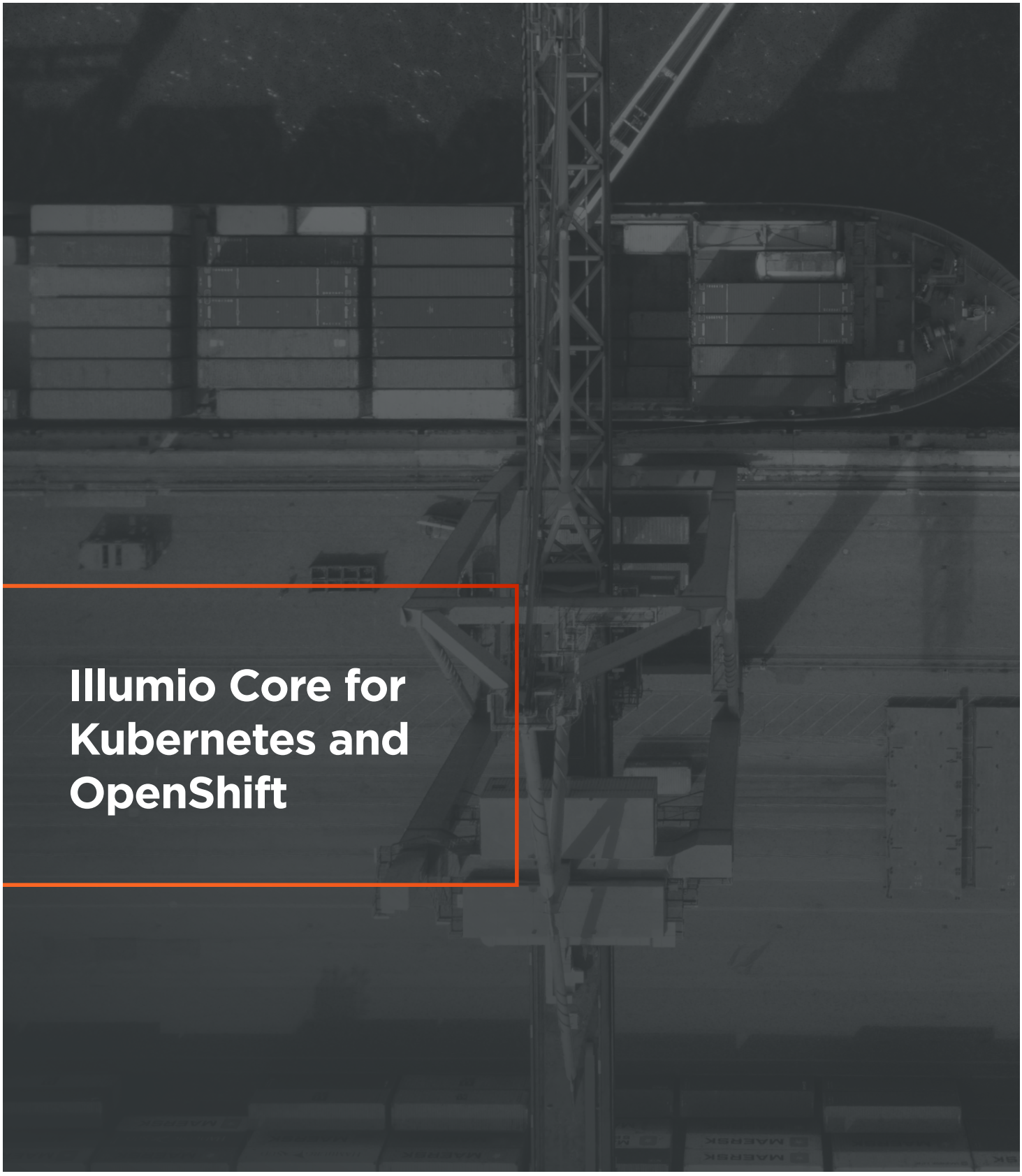
illumio

DATASHEET



# Illumio Core for Kubernetes and OpenShift

## Stop the Spread of Breaches – in Kubernetes, OpenShift, and the Rest of your Infrastructure

While containers offer speed and agility never before available in the data center, microservices are also exposed to many threats over the Internet – creating a new vector for attackers to exploit.

