BUSINESS PAPER

aruba
a Hewlett Packard Enterprise company

SUCCESSFUL WAN AND SECURITY TRANSFORMATION POWERS THE DIGITAL ENTERPRISE

BEST-OF-BREED SASE ARCHITECTURE PROTECTS ENTERPRISES FROM THREATS WHILE DELIVERING THE HIGHEST APPLICATION QUALITY OF EXPERIENCE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Enterprises continue to embrace digital transformation with the intent to increase efficiency, enhance customer satisfaction, pursue new market opportunities, boost profitability and maintain a competitive edge. The migration of enterprise applications to the cloud is integral to any successful digital transformation initiative. Why? Today, there are more applications running in the cloud than in traditional enterprise data centers, and the majority of these applications are being consumed as software-as-a-service (SaaS). Moreover, in the cloud-first world enterprises must ensure that applications are directly and securely accessible at any time, from any location using any device. They also want to ensure that the network consistently delivers the highest quality of experience to both employees and customers. Finally, the explosion of mobile and IoT devices in the enterprise has dramatically increased the attack surface, exposing enterprises to security breaches that can compromise data and result in network downtime.

Today's corporate networks were never designed for the cloud-first world and fall well short on delivering the agility and security required to address the requirements of digital transformation. It is critical that enterprises not only secure applications in the cloud but also protect users connecting to these applications across the wide area network (WAN). At the same time, today's competitive business environment demands that enterprises deliver the highest quality of experience to customers through a network that maintains the performance and availability required to keep their business up and running.

To realize the full promise of digital transformation, enterprises need to transform both their WAN and security architectures — not just one or the other. When all applications were hosted in the corporate data center, it made a lot of sense to backhaul application traffic to the data center, where next-generation firewalls were deployed for advanced security inspection (Figure 1). Today, many of those applications have moved to the cloud, which calls for a WAN and security transformation as traditional router-centric wide area networks impair application performance, increase employee frustration, and are expensive. Therefore, the strategic imperative is to adopt a more intelligent, highly automated software-defined wide area network (SD-WAN) that can be seamlessly integrated with cloud-delivered security services.

To realize the full promise of the cloud and digital transformation, enterprises will need to transform both their WAN and security architectures — not just one or the other. Companies have already made significant investments in their shift to the cloud so the ultimate challenge is how to achieve a multiplier effect from their cloud investments.

An advanced SD-WAN combines critical wide area network functions such as routing, firewall, intrusion detection and prevention (IDPS), segmentation, and WAN optimization into a single platform. An advanced SD-WAN steers application traffic intelligently according to a customer's business intent, improving the quality of experience for end users while reducing expensive MPLS backhauling costs.

Recently, Gartner coined the term Security Service Edge (SSE), which is a cloud-delivered security solution comprising Firewall-as-a-Service (FWaaS), Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA). Adopting SSE and SD-WAN eliminates the cost and complexity of managing multiple on-premises next-generation firewalls and forms the basis of a cloud-first, Secure Access Service Edge (SASE) architecture.

Since transitioning to a SASE architecture is a journey, an enterprise may start with modernizing its WAN or security, but to realize the true value of cloud investments, both aspects must be addressed. And it's equally important to avoid vendor lock-in by choosing technology solution partners that provide flexibility and freedom-of-choice. With transformed network and security architectures, enterprises can embrace new timely innovations to accelerate productivity, revenue growth and profitability, all while containing costs.

APPLICATIONS ARE DELIVERED IN THE CLOUD — SECURITY SHOULD BE TOO

With an increasing number of employees working outside of the corporate network and connecting directly to cloud applications, traditional enterprise WANs and perimeter-based security approaches are insufficient. The cloud and SaaS have forever changed the way users connect and interact with applications. By transforming their WAN and security architectures, enterprises can ensure direct, secure access to applications and services across multi-cloud environments regardless of location or the devices being used to access them.

