LEARNING MADE EASY

Introducing Zero Trust Segmentation

Illumio Edition

Like it or not, your business can't hide from cybercrime. If you haven't already, you'll be hit with a ransomware attack or some other act of cyber malfeasance sooner or later.

It's no longer realistic to think you can prevent all breaches or to hope that you can find breaches fast enough to fix them. These days, although your security goals should still include prevention and detection, they must go much further — you must *assume breach* and focus on limiting and containing inevitable breaches. That's the aim of Zero Trust Segmentation (ZTS).

ZTS is a remarkably effective way to build resilience in the face of increasingly scary threats. The objective is to stop the spread of breaches that inevitably will get through even the best defenses, limiting any damage they may cause. ZTS ensures that business can go on as usual, even in the face of a successful attack.

Read on to learn some of the basics of ZTS, and find out more by getting a copy of *Zero Trust Segmentation For Dummies*.

Trusting Nothing

A *Zero Trust architecture* is pretty much what its name suggests — it doesn't implicitly trust anything. A Zero Trust architecture is harder to breach, and it also makes it harder for a successful breach to spread.

With the Zero Trust mindset, every interaction between people, workloads,

networks, data, and devices must be verified before it can proceed. The principle of *least privilege* grants devices and users only the minimum access needed to get the job done.

With least privilege, workloads are granted only the permissions they need to perform an authorized task, and nothing more. That limits the potential attack surface because any particular workload doesn't have all the keys to the castle.

Appreciating Segmentation

Much about the way our lives work today would not be possible without the many interconnections that have made the world a smaller and much more convenient place. You hear a lot about the importance of breaking down organizational walls and siloes.

That's good advice for many parts of the organization, but when it comes to IT security, tearing down all the walls isn't the best way to go. On the contrary, there are really good reasons to break larger networks into smaller pieces, sometimes as small as the host and workload itself.

This is known as *segmentation*. It's essential for helping to prevent attacks and threats from moving laterally, or as some describe it, moving east–west across data networks, clouds, or campus networks. If your network is segmented (sometimes called *microsegmented*, depending on how it's achieved), a small security incident is contained to the place where it happened, so it won't turn into a bigger security disaster.

Lateral movement is a core tactic of cyber attackers. After they step through an endpoint and get inside the network under the guise of an authorized user, hackers aim to move deeper into the system in search of sensitive data, intellectual property, or other high-value assets. Segmentation puts a stop to lateral movement.

There are a number of ways to accomplish segmentation. You can rely on the network itself or deploy hardware firewall appliances. You can also enforce segmentation on the host workload itself, which gets the job done without touching the network.

ZTS is rooted in microsegmentation, which is sometimes referred to as *host-based segmentation*. It's an approach that relies on allowlist models to block all traffic other than what's specifically permitted. That's the Zero Trust security model at work, in which nothing is trusted and everything is verified.

Microsegmentation partitions the network down as far as individual workloads, allowing you to employ Zero Trust concepts to their maximum potential to ensure those segments are protected separately.

Using Zero Trust Segmentation

There are plenty of use cases for which ZTS is an ideal solution. Ransomware containment is of ever-growing importance and is a use case where ZTS really shines. It's a key to successful incident response, allowing you to quarantine parts of the infrastructure that may be compromised and create clean bubbles within the environment.

This capability is essential for preventing the lateral spread of malicious activity and ensuring that a small breach remains small. The more effectively you can contain the damage, the shorter the road to recovery. The desire is to make your organization's architecture not just more secure but more resilient, able to recover more quickly from the inevitable attack.

ZTS is also handy for a number of other important use cases. For example:

- ZTS helps your organization safely migrate workloads from an on-premises data center to the cloud, or from one cloud location to another.
- ZTS helps ensure that neither information technology nor operational technology is overexposed as they become more integrated.
- ZTS plays an important role in ensuring that your organization follows best practices for vulnerability management, risk mitigation, path management, and other activities.
- ZTS helps forward-thinking companies pursue powerful digital transformation while remaining serious about cybersecurity resilience.
- ZTS offers visibility into and control over how software interacts with the infrastructure where it lives.

Exploring ZTS

For organizations heading down the ZTS path, one of the first tasks is to establish security objectives. Visibility is a great initial aim. It's an essential part of improving your security posture and moving from reactivity to a more proactive posture.

A careful mapping of the attack surface shows the potentially vulnerable places and documents just what makes them vulnerable. That means taking into ac-

count all potential *attack vectors*, which are the paths that attackers use to breach the network.

Most organizations will want to keep moving forward with a focus on ransomware protection. Still another key step is establishing environmental segmentation. For some organizations, the ultimate success means ensuring that every single application is properly ring-fenced.

The very first step, however, is to keep building upon your knowledge about ZTS and how it can help your organization become safer and more resilient. *Zero Trust Segmentation For Dummies*, Illumio Special Edition, fills in a lot of the details introduced in this paper.

Download the full ebook today.

ISBN: 9781394181711