The Illumio Core™ prevents the spread of breaches through segmentation that gives you uniform security policy across environments, including Kubernetes and OpenShift platforms. It helps organizations limit lateral movement between applications and meet regulatory compliance standards such as SWIFT, PCI, and GDPR.

## Why Segment Containerized Applications

A pod running a vulnerable piece of code at runtime or an unprotected key can be compromised, either through the pod itself or by taking control of the host running tens or hundreds of pods for different applications.

This pod or host can then be used to move laterally from one containerized workload to another, potentially causing cascading attacks across the entire infrastructure.

With a proven architecture that can scale to hundreds of thousands of workloads within a data center, cloud, or hybrid deployment, Illumio Core visibility and segmentation capabilities extend to container clusters orchestrated with Kubernetes and OpenShift.

## Benefits of Illumio Core for Containers

**Full visibility:** Inventory container clusters and visualize real-time traffic between pods, their hosts, and the rest of your infrastructure.

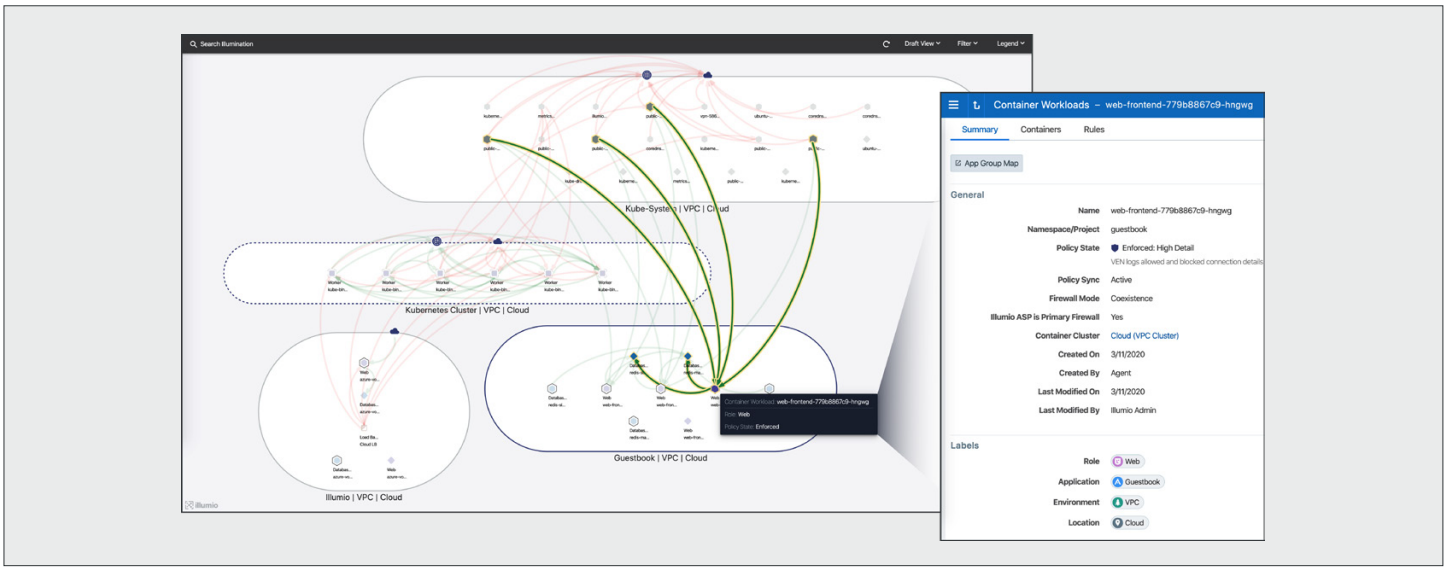
**Uniform policy across environments:** Prevent the spread of breaches between brownfield and greenfield IT with a single policy – and without hardware.

