Business white paper

The architect’s guide to VPN replacement

Old technology in a new world

Over the last few years, the work environment has changed dramatically. The landscape was already starting to shift with the invention and growth of the cloud, but the COVID-19 pandemic dramatically increased remote work.

This changed how we think about our architectural designs. Our users are no longer protected by a perimeter wall. The workforce is everywhere. And not only that, but the applications they need to access daily are now distributed between SaaS, on-premise, and IaaS locations.

Today, teams must support secure connectivity to both internal and external applications for a user base that can be located anywhere. Architects must support secure access to all legacy applications and also consider what application access will look like in the future.

The new world of cloud and mobility changes how we connect and also how we secure that connectivity. And legacy solutions, like traditional VPN, don't adequately address today's needs. Many organizations are replacing their VPN with a modern technology found within many Security Service Edge (SSE) platforms known as Zero Trust Network Access (ZTNA).

What is SSE and where does ZTNA fit?

SSE is part of the larger Secure Access Service Edge (SASE) framework, which Gartner® introduced in 2019. When remote work skyrocketed during the pandemic in 2021, Gartner® introduced SSE.

The SSE framework is a collection of integrated, cloud-centric security capabilities that facilitate safe access to private applications, software-as-a-service (SaaS) applications, and the internet with the following technologies: Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Secure Web Gateway (SWG).

- **ZTNA** gives Zero Trust access to private applications.
- **CASB** secures access to all SaaS-based applications.
- **SWG** ensures all access to the internet is secure.

An SSE platform should provide a single unified platform for all application access while decoupling application access from the corporate network. It should serve as an overlay on the existing network, allowing IT to modernize and simplify connectivity while strengthening security, without having to make complex network architecture changes.

Because an SSE platform consists of several core technologies that can be implemented independently, where do you start? How should you adopt SSE? The answer to this question is the same as with any security project or initiative: the areas of highest risk. In the new world of distributed applications and users, the place to start is by replacing your VPN technology and securing access to your private applications with ZTNA.

> **“By 2025, at least 70% of new remote access deployments will be served predominantly by ZTNA as opposed to VPN services.”**
>
> — **Gartner® Forecast Analysis:** Information Security and Risk Management, Worldwide, September 2022

ZTNA as an alternative to VPN

As teams navigate the complexities of securing remote work environments, ZTNA offers a compelling alternative to traditional VPNs. ZTNA addresses many of the limitations of traditional VPNs and provides the following benefits for modern enterprises.

Security

- **VPN challenge:** VPNs expose networks to threats like malware, ransomware, and DDoS attacks by exposing network IPs—allow attackers to access the entire network.
- **ZTNA solution:** ZTNA minimizes the risk of internet-based attacks by hiding private resources from the internet. Outbound-only connections ake your network and applications invisible and untraceable, while users are never given network access. Additionally, access is granted based on dynamic user identity, device, and data context—effectively preventing unauthorized lateral movement.

Scale and flexibility

- **VPN challenge:** Because VPNs are physical appliances, scaling infrastructure can be painful and challenging. As the mobile workforce grows, many organizations must significantly scale their investment in VPN infrastructure to support more connections and handle increased traffic.
- **ZTNA solution:** ZTNA’s cloud architecture allows for easy scaling and centralized remote access management. Zero Trust policies can be tailored to user and application levels and enforced globally in seconds.

Productivity

- **VPN challenge:** Because traffic is backhauled through the corporate network, VPNs can hinder connection speeds and application performance, leading to productivity loss and increased IT workloads for managing access.
- **ZTNA solution:** ZTNA optimizes user experience by bringing access as close to the user as possible through global cloud edge locations, which automatically routes traffic on the fastest access path. ZTNA eliminates VPN-related slowdowns, disconnections, and login hassles while integrating seamlessly with SSO and identity management systems.

Cost

- **VPN challenge:** VPNs incur high costs due to the need for expensive on-premises hardware and dedicated personnel for monitoring and management, not to mention the need for the extended inbound security stack to minimize the risk of VPN-related attacks.
- **ZTNA solution:** ZTNA eliminates the costs associated with traditional VPN hardware, DDoS protection, and firewalls and simplifies monitoring—freeing up resources for other critical projects.

