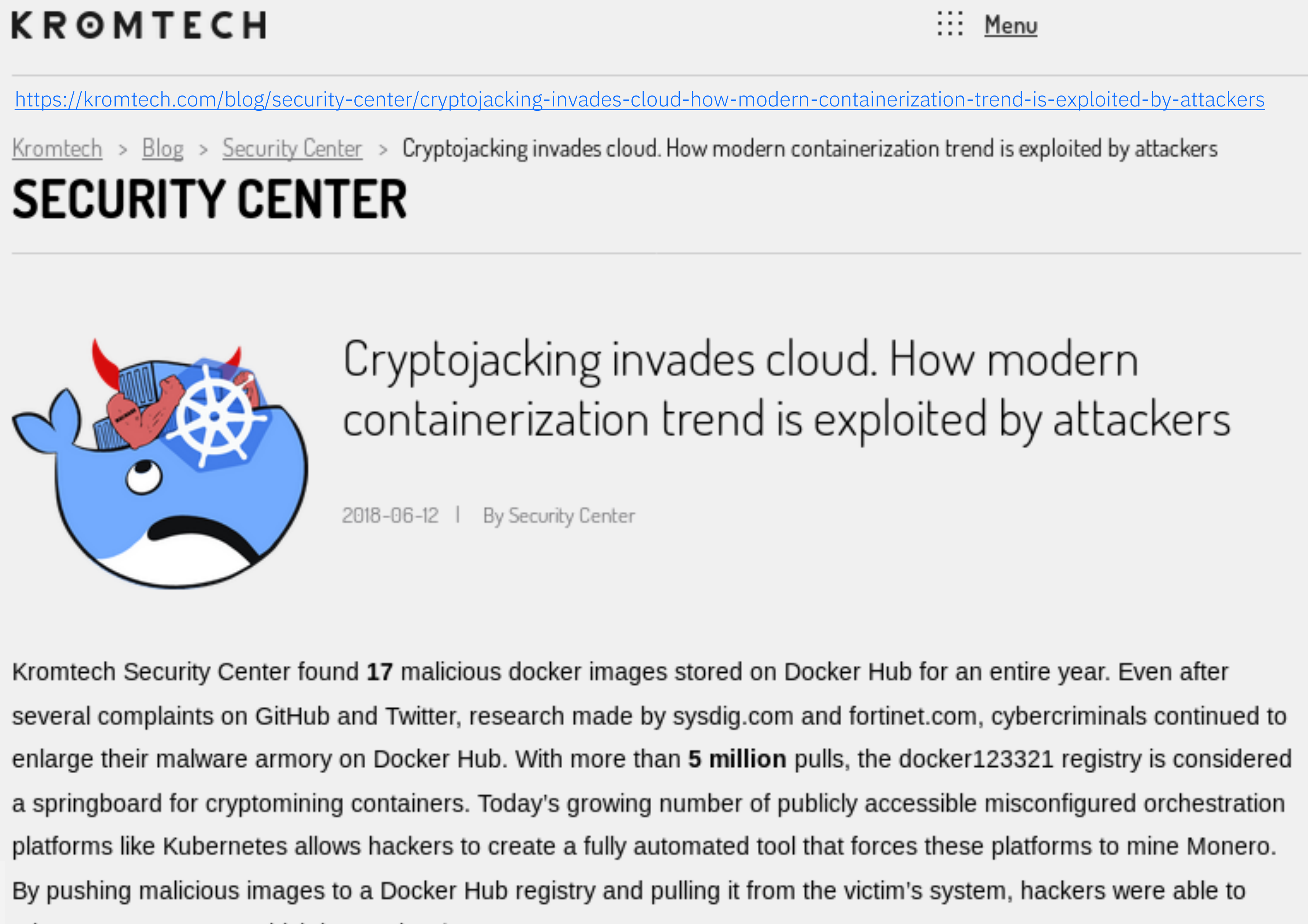


Apps with SPI?

- Rewrite yourselves
  - Encrypt the data… all of it? Metadata?
- Security consultancy
- **How to lock it down?**

Why should I care about containers' security ?