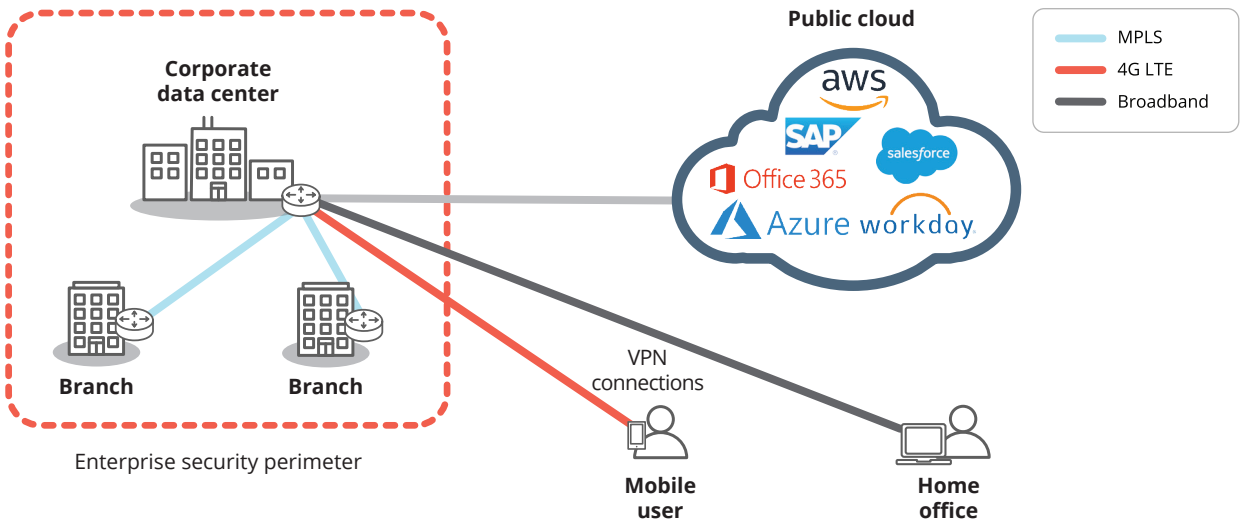


Figure 1: Traditional enterprise WANs and perimeter-based security approaches were not designed for the cloud. Backhauling all application traffic from branch locations to the data center impairs performance and delivers an inconsistent user experience.

A cloud-delivered security solution supports multiple network security functions that may include secure web gateway (SWG), firewall-as-a-service (FWaaS), cloud access security broker CASB) and zero trust network architecture (ZTNA). Previously, these were each unique and dedicated on-premise functions, but can now be delivered from the cloud in a unified manner as shown in Figure 2.

Some early adopters of cloud-delivered security solutions failed to implement an SD-WAN that could not apply adaptive internet breakout directly from branch office sites. Thus, they could not steer traffic directly from the branch office site to the cloud. Without the SD-WAN component, cloud-destined traffic was still backhauled to the data center, negatively impacting application performance.

Adopting a cloud-delivered security solution and SD-WAN eliminates the cost and complexity associated with managing multiple on-premise next-generation firewalls but still requires stateful zone-based firewall functionality at branch office sites to block any incoming threats. As shown in Figure 3, using an advanced SD-WAN solution, enterprises can connect directly to the cloud via adaptive internet breakout using broadband internet connections. The intelligence to recognize whitelisted applications enables local breakout from the branch office to the nearest point of presence (PoP), eliminating latency and delivering the highest quality of experience for trusted SaaS and cloud applications such as Microsoft Office 365, 8x8 and RingCentral. Application awareness also provides the ability to send other internet-bound traffic first to a cloud-delivered security provider for advanced inspection before forwarding to a SaaS provider.

