Illumio Segmentation for Containers

Segment containers with clear visibility and consistent policy across hybrid environments.

Enabling visibility and segmentation for containers

Get the speed of containers without losing confidence in stopping breaches from spreading. Illumio Segmentation provides visibility into containerized hosts and manages them alongside the rest of your environment.

You can apply consistent segmentation policies across data centers and clouds without adding new tools or redesigning your network.

Containers are fast and flexible, but that agility creates risk. Microservices increase exposure and expand the attack surface.

If a container runs vulnerable code or holds an unprotected key, an attacker can gain access and take control of the host. From there, they can move between workloads, turning a single compromise into a broader attack.

Most tools can't enforce one policy everywhere. Native cloud controls and point solutions work in silos, which leads to gaps, inconsistent policies, and misconfigurations — all common causes of breaches.

Why Illumio for containers?

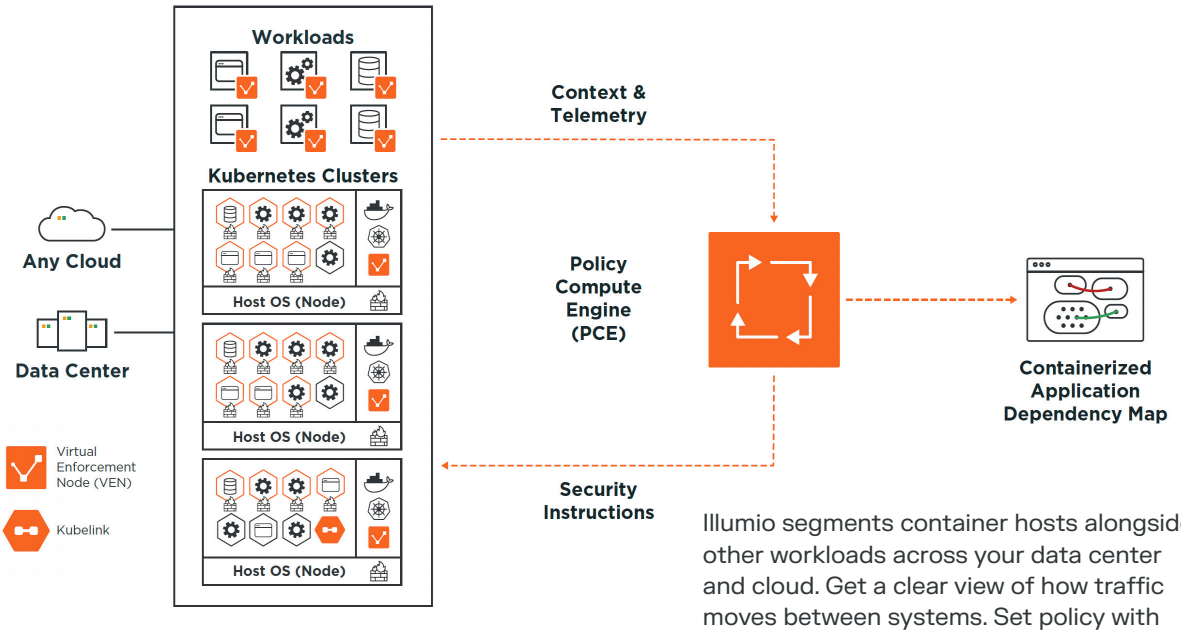
Perimeter defenses alone can't keep every attacker out of data centers, clouds, or container environments.

Illumio Segmentation limits access to critical systems so only approved users and workloads can connect. Illumio supports compliance with standards like SWIFT, PCI, and GDPR.

Gain visibility and control of containers

Illumio Core provides segmentation for containerized hosts across your entire environment.

- **Centralize visibility across environments.** See containers alongside all other resources, including on-premises, virtual machines, and public and private clouds. This gives you one clear view so you know what needs protection.
- **Apply consistent policy everywhere.** Use the same segmentation policy across containers and the rest of your environment. This keeps security consistent no matter where workloads run.



Illumio segments container hosts alongside other workloads across your data center and cloud. Get a clear view of how traffic moves between systems. Set policy with confidence and enforce at the host level, close to what matters most.

Containers don't live in a vacuum

Traditional network segmentation doesn't work well for containers. Containers can move beyond the network, which makes them hard to control with older methods.

