LEARNING MADE EASY

Do You Need Zero Trust Segmentation?

The potential for cyber catastrophe is real. You're not sure your business can continue operating amid a cyberattack. You're uncertain where all your high-value assets are, how they're connected, and how you can stop malware from reaching them. And you're not confident that your current security will keep up with cloud migration or advancing technologies.

Do you need Zero Trust Segmentation (ZTS)?

Recognizing the Danger

Research suggests three-quarters of organizations have had a ransomware attack in the last two years, and two-fifths suffer unexpected downtime every month due to attacks. The last thing you want is for your business to become a headline. **Do you need ZTS?**

☐ **YES!**

ZTS stops the spread of inevitable ransomware and breaches to ensure they don't become cyber disasters. It employs segmentation and strict management of communications, ensures that the most vulnerable ports are blocked, and declares all entities untrusted by default. You can rest easy knowing that any blast radius will be small.

Staying Up and Running

Like it or not, breaches are inevitable. Meanwhile, your need to keep the business up and running is nonnegotiable. You need a surefire way to carry on, even on the darkest of cyber days. **Do you need ZTS?**

☐ **YES!**

ZTS ensures that you have full visibility of the attack surface and can ring-fence your most critical assets — this ensures workloads only get access to these assets if they're authorized. ZTS keeps a breach isolated to one small area, so the rest of the business can proceed unaffected as you deal with the intrusion.

Halting Lateral Movement

You've implemented an endpoint detection and response (EDR) solution, but what happens when a cyberattack inevitably becomes a breach? If something bad gets past EDR, it can roam freely inside the system.
Do you need ZTS?

☐ **YES!**

A series of emulated attacks by Bishop Fox proved that ZTS stops attacks from spreading in 10 minutes, four times faster than endpoint detection and response (EDR) alone. Attacks aim to move laterally, or east–west, to dive deeper. Their plan is to move from one asset to the next, steal advanced access privileges, and ultimately find high-value, sensitive data. ZTS blocks all communication that's not essential, enforces least-privilege access, and segments your assets.

Gaining Visibility

Malware gets from one place to another by way of network connections, and the only way to keep ahead of it is to know your connections better than the malware does. **Do you need ZTS?**

☐ **YES!**

A ZTS solution should give you a map of the attack surface, showing vulnerable places and the possible connections that make them vulnerable. You'll learn what connections are open that shouldn't be, and where access rules may be overly permissive. It also lets you understand the context necessary to decide whether a particular communication is allowable and safe, or a threat.

Scaling Up

Digital transformation these days nearly always involves a cloud or hybrid environment that's flexible and scalable. That's the future at its most powerful, but you won't be as safe as you need to be with yesterday's data center security tools or cloud-hosted but siloed segmentation tools across various elements of a hybrid architecture. **Do you need ZTS?**

☐ **YES!**

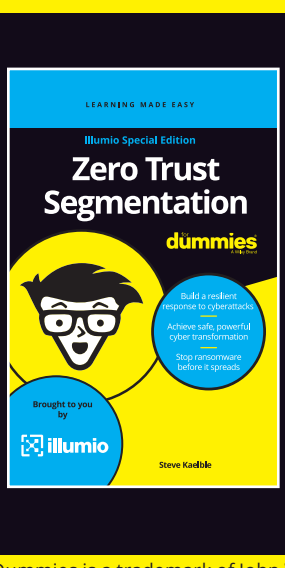
A strong ZTS solution is focused on the workload and is agnostic to the environment. Your security solution must be able to live-migrate workloads from one place to another as you scale up and effortlessly bring the enforcement along with it.

Thinking Ahead

In those simpler times (not all that many years ago, actually), it was easier to protect the network. But these days your IT and operational technology (OT) are moving in together. Are they safe enough? **Do you need ZTS?**

☐ **YES!**

ZTS protects not just the network but the assets across it. It provides visibility into, dependency mapping of, and asset-based segmentation for, everything that's converging to move your organization forward. That includes not just IT systems but manufacturing technology, healthcare telemetry devices, and powerful gadgetry along the supply chain or utility infrastructure.



To learn more about stopping the spread of ransomware and breaches, try *Zero Trust Segmentation For Dummies*.

READ THE E-BOOK

illumio

for dummies®
A Wiley Brand

For Dummies is a trademark of John Wiley & Sons, Inc.
All other trademarks are the property of their respective owners.

Wiley part no.: 9781394181728