Encrypting data in Kubernetes environments.

Protect your data, not just your Secrets

MAKSIM YANKOVSKIY
VICE PRESIDENT, ENGINEERING

About the presenter

Maksim Yankovskiy – VP Engineering

Maksim has over 20 years of experience delivering and managing enterprise encryption and database software across all the major high tech industries. During his tenure at Zettaset, he has been responsible for the engineering team that delivered the entire XCrypt product portfolio. He has also filed patents related to distributed and high-performance encryption. Prior to Zettaset, Maksim worked at Ingrian Networks and held various roles related to distributed database systems at Siemens Medical Solutions, Ross Stores and Adobe Systems.

Agenda

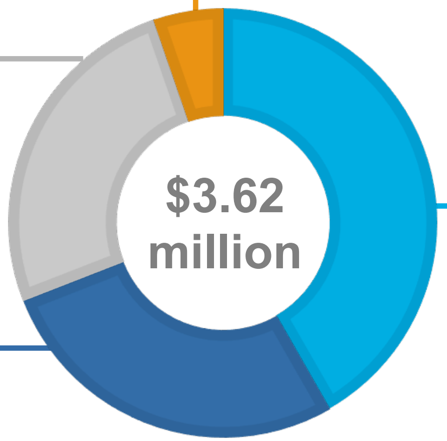
- Global security challenges
- Encryption: yesterday, today, and now
- Data breach protection for DevOps and DevSecOps
- Engineering with security in mind
- Keeping your secrets safe & protecting enterprise data
- Q&A

Data breaches and cyberattacks are **frequent** and **costly**

Recent survey:

- Data breaches will increase in frequency and diminish shareholder value
- Pessimistic about ability to protect from cyber threats
- Cybersecurity is still not considered a strategic priority
- Unsecured IoT devices will likely cause a data breach
- More investment to achieve regulatory compliance

Components of the $3.62 million cost per data breach



Notification $0.19 million
Disclosure of data breach to victims and regulators

Ex-post response $0.93
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

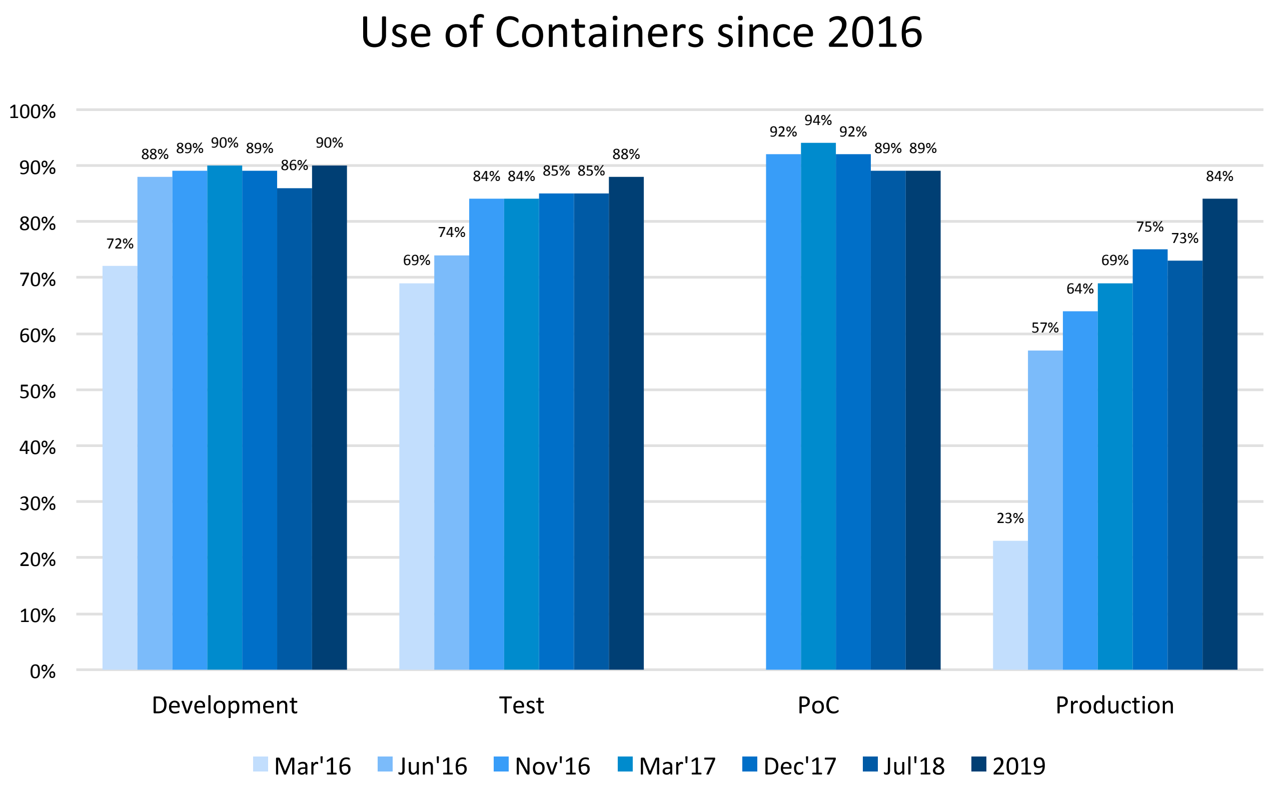
Lost business cost $1.51 million
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

Detection and escalation $0.99 million
Forensics, root cause determination, organizing incident response team, identifying victims

