WHY ZERO TRUST SECURITY MATTERS FOR SMBs

According to NIST, "Zero Trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets and resources. Zero Trust assumes there is no implicit trust granted." In simple terms, treat all networks as malicious and grant access only to verified users and devices.

Implementing Zero Trust Security within your business can help guard against data breaches, down-time, productivity loss, customer churn and reputational damage.

Over 70% of businesses planned deployment of Zero Trust in 2020 and it is even more important for SMBs in an era where workforces and networks are becoming increasingly distributed. [1]

COMMON MISCONCEPTIONS & TRUTHS

MISCONCEPTION #1:
Zero Trust Security is only for enterprises

TRUTH: The Zero Trust cybersecurity framework is a proven counter-threat strategy, and SMBs need to protect sensitive data and networks by taking measures to minimize internal and external vulnerabilities.

MISCONCEPTION #2:
It's too complex

TRUTH: By applying Zero Trust concepts at a scale that makes sense for your business, you'll realize it isn't as complex as you thought.

MISCONCEPTION #3:
The cost of implementing Zero Trust is too high

TRUTH: Focusing on your most critical applications and data sets first makes Zero Trust adoption operationally and economically feasible.

FIVE ZERO TRUST CYBERSECURITY ARCHITECTURE ASSUMPTIONS