illumio

SOLUTION BRIEF

# Illumio Core: Segmentation for Containers – and Everything Else

## Enabling Visibility and Segmentation for Containers

Gain the agility of containerized deployment, without compromising Zero Trust confidence in preventing the spread of breaches. Illumio Core™ now supports management and visibility of containerized hosts alongside your existing compute environments. Extend segmentation policy beyond your data center and public or private cloud to govern containers consistently with all other forms of compute – without administering a separate point solution, or re-architecting the network.

Containers, by nature, are lightweight, agile, sometimes ephemeral workloads, and can be easily spun up anywhere in the infrastructure. But micro services are also a new attack vector that can be exploited by attackers, as they are exposed to many threats over the Internet.

A container running a vulnerable piece of code at runtime or an unprotected key can be used to gain access to this container or even further, take control of the host running tens or hundreds of containers for different applications. This container or host can be then used to move laterally from one (containerized) workload to another and (as containers don't live on an island), potentially cause cascading attacks on the entire infrastructure.

Neither native cloud controls nor point container solutions can govern all environments with a single policy. In fact, administering multiple point tools for segmentation can lead to policy inconsistency and even misconfiguration – a leading cause of breach.

## Why Illumio?

Illumio Core delivers segmentation to prevent the spread of breaches, and to meet regulatory compliance standards such as SWIFT, PCI, and GDPR. Because the perimeter doesn't stop all bad actors from getting inside data center and cloud environments – or even through to your containers - segmentation from Illumio restricts access to critical systems to only authorized entities.

### Gain visibility and control of containers

Illumio Core delivers a full range of segmentation for containerized hosts:

- Centralize visibility of containers alongside other compute environments – gain a single view across containerized workloads and bare metal, virtual machines, private and public cloud - because you can't protect what you can't see.
- Enforce uniform policy across containers – and everything else – segment containers along with the rest of your overall data estate, with unified policy, regardless of the environment.

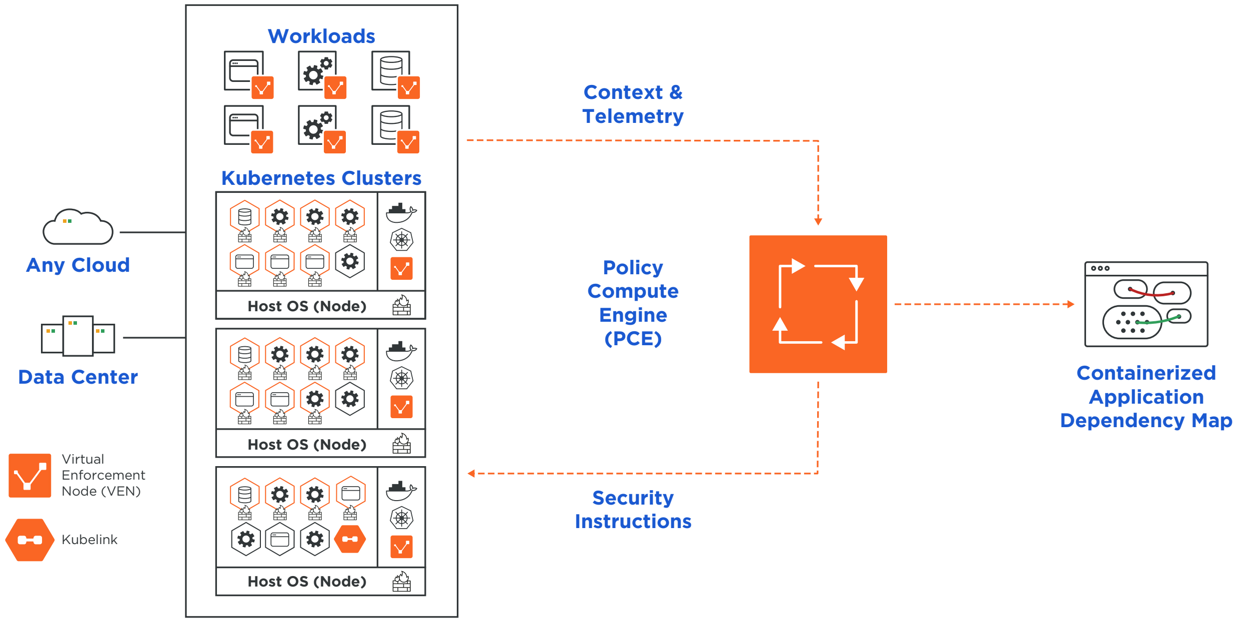


Figure 1. Illumio Core segments containerized hosts alongside other forms of compute across the data center and the cloud – providing centralized visibility of traffic communicating across your environments to define policy, and enforcement closest to what is being protected – at the host.