Start your SSE journey with ZTNA

ZTNA has evolved beyond the confines of mere remote access; it has become a fundamental concept for application access as a whole. It's not just a gateway. It's a transformative approach that paves the way to a broader, more comprehensive vision. ZTNA is a single, cloud-delivered service that addresses all your access requirements.

Choose where to start

When implementing ZTNA, it's crucial to pinpoint the driving force behind the decision. Is the primary goal to enhance security, streamline user experience, or save money? Understanding the underlying motivation will guide you in selecting the most appropriate starting point for your ZTNA journey.

> **"By the end of 2024, the change in the nature of work will drive up the total remote worker market to 60% of all employees, up from 52% in 2020."**
>
> — **Gartner® Forecast Analysis:** Information Security and Risk Management, Worldwide, September 2022

If **security** is your priority, identify the area with the highest risk and focus on secure access solutions for specific groups like third-party users or employees. If the goal is to **improve user experience**, pinpoint the user groups suffering from poor access (such as executives or remote workers) and enhance their access to private apps. If **cost savings** is the objective, analyze which legacy technologies are the most expensive (such as VPNs) and consider how ZTNA can replace them.

ZTNA use cases

Deciding on the initial use case can be a daunting task. To assist you, we've identified three predominant use cases. The following sections describe these scenarios and their the seamless integration of ZTNA.

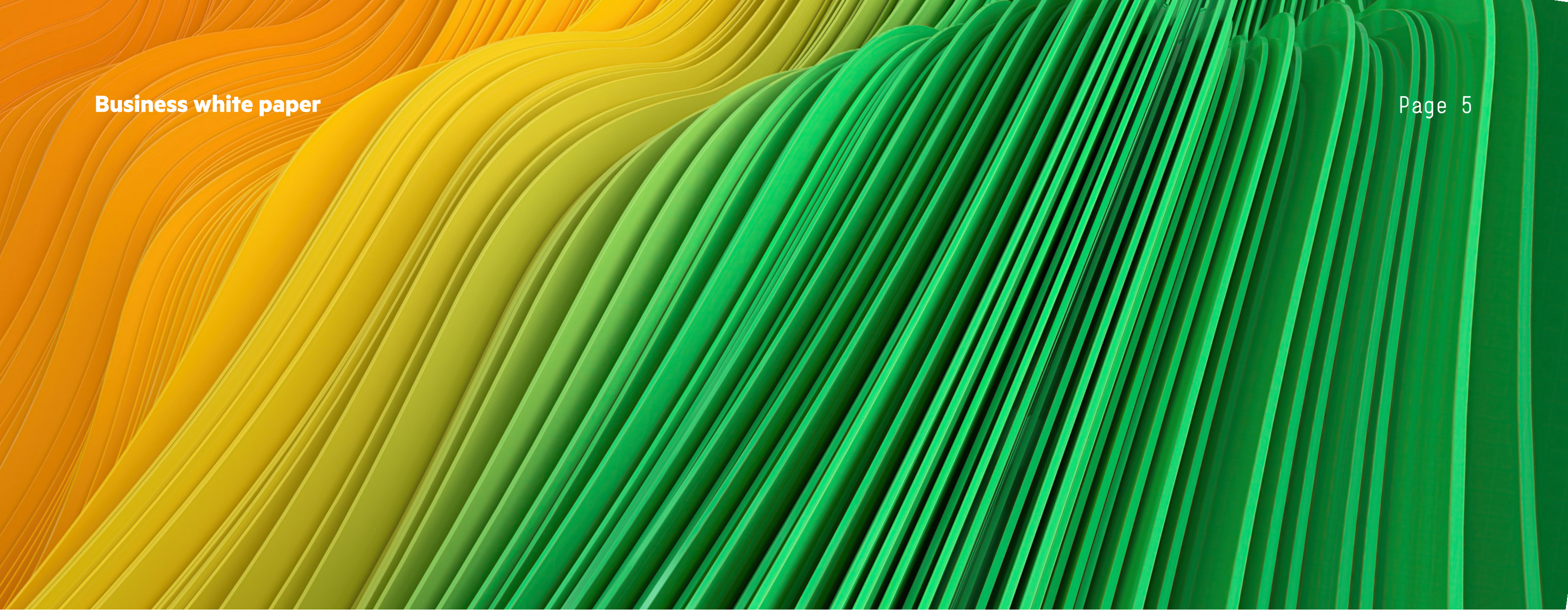
Secure remote & hybrid access for employees

In the mobile world, traditional VPNs struggle to keep pace. While VPNs were once pivotal in facilitating remote access for employees, they now pose significant security risks in terms of connectivity. With today's workforce operating from home, the office, or any transitional space, it's crucial to maintain a consistent, unobtrusive Zero Trust access approach.

