Zettaset

Protect data across your Kubernetes environment with XCrypt software-defined encryption

Although Kubernetes is a great platform for container orchestration and management, it doesn't address one of the most critical components of an overall security strategy – **data protection.** With Zettaset, you can transparently encrypt data-at-rest across your Kubernetes environment and further enable an efficient transition from DevOps to DevSecOps.

Kubernetes deployments are growing

With containers becoming so prevalent, it's easy to see why Kubernetes is said to be "taking over the world."

Usage is growing

A recent CNCF survey found that **78% of companies were using Kubernetes in production.**[1]

Market domination

The survey also found that of the 109+ tools to manage containers, **89% of respondents used Kubernetes.**

More cloud-native software

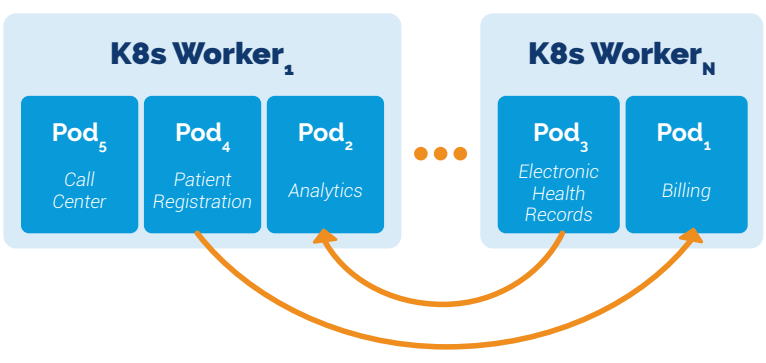
Kubernetes' growth has even spurred **the exponential growth of other cloud-native software and services.**

More sensitive data in production environments

69% of survey respondents **intend to store sensitive data in container environments.**[2]

But despite the growth, data protection remains a concern

As a platform, Kubernetes runs containers where it makes the most sense, so you may not always know where sensitive data is being used or if a given container has access to data that it shouldn't.



Kubernetes secrets aren't enough

They're great for securely storing passwords or tokens, but they don't protect your actual data.

Multi-tenant storage = new attack vectors

Kubernetes environments are often multi-tenant, which creates many new security vulnerabilities.

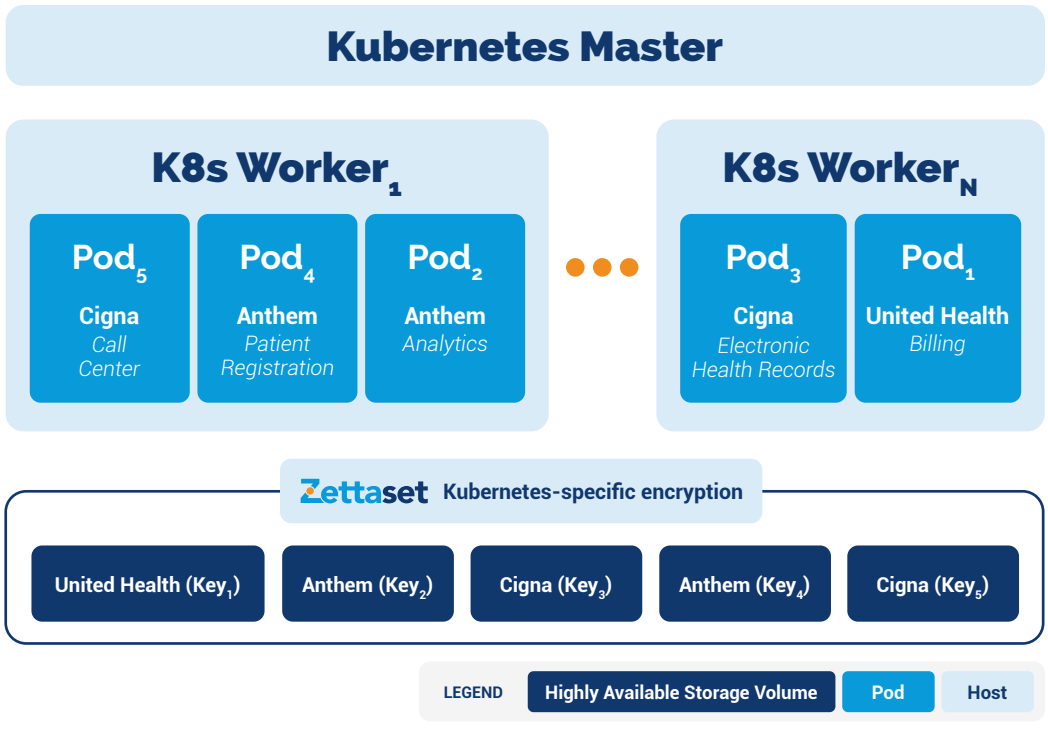
Usage of sensitive data

Because storage is shared, one compromised container may compromise sensitive data used by all containers.

Granular, data-at-rest encryption integrated into a Kubernetes storage layer is the only way to address the security vulnerabilities unique to Kubernetes deployments – **and that's why XCrypt Kubernetes Encryption was developed.**

Kubernetes protects your "secrets." XCrypt protects your data.

XCrypt Kubernetes Encryption is a software-only solution built specifically to protect data-at-rest in Kubernetes environments.



Provides a transparent, high performance layer of security for your entire DevOps pipeline.

Simplifies data protection while also acting as a 'last-line-of-defense' against new attack vectors in Kubernetes environments.

Integrates directly with Kubernetes storage layer and can be deployed without changes to existing processes.

Enables an efficient transformation to DevSecOps so developers can focus on building applications and driving innovation.

The value of XCrypt Kubernetes Encryption

Software-only for simple deployment

Negligible impact on performance

Container storage and data separation

Unique encryption key per each container volume

Automated encryption policy management

Secure erase of volumes rather than partitions

Learn more about XCrypt Kubernetes Encryption

Visit **zettaset.com/products/xcrypt-kubernetes-encryption/** to learn more and schedule a meeting to discuss how Zettaset can help you protect sensitive data across your Kubernetes environment.

SOURCE: [1]Cloud Native Computing Foundation Survey 2019 [2]State of Kubernetes and Container Security Survey, Stackrox Winter 2020

Zettaset