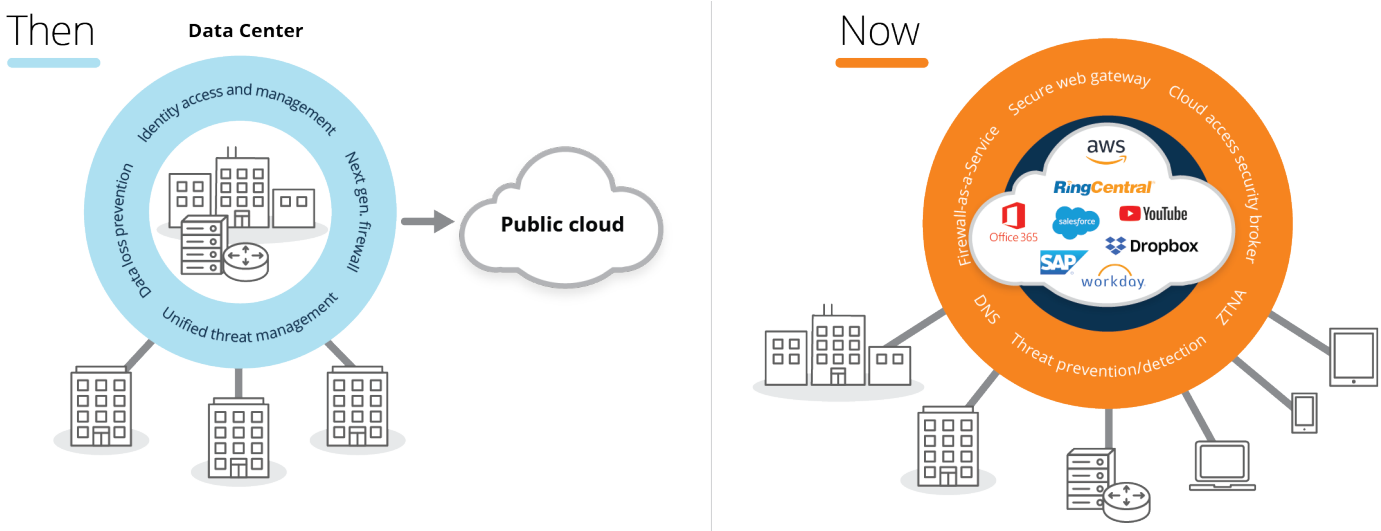


Figure 2: In the past it was all about securing the enterprise data center where applications were exclusively hosted. Now that applications have moved to and are being delivered from the cloud, enterprise perimeter-based security is becoming increasingly ineffective. It is imperative to think differently and move security to the cloud.

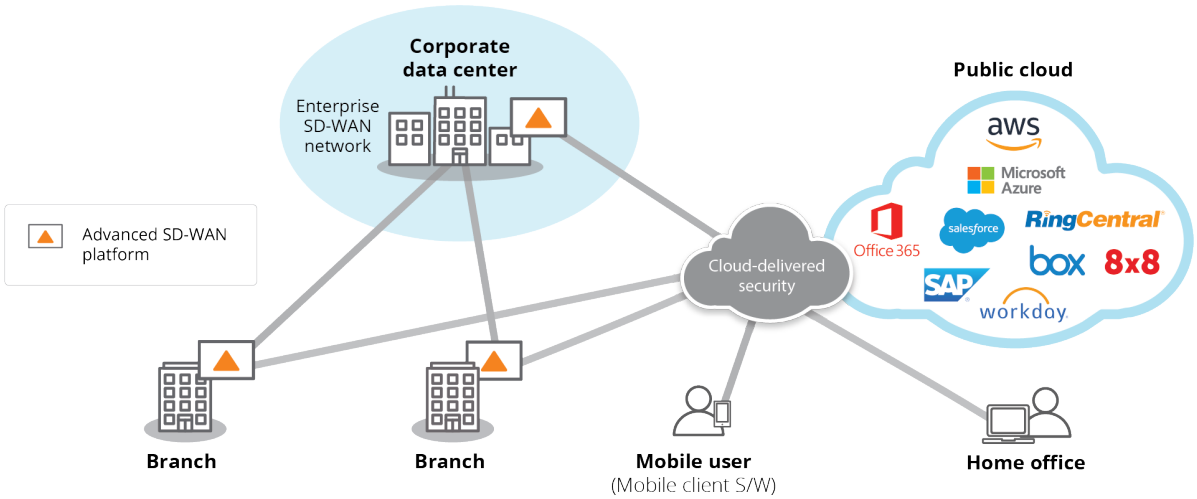


Figure 3: An advanced SD-WAN provides enterprises with a secure cloud on-ramp. Branch office locations can use broadband connections and adaptive internet breakout to directly connect users to cloud applications, optimizing application performance and user experience. Combining advanced SD-WAN and cloud-delivered security using a policy-based zero-trust network approach (ZTNA) ensures the enterprise WAN, users, devices, and applications are always secure.

Moreover, it's increasingly critical to examine network traffic flows for vulnerabilities, but it's challenging for today's IT environment. An advanced SD-WAN platform extends intrusion detection and prevention (IDPS) capabilities to the entire SD-WAN fabric, enabling enterprises to deliver east-west lateral security and secure internet breakout from branch office locations. Advanced SD-WAN capabilities integrated with modern cloud-delivered security services ensure consistent policy enforcement and access control for users, devices, applications, and IoT. This enables enterprises to meet compliance requirements, prevent downtime, and mitigate the risk of data compromise associated with a security breach.