Because……



KROMTECH

Menu

https://kromtech.com/blog/security-center/cryptojacking-invades-cloud-how-modern-containerization-trend-is-exploited-by-attackers

Kromtech > Blog > Security Center > Cryptojacking invades cloud. How modern containerization trend is exploited by attackers

SECURITY CENTER

Cryptojacking invades cloud. How modern containerization trend is exploited by attackers

2018-06-12 | By Security Center

Kromtech Security Center found **17** malicious docker images stored on Docker Hub for an entire year. Even after several complaints on GitHub and Twitter, research made by sysdig.com and fortinet.com, cybercriminals continued to enlarge their malware armory on Docker Hub. With more than **5 million** pulls, the docker123321 registry is considered a springboard for cryptomining containers. Today's growing number of publicly accessible misconfigured orchestration platforms like Kubernetes allows hackers to create a fully automated tool that forces these platforms to mine Monero. By pushing malicious images to a Docker Hub registry and pulling it from the victim's system, hackers were able to

Yet net?

ner-crypto-mining-botnet.html

Docker service configuration

Running the Docker daemon requires root privileges, which has some security implications.

The most one important is to control **who** has access to the (local) Docker Unix socket used to control the Docker daemon.

Most distributions packages change the group ownership of the Docker socket from root to docker, allowing users member of the docker group to gain control of the daemon (without using *sudo*).

```
blockchain@blkchndemo:~$ ls -al /var/run/docker.sock
srw-rw---- 1 root docker 0 Sep  3 16:54 /var/run/docker.sock
blockchain@blkchndemo:~$ id blockchain
uid=1001(blockchain) gid=1001(blockchain) groups=1001(blockchain),0(root),119(docker)
blockchain@blkchndemo:~$
```

Carefully evaluate and control **who** is given access to the docker group

Should you need access to the Docker daemon over the network, make sure TLS is configured appropriately to secure the access to the HTTP socket.

Docker containers images and build files

By default, the processes are running inside the container with root privileges.

How many times have I been bitten by files I couldn’t edit on the host because they were created in the container and by root ? I’ve lost count…

```
[guigui@t460 Org1 (master *%=)]$ ls -al
total 100
drwxr-xr-x. 3 root root  4096 Aug 27 14:59 .
drwxr-xr-x. 5 root root  4096 Aug 27 14:59 ..
-rw-r--r--. 1 root root   786 Aug 27 14:59 ca-cert.pem
-rw-r--r--. 1 root root 16031 Aug 27 14:59 fabric-ca-server-config.yaml
-rw-r--r--. 1 root root 61440 Aug 27 14:59 fabric-ca-server.db
-rw-r--r--. 1 root root   843 Aug 27 14:59 IssuerPublicKey
-rw-r--r--. 1 root root   215 Aug 27 14:59 IssuerRevocationPublicKey
drwxr-xr-x. 3 root root  4096 Aug 27 14:59 msp
```

Now imagine what could possibly go wrong if a process does rm a mapped volume from the host ?
It depends! On the volume.

If possible, prefer using a non-privileged user to run processes inside your containers.

Docker containers images and build files

How to check if the processes are running as users or as root ?

- Log into the container and look at the output of the ps command:

```
blockchain@blkchndemo:~/v1.1.x$ docker exec -it peer2.1 ps faux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        15  0.0  0.0  34424  2704 pts/0    Rs+  13:28   0:00 ps faux
root         1  1.6  0.1 311944 21748 ?        Ssl  13:28   0:00 peer node start
```

```
blockchain@blkchndemo:~/v1.1.x$ docker exec -it peer2.1 ps faux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root        42  2.0  0.0  20252  3252 pts/0    Ss   13:30   0:00 bash
root        49  0.0  0.0  17500  2116 pts/0    R+   13:30   0:00  \_ ps faux
root         1  0.0  0.0  20068  2828 ?        Ss   13:30   0:00 /bin/bash /docker-entrypoint.sh peer node start
root        24  0.0  0.0  44764  2692 ?        S    13:30   0:00 su fabric -c peer node start
fabric      25  0.0  0.0   4340   708 ?        Ss   13:30   0:00  \_ sh -c peer node start
fabric      26  1.4  0.1 328164 24320 ?        Sl   13:30   0:00      \_ peer node start
```

- Inspect the container from the host:

```
blockchain@blkchndemo:~/v1.1.x$ docker inspect peer2.1 --format '{{ .Id }}: User={{ .Config.User }}'
d468cae1409f9811662606a3fba69cc52b97689a41a78c5e44236c6c30baaac3: User=
```

If User is not set, there was no USER specified in the Dockerfile.