The below diagram shows how ZTNA technology replaces outdated VPN frameworks traditionally housed in data centers. ZTNA acts as an intermediary between the user and the application, granting access only to authorized users and sanctioned applications, irrespective of their location—whether on-premises or in the public cloud.

This is achieved through a lightweight application connector sitting within the application's environment, only allowing access if it meets contextual requirements. After criteria is met, an outbound connection is established, which ensures users are not placed directly on the network and are granted access to the designated authorized application only.

Additionally, transitioning from remote to in-office access does not affect the user experience, as ZTNA operates seamlessly in the background. It even safeguards the network by preventing access from potentially compromised devices while on company premises.



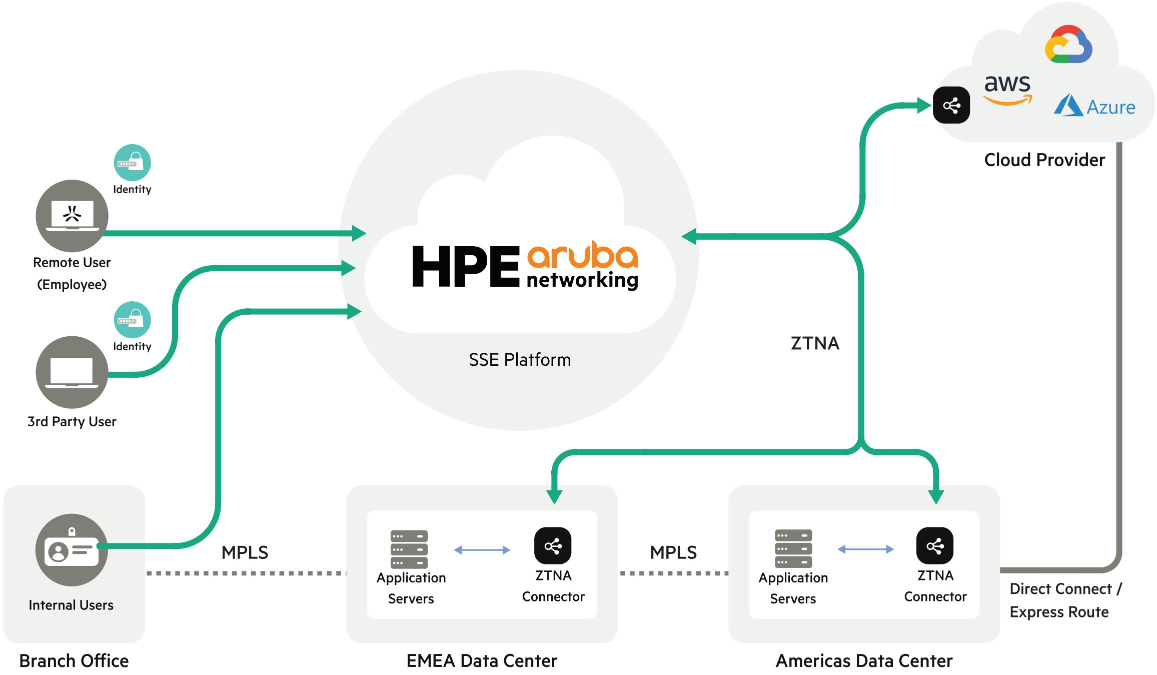


Figure 1. Secure remote and hybrid access

Secure third-party & BYOD access

Traditionally, third-party access relied on remote access VPN technology. Users had to install a client, wait for manual updates to ACL and FW policies by an admin, and then attempt to connect. Successful connections granted access to sensitive assets, greatly exposing the network to risk. VPN extends network access to untrusted users on untrusted devices from untrusted networks, and once a third-party user is on the network, they can often freely access the entire network.