Container security tools also fall short. They don't stop communication across environments and often add another tool to manage.

Illumio makes it easier to segment both containerized and non-containerized applications. It gives you better visibility and consistent policy management across your environment.

- **Centralize visibility.** See what's running in your clusters and how it communicates, all within a full application dependency map.
- **No firewall rule writing.** Create simple policies using labels and business context instead of complex rules. These policies are applied close to the workload.
- **Adaptive security.** Policies adjust as your environment changes, without manual updates or scripts.
- **Maintain container agility.** Avoid delays in your CI/CD pipeline with built-in segmentation that follows each workload and updates automatically.

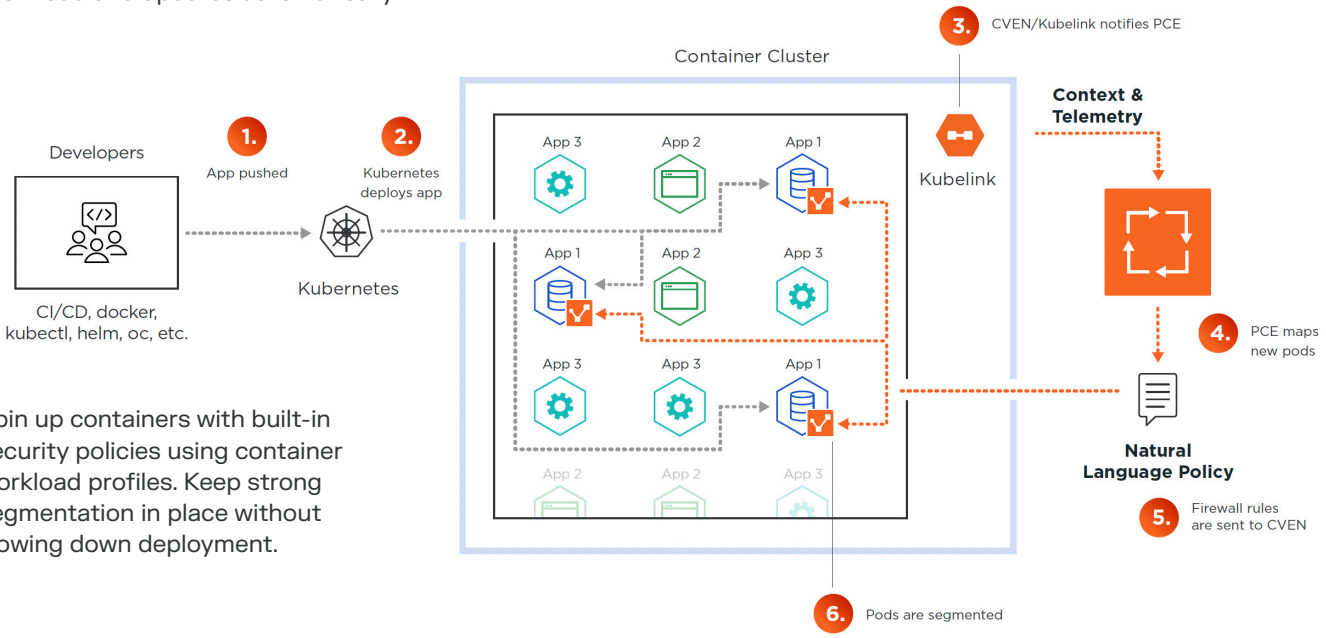
Segmentation that follows every container

Containers let developers launch new applications in seconds. This brings speed and flexibility that traditional data centers never had.

But securing these fast-moving workloads requires a flexible approach as well.

Illumio Segmentation helps security teams manage and segment dynamic environments as soon as they come online, whether in Kubernetes or platforms like Red Hat OpenShift.

- **Dynamic discovery of Kubernetes objects.** Automatically find namespaces, pods, and services as teams create them, without manual setup.
- **Automatic labeling and policy inheritance.** Apply security policies as soon as pods start by using labels. Profiles ensure each new application follows a default policy across clusters.
- **Pre-built segmentation templates.** Use ready-made templates for environments like Red Hat OpenShift. These templates apply proven policies to protect cluster nodes and core services, separate from the workloads running on them.



Spin up containers with built-in security policies using container workload profiles. Keep strong segmentation in place without slowing down deployment.

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments – stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.