illumio

4 Steps to Zero Trust Segmentation

Secure your network, isolate your critical systems, and build a true Zero Trust architecture in just four steps

The Key to Stopping Your Biggest Threats

Zero Trust Segmentation builds security beyond the breach, closes risky connections in your network, and stops attacks from spreading. Here are four simple steps you can follow to capture quick wins, improve your security, and quickly build Zero Trust.

How to Build Zero Trust Segmentation in 4 Steps

STEP 1

See Your Systems

- Create a real-time map of how your systems connect and communicate
- Establish what "normal" traffic behavior looks like on your network
- Spot your risks by identifying open pathways for attacks
- Identify which pathways you can leave open and which you must lock down

STEP 2

Close Risky Pathways

- Focus on high-risk pathways that cybercriminals like to exploit (e.g., RDP, SMB, FTP)
- Proactively close as many of these ports and pathways as possible
- Create a more restrictive set of policies you can trigger during an attack

STEP 3

Expand Your Segmentation

- Create environmental segmentation (e.g., separate DEV from PROD)
- Limit admin access rights and privileges for commonly exploited apps
- Enforce policy on core, highly-connected services like Active Directory

STEP 4

Implement Microsegmentation

- Create granular microsegmentation unique to your environment, including:
  - Build micro-perimeters around critical systems
  - Secure cloud systems and hybrid environments
  - Ring-fence assets
  - Enforce compliance-specific policies
  - Apply identity-based segmentation for users and endpoints

Pick the Right Zero Trust Tools

Not every network or security tool can build scalable, granular microsegmentation across modern networks. When evaluating tools, make sure yours:

- ✓ Monitor both north-south and east-west traffic to detect movement outside and inside your network.
- ✓ Perform host-based segmentation to configure the native firewall controls already in your systems.
- ✓ Create allow lists and deny lists to more accurately manage the communications in your network.
- ✓ Automate all four stages of policy management — discovery, authoring, distribution and enforcement.
- ✓ Automatically maintain segmentation by adapting policies and recalculating rules as your network changes.
- ✓ Segment multi-cloud, hybrid cloud, and on-premises environments.
- ✓ Create a real-time, centralized source of truth for network, infrastructure, security and leadership teams.
- ✓ Operate either on-premises or in the cloud, with minimal infrastructure or maintenance requirements.

Start Building Your Zero Trust Defenses Today!

Learn More:
www.illumio.com

Go Deeper:
Achieving Zero Trust Segmentation With Illumio
https://www.illumio.com/resource-center/guide/achieving-zero-trust-segmentation-illumio

Schedule a Chat:
Free consultation and demo
https://www.illumio.com/contact

illumio