**Secure Kubernetes control plane:** Protect your Kubernetes hosts from unwanted communications, and ensure the control plane is isolated.

**Simplified security policy:** Create natural-language policies to prevent unauthorized east-west traffic, using labels and metadata.

**Baked-in security to expedite DevOps:** Use profiles to automatically assign labels to your containerized assets and define security policies for your applications at creation.

**Seamless integrations:** Confidently simplify container security by instrumenting existing reliable tools in the Linux kernel of your Kubernetes hosts (iptables).




Illumio Core segments hosts running containers alongside other forms of compute across data centers and clouds – providing centralized visibility of traffic communicating across your environments and deep insights into your container clusters.

## Key Features

### Kubernetes clusters insights

**Discover namespaces, pods, and services dynamically**

Inventory all clusters reported to Illumio's Policy Compute Engine (PCE), which centralizes all information related to Kubernetes clusters and other workloads. Pods and services are described with Kubernetes metadata to offer more context about the different microservices deployed in your containerized applications. This multi-cluster capability helps security teams understand each element without specializing in Kubernetes or OpenShift.

Customize columns | 50 per page | 1 – 23 of 23 Matched

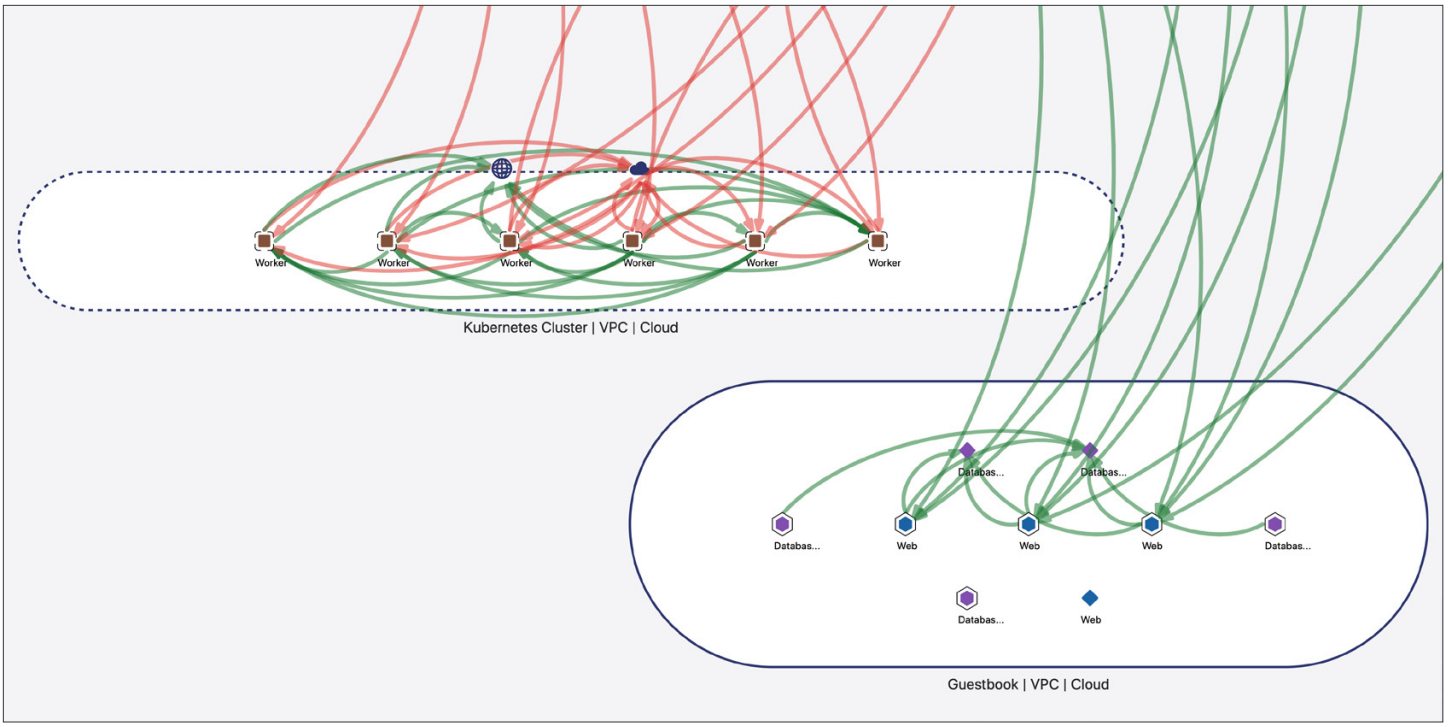
