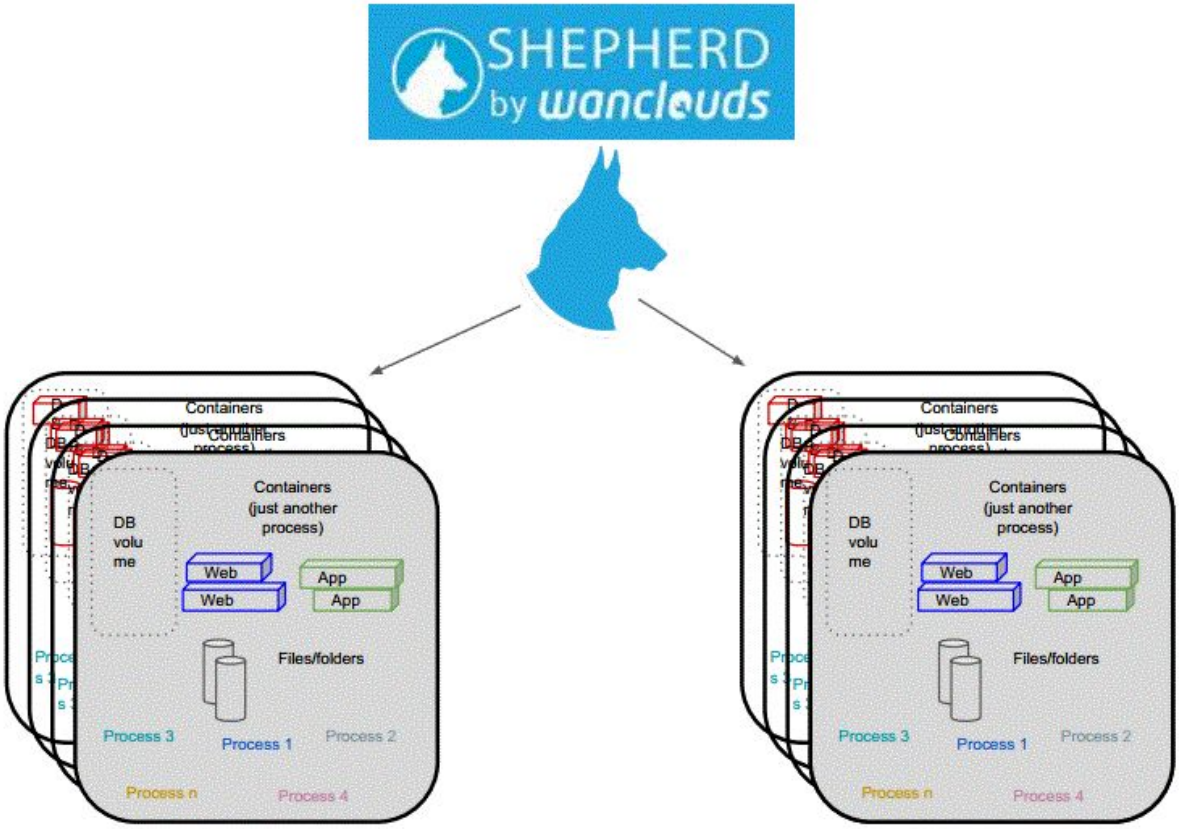
Shepherd by Wanclouds:

Free Trial Instance and Sandbox: https://trial.shepherd.one

Solution Webpage: https://www.shepherd.one

Solution Overview:

Shepherd is a mandatory access & integrity controller designed for linux virtual machines and containers (mainly Kubernetes). Shepherd leverages SElinux and other integrity controls to ensure the infrastructure (linux hosts) hosting Kubernetes cluster remains in a trusted state. 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. To ensure such processes are kept in check, Shepherd leverages SElinux as well as other integrity monitoring techniques to make sure that even if a host is compromised, no harm is done to the containers and important files/DB volumes. In general, deploying and managing SElinux policies are very cumbersome, time-consuming to deploy, and hard to manage. There is no centralized utility today where you can build, deploy, and manage these MAC policies for your container and VM environments. Shepherd helps address these concerns. It also offer FW rules implementation Kubernetes cluster level as well as performing run-time integrity monitoring. In case a Kubernetes cluster is deployed on bare metal servers, Shepherd has built-in integration with Intel's Cloud Integrity Technology (CIT) solution which measures "integrity at rest" such as OS, boot process. You can run your clusters in a private in-house cloud, or public cloud and deploy/manage security, integrity and compliance from a single control point. Below diagram shows how Shepherd monitors different containerized clusters for security and integrity.