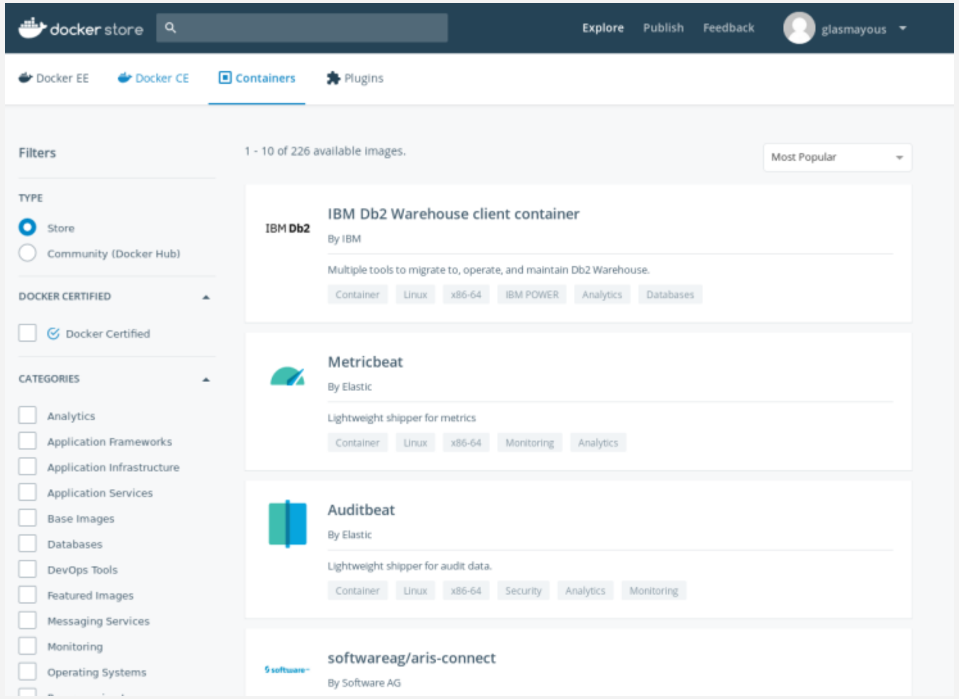
Docker containers images and build files

Docker containers are all about reuse:

- Reusing existing code layers, as a result of successive images creation.
- Reusing existing images as base for your own.

Docker provides thousands of base images (of varying quality) through the [Docker Hub](#) and the [Docker Store](#):

- Docker Hub claims 1M+ images available from the community
- Docker Store has 226 images available.



Filters

TYPE

● Store

○ Community (Docker Hub)

DOCKER CERTIFIED

□ Docker Certified

CATEGORIES

□ Analytics
□ Application Frameworks
□ Application Infrastructure
□ Application Services
□ Base Images
□ Databases
□ DevOps Tools
□ Featured Images
□ Messaging Services
□ Monitoring
□ Operating Systems

1 - 10 of 226 available images.

IBM Db2 Warehouse client container
By IBM
Multiple tools to migrate to, operate, and maintain Db2 Warehouse.
Container · Linux · x86-64 · IBM POWER · Analytics · Databases

Metricbeat
By Elastic
Lightweight shipper for metrics
Container · Linux · x86-64 · Monitoring · Analytics

Auditbeat
By Elastic
Lightweight shipper for audit data.
Container · Linux · x86-64 · Security · Analytics · Monitoring

softwareag/aris-connect
By Software AG

Docker containers images and build files

With so many images to choose from, it is key to carefully select the base image to use to build your containers.

As a general recommendation, I would advise:

- To select images from the Docker Store whenever possible
- To use the vendor-provided Docker images
- To stick to well established providers.

It is usually reasonnable to assume that the smaller the base image, the least vulnerable the container. But it may have performance implications that need to be reviewed.

In order to assist with the vulnerability assessment of the base images stored by Docker, the Hub provides a security scanning mechanisms where images will be scanned when uploaded to the repository.