| Policy State | Policy Sync | Namespace/Project | Name | Role | Application | Environment | Location |
|---|---|---|---|---|---|---|---|
| Enforced: + High Detail | Active | guestbook | redis-slave-64f9bbb8ff-d7zxf | Database | Guestbook | VPC | Cloud |
| Enforced: + High Detail | Active | ns00ei900035 | azure-vote-back-76cfd78d55-7mknj | Database | Illumio | VPC | Cloud |
| Enforced: + High Detail | Active | guestbook | redis-master-7598d9cb9c-8tr6m | Database | Guestbook | VPC | Cloud |
| Enforced: + High Detail | Active | guestbook | redis-slave-64f9bbb8ff-rbsrt | Database | Guestbook | VPC | Cloud |
| Enforced: + High Detail | Active | guestbook | web-frontend-779b8867c9-hngwg | Web | Guestbook | VPC | Cloud |
| Enforced: + High Detail | Active | ns00ei900035 | azure-vote-front-755f8ff6-mhmfl | Web | Illumio | VPC | Cloud |
| Enforced: + High Detail | Active | guestbook | web-frontend-779b8867c9-22jr7 | Web | Guestbook | VPC | Cloud |
| Enforced: + High Detail | Active | guestbook | web-frontend-779b8867c9-lpk46 | Web | Guestbook | VPC | Cloud |
| Build | Active | kube-system | public-crbln8bomd05142elk0gd0-alb2-7696f85b78-g9ch6 | | Kube-System | VPC | Cloud |
| Build | Active | kube-system | public-crbln8bomd05142elk0gd0-alb2-7696f85b78-h5ptv | | Kube-System | VPC | Cloud |
| Build | Active | kube-system | coredns-7789d4b879-ccw97 | | Kube-System | VPC | Cloud |
| Build | Active | kube-system | kubernetes-dashboard-7756dcb98b-9lqd5 | | Kube-System | VPC | Cloud |

