



Illumio for App Owners

Prevent application downtime with Zero Trust Segmentation

Breaches impact application performance

Security awareness is everyone's responsibility. This is more important than ever because attackers aren't slowing down — in the past two years alone, [76 percent](#) of organizations were attacked by ransomware, and a ransomware attack occurred every 11 seconds.

If an attacker does get into an organization, the risk to the business is great. They can steal confidential data, protected health information (PHI), or halt all business operations.

As application owners, your responsibility is to keep applications running, no matter what. We understand how critical this is to both the business and your role. It helps preserve the business's reputation and keeps operations running. Any possible downtime is a risk.

Security is working alongside you to be proactive in preparing for attacks and ensure your application isn't a part of a breach that could potentially cause a catastrophic downtime.

The solution

Illumio has been selected as part of the strategy against cyberattacks, preventing attackers from shutting down business critical applications.

Illumio provides **Zero Trust Segmentation**. This manages connections throughout the business environment to proactively protect against attackers who want to stop our business.

A key strategy for attackers when they access an organization is to rapidly spread to as many workloads as possible. Illumio helps prevent this.

Illumio improves uptime

5
cyber disasters
[averted](#) annually

\$20.1 million
[saved](#) in annual
downtime costs

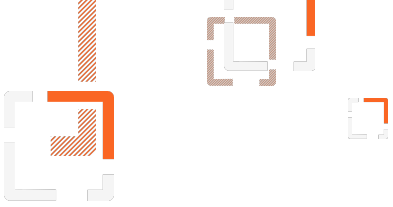
10 minutes
stop ransomware attacks in 10
minutes, [4x faster](#) than
detection and response alone

Defining Zero Trust Segmentation

First, let's define what is meant by Zero Trust. A **Zero Trust architecture** means that it doesn't implicitly trust anything. With this approach, the principle of least privilege is followed. This limits the potential attack surface that can be exploited.

Segmentation is the ability to break larger networks into smaller pieces which allows us to prohibit unpermitted connections. A small security incident is contained to where it occurred rather than spreading throughout the network and impacting multiple applications.

Zero Trust Segmentation is the combination of these strategies. It's an approach that can partition the network down as far as individual workloads. Nothing is trusted, and everything is verified.



Benefits for app owners

Using Illumio ZTS helps tear down silos between teams by offering these key benefits.

Business continuity

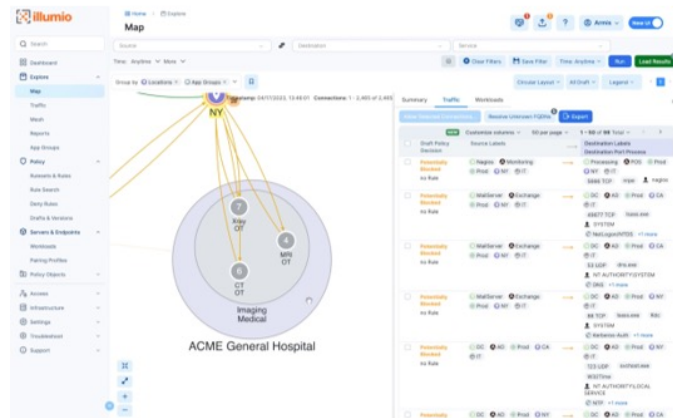
Maintain high availability and uptime by preventing unnecessary connections between applications. With additional benefits such as application ringfencing, other applications' changes will no longer impact yours. If you do notice a change, it's easy to detect where the unwanted traffic is coming from.

Illumio's lightweight agent is not in-line to communications, meaning it won't impact application performance. It doesn't redirect application traffic, so there's no added latency or CPU tax. The focus is on protecting your applications.

Unprecedented visibility

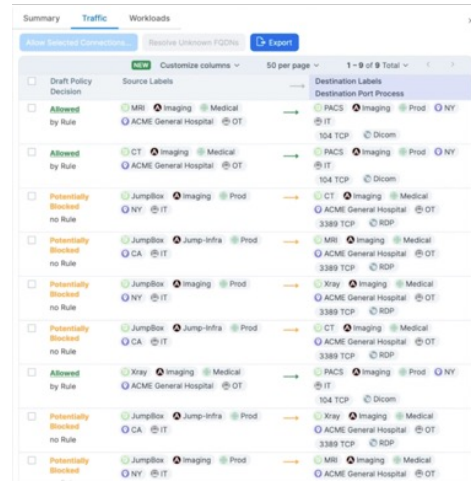
Illumio provides a clear view of all application processes. This gives you, the application owner, a new and improved understanding of who and how your application communicates within the network environment.

This provides visibility throughout the hybrid environment, whether on-premises or in the cloud, eliminating silos or confusion of what other teams are doing.



Easy to use

Get the information you need in seconds with a simple-to-use solution. We'll provide you with the setup, and all data is written in plain language, making it easy to understand. Filter through data in just a few clicks to get to specifics about applications you own.



Implementing Illumio is a powerful way for your organization to prepare for the worst. In proactively protecting applications, we are working together to improve business resiliency and application uptime.

Get started today

Learn how [Illumio's lightweight agent](#) supports your team

About Illumio



Illumio, the Zero Trust Segmentation company, stops breaches and ransomware from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.