IBM Cloud Hyper Protect Services

IBM-hosted services:

IBM Cloud Hyper Protect Crypto Services

IBM Cloud Hyper Protect DBaaS

IBM Cloud Hyper Protect Containers

IBM Cloud Hyper Protect Services

IBM-hosted services:

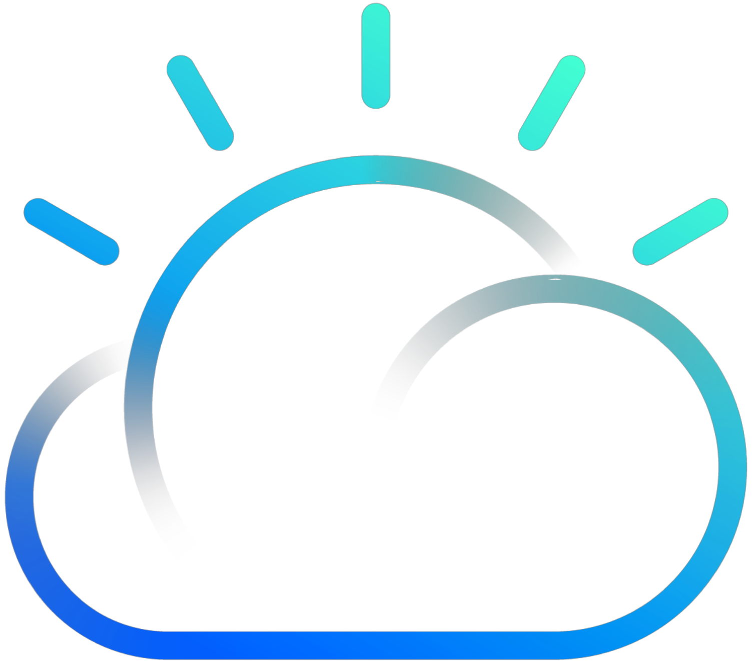
IBM Cloud Hyper Protect Crypto Services

IBM Cloud Hyper Protect DBaaS

IBM Cloud Hyper Protect Containers

Cloud computing

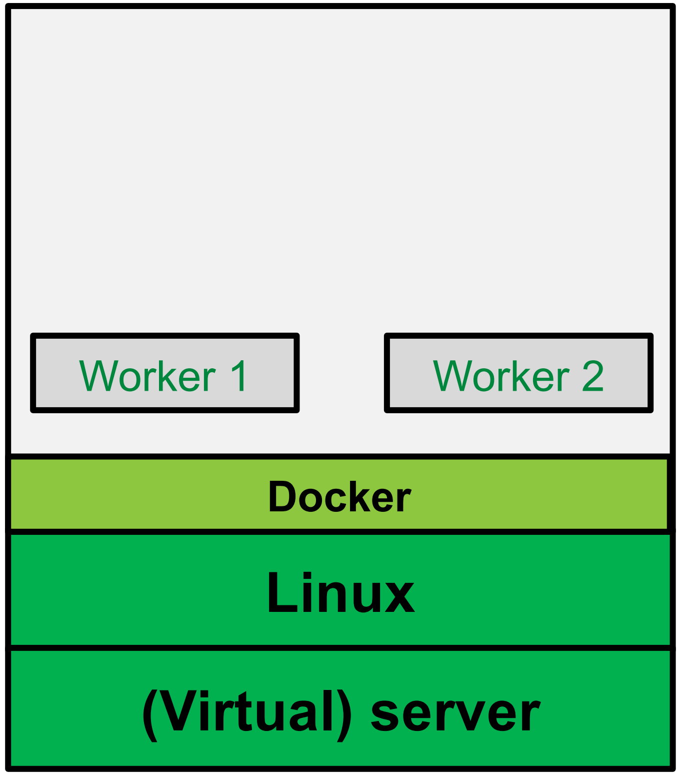
- Abstract away the infrastructure
- Who do you trust?