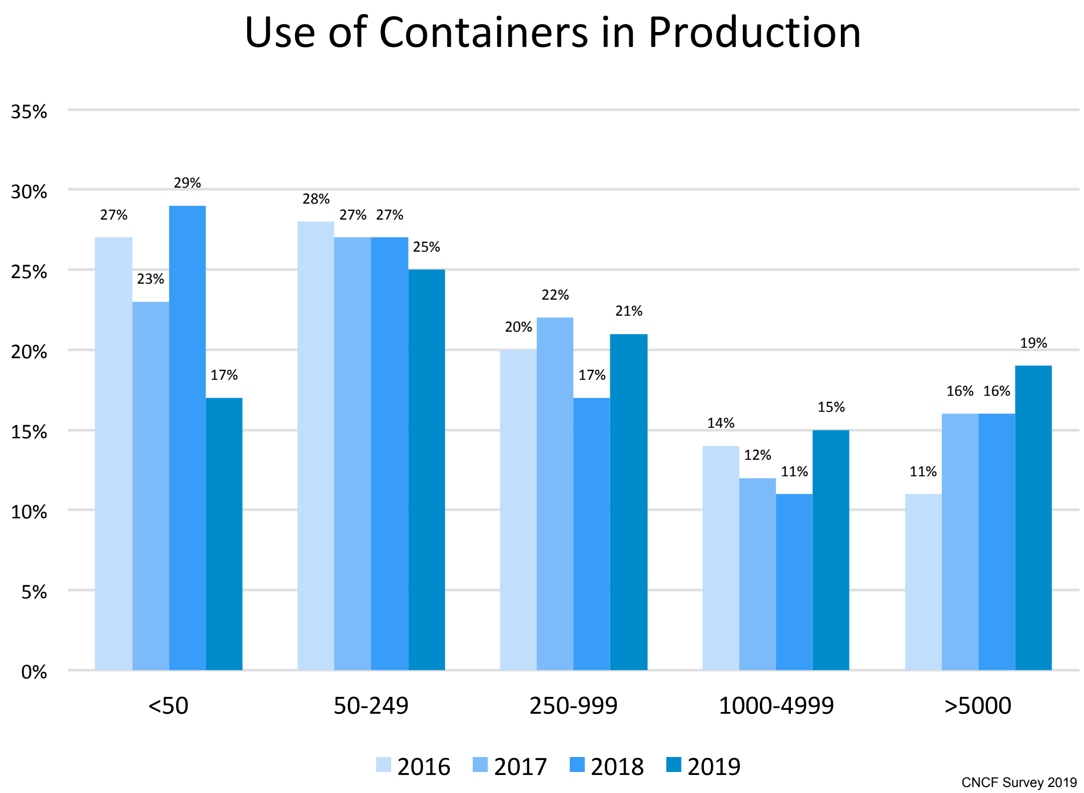
Data breaches have happened to many organizations:

- Equifax
- Yahoo
- Uber
- Whole Foods
- Verizon
- Dun & Bradstreet
- Saks Fifth Avenue
- UNC Healthcare
- IRS
- Kaspersky Lab
- Blue Cross
- Chipotle
- Docusign
- OneLogin
- Kmart
- SEC
- Sonic
- Hyatt
- Forever 21
- eBay
- Verifone
- Deloitte
- Alteryx
- Arby's
- Imgur
- Deep Root Analytics
- CA Association Realtors
- SVR Tracking
- Univ of Oklahoma
- Washington St. University
- Brooks Brothers
- TIO Networks
- Intercontinental Hotels
- Maine Foster Care
- America's JobLink

Containers in production



Use of Containers since 2016



Use of Containers in Production

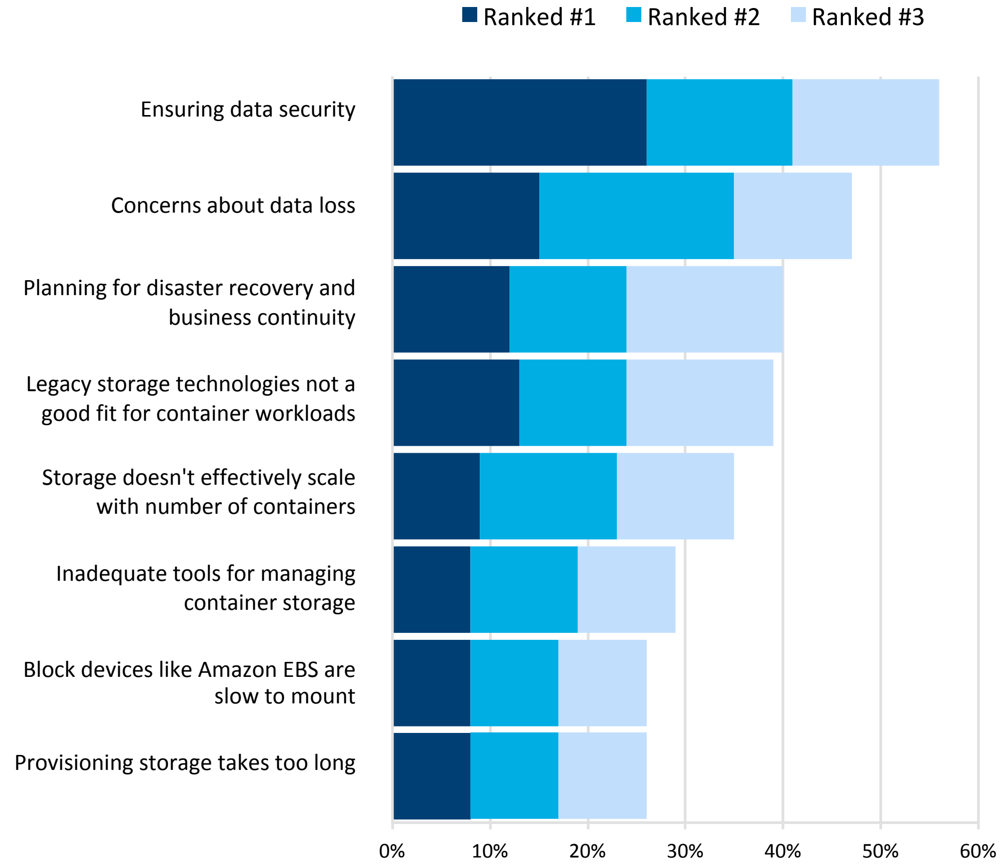
CNCF Survey 2019

- 69% of respondents intend to store sensitive data in containers
- 76% of container usage from Tech, FinServ & Healthcare
- 89% of container runtime is Docker
- 94% experienced a security incident in last 12 months
- Security is top barrier to further container adoption