ZTNA overcomes the risks of this approach with its outbound-only connections. ZTNA conceals network infrastructure, business applications, and third-party portals from the Internet—safeguarding them against location discovery and DDoS attacks, as they can't be found by inbound probes. Private applications and third-party portals are securely tucked behind an application connector, which only permits traffic via the ZTNA cloud.

ZTNA also enables the enforcement of least-privilege access policies, even for third-party BYOD users. Seamless integrations with all major SSO solutions facilitate a smooth access experience to private applications through a simple web browser, without compromising security.

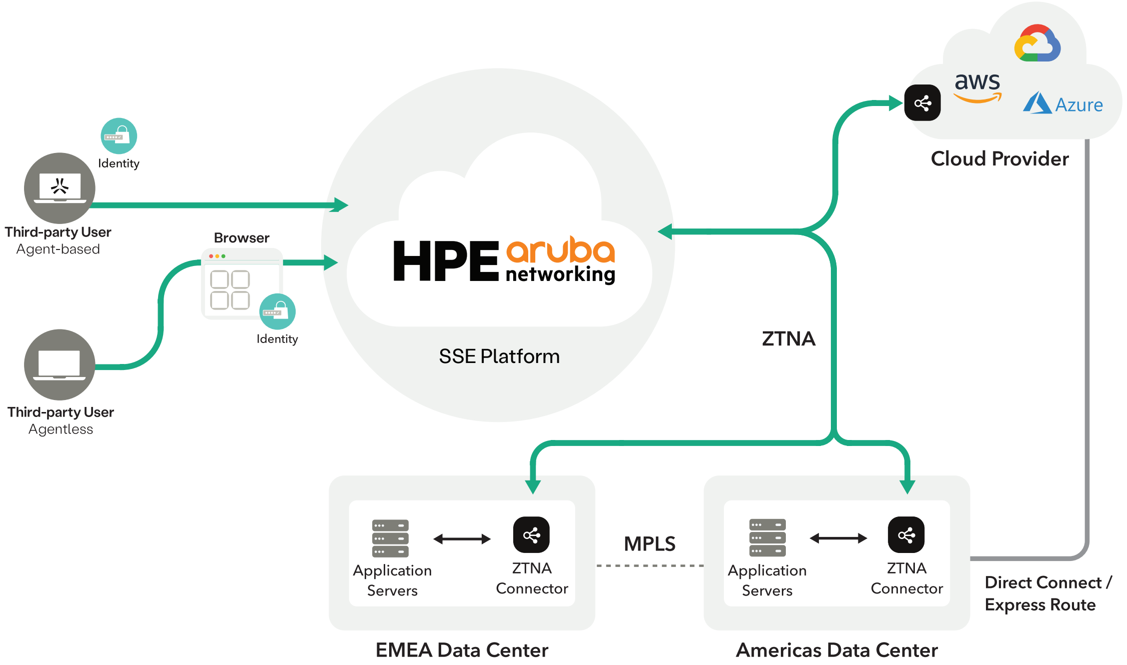


Figure 2. Secure third-party and BYOD access

Accelerate mergers & acquisitions

Mergers and acquisitions (M&A) present complex challenges, but ZTNA offers a streamlined solution for immediate access to critical applications from day one. This approach eliminates the need for VPNs, network integration, or infrastructure changes. The strategy hinges on a predefined list of essential applications—such as HR systems, ERP, and other web-based tools—accessible via the SSE platform.

ZTNA includes a robust identity strategy, ensuring users can securely authenticate and access applications, even before the consolidation of directories, users, and groups across merging entities. The SSE platform integrates with various identity providers—crucial for fulfilling the diverse application access needs of all users.

ZTNA's agentless capabilities expedite the M&A process by providing users with secure, browser-based Zero Trust access—significantly accelerating integration timelines.