## Containers don't live in a vacuum

Traditional network approaches to segmentation don't scale for containers, which can travel outside the network infrastructure. Likewise, container security point solutions don't prevent container communications across existing environments – creating another segmentation tool to configure and synchronize.

Illumio enables customers to segment containerized and non-containerized applications with greater range of visibility and uniform policy management than either container security point tools or traditional networkbased methods:

- Centralize visibility - view what's in your cluster(s) and what it's communicating with – in the context of your larger application dependency map.
- No firewall rule-writing required – simplify policy with granular metadata-based rules in natural language, based on business logic, centralized and distributed on the workload – as close as possible to the source.
- Adaptive security - conform policy to any changes, without the complexity of manual or script-based firewall re-writing.
- Gain container agility - Avoid deployment delays in your CI/CD process with baked-in adaptive segmentation policy that seamlessly follows the workload and adjusts automatically.

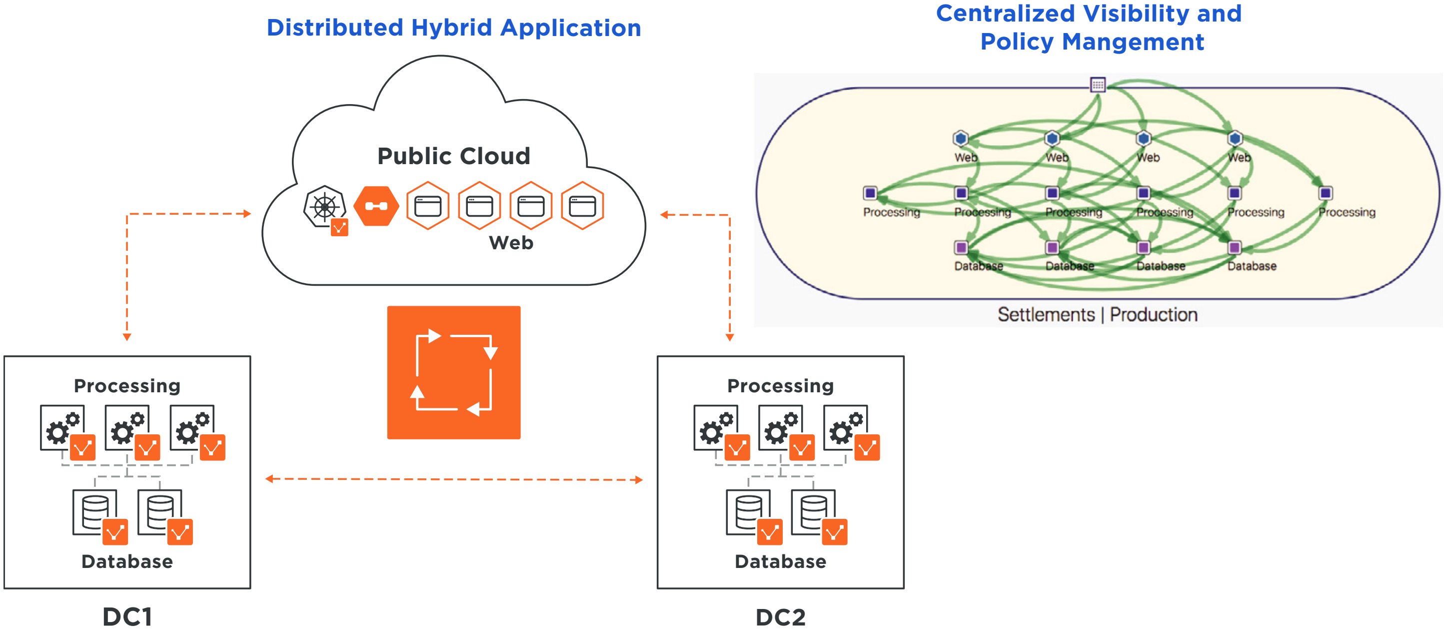


Figure 2. Illumio Core's application dependency map lets you visualize containerized workloads alongside other compute environments to manage policy uniformly across your data estate.

