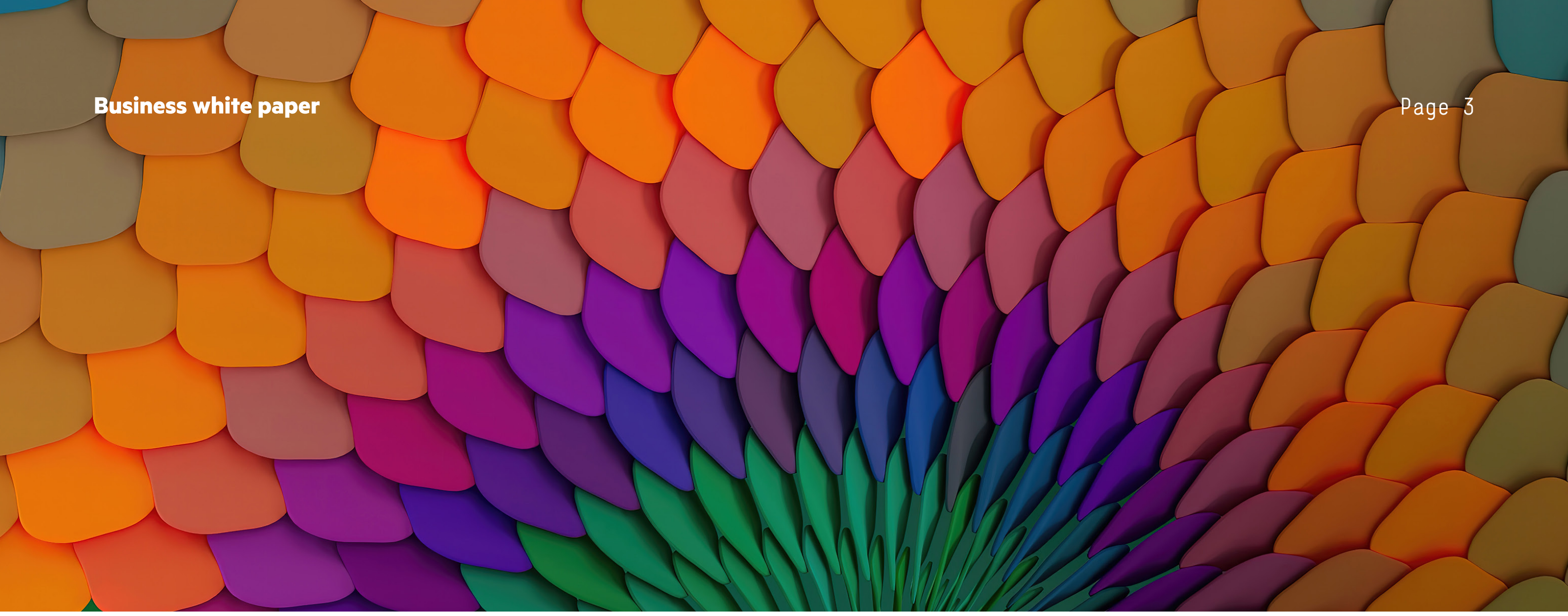
Business white paper

Making the switch from VPN to ZTNA

The benefits of ZTNA and where to start

Table of contents



60%

of organizations will be replacing their VPN with a ZTNA service

The advent of remote work has brought about new security challenges for organizations. With an increasing number of employees working from everywhere, organizations must find ways to secure remote and hybrid access to their networks and data. One solution that has traditionally been used is the Virtual Private Network (VPN). However, as cyber threats continue to evolve, VPNs have proven to be inadequate in protecting against modern threats. Zero Trust Network Access (ZTNA) is a more effective solution for securing remote access.

What is ZTNA?

Created in April of 2019 by Gartner, the term Zero Trust Network Access (ZTNA) represents a set of new technologies designed for secure access to private applications. ZTNA uses granular access policies to connect authorized users to specific applications, without granting network access, enabling segmented least-privileged access, while never exposing app locations to the internet like VPNs.

Gartner expects that by 2023, 60% of organizations will be replacing their VPN with a ZTNA service. This has led ZTNA to become the fastest growing zero trust product in the industry, with 44% of IT leaders making ZTNA the starting point for those looking to adopt a Security Service Edge (SSE) platform as part of a greater Secure Access Service Edge (SASE) framework.

