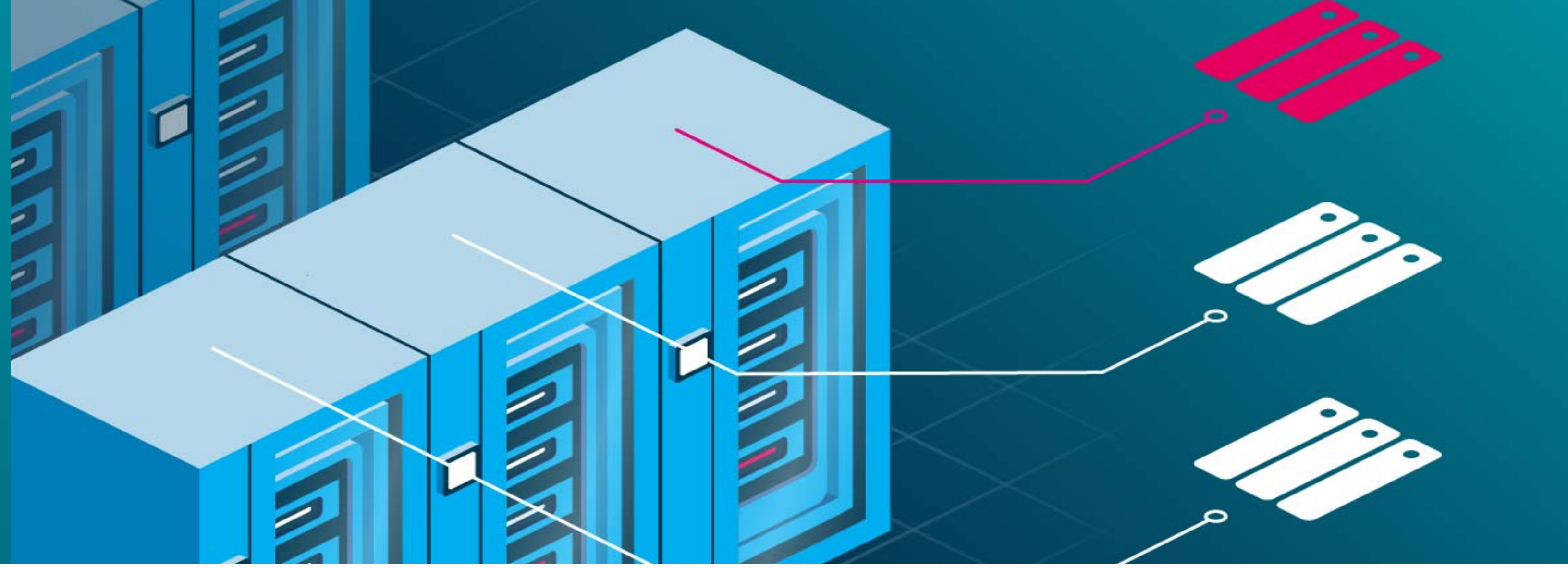
Cetas

# Securing Containerized Deployments

Application security through server-less cluster configuration monitoring and access management.

