COSMOS®
Navigate the Compliance Universe

# Report on Supply Chain Compliance Volume 2, Number 22. November 21, 2019
# Zero access replacing virtual private networks as organizations seek greater data security

By Sascha Matuszak

After a year in which cloud cybersecurity reached the mainstream consciousness through high-profile data breaches at Marriott and British Airways, organizations are looking to new methods to secure their networks. A solution that is gaining some traction in the cybersecurity world is zero trust network access (ZTNA).

The basic idea is that the network is completely sealed off from outside users and the internet, and only accessible by network operators with proper authentication. This seems like a simple concept—something that should have been the case from the start—but the reality is that most networks, cloud-based or not, involve giving outside users access to compartmentalized nodes within the overall network. Most of the data breaches that we have seen involve situations where those nodes proved to be less than secure, and hackers were able to breach the internal network.

The difference between ZTNA and the traditional method of hosting networks on private virtual private network (VPN) servers goes deeper than just how or where the user gains access.