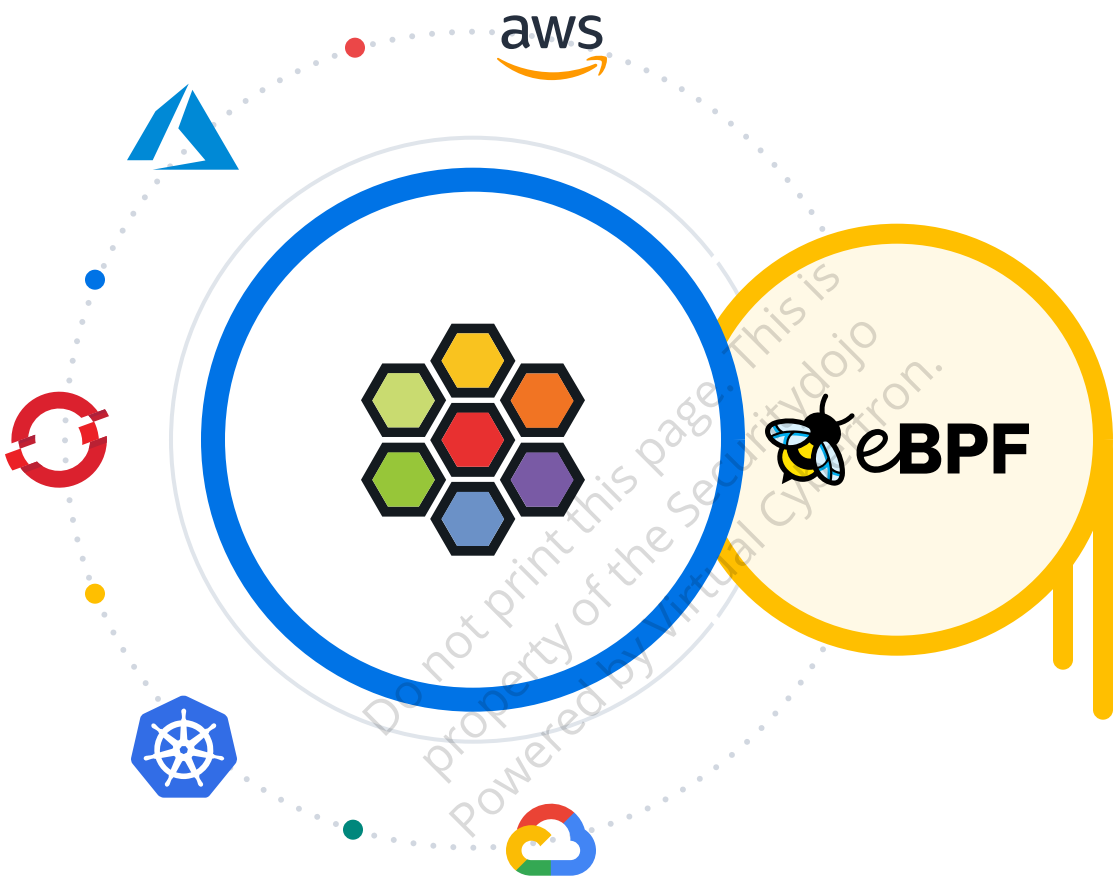
