

Illumio for Criminal Justice Information Services

Contain breaches, protect sensitive data, and keep vital public services running with Illumio.

In April 2026, one [phishing email](#) opened the door to the police servers in Ardmore, Oklahoma. Attackers encrypted six months of criminal complaints and active investigations, then demanded \$300,000 to keep it all off the internet.

The city's network was segmented by department, so billing and 911 stayed up. But inside the police environment, nothing stood between the attacker and the records they sought.

Ardmore is a reminder that an agency doesn't have to be big to be worth attacking.

Criminal justice information services (CJIS) teams hold key data and run vital public services. Attackers may steal funds or data. They may spread false claims or shut down key work. A breach can slow a case, halt work, and harm public trust.

Federal rules call for a Zero Trust plan. Teams must validate each request, limit traffic to only what's required, and plan for a breach. Illumio helps CJIS teams put this plan to work.

Illumio helps you see how apps and systems connect in real time and then segment traffic between them. Breaches are inevitable, but with Illumio, they have fewer ways to spread.

Illumio helps you secure:

- **Interior (east-west) traffic.** Most agencies have far more connections between workloads than they need, few barriers between them, and policies tied to IP addresses that break when things move.
- **Perimeter (north-south) traffic.** Illumio integrates with Zero Trust network access (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

Illumio gives CJIS teams the visibility and control to stop a breach from spreading.

Achieve federal Zero Trust compliance

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

See all application dependencies

Illumio eliminates blind spots by showing all traffic flows between all applications across your entire hybrid multi-cloud so you know where to segment.

Reduce cyber insurance costs

Get lateral segmentation that meets cyber insurers' requirements to reduce premiums.

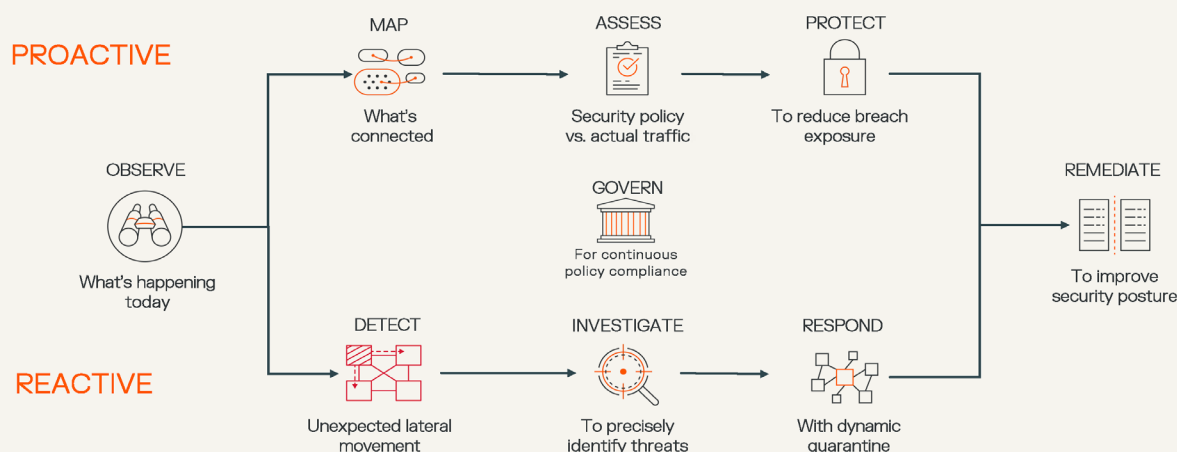
Meet Zero Trust security audits

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



The Illumio Breach Containment Platform

Complete lateral movement coverage for the AI era



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.

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

When a breach happens, Illumio makes sure that the first compromised workload stays isolated. This helps you create a Zero Trust foundation that keeps a small security incident from becoming a catastrophe.

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

- 1. Install Illumio Segmentation.** Find systems and map how traffic moves across your agency.
- 2. Use Illumio Insights.** Turn traffic data into a clear view of app behavior. See suspicious traffic and high-risk connections. Use that context to set policy.
- 3. Add context.** Label each system by role, app, environment, and site. Illumio can then find links by business use, not just by network address.
- 4. Set least-privilege policy.** Allow only the traffic each app needs, and block all other traffic by default. For example, limit SSH and RDP access to approved admin hosts. Fewer connections between workloads make it harder for a breach to spread.

Learn more about
securing criminal
justice infrastructure:



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

Copyright © 2026 Illumio, Inc. All rights reserved. Illumio® is a trademark or registered trademark of Illumio, Inc. or its affiliates in the U.S. and other countries. Third-party trademarks mentioned in this document are the property of their respective owners.