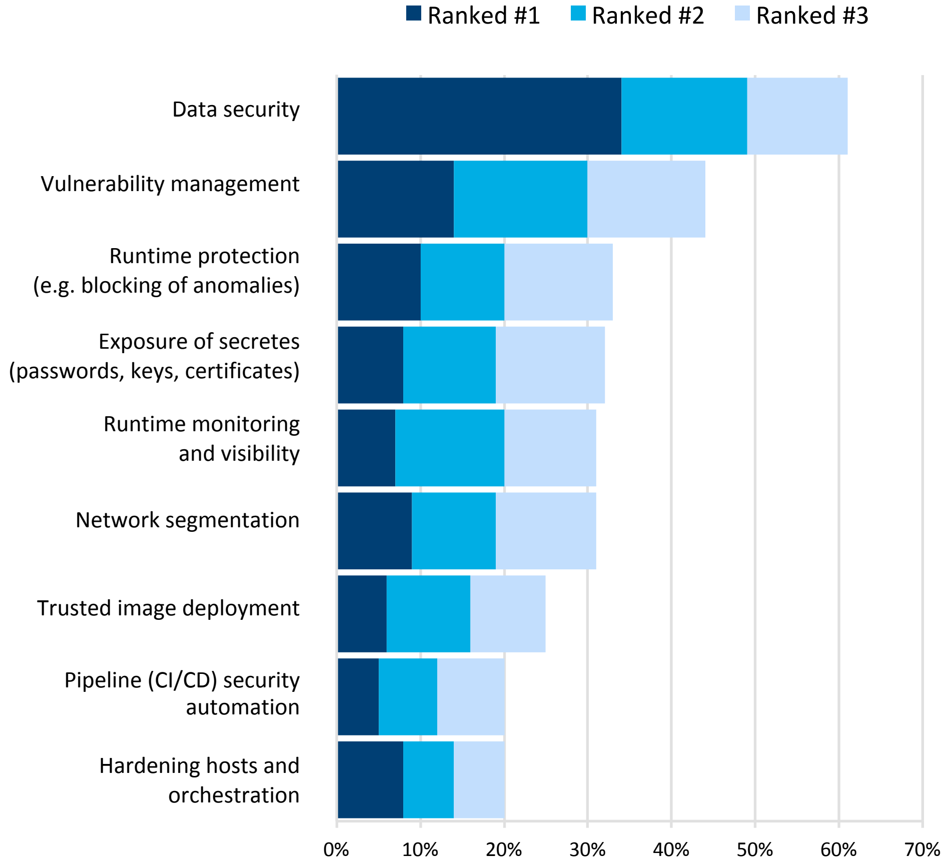
State of Kubernetes and Container Security Survey, Stackrox Winter 2020
2020 Thales Data Threat Report Survey, IDC, November 2019

Protect the Data

What are your top 3 storage challenges with containers?



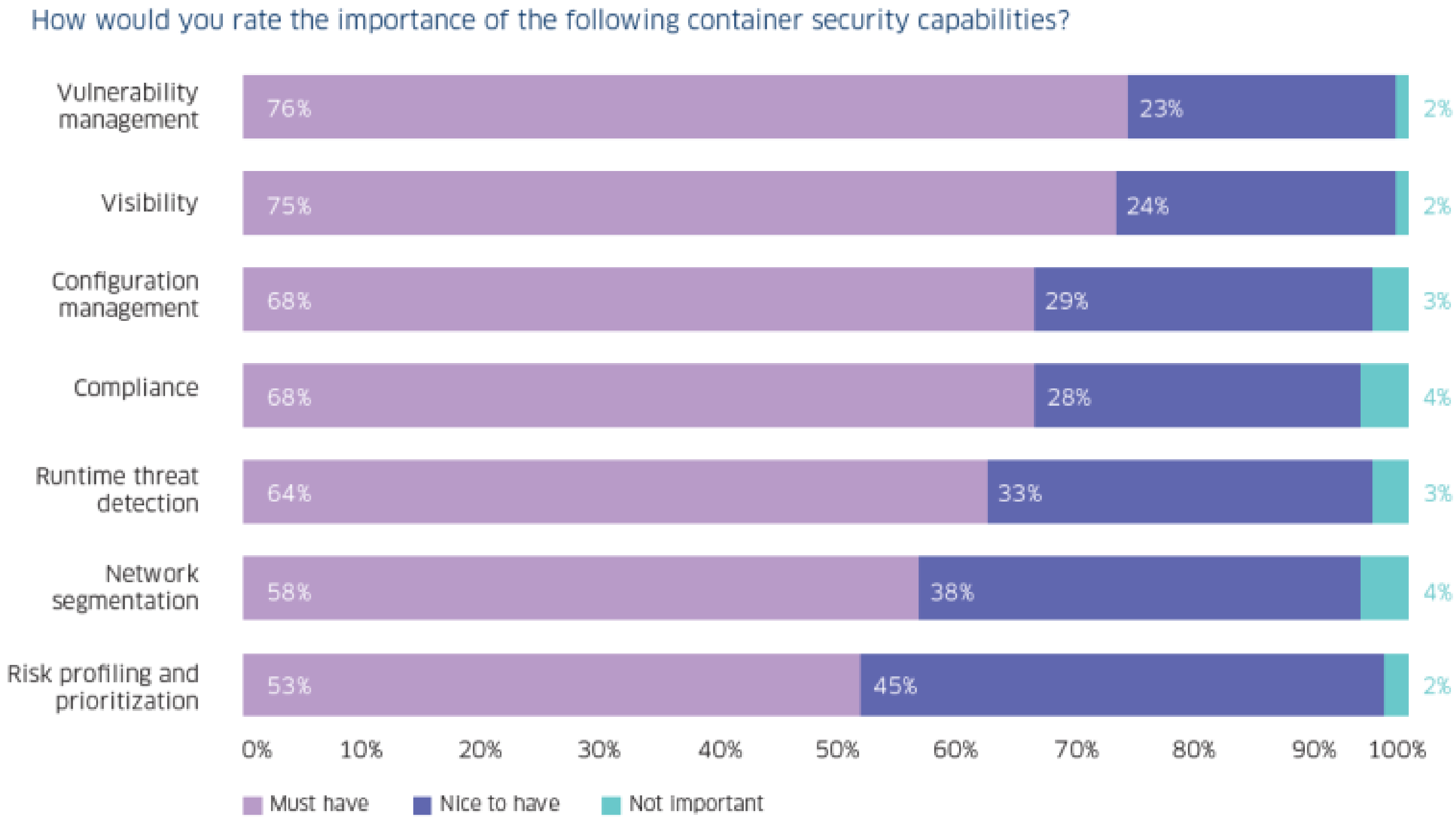
What are your top 3 security challenges with containers?



