illumio

INDUSTRY BRIEF

Illumio for Criminal Justice Information Services

Contain ransomware attacks and maintain operations with Zero Trust Segmentation

CJIS agencies are prime targets for cyberattacks

According to a recent report from the FBI Internet Crime Complaint Center, government facilities were the third most-targeted infrastructure sector by ransomware attacks in the US in 2023.

Criminal justice resources are at high risk for breaches. CJIS agencies are often targeted by threat actors who want to steal money, spread propaganda, or disrupt critical infrastructures. To protect these resources, CJIS agencies need to follow Zero Trust security guidelines which were recently issued by the White House. A Zero Trust architecture brings CJIS agencies in line with federal guidelines — and can lower cyber insurance costs.

Illumio helps you put these guidelines in action with Zero Trust Segmentation (ZTS). ZTS allows you to discover and control all traffic moving laterally between workloads, whether in on-site data centers or in the public cloud. Illumio helps you secure:

- **Interior networks (east-west):** This includes security risks such as excessive workload-to-workload dependencies, the lack of workload segmentation barriers, and inflexible control from relying too much on IP addresses.
- **Perimeter networks (north-south):** Illumio integrates with ZTNA platforms to share context on how workloads are communicating. This notifies the ZTNA enforcement point of changes to workload metadata. By integrating Illumio with a ZTNA tool, you can build a complete Zero Trust architecture end-to-end.

Key benefits of Illumio

Achieve federal Zero Trust compliance

Illumio helps you align your Zero Trust infrastructure with federal cybersecurity requirements.

Discover all application dependencies

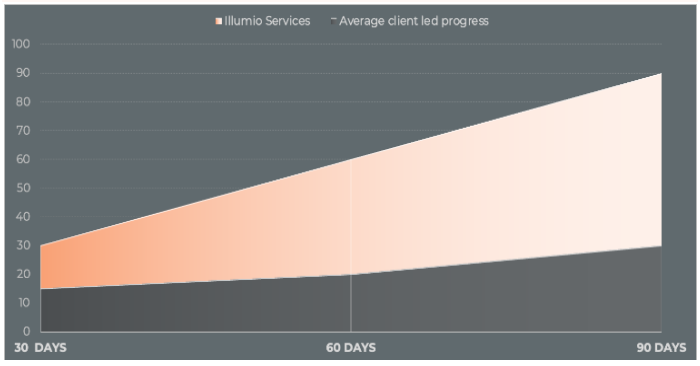
Illumio eliminates blind spots by showing all traffic between all applications across the entire hybrid infrastructure so you know where to segment.

Reduce cyber insurance costs

Illumio's platform delivers lateral segmentation that meets cyber insurers' requirements to reduce premiums.

Meet Zero Trust security audits

Illumio enables a true Zero Trust architecture with granular control of traffic between all workloads.



Illumio makes it possible to get quick time to value with Zero Trust Segmentation.

How it works

Modern networks don't have clear perimeters anymore — the perimeter is everywhere. People can access sensitive or even classified information remotely from anywhere. So why are we still using traditional perimeter security methods?

Illumio assumes that breaches will happen. Illumio helps you find and see all network traffic between all applications and workloads. With this information, you can proactively segment all workloads across your entire hybrid, multi-cloud environment and allow exceptions when needed. This helps prevent a breach or ransomware attack from spreading, even if the threat goes undetected.

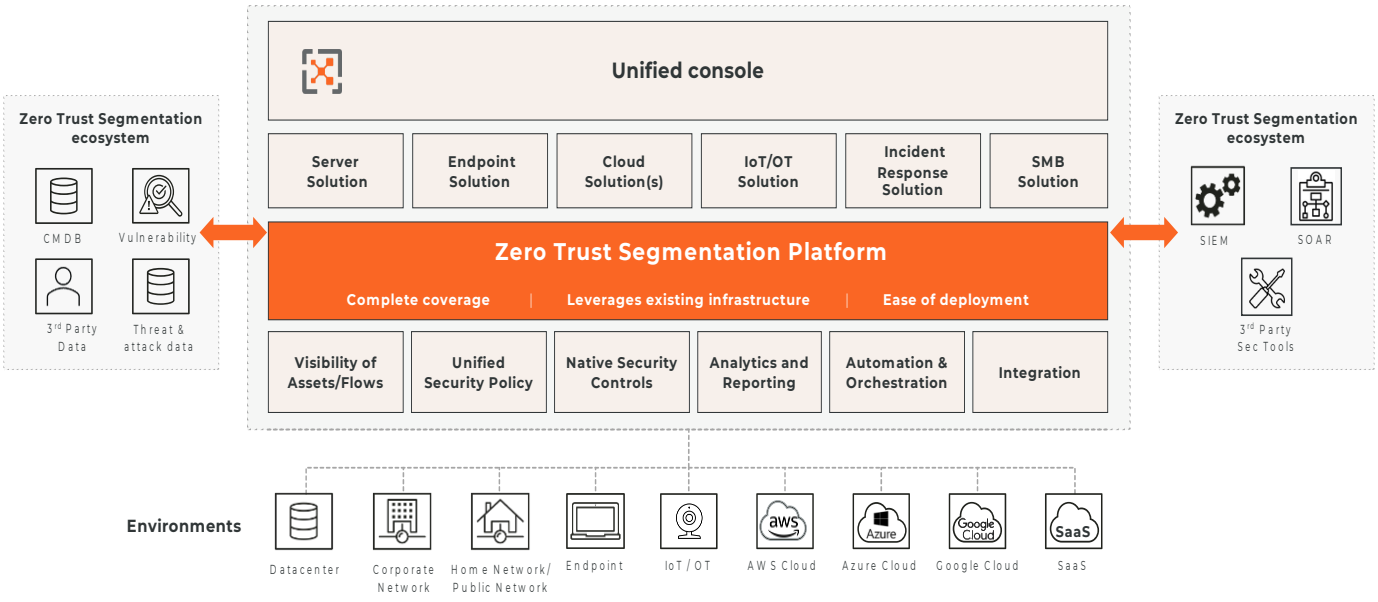
If a breach happens, Illumio makes sure that the first compromised workload stays isolated. ZTS helps you create a Zero Trust foundation that keeps a small security incident from becoming a big problem.

Within a few hours of using Illumio, you can see all application traffic across your entire network and start segmenting workloads.

1. **Install Illumio Core** on your east-west network. Discover all workloads and see how traffic moves across your agency.
2. **Label all workloads** with contextual data, such as Role, Application, Environment, or Location. This creates metadata that Illumio can use to identify application dependencies by owner, not by network addresses.
3. **Create an allow-list policy model** that allows only necessary traffic to move between workloads and blocks all other traffic by default. For example, you can block SSH and RDP between all workloads and only allow it from central administrative hosts. This reduces the number of connections between workloads and makes it harder for a breach to spread.

Learn more at illumio.com/solutions/government.

Illumio Zero Trust Segmentation Platform



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.