illumio

PRODUCT BRIEF

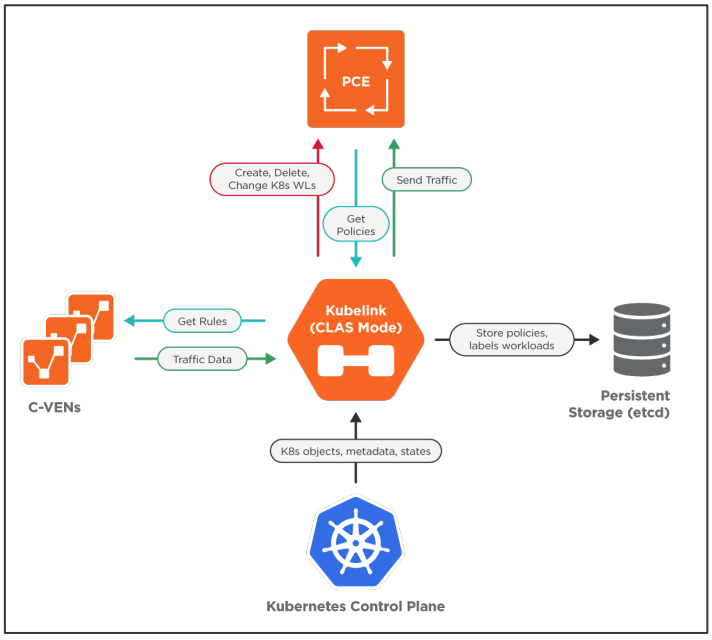
Secure Kubernetes and OpenShift With Illumio Core

Extend Illumio's industry-leading segmentation to container deployments

Stop the spread of breaches – in Kubernetes, RedHat OpenShift, and organization-wide

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.

Illumio Core prevents the spread of breaches through Zero Trust Segmentation (ZTS). ZTS delivers uniform security policy across environments, including Kubernetes and RedHat OpenShift platforms. It helps organizations limit the spread of breaches between applications and meet regulatory compliance standards such as SWIFT, PCI, and GDPR.



Illumio Container Architecture

Key benefits

Full visibility
Inventory container clusters and visualize real-time traffic between pods, their hosts, and across the entire infrastructure.

Uniform policy across environments
Prevent the spread of breaches with a single policy across all workloads – and without hardware.

Follow DevOps best practices and integrate into existing workflows
Easily deploy with the Helm Chart and support existing CICD processes.

Seamless segmentation
Simplify container security with a system that supports the highly dynamic and ephemeral nature of pods.

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 hundreds of pods for different applications. Attackers can then use this to move laterally from one 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 stop the spread.

Innovative capabilities

Discover namespace, pods, and services dynamically

Inventory all clusters reported to Illumio. Pods and services are described with Kubernetes metadata to offer more context about the microservices deployed in containerized applications.

Real-time application dependency map

Display pods alongside all other workloads, whether VM or bare metal, on a full visual map across all data center, cloud, and end-user workloads.

Lateral movement detection

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

Secure Kubernetes control plane for business-critical applications

Secure communications between nodes in a Kubernetes cluster with an allow list and protecting clusters running critical business applications.

Granular policy models

Choose between a simple ringfence around the cluster or a more granular role-based model to prevent lateral movement between pods or undesired communications between different environments running on the same cluster.

Incoming and outgoing traffic control

Control incoming traffic by securing applications exposed via ingress controllers and/or load balancers. Analyze outbound flows to and from pods easily and use this data to define security policies.

Expedite DevOps with automated container workload profiles

Dramatically reduce the time required to implement security policies on pods and services within Kubernetes clusters. Pods and services inherit associated policies dynamically and come online fully secure, allowing DevOps teams to confidently deploy applications.

How Illumio Core works

Illumio Core includes three software components:

- **Policy Compute Engine (PCE):** Central software that aggregates all information from container clusters and agents to offer central visibility, write policy, and provide seamless integrations.
- **Kubelink:** 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.
- **Containerized Virtual Enforcement Node (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.

Illumio is Red Hat OpenShift certified

Get access to the Helm Chart in the Red Hat Ecosystem Catalog.

About Illumio

Illumio, the Zero Trust Segmentation company, prevents breaches from spreading and turning into cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.