## Full visibility

**Real-time application dependency map (Illumination)**
Display pods as first-class citizens alongside all other workloads, whether VM or bare-metal, on a full visual map (called “Illumination”) of your data estate.

**Traffic visibility**
Visualize real-time IP-based or DNS-based traffic between pods, services, and hosts – and the rest of your infrastructure.

**Lateral movement detection**
Easily view, detect, and investigate any potential undesired connections between pods, services, and hosts or namespaces.



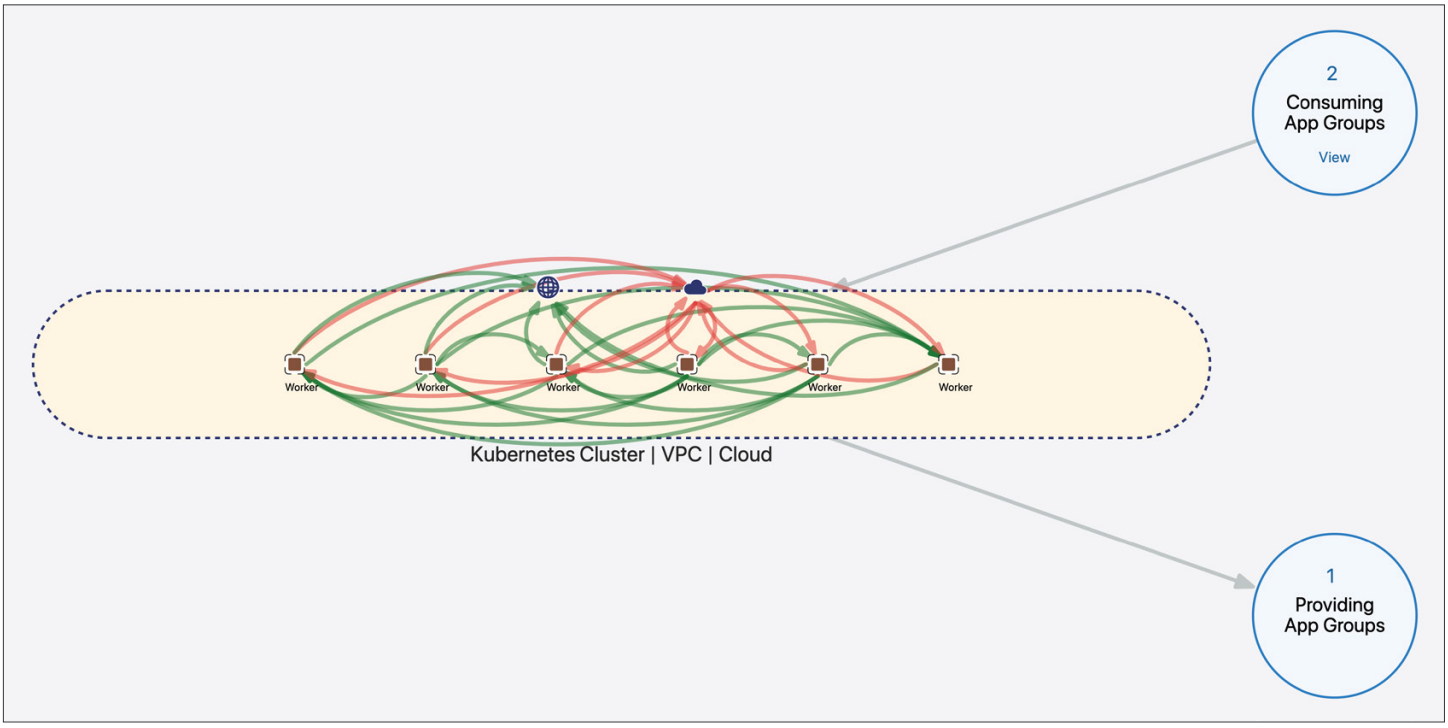



illumio

## Container cluster segmentation

**Secure Kubernetes control plane for highly-available platforms**
Allowlist communications between nodes in a Kubernetes cluster and increase the uptime of the clusters running critical business applications.

**Granular policy models**
Choose between a simple ringfence around the cluster or a more granular role-based policy model to protect specific services from unwanted connections, for example, an etcd database cluster should be properly segmented to secure confidential information.