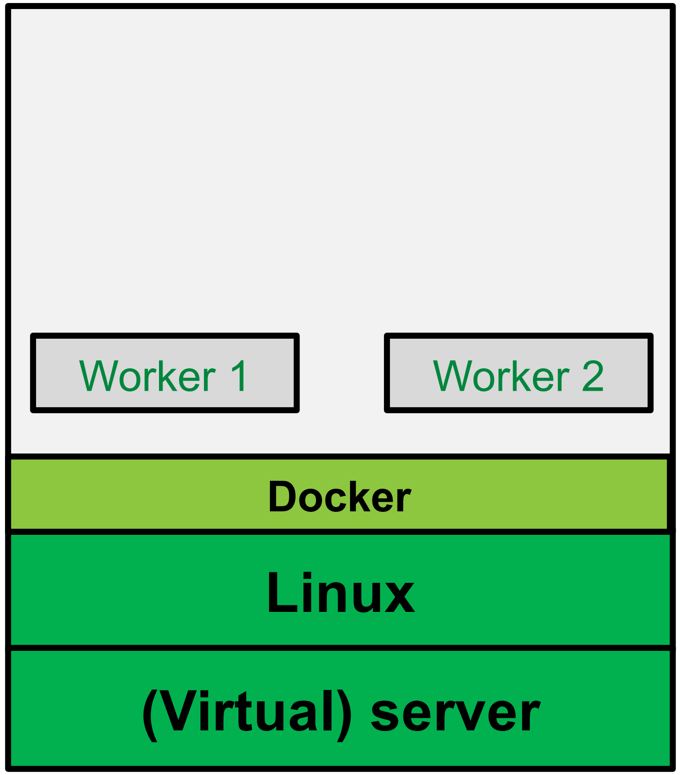
Attack vectors

- Insider threat: sysprogs
- Remote access
- Privilege escalation

Existing cloud



Existing cloud



Worker 1

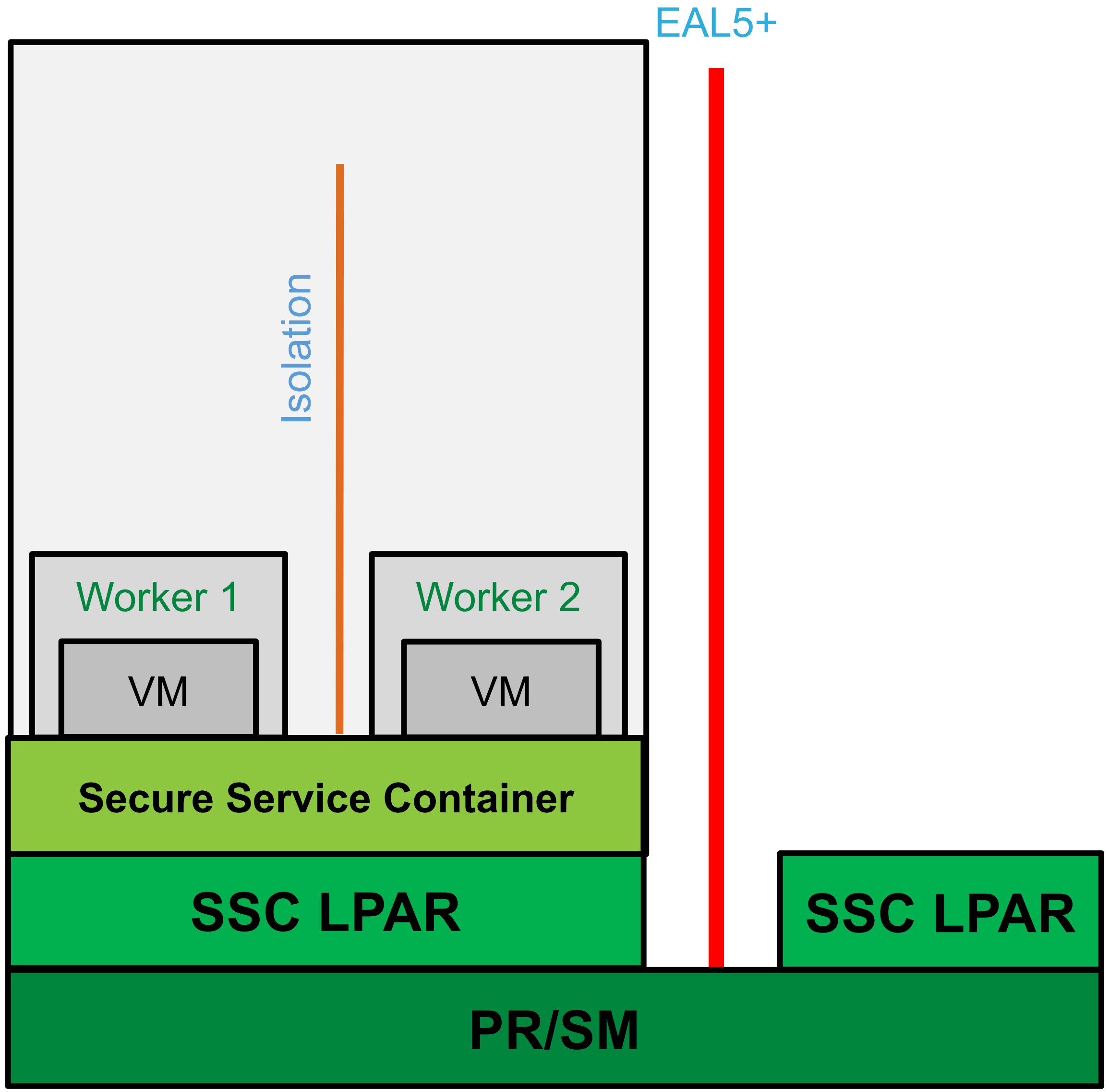
