Many organisations have started their Zero Trust security journey. Even the U.S. federal government has issued an executive order mandating its agencies implement Zero Trust-based architectures. The best way to describe Zero Trust is the first way it was defined in 2010 by John Kindervag, the “father of Zero Trust.”

“There is a simple philosophy at the core of Zero Trust. Security professionals must stop trusting packets as if they were people. Instead, they must eliminate the idea of a trusted network (usually the internal network) and an untrusted network (external networks). In Zero Trust, all network traffic is untrusted.”

To help you suss out Zero Trust facts from fiction, here’s a Zero BS cheat sheet.

**THE “CLAIM”**

**BS? TRUE OR FALSE?**

- **Zero Trust is a mindset. It can’t be bought.** TRUE. The National Institute of Standards and Technology (NIST) defines it as “a set of guiding principles for workflow, system design and operations.”

- **Zero Trust is a multi-year journey.** TRUE. There are varying degrees of Zero Trust maturity and every organisation is different. Built there are a few rules of thumb. First, think long-term. You don’t need to “rip and replace” your entire architecture. You can anticipate future requirements before starting.

- **Zero Trust requires that we scrap existing investments.** FALSE. Zero Trust is a mindset and philosophy. Many modern tools that enable ZT maturity work with existing investments to improve them while eliminating security silos.

- **VPNs are built on the principles of Zero Trust.** FALSE. VPNs were built in 1996 as a remote connectivity tool. They were never designed to address the core principles of Zero Trust.

- **Zero Trust means I shouldn’t trust anyone, not even my employees.** FALSE. Zero Trust’s default isn’t inherent or implicit trust. It means the ability to extensively verify identities, establish trust in the context of your request and grant access to limited resources based on privileges and risk posture.

- **Zero Trust is difficult and expensive.** TRUE. Many vendors claim “Zero Trust” without the technology chops to back it up. That’s why we say, “Zero Trust. Zero BS.” Implementing multi-factor authentication achieves Zero Trust. FALSE. Implementing MFA is just a single (yet critical) part of any Zero Trust journey.

- **Zero Trust benefits the whole business, not just security.** TRUE. Zero Trust solutions can, and should be, built into the fabric of the organisation and its workflows in order to remove security roadblocks and improve business velocity.

- **I can’t achieve true Zero Trust with legacy IT architecture.** FALSE. Zero Trust is a journey. You can build a Zero Trust architecture that overlays or sits alongside legacy architecture or infrastructure that you can gradually phase out over time. Approach it incrementally with individual use cases while keeping the end goal in sight.

- **Implementing multi-factor authentication achieves Zero Trust.** FALSE. Implementing MFA is not a single (yet critical) part of any Zero Trust journey.

- **Zero Trust is a technology problem.** FALSE. Zero Trust is much more than a technology solution. It’s a mindset shift to transformation, efficiency and productivity gains. In addition to buy-in from IT and the C-suite, it requires a multi-year evolutionary process that new technology, like Zero Trust Network Access, can jump-start.

**KEY TAKEAWAY**

At its core, Zero Trust security is a framework that, for many, starts with secure access. When implemented properly, an architecture built with Zero Trust security principles in mind has the power to yield benefits beyond IT. For example, Appgate SDP, our Zero Trust Network Access solution:

- Starts where you are in your technology and transformation journey
- Accelerates your organisation’s path forward by eliminating complexity
- Protects your organisation’s future—from the tangible (your actual network, assets and technology) to the intangible (your organisation’s goals and growth strategies)

If you want a BS-free Zero Trust conversation, pick a convenient time to attend one of our weekly live democasts by registering here.