2019 Container Adoption Survey, Portworx and Aqua Security

Zettaset

Kubernetes Security



State of Kubernetes and Container Security Survey, Stackrox Winter 2020

CNCF Survey 2019

- 89% using forms of Kubernetes
- 78% of respondents are using Kubernetes in production
  - up from 58% in 2018
- Users are expecting more security with Kubernetes deployments
- Growth of production deployments brings greater need for protection and compliance

CNCF Survey 2019

Zettaset

How do you protect your data?

Top three data breach protection methods universally recommended by security experts and organizations in many surveys and panels:

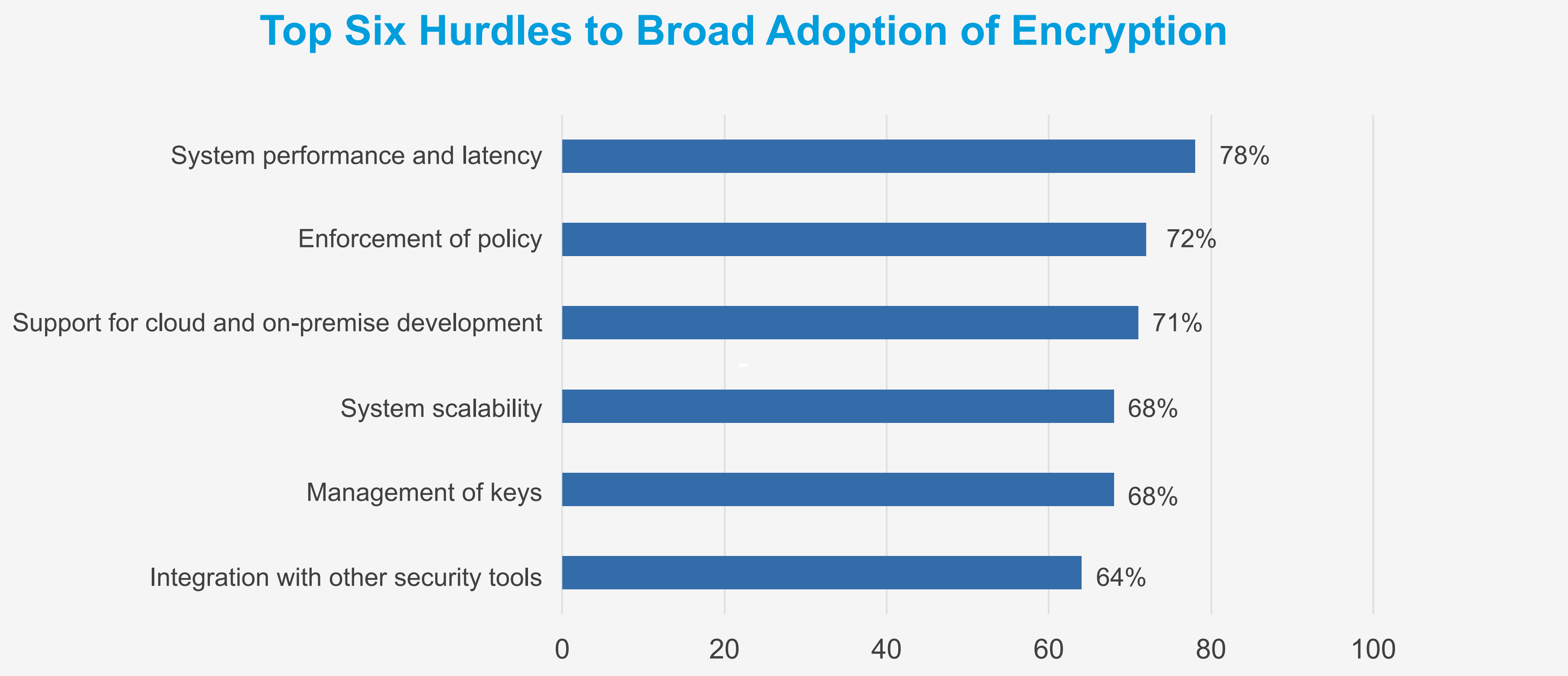
1. Encrypt data throughout the process of collection, viewing and manipulation - preferably at the source.

2. Any sensitive data that must be stored or is "at rest" needs to be encrypted and the keys can't be stored at the same location as the data.

