3 easy wins with Illumio Segmentation

Get real-time visibility into east-west traffic and shut down the pathways attackers use to move.

Most security tools watch your network's front door, but can't see past the perimeter. That means attackers can spread unchecked, moving laterally through east-west traffic that's invisible and wide open in most organizations. Here are three first steps you can take with Illumio Segmentation to get live view of that traffic — and the controls to shut it down.

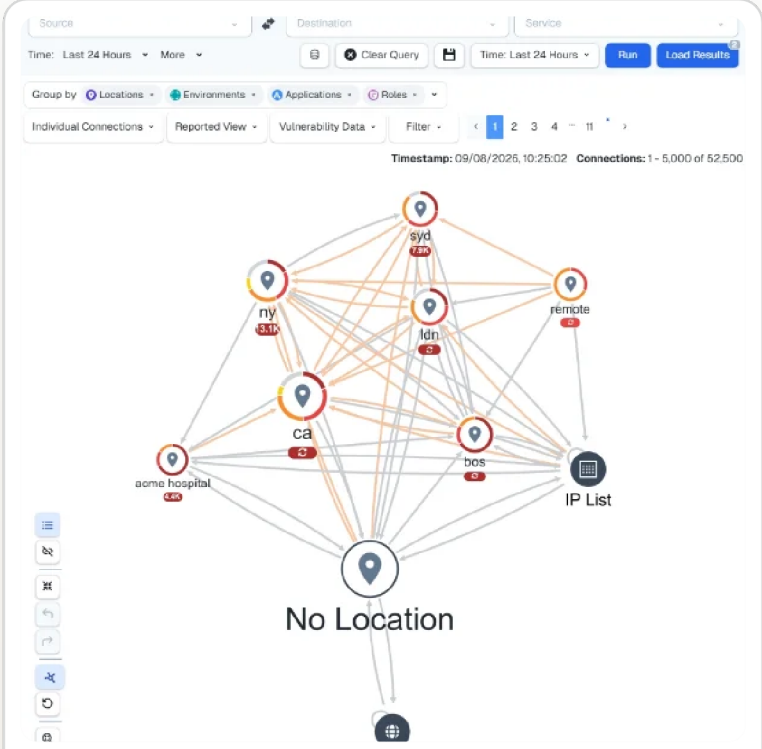
STEP 1

See everything instantly

Get a live view of every connection between every workload.

ACTION

Deploy the Illumio virtual enforcement node (VEN), our lightweight software sensor, across your environment. Within hours you have a live map of every connection between every workload, with no network changes and no downtime. That same sensor doubles as a control point, so the moment something looks suspicious you can shut down traffic.



The Illumination Map: every workload and every connection between them, live.

RESULT

A live map of every connection — and a control point on every workload.

STEP 2

Close the easy lateral pathways

Shut down the high-risk, rarely used ports that give intruders room to roam.

ACTION

Block the four ports that show up again and again in remote access, credential theft, and ransomware attacks.

RDP TCP 3389

A top target for ransomware crews and brute-force attacks

SMB TCP 445

Used to spread ransomware and steal credentials across Windows systems

NetBIOS TCP/UDP 137–139

Legacy services few environments still need

WinRM TCP 5985/5986

A remote admin tool attackers reuse once they're inside

RESULT

An attacker who lands a foothold has far fewer ways to spread ransomware or reach your critical assets.

STEP 3

Extend protection to workstations

Close the gap where most organizations have the least visibility: traffic between workstations.

ACTION

Write policy that stops employee laptops from talking directly to other employee laptops. Very few laptops have any reason to, yet those paths stay open by default at most companies. Workstation policy is simple to write, with very few exceptions to carve out, so it can go live quickly.

RESULT

Thousands of needless peer-to-peer attack paths disappear — including the ones WannaCry and NotPetya used.

NEXT STEPS

See your environment mapped in real time.

illumio.com/try-illumio-segmentation