Illumio for DevSecOps

DevSecOps teams can automatically build Zero Trust security enforcement into software releases, tailoring microsegmentation policies for roles, applications, environments, and locations

Agile DevOps Can't Afford to Neglect Security

DevOps agile practices accelerate software development and deployment, but often do so without fully accounting for security. Applications are built and released quickly, but once deployed in any environment, they may still be vulnerable to attack.

As development cycles speed up, security must keep pace. DevOps teams need a way to address risk across every stage of the development pipeline: plan, build, test, deploy, and monitor — without slowing down delivery.

At the same time, it's unrealistic to expect developers or operations teams to become security experts. Security must align with the speed and automation that DevOps demands.

That means making it easier to design and deploy software with strong, consistent security controls already in place — no matter how fast the pipeline moves or where the application runs.

Illumio Makes It Easy to Build Zero Trust Security into DevOps

Illumio protects software and networks by making it easy for organizations to define segmentation policies. Organizations can then quickly enforce those polices.

Zero Trust mandates that no user, process, or system is trusted unless specified in a security rule. By blocking all network traffic over ports and addresses, except those identified as necessary for specific applications and people, Illumio prevents cyberattacks from succeeding. It blocks malware and hackers from moving across your network and production environments.

Security that Closes the DevOps Gap

Illumio closes the DevOps security gap, delivering built-in protection against ransomware and other threats.

Zero trust security that fits into agile processes
With Illumio, DevOps teams and security analysts can define and enforce precise security policies without having to program thousands of firewall rules. Illumio translates high-level policies into detailed rules automatically.

Security flexible enough for DevSecOps
Illumio makes it easy to define and enforce segmentation policies for roles, applications, environments, and locations, so DevSecOps organizations can tailor policies as needed.

Security that stops attacks in progress
Illumio allows teams to instantly isolate ransomware and other attacks on critical applications and data. Teams can see communications traffic in real time and immediately block infected systems from the network.

Using Illumio, DevOps and security teams can collaborate to define the traffic patterns software should support while blocking all other communications.

Applications produced through DevSecOps processes implement these Zero Trust segmentation rules automatically, guarding against a broad range of attacks.

Illumio provides the visibility and automation DevSecOps teams need

By automatically computing firewall rules based on high-level policies, Illumio makes it easy to build security into software and computing services.

Illumio provides real-time mapping of application traffic. With Illumio, you can identify exactly which traffic you should allow on your communication pathways.

Once developers, operations engineers, and security analysts identify traffic that should be permitted for an application or service, they can use Illumio to quickly define Zero Trust policies, blocking all other traffic. DevSecOps organizations can then customize policies based on:

- Roles within the application
- The application itself
- The environment the application runs in, such as development, test, or production
- The environment's location: for example, a production environment at a data center in California

To enforce those policies and to monitor traffic for lateral movement, the DevSecOps team simply adds an Illumio Virtual Enforcement Node (VEN) to a software build. The VEN is Illumio's lightweight, fail-safe agent that works with the built-in firewall on the application's host.

Once running in the application environment, the VEN enforces Zero Trust policies, raises alerts upon detection of suspicious lateral movement, and curtails traffic in response to active attacks, isolating infected endpoints from the rest of the network.

Illumio provides a single, easy-to-use, flexible platform for building security into DevSecOps processes — without extensive training, expense, or overhead.

Teams can define and test policies in the plan, build, and test phases of the DevOps pipeline, then monitor traffic for threats in the deploy and monitor phases.

The Illumio Platform provides Zero Trust segmentation wherever applications and services are deployed, including:

- Data centers
- Public, private, or hybrid clouds
- Endpoints

> "Illumio has played a critical role in allowing us to better understand our risk, control security policy, and secure our data."
>
> **Security Executive**
> Leading Financial Institution

Segmentation for DevSecOps

Learn how Illumio can help software development teams build security in applications of all kinds.

Contact Illumio today at:
www.illumio.com

About Illumio

illumio

Illumio, the most comprehensive Zero Trust solution for ransomware and breach containment, protects organizations from cyber disasters and enables operational resilience without complexity. By visualizing traffic flows and automatically setting segmentation policies, the Illumio Platform reduces unnecessary lateral movement across the multi-cloud and hybrid infrastructure, protecting critical resources and preventing the spread of cyberattacks.