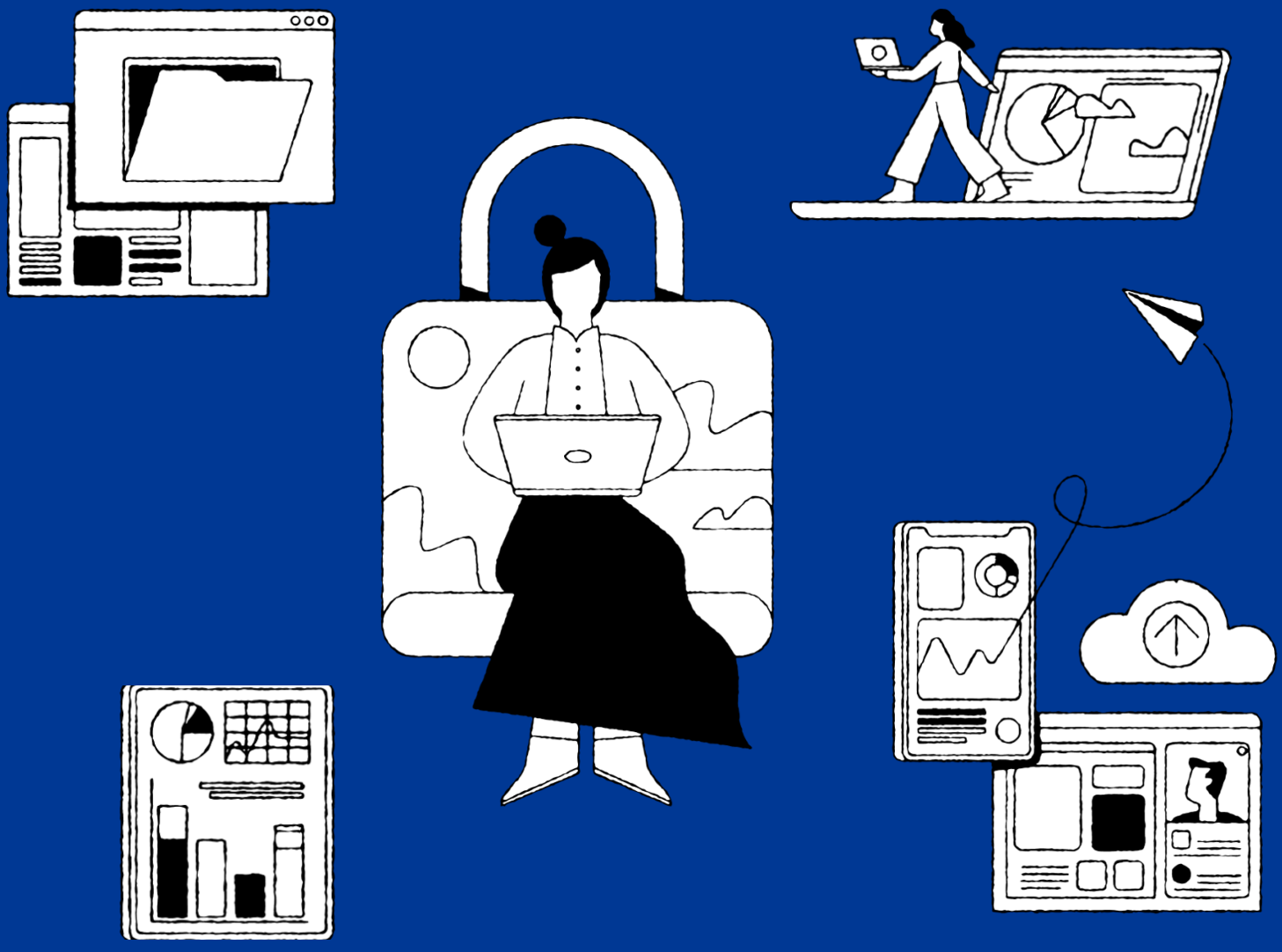
citrix

Evaluating ZTNA vendors for the best customer experience

With more organizations looking for a ZTNA solution, it's a good time to explore the features your channel services company should expect from a vender partner. Choosing the right ZTNA vendor can be a complicated process, but studying the offerings on the market and the capabilities of the latest technology is the first step.



White Paper

Zero trust network access (ZTNA) has been a watchword in digital security for years. Recently, the technology reached a tipping point. Two parallel trends have increased the importance of using ZTNA to connect users with companies' digital resources. First, ongoing development has made ZTNA solutions more affordable and feature-packed. Second, greater use of remote and hybrid work models has necessitated that businesses have versatile, secure ways to support employees outside of the office walls.

Now, with more organizations looking for a ZTNA solution, it's a good time to explore the features your channel services company should expect from a vender partner. Choosing the right ZTNA vendor can be a complicated process, but studying the offerings on the market and the capabilities of the latest technology is the first step.

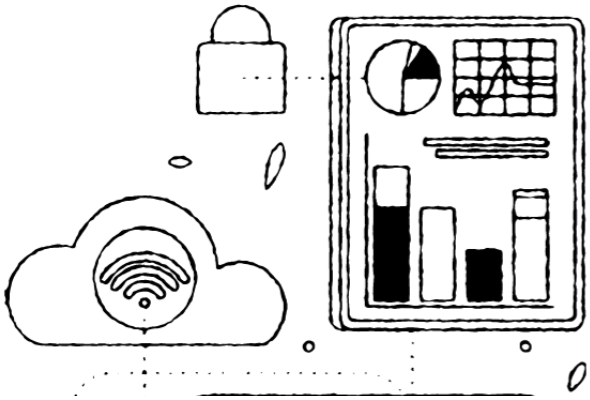
The State of ZTNA Today

Before comparing the in-depth features offered by ZTNA vendors, let's quickly talk about the general state of ZTNA offerings.

