netskope +

eBook +

5 Key Considerations for Selecting a Zero Trust Network Access Solution

5 Key Considerations for Selecting a Zero Trust Network Access Solution

Enterprises are rapidly adopting security service edge (SSE) to enable security transformation in the modern cloud and hybrid work era.

A critical piece of SSE is a zero trust network access (ZTNA) Solution. As a remote access VPN replacement, ZTNA enables application-specific connectivity for users anywhere. Security Service Edge supports the consolidation of security functions, a lower total cost of ownership, and improves operational efficiency in the long term, leading to better overall security.

01

Platform matters

Platform matters

Whether you are selecting and implementing ZTNA to replace remote access VPN, as an initial project on a zero trust security journey, or you have a fully mapped out vision for SSE and SASE, it is best to work with a vendor with a full SSE platform: a single agent, single console, and single policy engine, with support for a multi-cloud environment.

Gartner estimates that “By 2025, 70% of organizations that implement agent-based zero trust network access (ZTNA) will choose a security service edge (SSE) provider for ZTNA, rather than a stand-alone offering, up from 20% in 2021.”*

*Gartner,“Magic Quadrant for Security Service Edge,” John Watts, Craig Lawson, Charlie Winckless, Aaron McQuaid, February 15, 2022

02

Enable hybrid work anywhere

To enable hybrid work from anywhere, it's important to select a vendor that has a footprint that can match your global expansion plan and enterprise agility. Ensure you work with a ZTNA provider that has data centers in all major geographic locations where your employees may be connecting from.

Your vendor selection should not solely be based on counting data centers but choosing one that has the full security stack available in every region—with full compute at the edge close to your users—with low-latency on-ramps combined with extensive peering for the best user and application experience.

03

Easy-to-set policy

In addition to a single agent, there should be only one step required to configure identity and access policies using a unified console. You will gain the benefit of enabling access to cloud and private applications in days to support M&A and other time-sensitive activities.

If your goal is to replace legacy remote access VPN, don't get stuck with an application VPN and complex firewall rules masquerading as true ZTNA.

04

Protect data everywhere

Your ZTNA solution should detect data usage, activities and behavior anomalies (UEBA), enforce advanced DLP rules and policies, and apply adaptive access policy based on user risks.

ZTNA securely connects users to private applications and resources. Often these resources are the crown jewel of the organization, from code to other forms of proprietary data such as trade secrets. Select a solution that provides multiple options to help your organization protect the information. For example, a modern ZTNA solution should provide the options to inspect traffic and apply DLP to protect data. However some organizations may prefer UEBA and user risk ratings to gain real-time context without decrypting traffic and to minimize insider risk.

05

Effective third-party integration

With the right integrations and exchanges in multi-vendor environments, ZTNA can thrive. The best exchanges offer user and device trust scores that are normalized across the environment and can trigger adaptive access controls, user group settings, and automated ticketing for investigation.

Conclusion

Remember that zero trust does NOT mean trust no one, because in order to enable business, you have to extend access (trust). The key to leveraging zero trust principles across your organization, whether specifically with ZTNA or otherwise, is to use technology to make better, context-aware decisions about trust and access for a given user and to continuously monitor and adapt to mitigate risks. This context is based on a number of factors, such as user role and identity, device identity, security posture, app type, app risk, and app instance, plus the sensitivity level of the data. Contextual decisions result in robust access policies that are risk-optimized, and can uniformly be applied across the cloud, web, and private apps, while enabling business agility and user productivity.