## Segment containers automatically, with policy baked in

Containers allow developers to spin up new applications in seconds, offering agility and flexibility the data center never did. Adequately securing these containerized workloads requires a similarly dynamic approach. Illumio Core provides a set of tools to empower security practitioners and segment dynamic assets when they come online in native Kubernetes deployments, or within integrated platforms like RedHat OpenShift:

- Dynamic detection of Kubernetes objects – discover namespaces, pods and services when they are configured by application owners without touching Illumio Core.
- Automatic labeling and policy inheritance using profiles – push security policies when pods come online by assigning labels to namespaces and objects nested into it. By using profiles, security administrators can ensure a default security policy is assigned to any application created in and across clusters.
- Segmentation templates – for well-defined environment like Red Hat OpenShift, Illumio provides segmentation templates that can be applied directly on OpenShift nodes to offer a validated set of policies that will secure cluster nodes and infrastructure services independently from containerized workloads running on it.

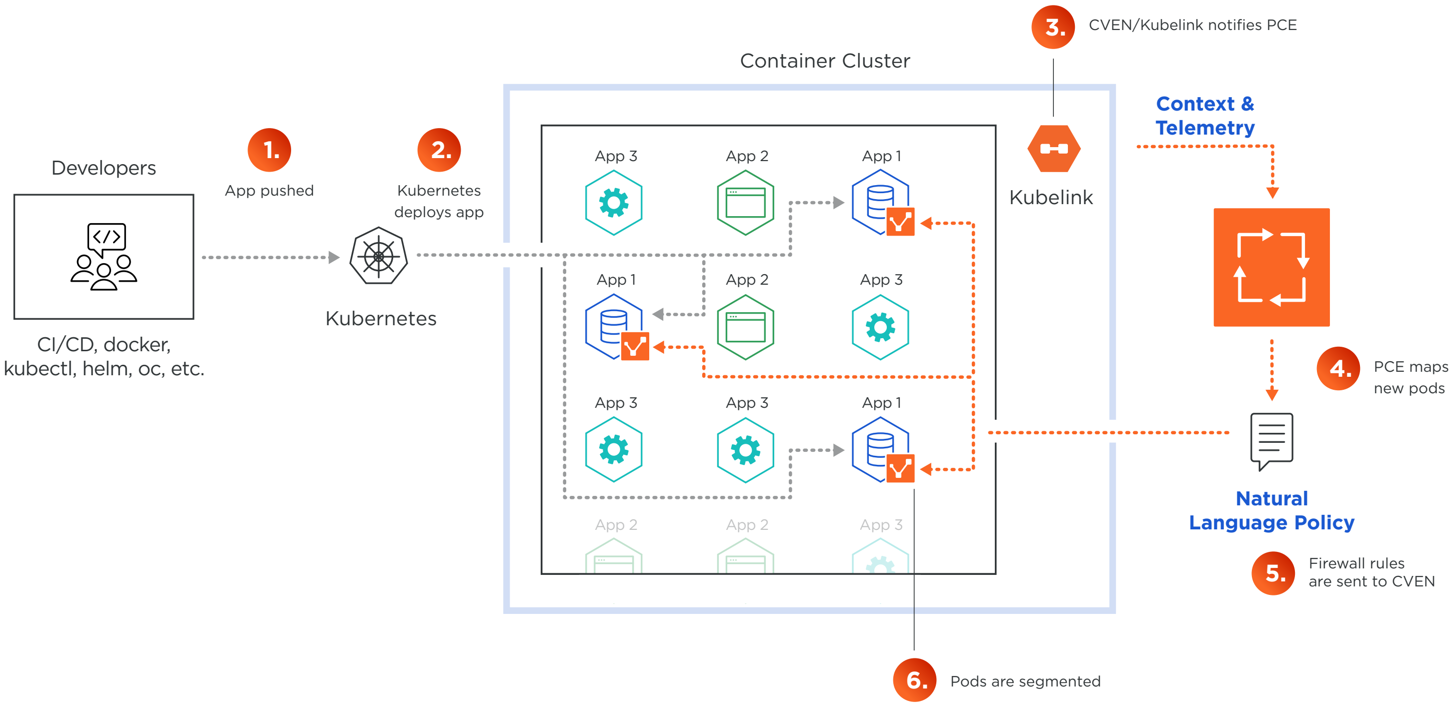


Figure 3. Spin up containers with baked-in security policy through container workload profiles, for secure segmentation without impacting agility of deployment.

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.