Key Features:

Containers Isolation

Enables kernel level isolation using SELinux policies along with monitoring the integrity of the security policies applied to containers.

Restricting access to DB Volumes

Policies can be created to restrict Read/Write access to mounted volumes while creating containers and applying customized policies on it. These policy modules have different access permissions associated with the mounted volumes. Any tampering with the DB containers or the hosts are being monitored.

Integrity Checks

Shepherd tracks the ongoing integrity of the cluster. It has pre-integration with Intel's CIT for boot time integrity for clusters deployed on bare metal nodes. Shepherd creates visibility of the attack surface and issues alerts for changes into container policies and host.

Compliance

Uniform policies and active monitoring of the attack surface across different clouds and customer's own Data Centers. It strengthens compliance for regulations such as GDPR to ensure access to user data is restricted.

Firewall Rules for containers/VMs

IP table rules can be applied at the host level as well Kubernetes cluster level inter-pod or inter-deployments policies.

Health Monitoring

It allows you to monitor your hosts and containers for general health (CPU, memory utilization, Storage, and more)

Multi-Cloud Support

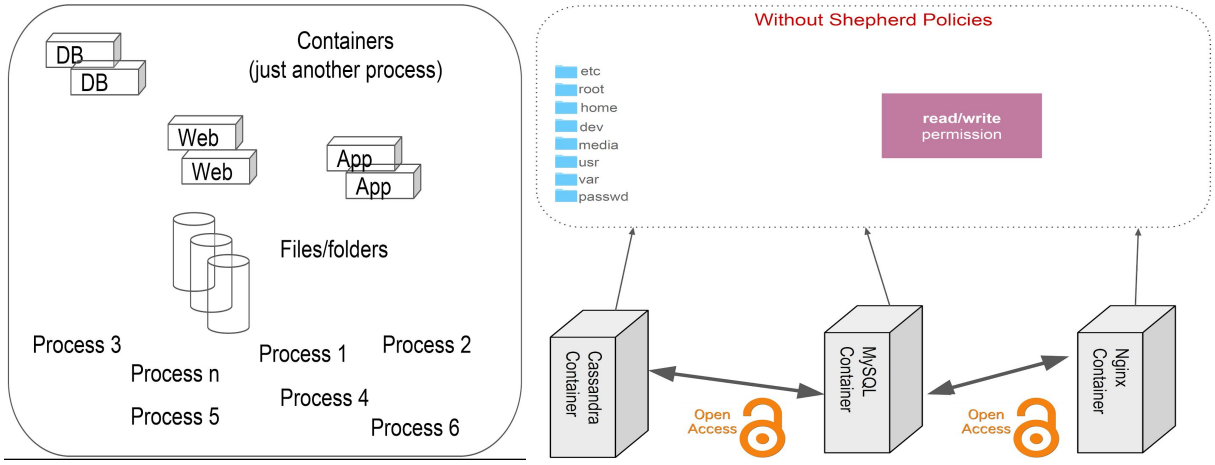
Shepherd can be deployed in a private or public cloud and it supports multiple clusters deployed

Ops Rules and Alerts

Integration with ServiceNow, Slack, and email alerts for any operational rules that gets violated. A user can set his/her own operational rules.