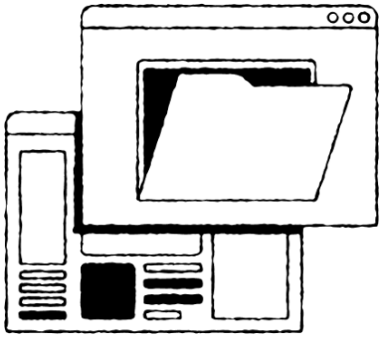
The core concept behind all zero trust network access solutions is that they represent a way to verify (and re-verify) the identity of remote users requesting access to applications, files, and other network assets. This is a contrast to other methodologies that grant continuous access after a user has entered credentials such as a password.

In its 2022 Gartner® Market Guide for Zero Trust Network Access, the research company notes that the ZTNA market was once seen merely as an alternative to virtual private network (VPN) offerings. Now, however, companies are seeing the unique security value of zero trust access. Using ZTNA creates a smaller attack surface because access control is based on denying entry unless a user is authorized and appears safe at that moment, rather than giving blanket access and implicit trust to someone with the password. Furthermore, ZTNA does not require exposing resources to the internet, removing another potential attack vector.

Gartner sees the ZTNA application market growing at a year-over-year rate of 60 percent. The report notes, however, that ZTNA loses some of its appeal as an isolated solution. Increasingly, companies will use zero trust networking as a component of an overarching secure services edge security posture. Channel partners should be ready to offer that integrated security layer, starting with the right ZTNA offering.



ZTNA Vendors: Features to Look For



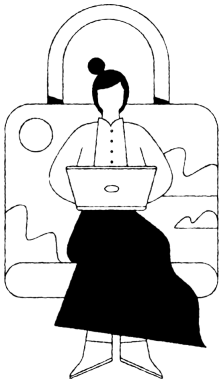
As part of Gartner's research into the landscape of ZTNA providers, the research firm pulled out several of the pros and cons of various vendors. Let's walk through a few of the capabilities ZTNA vendors can offer, along with some details on how and why these features will help you better serve your customers.

In-house security and monitoring operations

Since the infrastructure underlying a ZTNA solution is responsible for keeping your company's connections safe, it's natural to have some questions about how these systems are observed and monitored. Gartner asserts that companies should favor vendors that have their own teams assigned to keep up security protocols and watch for any sign of integrity issues.

High-performance SLAs to limit service disruption

As with any software, a ZTNA vendor's service license agreements (SLAs) have a role to play in reliability and uptime. It's worth checking on the SLAs for the vendor before signing the dotted line. You don't want to deal with downtime that hamper your customers' ability to use their ZTNA solution.



Reliable trust broker access

The connection between a ZTNA system and its trust broker solution should enable quick access to prevent excess latency. Vendors with large amounts of points of presence (PoPs) distributed around the world may be best suited to create high-redundancy, low-latency connections for all users.

Trust broker failover capabilities

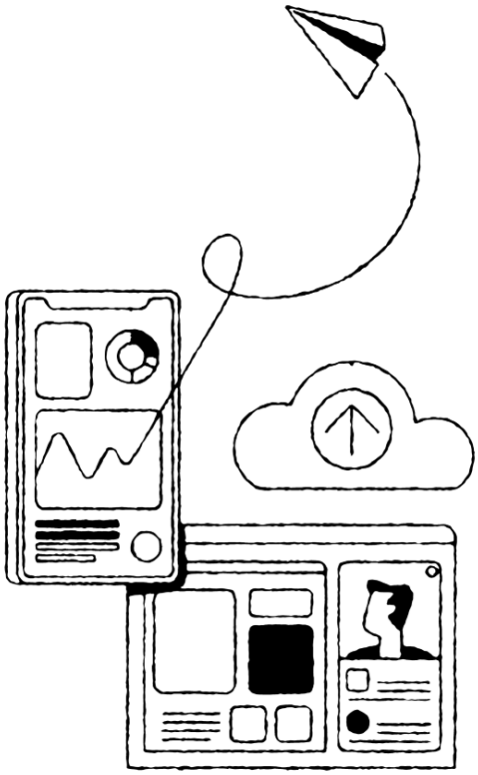
What happens when a trust broker's tenant isolation fails and an attacker threatens that system? Ideally, the trust broker switches to a redundant system, or at least shuts down entirely and disconnects. These are capabilities to look for in a ZTNA vendor, to defend against rare cases when hackers make a successful attack on the trust broker.

Strong administrator authentication requirements

Just because a ZTNA solution is an advanced approach to security, that doesn't mean it has no possible attack surface. Administrator accounts can cause harm if compromised, so it pays to find a vendor that employs strong authentication for admin access.

Support for the DTLS protocol

The datagram transport layer security (DTLS) protocol is one method of protecting information during digital communications. In a ZTNA context, it's especially important as an enabler of real-time communication applications. Gartner recommends finding a vendor that does employ DTLS if your customers want to use these real-time solutions via ZTNA.



Types of applications supported

Do your customers plan to run legacy on-premises applications through ZTNA? If so, this is something to consider during ZTNA vendor selection. Some ZTNA providers only support HTTP and HTTPS web applications, making it difficult to use legacy apps via their solutions.

Considering this list of ZTNA characteristics when researching the right security platform to fully enable your channel services business to best serve your particular customer base.

Download the Gartner report to compare the pros and cons of various ZTNA approaches
https://cit-rx.com/3KBia5E

Learn more about Citrix ZTNA
citrix.com/solutions/zero-trust-network-access