

ILLUMIO ADAPTIVE SECURITY PLATFORM®: 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's Adaptive Security Platform (ASP) now supports management and visibility of containerized hosts, alongside your existing compute environments. Extend segmentation policy beyond your datacenter 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? The Illumio ASP 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's ASP 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.

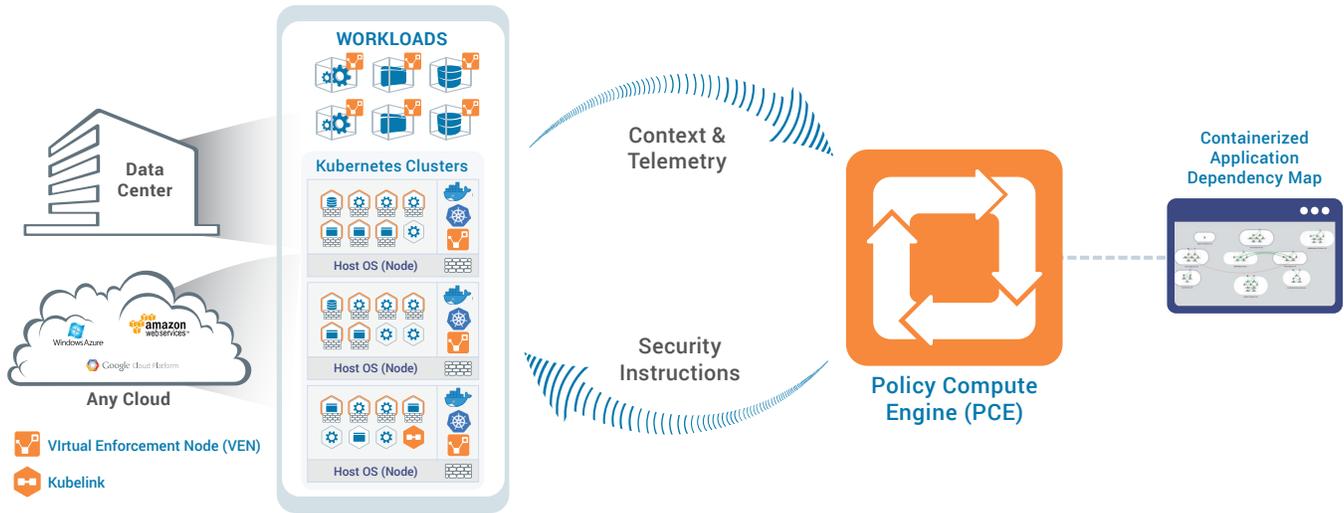


Figure 1. Illumio ASP segments containerized hosts alongside other forms of compute across the datacenter and the cloud – providing centralized visibility of traffic communicating across your environments to define policy, and enforcement closest to what is being protected – at the host.

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 network-based 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.