ZTNA improves security

One of the main reasons businesses are adopting ZTNA is because of the improved security it provides. With a VPN, users are brought directly onto the corporate network. Once a user gains access to the network, they can move laterally and potentially access sensitive data or resources. It's no wonder that "granting users too much trust" has been found to be the biggest challenge with existing secure access solutions according to the 2024 SSE Adoption Report. While you could say this matters less for internal users, however, it's a daunting thought knowing an attacker would benefit from the lack of segmentation.

In contrast, ZTNA never extends network access and grants access based on context: the identity of the user, the device they are using, and the application and data they are trying to access. This means that even if an attacker attempts to gain access to the network, not only will they not be able to access sensitive data without proper authentication, but the ZTNA service will cloak the very existence of the network, making it invisible and untraceable.

ZTNA solutions are typically less expensive to implement and maintain than VPN solutions. The cost of VPN goes far beyond the simple cost of the box.

ZTNA increases scale and flexibility

Another reason businesses are adopting ZTNA is because of the increased scale and flexibility it provides. While VPN solutions are generally hardware and appliance-based, ZTNA solutions are cloud-delivered meaning that they can be easily accessed by users and managed by IT from any location. This is particularly useful for businesses with employees who are hybrid/ remote or need to access resources from different locations. While VPNs have static capacity limits based on appliance size, the nature of ZTNA's cloud-delivered architecture allows businesses to easily be scaled up or down to meet the evolving needs of a business.

More importantly, ZTNA services provide hyper-granular and flexible access control policies that can be applied down to the user and application level. Access segmentation with VPN means complex network segmentation, but with ZTNA, implementing least-privilege access is as simple as a policy adjustment.

ZTNA enables better productivity

ZTNA solutions provide a better access experience than VPNs. VPNs cut into business productivity as users are left to deal with slow connection speeds (due to VPN backhaul), inconvenient and constant disconnections, and complex and repetitive logins. All of which disrupt users work and create frustration.

ZTNA, on the other hand, provides a more user-friendly experience for end-users. It enables end-users to easily access private apps by eliminating traffic backhaul, remaining always-on even through network changes, and creating seamless login process with deep integrations with SSO and other identity management solutions.

ZTNA is more cost-effective

ZTNA solutions are typically less expensive to implement and maintain than VPN solutions. The cost of VPN goes far beyond the simple cost of the box. In addition to VPN concentrators, VPNs require expensive on-premises hardware, such as DDoS protection, internal and external Firewalls, load balancers, etc. All this is for a single inbound security stack (organizations have 3–5 on average). On top of that, security teams usually require one or more personnel to be dedicated to the monitoring and management of VPN. This takes resources away from other, more urgent and important projects. Maintaining this perimeter-centric approach to secure access is costly to maintain.

In contrast, ZTNA solutions do not require expensive hardware or software to be installed and maintained on-premises. Further, organizations want SSE platforms to eliminate the need for VPN concentrators (66%), SSL inspection (37%), anti-virus (36%), and DDoS protection (44%). In fact, the best SSE platforms offer ZTNA technologies that completely eliminate VPN and the inbound security stack resulting in massive cost savings. ZTNA is also intuitive and easy to manage, allowing organizations to dramatically cut down the number of resources and teammates needed to manage secure access. Lastly, ZTNA solutions leverage a subscription based pricing model which gives transparency to costs and means organizations aren't overpaying for licenses.

Don't let VPN hold you back

As the number of remote and hybrid workers continues to grow, it's crucial for companies to have a modern secure access solution in place. ZTNA is a modern solution that addresses the limitations of VPNs and provides enhanced security, flexibility, scalability, performance, and cost-effectiveness for remote access.

The best part about ZTNA is that it's part of a greater security strategy. As organizations look to embrace a Security Service Edge (SSE) platform we see that the majority are beginning with ZTNA adoption. Where will you begin?

Fully replace VPN with HPE Aruba Networking

Learn more about using HPE Aruba Networking as a VPN alternative

Check out the HPE Aruba Networking SSE platform

arubanetworks.com/products/sse

Make the right purchase decision.
Contact our presales specialists.

Chat now (sales)

☎ **Call now**

Visit **ArubaNetworks.com**

Get updates

Hewlett Packard Enterprise