3. All access and manipulation of data must be logged.

Zettaset

Factors impeding broad adoption of encryption

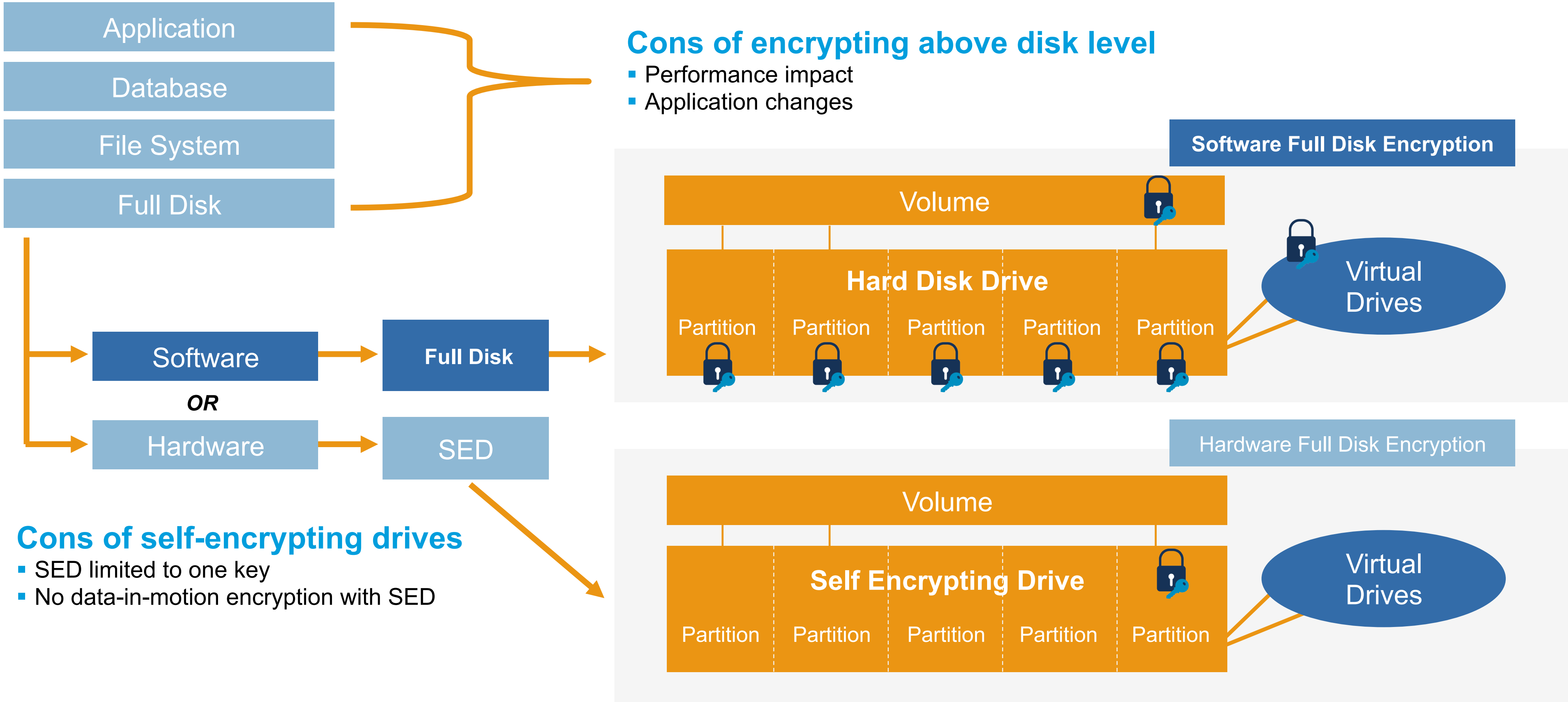


Global Encryption Trends Study 2017, Ponemon Institute and Thales

What to look for in an encryption solution

Performance	▪ Negligible performance impact on existing processes
Transparency	▪ Should not introduce changes to existing processes
Scalability	▪ On demand flexibility in physical, virtual or cloud – software-only solution recommended
Ease of Use	▪ Automated solutions that don’t require specialized cryptographic expertise ▪ Compatibility with Key Management & Hardware Security Module vendors
Supports Compliance Initiatives	▪ Provides regulatory and corporate compliance – PCI, DSS, HIPAA, FINRA, GDPR

Why not SEDs, or file, or column, or app, or API, or…?



Cons of encrypting above disk level

- Performance impact
- Application changes

Cons of self-encrypting drives

- SED limited to one key
- No data-in-motion encryption with SED

Engineering with security in mind

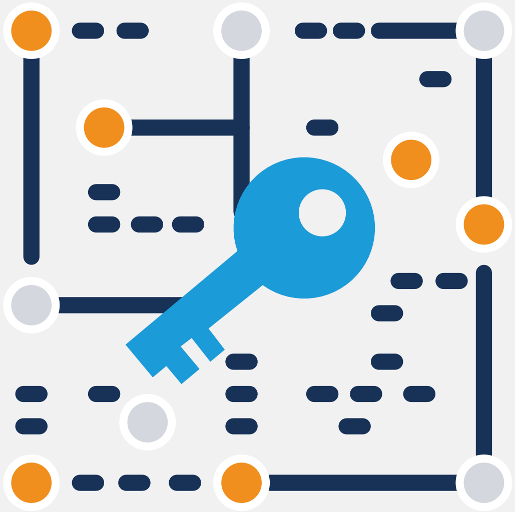
- Security as an afterthought is bad idea!
- Identify primary drivers for your security initiatives
- Balancing security and regulatory compliance
- Identifying security solutions
- Secrets and passwords protect your processes, not your data

Zettaset

Trust your encryption environment - Certificate Authority

- Signs and issues certificates for all services
- Ensures encryption services are not compromised
- Maintains Certificate Revocation List (CRL)
- Allows secure removal of suspect services

No keys under the doormat – meet your Key Manager



- You own your keys, not your infrastructure provider
- KMIP-compliant key manager
- Maintains key database
- Verifies node certificate using Certificate Authority
- Delivers volume keys
- External KMIP-compliant key managers are supported

Protect your master key - Security Module

- PKCS #11 compliant security module
- Stores master key used to encrypt the key database
- External PKCS#11-compliant Hardware Security Modules such as Thales and SafeNet, Utimaco supported

Data at rest protection in containerized environments

Secure Container Storage

Key Points

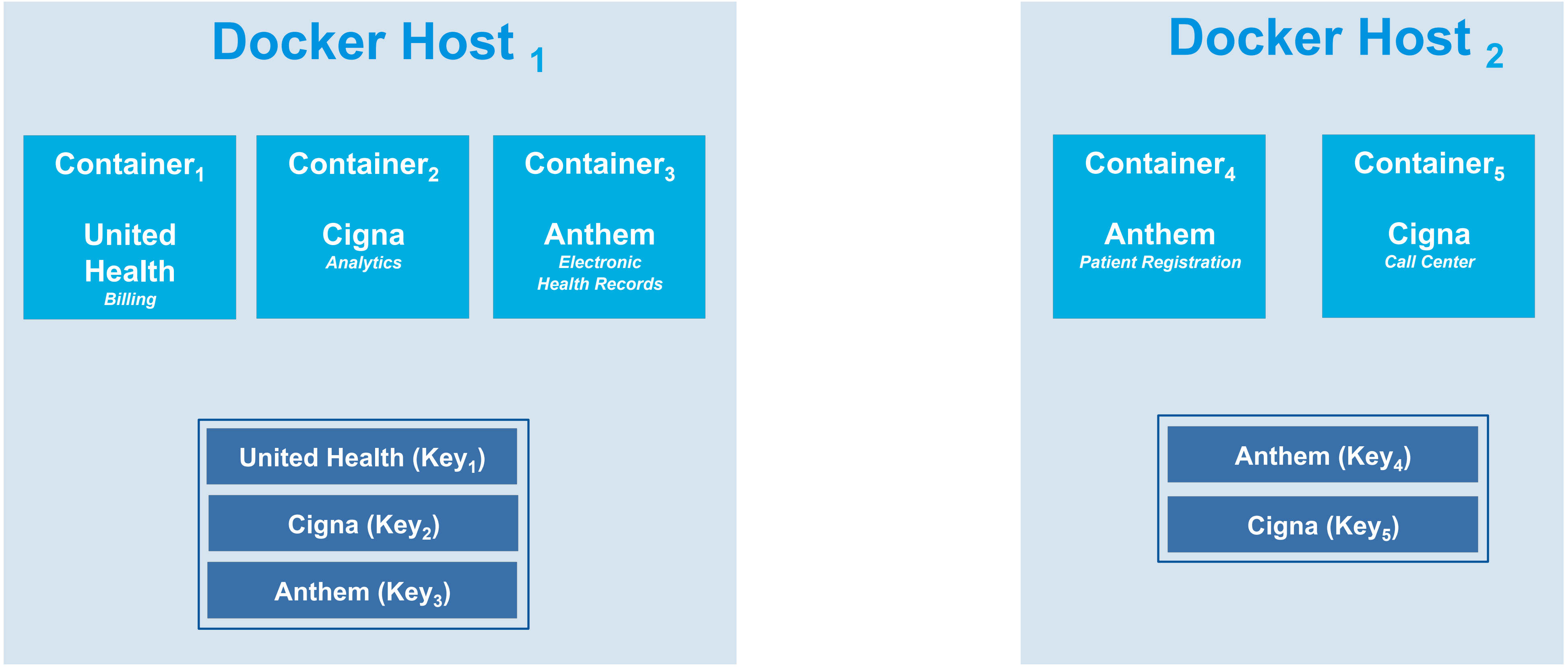
1. **Encryption must follow storage.** Containers will share storage in multitenant environment, but they must not share encryption keys. Otherwise, one compromised container compromises the entire environment.