www.cetas.ai | info@cetas.ai | 586-789-9878



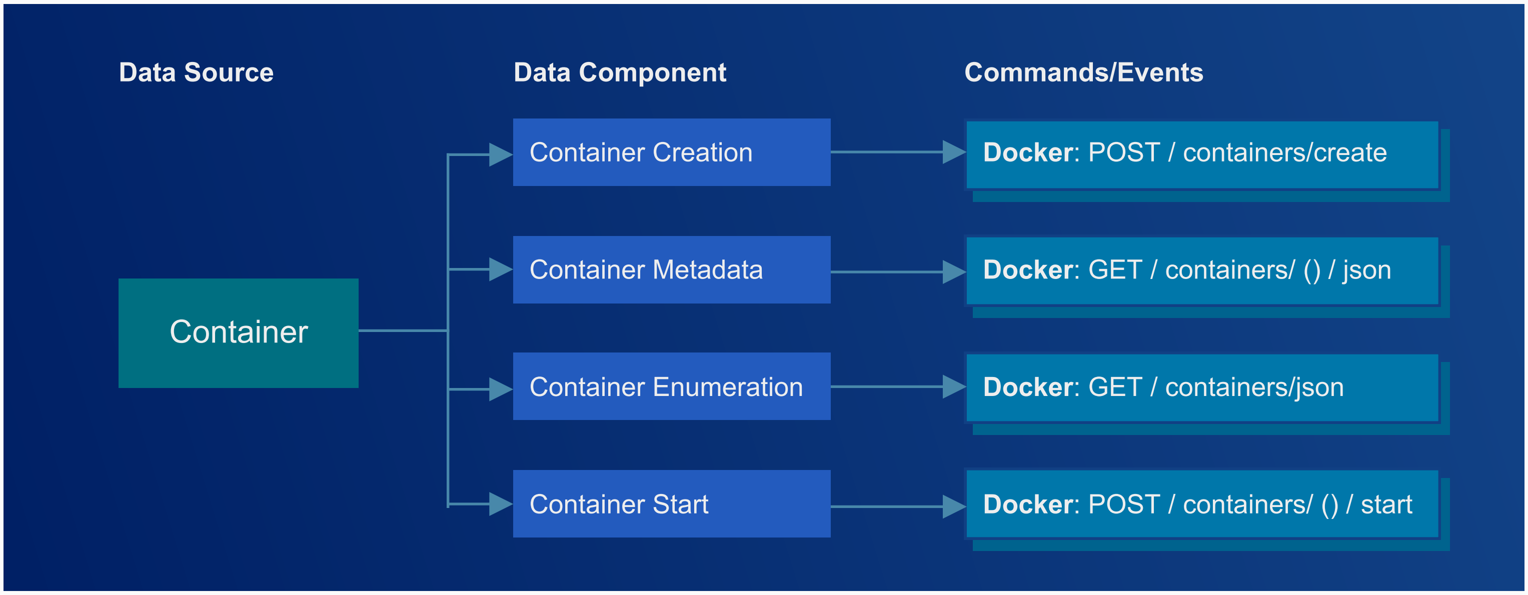
## Background

The jump from virtual machines (VMs) to Docker containers managed by Kubernetes was an inevitable leap. Organizations needed more efficient solutions for allocating resources and building/testing their products to continue growing. The result was containerization and this process has given developers the ease of simple container image creation and the ability to spool up processing power/capacity as needed to match demand.

The process of building an application became faster, cheaper, and overall more efficient. Unfortunately, just as full OS deployments on real hardware or VMs are vulnerable, so are containers. The orchestration between container and host cloud instance presents an array of challenges that require total visibility on relevant data sources that would give information on a configuration and event level.

Consider the CVE-2018-15664 vulnerability more famously known as the Docker vulnerability that led to cryptojacking attacks. Once a malicious image was downloaded on a privileged container, attackers were able to gain root access to the host machine to use its resources for crypto mining or other malicious activities like stealing sensitive data, phishing, or DOSing the organization. The best way to confront these vulnerabilities is through complete visibility on the configurations of all containers and clusters.

Cetas is cognizant of these overlooked vulnerabilities and developed a rich library of models to defend against serverless exploits on applications deployed through Kubernetes, AWS Lambda, and Azure Automation.



| Data Source | Data Component | Commands/Events |
|---|---|---|
| Container | Container Creation | **Docker**: POST / containers/create |
| | Container Metadata | **Docker**: GET / containers/ () / json |
| | Container Enumeration | **Docker**: GET / containers/json |
| | Container Start | **Docker**: POST / containers/ () / start |

[1] *Gartner Research. Mezzera, P. (2020). Managing Privileged Access in Cloud Infrastructure*

## Introducing Cetas

Cetas container-based models analyze events such as creation, deletion, and enumeration at the command level (POST, GET). It can capture these events in the cloud from AWS CloudTrail, Azure Event Monitoring, and GCP Stackdriver.

