The Top 8 Reasons to Switch to **Zero Trust Network Access**

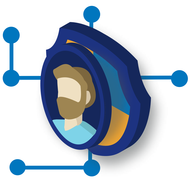
More organizations are moving away from traditional network access and looking to a zero trust network access (ZTNA) model. Why? Well, here are the top 8 benefits of ZTNA:

1 No need for legacy appliances

ZTNA allows organizations to rid themselves of legacy remote access appliances, such as VPNs, and leverage a 100-percent software-based access solution.

2 Seamless user experience

With ZTNA, user traffic isn't backhauled through the datacenter. Instead, users get fast, direct access to the desired application.



3 Supports all private apps

ZTNA was designed to support all types of internal apps, whether in the cloud or the datacenter. Regardless of an app's location, ZTNA requires no additional infrastructure or configuration by IT.

4 Effortless scale

A cloud ZTNA service makes scaling capacity easy. An organization just leverages additional licenses.

5 Infrastructure is invisible

ZTNA allows users to access applications without connecting them to the corporate network. This eliminates risk to the network while keeping infrastructure completely invisible.

6 Achieve app segmentation

Since ZTNA isn't tied to the network, organizations can segment access down to individual applications rather than having to perform complex network segmentation.

7 More control and visibility

Managing ZTNA solutions is easy with a centralized admin portal with granular controls. See all users and application activity in realtime and create access policies for user groups or individual users.

8 Fast deployment

Unlike other solutions that can take weeks to months to deploy, ZTNA can be deployed from anywhere and in a matter of days.

But don't just take our word for it. Check out what Gartner has to say about ZTNA. Or read this ZTNA adoption report from Cybersecurity Insiders.