SOLUTION BRIEF

Illumio for DevSecOps

DevOps teams can automatically build Zero Trust security enforcement into software releases, tailoring micro-segmentation 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 accounting for security. Applications are developed quickly and efficiently, but once deployed in any environment, they're vulnerable to attack.

DevOps teams need a fast, easy way to build security into software moving through all stages of a development pipeline: Plan, Build, Test, Deploy and Monitor. Yet, it's not practical to expect developers or operations engineers to become security experts.

DevSecOps is the practice of building security into DevOps processes so applications and services automatically include security controls to guard against threats such as ransomware and other types of malware.

DevSecOps makes it easy for developers to design security into new software, so when it's deployed, security controls are already built in.

Illumio Makes It Easy to Build Zero Trust Security Into DevOps

Illumio protects software and networks by making it easy for organizations to define Zero Trust segmentation policies. Organizations can then quickly enforce those polices using the firewalls built into common operating systems.

Zero Trust mandates that no user, process or system is trusted unless specifically identified in a security rule.

By blocking all network traffic over ports and addresses except those identified as necessary for certain applications and people, Illumio prevents cyberattacks from succeeding. It blocks malware and hackers from moving across your network and production environments.

Using Illumio, DevOps teams and security teams can work together 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.

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 DevOps

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

Security That Stops Attacks in Progress

Illumio gives teams the ability 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.

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 — the basis for Zero Trust security.

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

> “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**

To enforce those policies and to monitor traffic for lateral movement, the DevOps 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 DevOps processes — without extensive training, expense or overhead. Teams can define and test policies in the Plan, Build, and Test phases of a DevOps pipeline, then monitor traffic for threats in the Deploy and Monitor phases.

The Illumio product suite provides Zero Trust segmentation wherever applications and services are deployed, including endpoints in:

- Data centers: Illumio Core
- Public, private or hybrid clouds: Illumio CloudSecure
- Endpoint devices: Illumio Edge

Zero Trust Segmentation for DevSecOps

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

Contact Illumio today

Visit: www.illumio.com

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming 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.