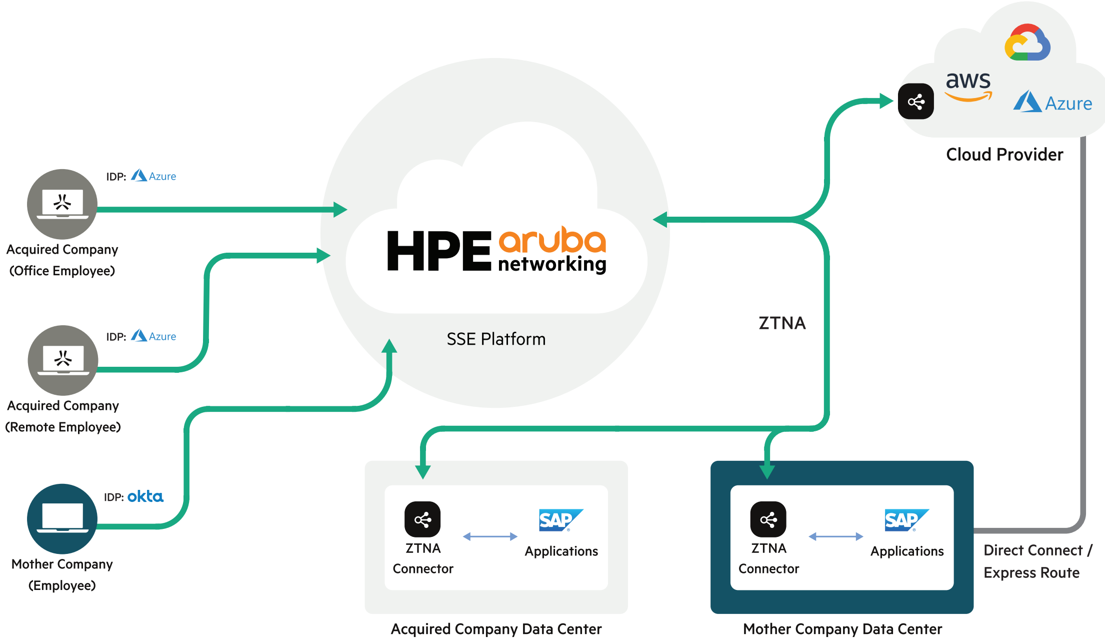

IDP: Azure
Acquired Company (Office Employee)
IDP: Azure
Acquired Company (Remote Employee)
IDP: okta
Mother Company (Employee)
HPE aruba networking
SSE Platform
ZTNA
aws
Azure
Cloud Provider
ZTNA Connector
SAP
Applications
Acquired Company Data Center
ZTNA Connector
SAP
Applications
Mother Company Data Center
Direct Connect / Express Route

Figure 3. Accelerate mergers & acquisitions

HPE Aruba Networking ZTNA: the ultimate VPN replacement

Starting your SSE journey doesn't have to be hard. Our SSE experts are here to help. Here are just a few reasons why teams like yours have chosen to partner with HPE Aruba Networking for their SSE journey and beyond.

- **Total VPN replacement:** HPE Aruba Networking ZTNA surpasses the market with its extensive support for private applications. It manages all TCP/UDP traffic, including VOIP and peer-to-peer, and is compatible with modern web apps like SSH, RDP, Git, and databases.
- **Least-privilege access without segmentation:** Without requiring complex network segmentation, our ZTNA service restricts access to specific resources, reducing the attack surface and preventing unauthorized network traversal.
- **Flexible agent or agentless access:** Users can access applications seamlessly from any device, with or without a client. Our clientless option facilitates browser-based RDP sessions, eliminating the need for VDI.
- **Granular traffic inspection:** Obtain detailed visibility into private resource traffic. Track user actions, file downloads, and command usage—and block harmful activities.
- **Adaptive access controls:** Our API-driven controls adjust access rights based on user location, identity, and device status—enhancing data security.
- **100% cloud architecture:** With HPE Aruba Networking SSE, connections are managed through the best SSE edge location, ensuring consistent uptime without the need for VPN appliance management.

Get started with HPE Aruba Networking ZTNA

Evaluate your specific use case needs and contact our seasoned professionals to pinpoint the areas where ZTNA can deliver significant benefits for your organization. Begin fortifying your most critical applications with our cutting-edge security solutions today.

Learn more

Contact an SSE expert

Test Drive ZTNA free for 24 hours

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

Hewlett Packard
Enterprise