2. **Storage must be independent of host and containers.** Using legacy approach of hardware-defined storage provisioning will lead to data loss if host reboots or dies.

3. **Separation of duties.** Developers and platform operators should not have visibility into or knowledge of encryption keys and processes. Encryption must be granular, yet transparent.

Zettaset

Container encryption for Docker - Fixed Topology



Docker Host $_1$

Container$_1$

United Health

Billing

Container$_2$

Cigna

Analytics

Container$_3$

Anthem

Electronic Health Records

United Health (Key$_1$)

Cigna (Key$_2$)

Anthem (Key$_3$)

Docker Host $_2$

Container$_4$

Anthem

Patient Registration

Container$_5$

Cigna

Call Center

Anthem (Key$_{4}$)

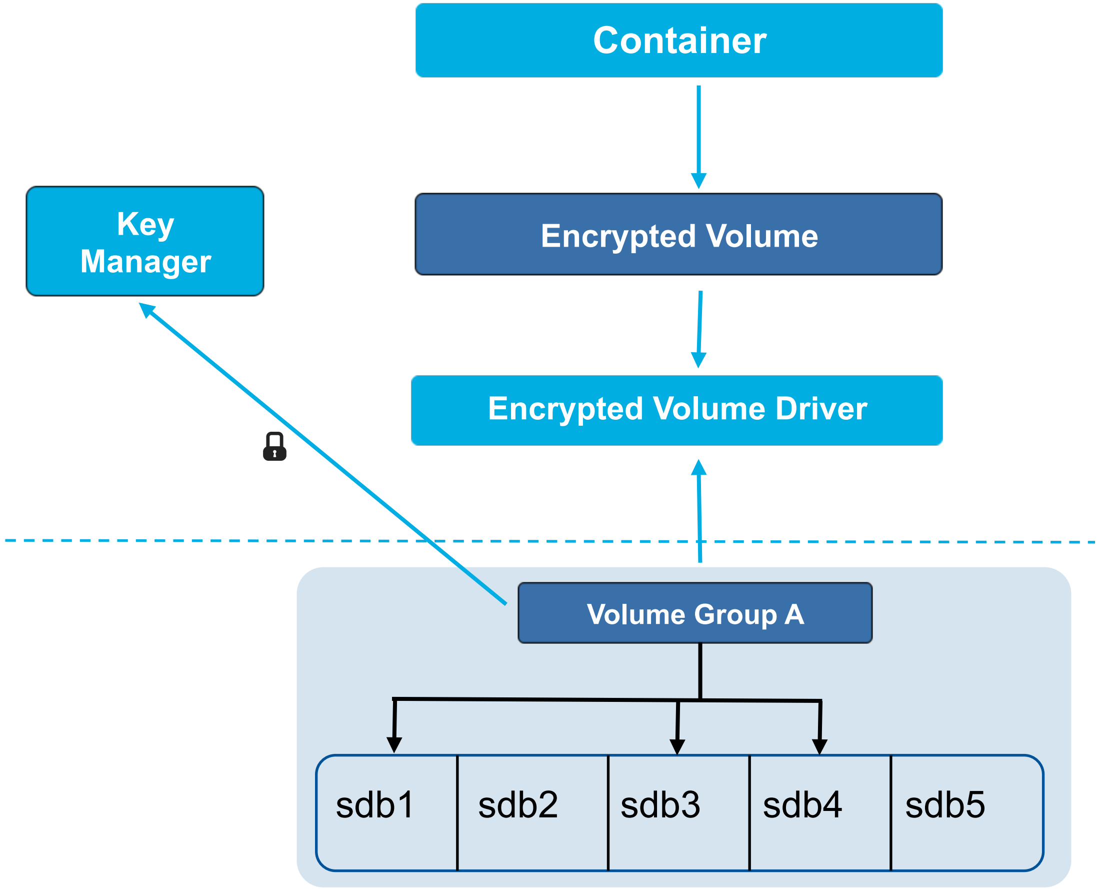
Cigna (Key$_5$)