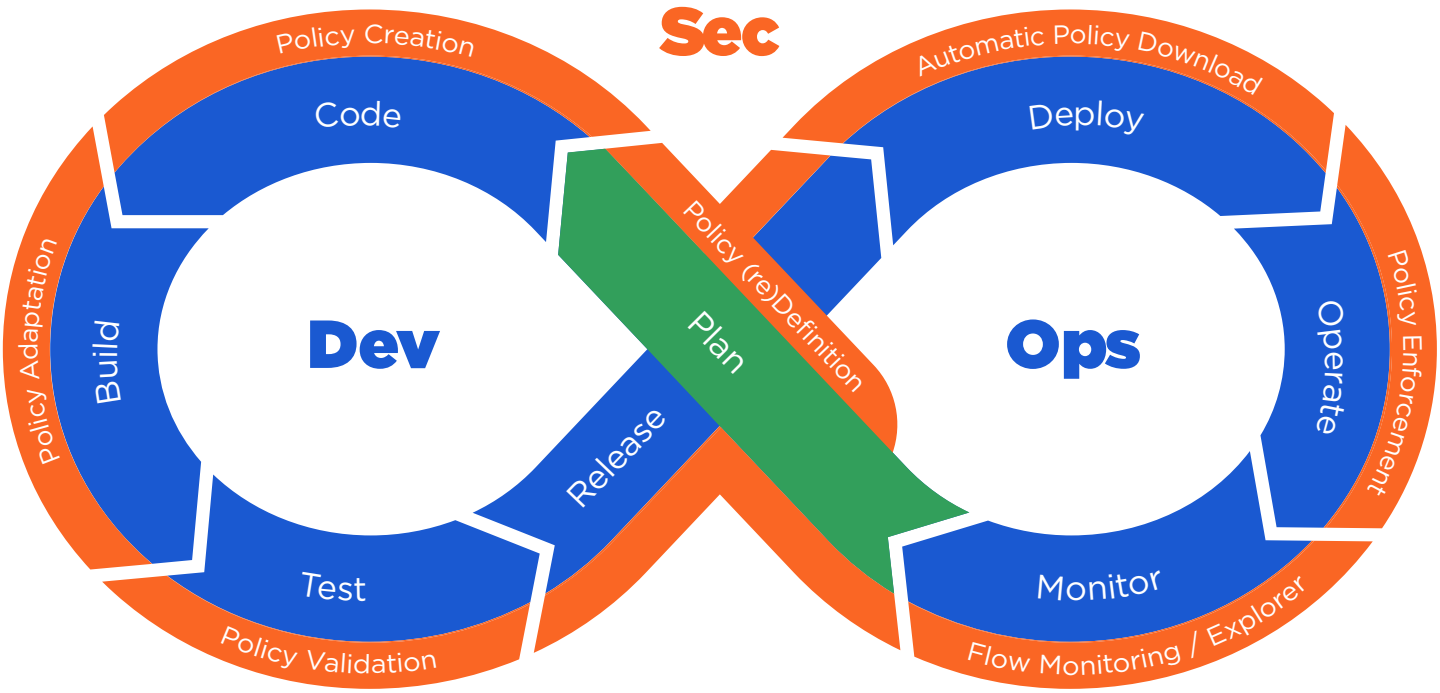

## Simple and flexible segmentation policies

**Intuitive policy creation**
Illumio Core enables your security team to easily program security rules for your nodes and your pods and services to prevent namespace-to-namespace communications in shared clusters. With a simple ringfence of your applications or a service-based policy, you can prevent lateral movement between pods or undesired communications between different environments running on the same cluster.

**Ingress and egress control**
In addition, you can gain better control over ingress flows by securing applications exposed via ingress controllers and/or load balancers. Analyzing egress IP-based or DNS-based flows to and from your pods becomes easily achievable and helps define security policies for them.