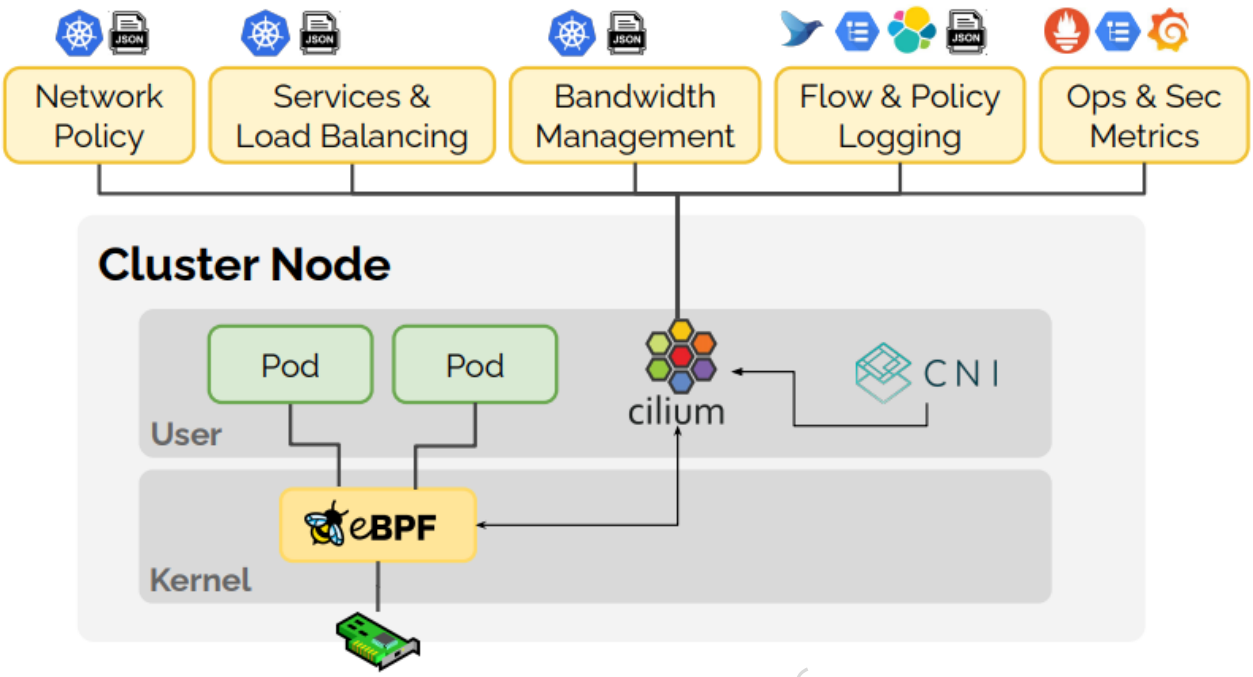
Network Fabric: Cilium

