HPE aruba networking

VANDIS

VPN vs. ZTNA Checklist

For decades, VPNs have been a steadfast technology for remote access for the business, a digital drawbridge to the corporate castle. Yet, with applications migrating to the cloud and users now mobile, VPN technology finds itself outpaced as both security and experience leave the business wanting for more.

Replace your VPN with a modern technology, Zero Trust Network Access (ZTNA). See why many organizations are turning to ZTNA as a VPN alternative.

Security

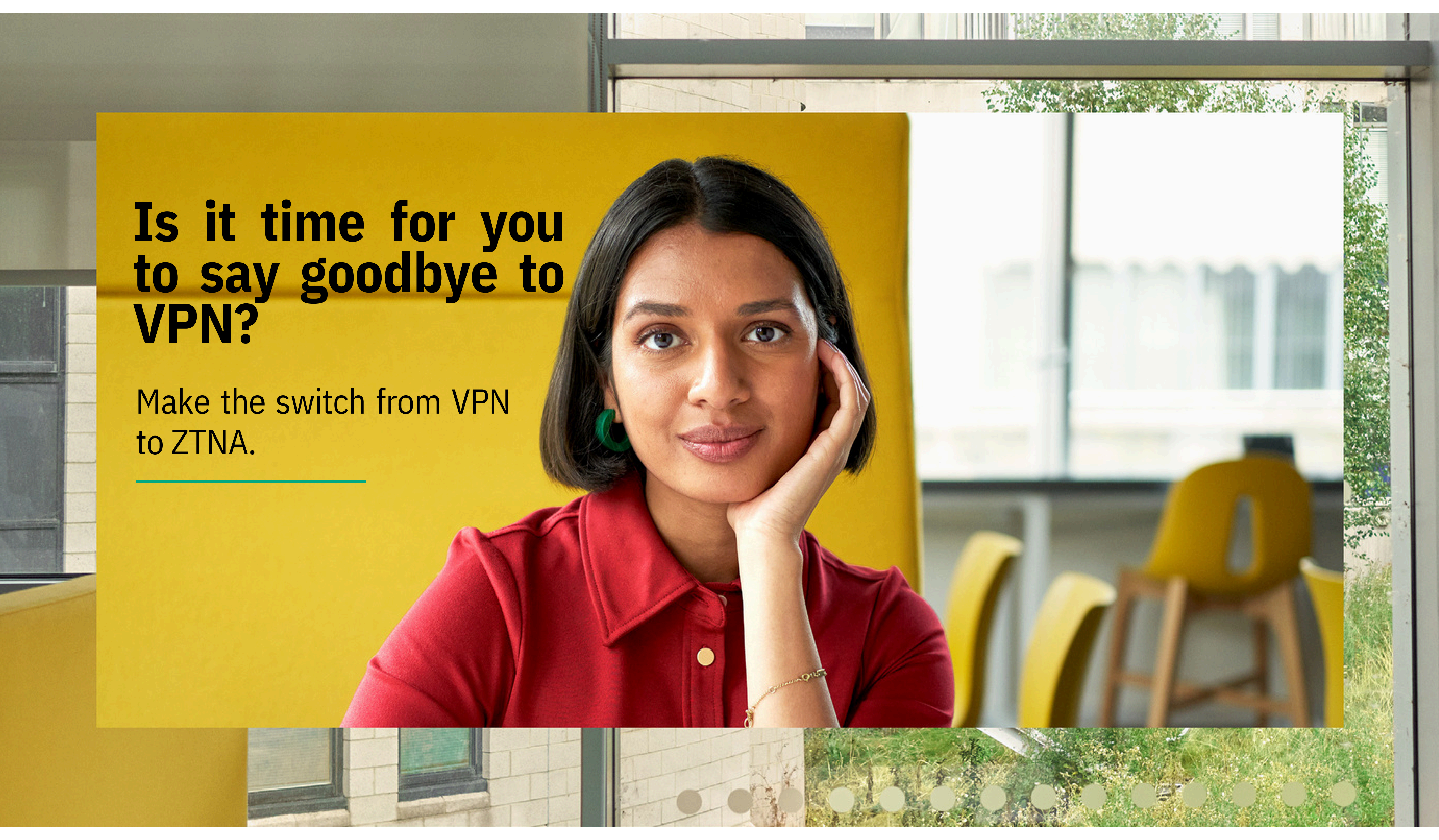
VPN	ZTNA
⊘ VPNs reinforce the traditional perimeter-based security model, which grants implicit trust to any device, user, and application within the network boundary.	✓ ZTNA implements the zero-trust security model, which works on a “never trust, always verify” basis and does not rely on a fixed perimeter.
⊘ VPNs expose ports to the internet to allow network access, making it a target for malware and ransomware attacks.	✓ ZTNA solutions never expose IPs to the internet, making the corporate network invisible to unauthorized users or bad actors.
⊘ VPNs provide users full access to a network’s resources and run the risk of exposing the network.	✓ ZTNA limits lateral movement and user connections to specific applications and continually verifies the user and device trust, reducing risk and building security resilience.
⊘ VPNs work on the network level and only have control and visibility of low-level network traffic.	✓ ZTNA works on the application level and can set up granular access policies based on a user-to-app basis. The result is higher levels of control and in-line visibility of activity.
⊘ VPNs allow BYOD devices to access the corporate network from unmanaged, non-corporate endpoints, which may introduce malware or other cyber threats.	✓ ZTNA can enforce strict device posture checks and policies before granting access to any resource, ensuring that only the compliant devices can connect.
⊘ VPNs are vulnerable to distributed denial-of-service (DDoS) attacks that can overwhelm the VPN server and disrupt the service.	✓ ZTNA solutions can mitigate DDoS attacks by using distributed cloud infrastructure that can scale up or down as needed, as well as applying rate limiting and filtering mechanisms.

Flexibility

VPN	ZTNA
⊘ VPNs are designed to provide secure remote access to the corporate network, but often have limited support for cloud-based resources.	✓ ZTNA can provide secure remote access to both on-premises and cloud-based resources, as well as hybrid environments.
⊘ VPNs often suffer from performance issues due to bandwidth limitations, network congestion, and latency.	✓ ZTNA solutions can optimize performance by using cloud-based architecture that ensures the closest access path to the user and the application, as well as scaled capacity as a result of the cloud.

Management

VPN	ZTNA
⊘ VPNs require users to install and configure client software on their devices which can be cumbersome and prone to errors.	✓ ZTNA solutions can provide clientless access to applications via a web browser, which simplifies the user experience and reduces IT support costs.
⊘ VPNs are difficult to monitor and audit as they do not provide granular visibility into the user activity and application usage.	✓ ZTNA solutions can provide detailed logs and reports on user identity, device posture, application access, and network traffic, enabling better compliance and security analysis.



Is it time for you to say goodbye to VPN?

Make the switch from VPN to ZTNA.

Make the right purchase decision. Contact our presales specialists.

Contact us

Vandis is an HPE Aruba Networking Platinum Partner. Our entire team of engineers is certified on the Aruba SSE platform. Contact us to learn more.

info@vandis.com
(800) 397-3146

VANDIS

HPE GreenLake

VPN-vs-ZTNA_RB_011424 a00137056enw