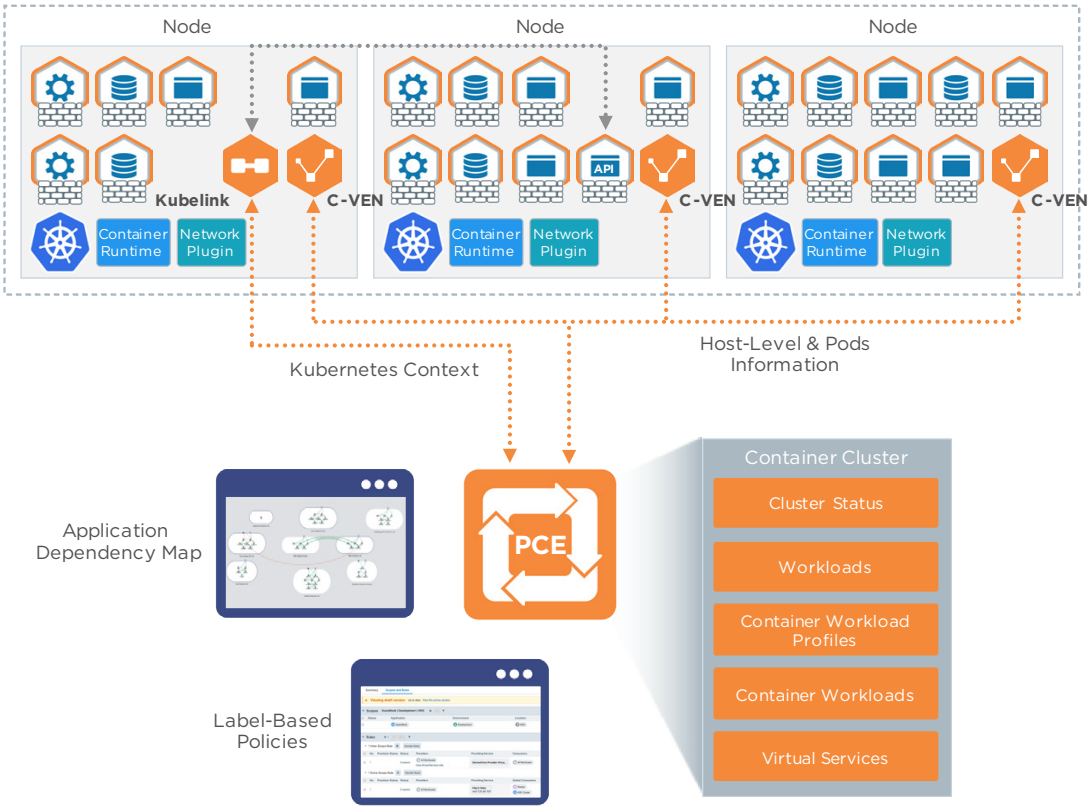
## Dynamic security policy assignment at inception for streamlined CI/CD

**Automated container workload profiles**
Dramatically reduce the time required to get security policies downloaded and converged on pods and services within Kubernetes clusters. Use profiles to assign labels to your containerized assets and define namespace security policy. Pods and services inherit associated security policies dynamically and come online fully secure. DevSecOps teams can confidently deploy applications with pre-defined policies based on the labels assigned to namespaces in the PCE or derived from the annotations used in the manifest files.



## Seamless integration

**Adaptive to your existing environment**
Kubernetes and OpenShift clusters come with a list of components already built-in for different functions. Illumio does not require you to replace any component within the cluster (container runtime, network plugin, etc.) and is transparent to your application infrastructure.




# Minimum Software Requirements

Illumio Core includes three software components:

**C-VEN:** Lightweight Illumio agent, running as a pod on each node in the cluster, that protects the node and all the pods running on it. The C-VEN is delivered as a DaemonSet to scale up and down as the cluster evolves.

**PCE:** Central component that aggregates all information from agents and container clusters to provide central visibility with the application dependency map and flexible control with label-based policy creation.

**Kubelink:** Illumio service that monitors the Kubernetes API server to learn about resources within the cluster and provide Kubernetes context to the PCE. It is delivered as a Deployment and requires only one replica per cluster.

## Supported Platforms and Components

| Orchestration Platforms | Version | Nodes Operating Systems | Container Runtime | Networking | Kube-proxy mode | Ingress Load Balancer |
|---|---|---|---|---|---|---|
| Kubernetes | 1.17 (Qualified)<br>1.16 (Qualified)<br>1.15 (Qualified)<br>1.14 (Qualified) | RHEL 7.7<br>CentOS 7.7<br>Ubuntu 16.04 | Docker<br>Containerd<br>Cri-o | Calico (IP-in-IP)<br>Flannel (Overlay) | iptables | NGINX Ingress Controller (HostNetworked) |
| OpenShift | 3.11* (Qualified) | RHEL 7.7<br>CentOS 7.7 | Docker | OpenShift SDN (OVS) | iptables | OpenShift Router (HostNetworked) |

*OpenShift 3.11 platform is supported only using the standard VEN on RHEL or CentOS and does not require the C-VEN package to be installed.

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.