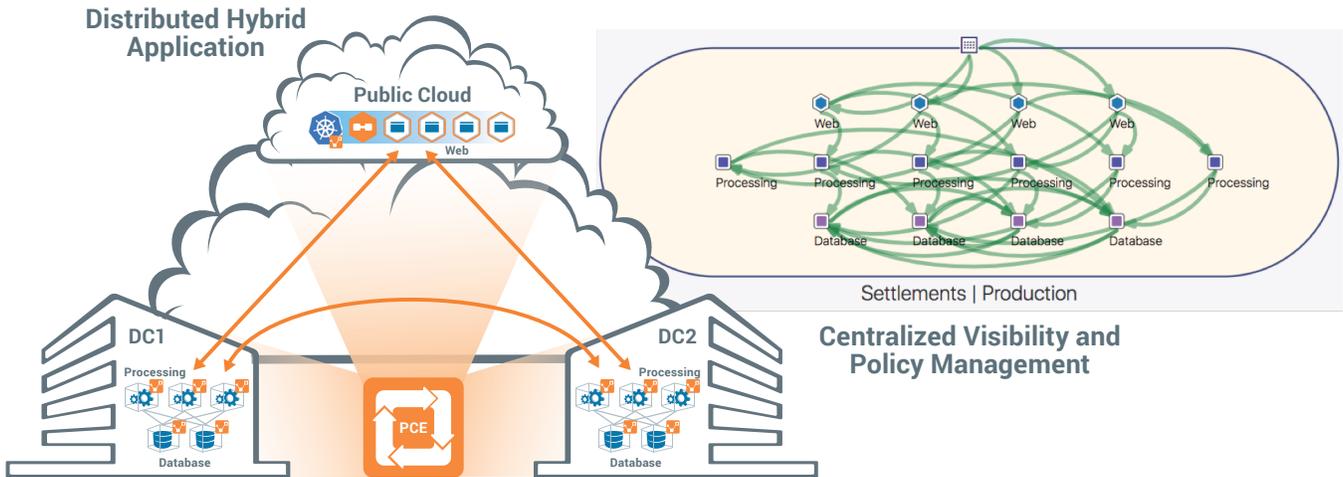


Figure 2. Illumio ASP application dependency map lets you visualize containerized workloads alongside other compute environments, to manage policy uniformly across your data estate.

Segment containers automatically, with policy baked in. Containers allow developers to spin up new applications in seconds, offering agility and flexibility the datacenter never did. Adequately securing these containerized workloads requires a similarly dynamic approach. Illumio ASP 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 ASP.
- **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.

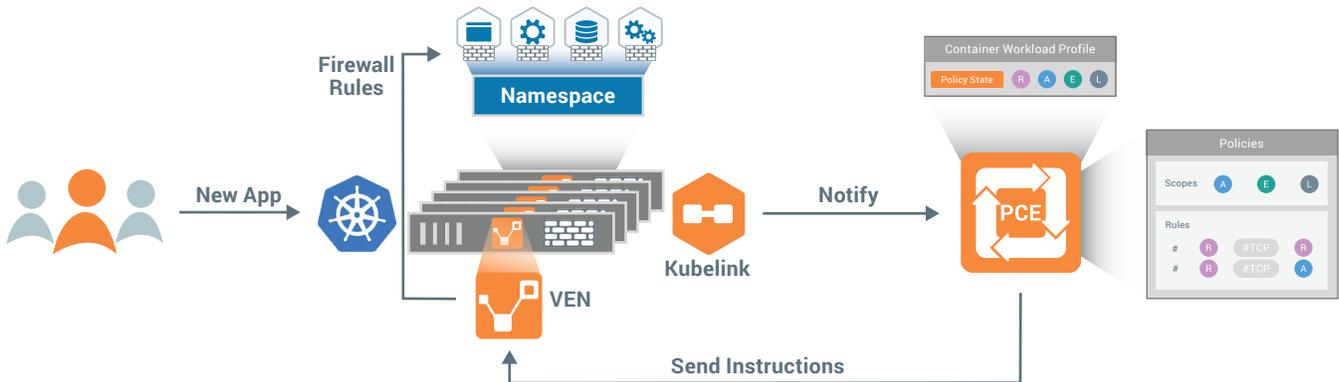


Figure 3. Spin up containers with baked-in security policy through container workload profiles, for secure segmentation without impacting agility of deployment.

ABOUT ILLUMIO

illumio, a cybersecurity leader delivering segmentation solutions, prevents the spread of breaches inside data center and cloud environments. Enterprises such as Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite use illumio to reduce cyber risk and achieve regulatory compliance. The illumio Adaptive Security Platform® uniquely protects critical information with real-time application dependency and vulnerability mapping coupled with segmentation that works across any data center, public cloud, or hybrid cloud deployment on bare-metal, virtual machines, and containers. For more information, visit www.illumio.com/what-we-do and:

- [Engage with illumio on Twitter](#)
- [Follow illumio on LinkedIn](#)
- [Like illumio on Facebook](#)
- [Subscribe to our YouTube Channel](#)

CONTACT US

For more information about illumio ASP and how it can be used to achieve visibility behind the firewall, email us at illuminate@illumio.com or call 855-426-3983 to speak to an illumio representative.

illumio, Inc. 920 De Guigne Drive, Sunnyvale, CA 94085 Tel (669) 800-5000 www.illumio.com

Copyright © 2019 illumio, Inc. All rights reserved. This document is protected by U.S. and international copyright and intellectual property laws. illumio's products and services are protected by one or more U.S. and international patents listed at <https://www.illumio.com/patents>. illumio® is a trademark or registered trademark of illumio, Inc. or its affiliates in the U.S. and other countries. To review a list of illumio's trademarks, go to <https://www.illumio.com/trademarks>. Third-party trademarks mentioned in this document are the property of their respective owners.