Worker 2

Docker

Linux

(Virtual) server

Hyper Protect cloud



EAL5+

Isolation

Worker 1

VM

Worker 2

VM

Secure Service Container

SSC LPAR

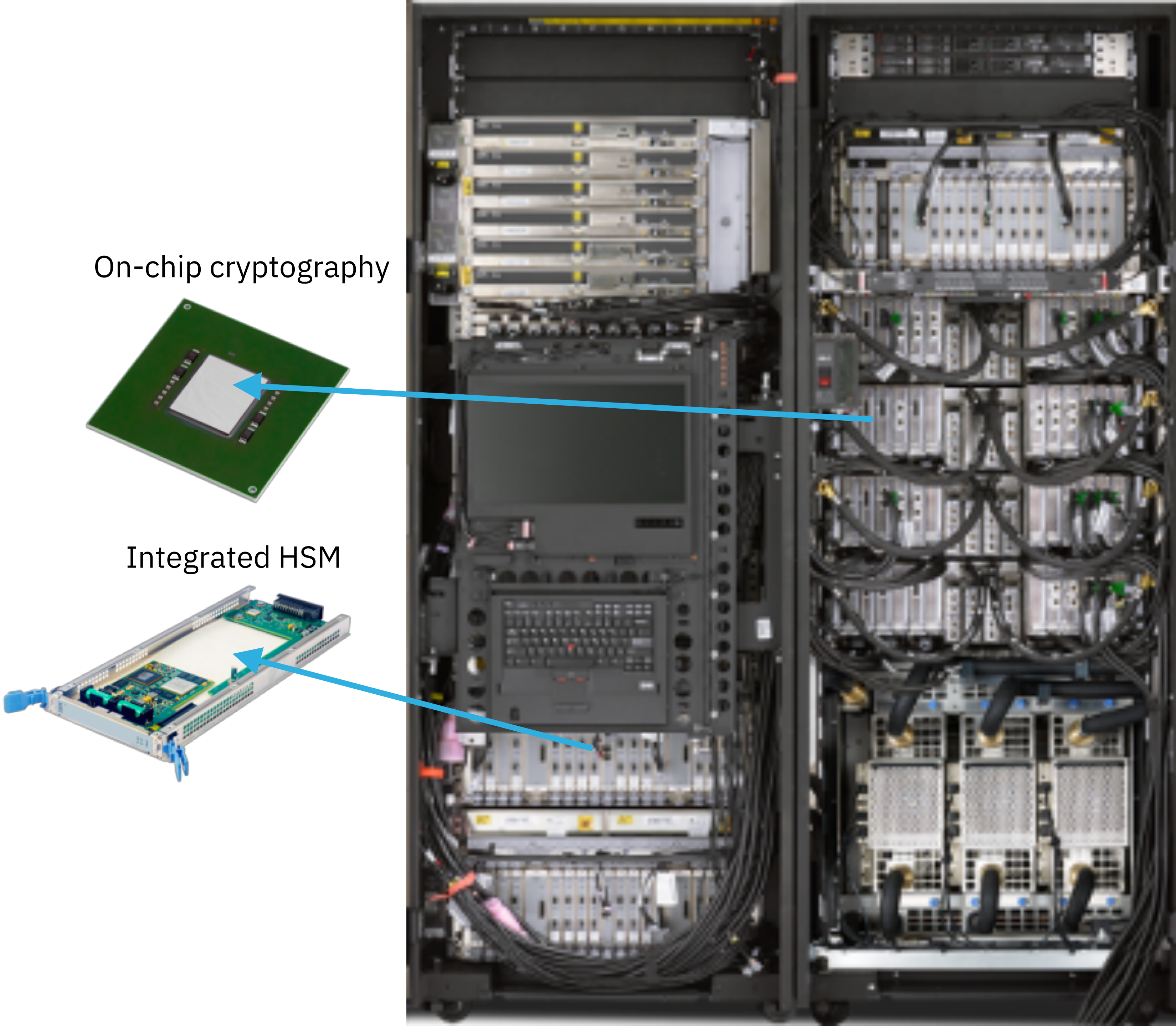