Introduction



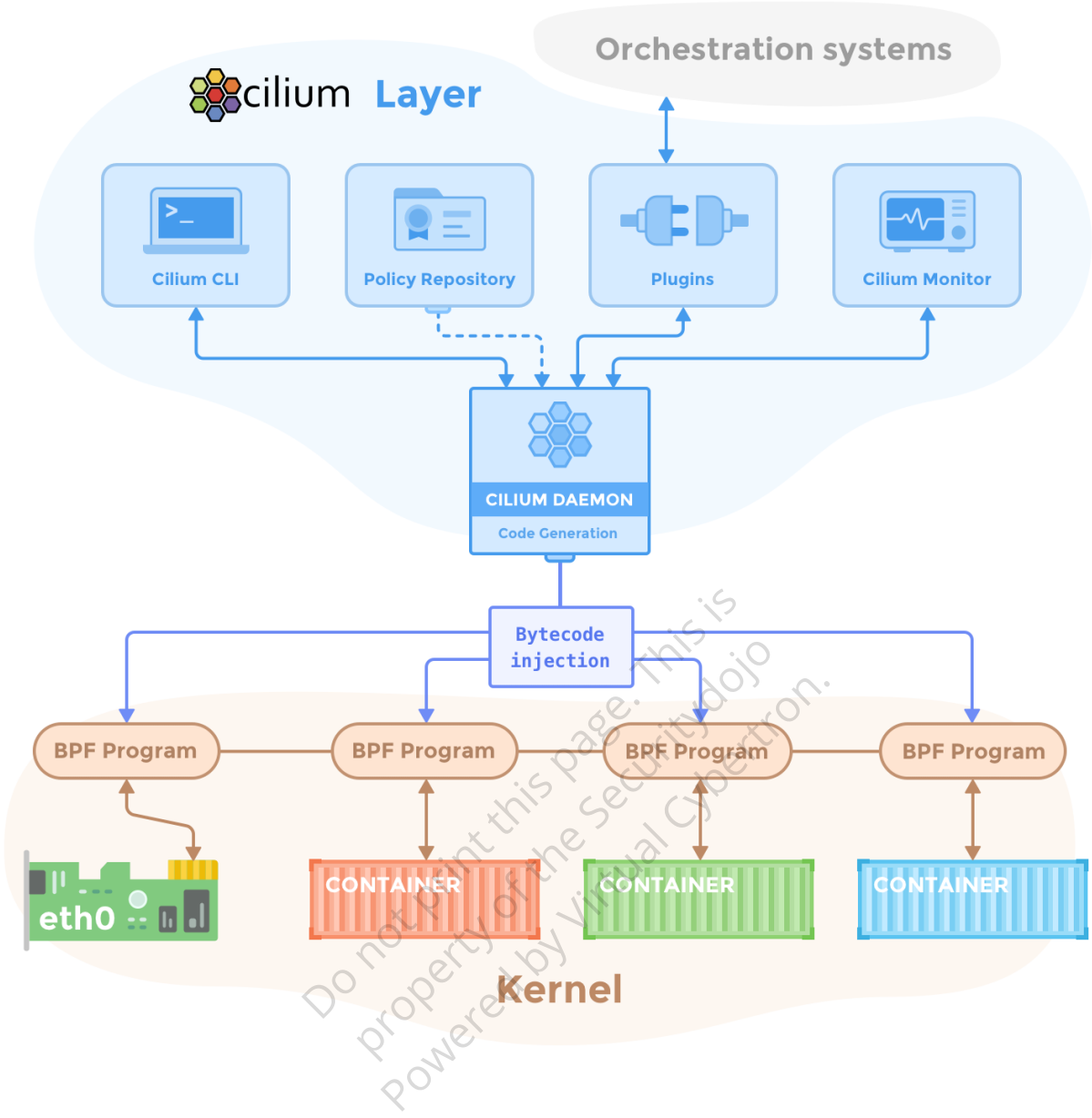
- Cilium is an open-source tool that manages and secures network communication between containerized applications.
- It leverages a powerful Linux technology called eBPF, enabling fine-grained, efficient networking and security policies.

EBPF



- eBPF, short for Extended Berkeley Packet Filter, is a technology built into the Linux operating system.
    - It's like a mini-programming language that allows developers to create tiny programs that get executed directly within different parts of the OS, often for monitoring or modifying network behavior. e
    - They are written in a C-like language and compiled into eBPF bytecode, which is then loaded into the kernel. eBPF programs are executed in response to specific events, such as a network packet arriving at a network interface or a system call being made.
    - eBPF programs can be used to monitor and modify the behavior of the Linux kernel, as well as to implement new features. eBPF programs are used by Cilium to implement network and security policies.

Cilium Architecture



The architecture of Cilium consists of a few primary components:

- Agent
  - Agent runs on each node, is in charge of maintaining network and security rules and creating connections with the Kubernetes API server. The Linux kernel is modified to include security and networking controls using eBPF.
- Operator
  - Cilium Operator manages cluster tasks for the entire cluster; it is not necessary for making decisions about network policy. The Operator is responsible for installing and upgrading Cilium on each node, as well as for configuring the Cilium API server.

- Cilium CLI
    - The command-line interface (CLI) is used to interact with the Cilium API server and manage Cilium's policies as well as configuration.
- CNI Plugin
    - CNI(Container Networking Interface) plugin is used to configure the network interfaces of containers. Cilium can be used as a CNI plugin to configure the network interfaces of containers.

Cilium's architecture is highly scalable and can handle complex network topologies. It can be used to manage the network and security policies of thousands of nodes and millions of containers.

Hubble

- Hubble is a fully distributed networking and security observability platform for Cloud Native workloads.
- It is built on top of Cilium and eBPF to enable deep visibility into the communication and behavior of services as well as the networking infrastructure in a completely transparent manner.