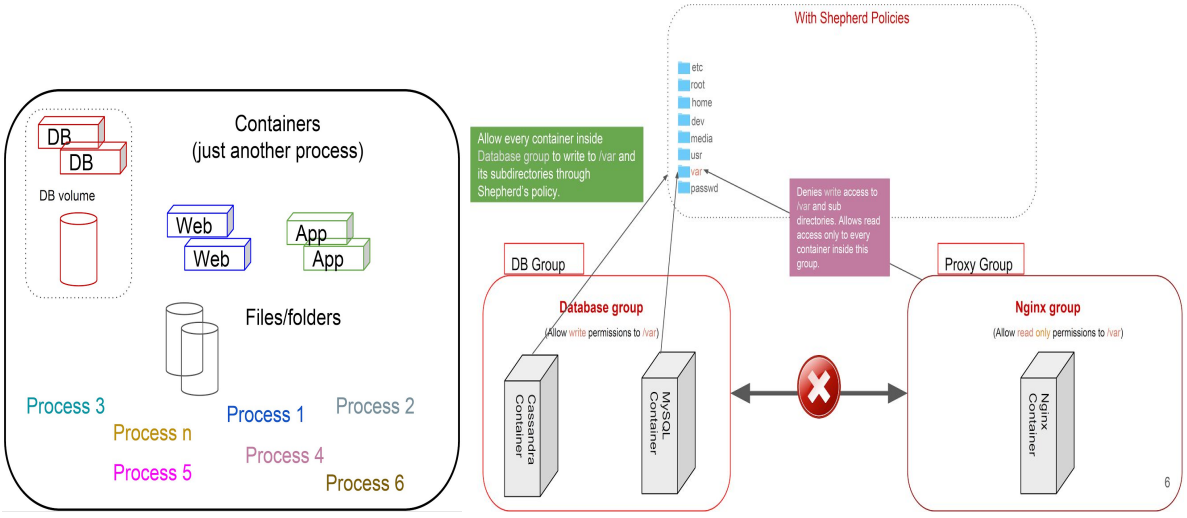
A use-case scenario

Unconfined processes and no host integrity tracking

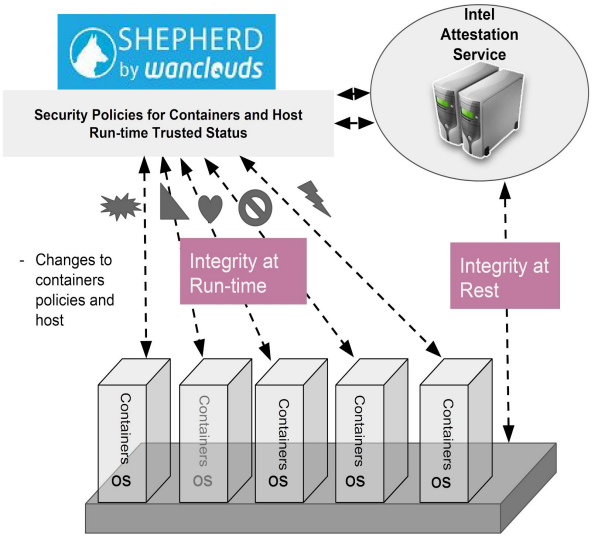


The above diagram shows processes running in an unconfined state where any process can potentially access other processes such as an Ngnix container can get to a cassandra container and perform read, write operations. Processes such as containers running with root capabilities or any process running in unconfined state presents a security threat. As unconfined label 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 etc? Shepherd provides answers to such questions by leveraging SElinux and host integrity tracking. At a higher level, It also allows the operator to implement perimeter security at the host level using IPTables rules. Finally, “integrity at rest” for OS, Boot process, and geo tagging can be applied to Kubernetes cluster deployed on bare metal (Intel servers) since Shepherd has pre-built integration with Intel’s CIT solution.

The diagram below shows how container/process level isolation is achieved with Shepherd by applying SElinux and enabling ongoing monitoring of the cluster integrity. Following the same example from above, an Ngnix container cannot perform read/write operation on a cassandra container when proper policies are deployed and tracked.



This diagram shows how Shepherd is integrated with Intel's CIT to ensure integrity at rest and run-time.



About Wanclouds Inc: Wanclouds is a Silicon Valley based startup focusing on solutions and services related to cloud automation, DevOps, and Security. 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. Please contact us for any demo or review of the solution at services@wanclouds.net or check out the solution walkthrough and sandbox at https://trial.shepherd.one