Container Platform Compliance

Wanclouds Inc.

http://wanclouds.net/Shepherd.html

Table of Contents

Introduction:

The General Data Protection Regulation, or GDPR, will set a new bar globally for privacy rights, security, and compliance. We believe privacy is a fundamental right and that the GDPR is an important step forward in protecting and enabling the privacy rights of individuals. This white paper serves as an introduction to Container Platform Compliance (CPC). For more details please visit **https://www.wanclouds.net/Shepherd.html** .

What is CPC?

Security has been gaining steam over the last few years. A great number of organizations are using container technology however before running their container, they need to consider security for the platform where these containers are deployed, or else there is a greater probability the platform could experience attack where the data could be compromised. We believe *Container Platform Compliance* (CPC) has to be considered as one of the fundamental requirements for cloud computing that allows users to focus on platform compliance to strengthen their security and enhance their regulatory compliance while running cloud native applications.

CPC needs to be considered in order to prevent container breaches from affecting the host. For this, Linux provides several out-of-the-box security modules. Some of the popular ones are **SELinux**, **AppArmor** and **Seccomp**.

Ignorance of CPC is not an excuse, why?

While running containerized apps, it is not uncommon to see processes such as containers running with root capabilities or any other unconfined processes active in the hosts which are considered to be a security threat. An unconfined process can access any container or its mounted data folder. As unconfined process can transition to almost any domain, so we make sure to transfer any unconfined label to confined domain. If a host is compromised, can a hacker perform read/write/copy on the database? Are changes to the attack surface (Integrity) being tracked such as a new kernel module being loaded, a new port being opened? How CPC is key requirement for GDPR? Shepherd provides answers to such questions by leveraging SElinux and host integrity tracking.

How SELinux best suits CPC

Security Enhanced Linux or SELinux is an advanced access control mechanism built into most modern Linux distributions. SELinux is a way to fine-tune such access control requirements. With SELinux, you can define what a user or process can do. It confines every process to its own domain, so the process can interact with only certain types of files and other processes from allowed domains. This prevents a hacker from hijacking any process to gain system-wide access.

Only privileged users can access and update the data where needed.

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

SELinux is the best suit for integrity and confidentiality, through its labeling system, unique groups with associated permissions, security level for container environment and categories in labels for containers isolation.

Wanclouds Can Help

Wanclouds is focusing on solutions and services related to Container platform Compliance. It has team members based in Santa Clara, CA as well as offshore. Wanclouds has technology and services partnerships with IBM, Red Hat,

Cisco, Intel, HP and others.

Introduction to Shepherd

To help enhance the Container Infra Compliance, we just released our Kubernetes security platform called **Shepherd by Wanclouds**. It helps restrict access to database volumes and containers and the ability to create custom compliance checks and alerts. As containers are built and deployed at increasing speeds, security professionals need solutions that leverages a more simplified approach and management. Shepherd is able to tracks all the users on your Kubernetes platform/linux level who have access to a particular volume. Records the historical information about the privileged users. Manages root level access to the corresponding VM

At the OS level, Shepherd monitors all activities such as users additions/deletion, unconfined processes, kernel modules, firewall rules changes on an ongoing basis

Tracks the integrity of the platform that hosts your Kubernetes cluster round the clock Generates alerts for integrity violations

Manages access control at the Linux OS level

How does Shepherd addresses key GDPR requirements and CPC

Cloud platform Compliance revolves around three main principles:

Assessment

It is specified in article 32 that the Data Controller or Data Processor must take steps to ensure that any natural person with access to personal data does not process the data except on instruction of the controller, processor, European Union law, or member state law, So Shepherd performs an initial assessment of all the VMs being registered to assess an attack surface of the whole cluster. These assessments are stored and can then be compared with the attack surface after Shepherd takes control of the Data center security.

Prevention

According to article 32, the controller and the processor shall implement appropriate technical and organizational measures, to ensure a level of security appropriate to the risk, including inter alia, as appropriate: kernel level security policies."

Shepherd's SELinux Policies for containers data protection are:

Shepherd's Guarded Mode which disables all root access to a VM, Shephed enforces kernel level Selinux policies to ensure that db volumes used by containers are isolated from other host/VM processes.

Shepherd provides Containers grouping through which policies can be applied across the clusters uniformly. For scenario where containers are deployed on bare metal servers, Shepherd leverages Intel CIT for measuring boot time integrity.

Detection

Each Member State shall provide for one or more independent public authorities to be responsible for monitoring the application of this Regulation, in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union (article 51) and Shepherd introduces **run time integrity measurement & Verification** for virtual machines (VMs) across private and public clouds. It monitors the platform's integrity status (VMs/hosts across the cluster) and builds history. The valuable data can then be used for **forensics** purposes as well. Shepherds **Rule Engine** further strengthens **detection**

Shepherd helps organizations globally address the challenges Container platform compliance, GDPR compliance and to meet your GDPR compliance objectives.

For More Information

You can checkout Shepherd and use its free online instance at https://www.shepherd.one