Legend

Highly Available Storage Volume	Container	Host

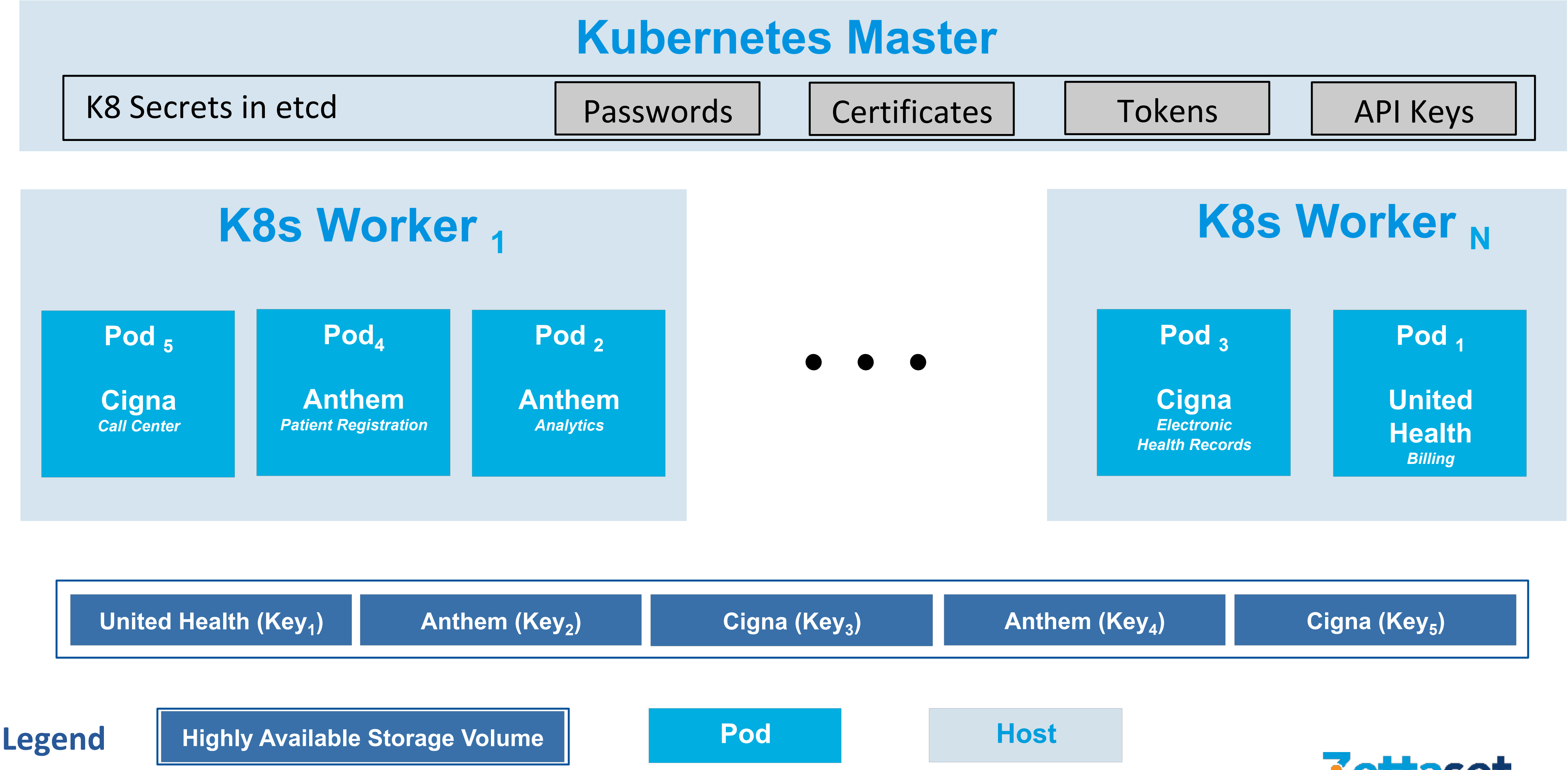
Container storage volume encryption

1. Container requests an encrypted storage volume
2. Volume driver requests a volume from the host
3. Volume manager constructs a volume from various partitions on the device and creates a volume group
4. Volume manager communicates with the key manager to create a key and encrypts the volume with this unique key
5. On container destruction, the encryption key is destroyed, and volumes are made available again



Zettaset

Container encryption for Kubernetes - Fluid Topology



Kubernetes Master

K8 Secrets in etcd

Passwords

Certificates

Tokens

API Keys

K8s Worker $_1$

Pod $_5$ Cigna *Call Center*

Pod$_4$ Anthem *Patient Registration*

Pod $_2$ Anthem *Analytics*

• • •

K8s Worker $_N$

Pod $_3$ Cigna *Electronic Health Records*

Pod $_1$ United Health *Billing*

United Health (Key$_1$)

Anthem (Key$_2$)

Cigna (Key$_3$)

Anthem (Key$_4$)

Cigna (Key$_5$)