SSC LPAR

PR/SM

On-chip cryptographic accelerator

Crypto Express HSM

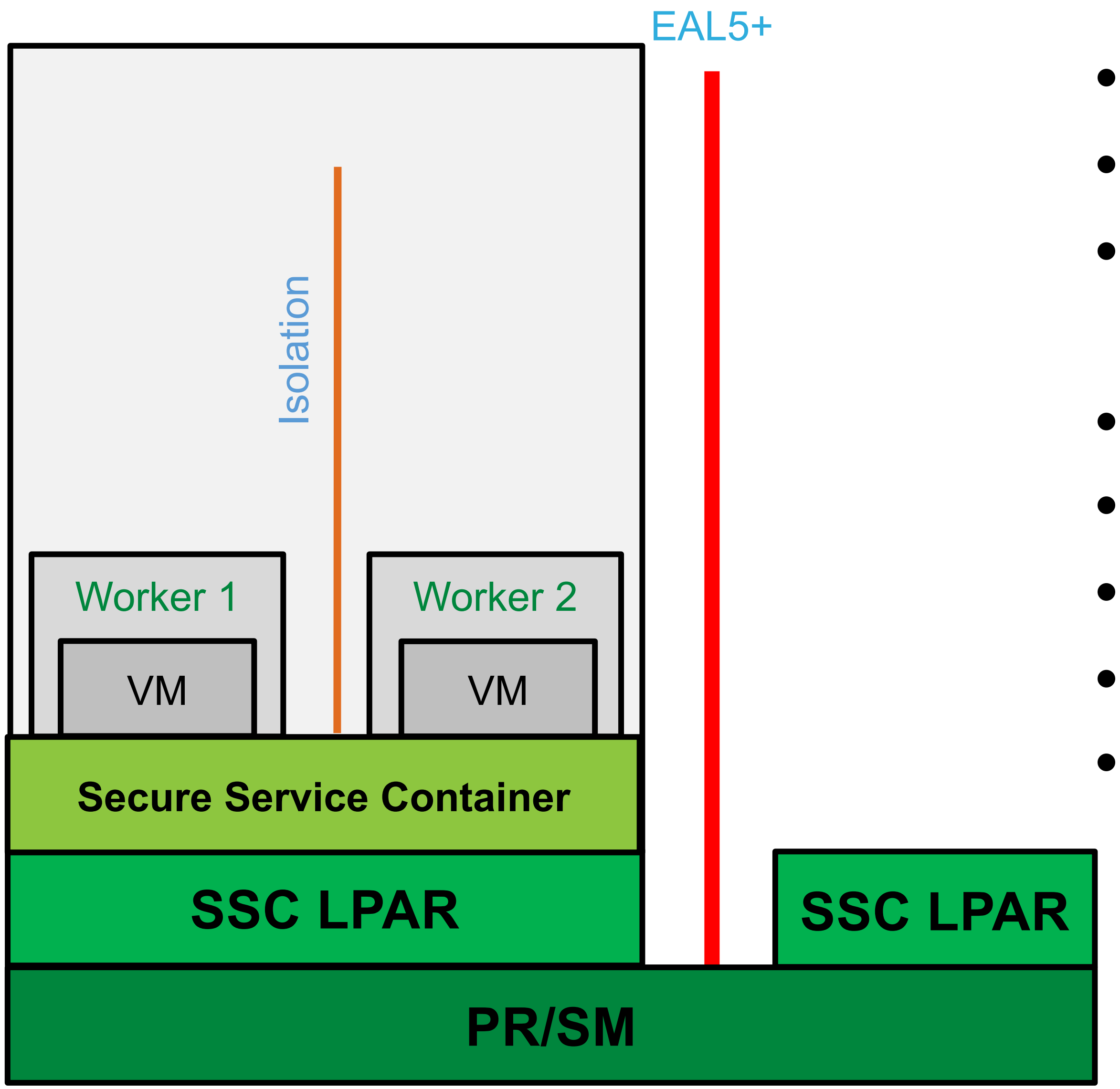
- Tamper resistant Secure Key
- FIPS 140-2 Level 4
- Keys never leave the HSM



