Troy Thomas, Sales and Marketing Associate

https://www.leonardmcdowell.com/

# What is Zero-Trust Security?



Not too long ago, going into your office was similar to entering a fortress. Organizational data was managed from inside the premises, and security was built to defend the office and its data from outside attackers. The concept behind this is that if your attackers can't get inside your office, your data is safe and reliable.

Today, this concept has been completely changed. Cloud based service with users accessing from their mobile devices anywhere they want is what's common, and data is no longer constricted to the walls of a singular compound. Especially with the recent COVID and stay-at-home working, cloud based servers have seemingly become a necessity. However, this makes the job of hackers 100 times easier, as your data is no longer simply safe inside your office. Because of this, a new security system had to be invented to fight back against these hackers, and that is how Zero-Trust Security was conceptualized.

The Zero-Trust Concept is very easy to understand, no device that is used to log into the network is trusted by default. This means that every device that is connected to the network is

treated as a threat until proven otherwise. No matter the previous history, location, or person, all devices are to be treated the same, and they all require the same authentication.
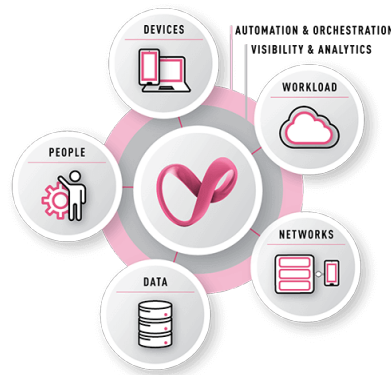


Through Zero-Trust, your network is protected through defined micro-segments that continuously check and ensure safe connections without breaches. In the event of a breach, the threat is almost immediately contained at the entry point. Not only is your Network protected, but your data is also kept safe through Zero-Trust. As your data is being transferred through servers and databases, the data itself is encrypted and practically put inside of an indestructible "bubble" allowing safe passage of data, without having to worry about hackers accessing it during its normally vulnerable transferring stage.

Zero-Trust Security is not just a concept we can fantasize about, it is the new age form of security. According to surveys, over 60% of security professionals in America have already converted to some kind of Zero-Trust System. As the world and the internet evolves, we need to be more careful and conscious about how we protect our data. Over 85% of data breaches come from stolen devices and credentials, which means the standard way of securing your data is simply not enough. When your passwords get leaked, hackers can get into your data for free, but Zero-Trust prevents all of that entirely. As more and more professionals and businesses transition to a Zero-Trust system, it's important to not let your network fall behind, and become susceptible to attackers. Convert your networks now and save yourself hours of work down the line. Contact Frank Leonard with LeonardMcDowell through phone (317-407-0642) or email (frank@leonardmcdowell.com) to set up a demo to become more involved with Zero-Trust security.