Legend

Highly Available Storage Volume

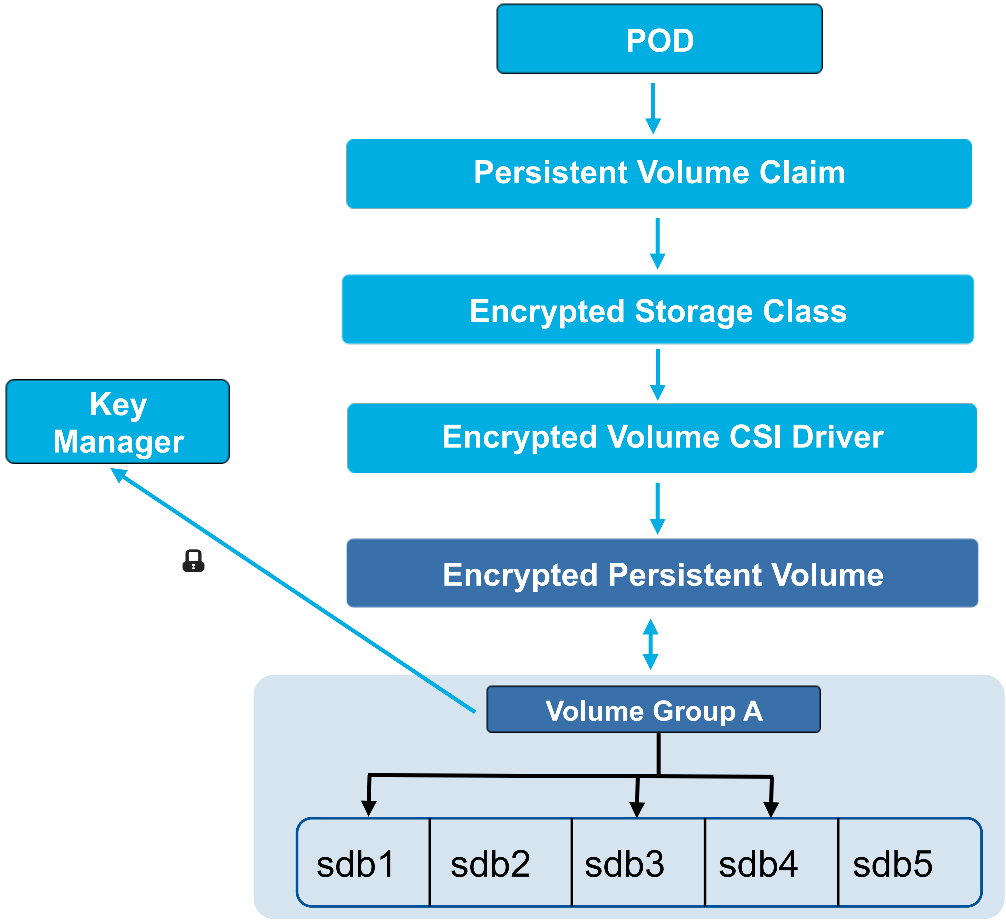
Pod

Host

Zettaset

Kubernetes persistent volume encryption

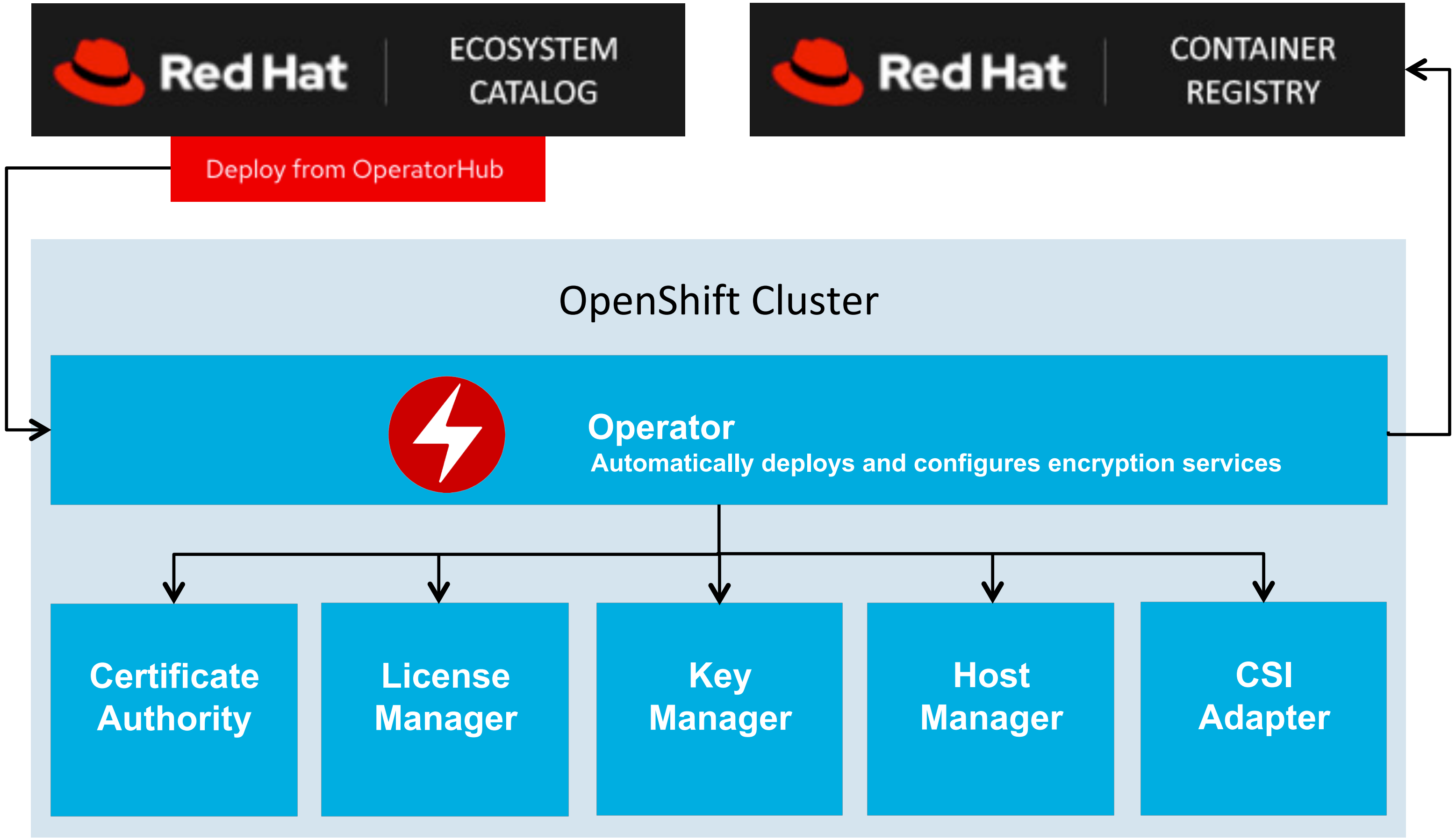
1. Admin configures a storage profile using encrypted volume storage class
2. Developer (POD) makes persistent volume claim (PVC) using encrypted volume storage profile
3. Volume driver requests a volume from the host
4. Volume manager constructs a volume from various partitions on the device and creates a volume group
5. Volume manager communicates with the key manager to create a key and encrypt the volume with this unique key
6. Using storage classes supports dynamic provisioning



Enterprise use case: Kubernetes encryption in Red Hat OpenShift

OPENSHIFT

1. Red Hat Certified Operator manages automatic deployment of all encryption services
2. All services are based on Red Hat Universal Base Image (UBI)
3. All required encryption services are automatically provisioned
   - Certificate Authority
   - License Manager
   - Key Manager
   - Host Manager
4. All container images are certified by Red Hat and come directly from Red Hat Container Registry
5. Operator available from Red Hat Ecosystem Catalog



Zettaset

Advantages of native container encryption

Unique Key Per Volume

Each persistent volume is encrypted with a unique encryption key. One compromised container does not compromise the entire environment.

Container Data Protection

Secrets are not protected by default and do not protect container data. Separate data protection solution required.

Secure Data Erase

Secure erase of individual storage volume: no need to physically erase volume data and no impact on other volumes.

Secure Node Removal

A compromised worker node can be removed from the cluster with administrative command that does not require access to the node.

Storage Separation

Granularity and OS level storage separation superior to using infrastructure encryption to encrypt entire volumes.

Thank you!

Zettaset