On-chip cryptography

Integrated HSM

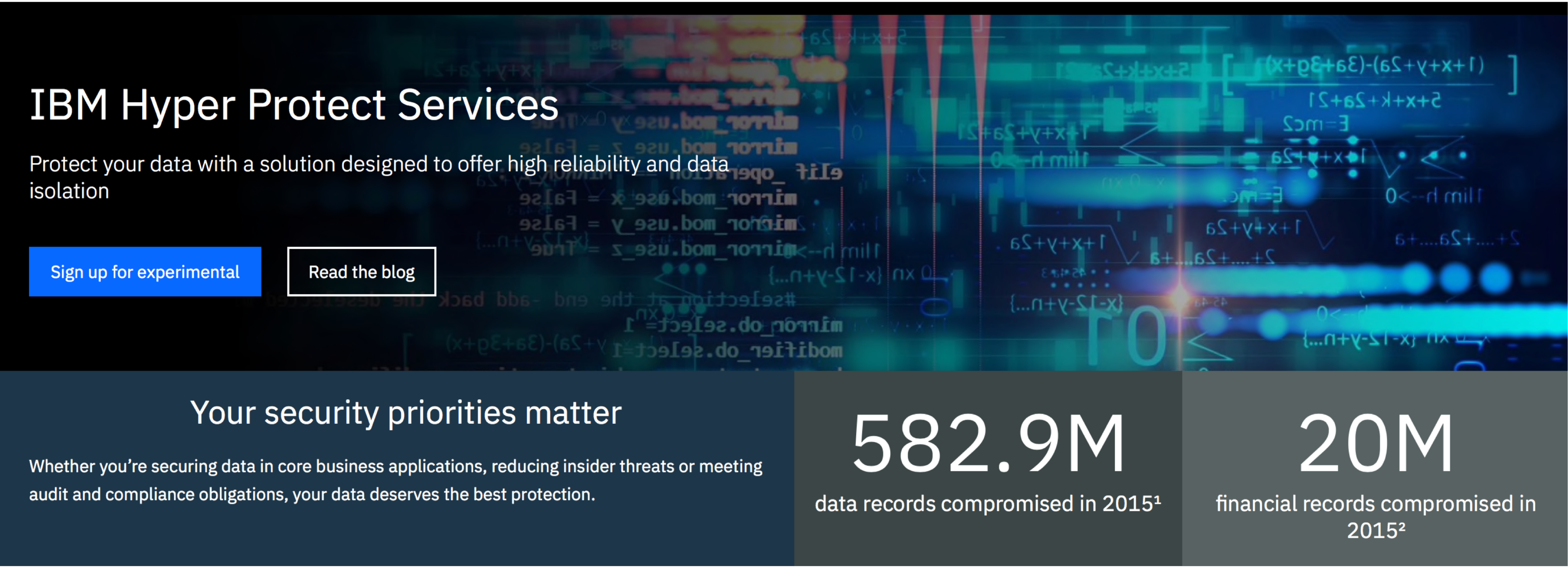
Secure Service Containers



- No system admin access
- Data at rest, transport protection
- Once the appliance image is built, OS access (ssh) is not possible
- Memory access disabled
- Encrypted disk
- Debug data (dumps) encrypted
- Signed docker images
- Secure boot

Demo

ibm.com/**cloud/hyper-protect-services**



IBM Hyper Protect Services

Protect your data with a solution designed to offer high reliability and data isolation

Your security priorities matter

Whether you’re securing data in core business applications, reducing insider threats or meeting audit and compliance obligations, your data deserves the best protection.

582.9M

data records compromised in 2015[1]

20M

financial records compromised in 2015[2]

Summary

Creating an app, want encryption to tick the compliance boxes?

- **Security without code change**
- Cloud-hosted Kubernetes, DBaaS, and crypto services

- **Starter kits**
- **Trial offerings**

chrispoole@uk.ibm.com
@chrispoole

We want your feedback!

- Please submit your feedback online at ….
  - ➢http://conferences.gse.org.uk/2018/feedback/CA

- Paper feedback forms are also available from the Chair person

- This session is CA