We are then able to take this event-level data and identify probabilistic patterns to determine what is normal behavior. These patterns are constantly evolving as we observe, for example, changes in access for a user and through the Cetas Brain Transferred Learning mechanism, we are able to create a highly accurate and holistic view on every user to ensure positive identification of identity and access misconfigurations. Here is a scenario to illustrate how this is accomplished:

**Scenario: Container Misconfiguration Detection**

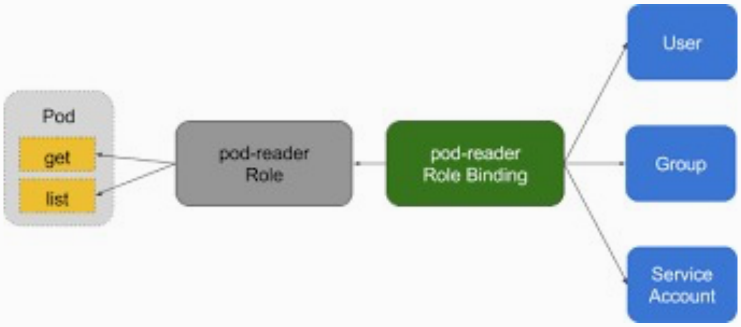
- A commonly seen vulnerability in Kubernetes is misconfiguration of both privileges for users as well as insecure port usage.
- Granting excessive privileges to allow read/write access on insecure ports for critical endpoints is typically a result of providing additional access to engineers for testing purposes.
- The risk comes into play when these changes are not reverted to a non-idempotent state. A misconfiguration can result in sensitive data exposure such as credentials of other users.

## The Catch

At a surface level, this challenge seems easy to fix. Why not just make sure that privileges get changed as needed for every container used? In theory, maintaining these security practices would be very beneficial and likely prevent breaches through immutable infrastructure. However, the scale of environments in companies today presents a unique threat that is difficult to attack with most tools.

Traditionally, VMs have been used to set up testing environments where an application can be built or tested. In many cases, the setup of this environment involved a security minded person or team to apply configuration settings and ensure a secure infrastructure. Today, with containers, security teams aren't always privy to when and how they are set up. The ownership of the containers is usually with someone in the application development team rather than a member of the security team which leads to a disconnect between the two organizations.

Since app development rarely employs a security-first mindset, there is a lack of understanding of configuration requirements and the importance of a secure workspace, which results in containers being far easier to breach. Many security tools were not built to handle the advances that frameworks like Kubernetes have introduced into the industry and, as a result, do not provide the visibility that security teams need to do their job.



## The Cetas Approach

Cetas can provide 360-degree coverage of user behavior on the most critical application infrastructure. The Cetas Brain is able to determine insecure port usage through rarity modeling. By using probabilistic comparison, Cetas is able to compare employee activity to port access over time and provide the analyst an understanding of the likelihood that an individual should be using a given port. If some uncommonly used port is employed, an alert would be in front of an analyst immediately. Through a combination of knowledge engineering, deep learning and evolutionary learning, the Cetas Brain would be able to detect any slight change in the users' privilege profile.

## Conclusion

This product was built as a result of first-hand experience by analysts expressing their challenges and frustrations regarding securing the modern stack. We believe that by building a product that resolves the problems we have seen across many Fortune 500 companies, we will hopefully resolve any similar challenges you may also be facing in your environment. Through our first-hand experience of working through the complexity of cloud configurations and access control, we have made complete visibility the top priority of this product. Our dedication to detection engineering gives analysts insight across computing workloads, data stores, containers, and more. We want to provide analysts not only the information they need to investigate, but also automated detection and response capabilities that further allow them to work smarter not harder and use their mind for more strategic analysis.

## Schedule a Demo Today!

https://www.cetas.ai/request-demo/

Cetas

www.cetas.ai | info@cetas.ai | 586-789-9878