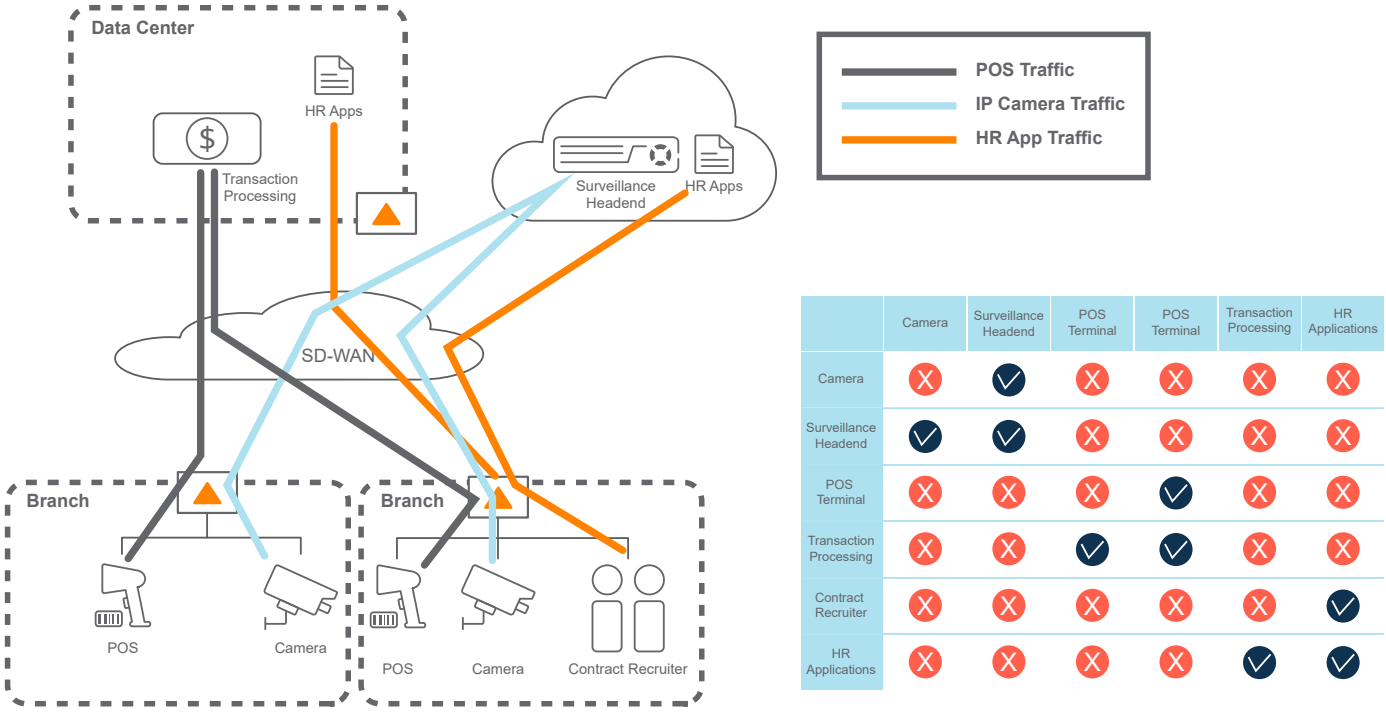
ZERO TRUST: SECURING THE EDGE BY ROLE, CONTEXT, AND APPLICATION

The proliferation of IoT devices across enterprises brings new ways to monitor, report, alert, automate and optimize business processes — from manufacturing lines to automating HVAC and lighting for energy savings. IoT makes businesses more efficient through automation, however, it also increases the attack surface by adding a new dimension of complexity. Since IoT devices such as IP cameras, point-of-sale (POS) terminals, and HVAC systems are agentless, running a third-party software agent on them is impossible. Because of this, enterprises require a different security solution for IoT devices to protect corporate networks from potential vulnerabilities that could breach the network and disrupt day-to-day business operations.

With the Aruba ClearPass zero-trust security framework, the network can identify IoT devices (and users) and their role in the business. ClearPass segments traffic at the network edge and isolates it from other traffic in the network; ClearPass only allows users and devices to reach destinations on the network that are consistent with their role in the business. This additional identity-based context enables consistent security policies that can be enforced network-wide, from edge-to-cloud, while also accelerating troubleshooting and problem resolution. Aruba ClearPass integration with an advanced SD-WAN platform like the Aruba EdgeConnect Enterprise SD-WAN platform augments application intelligence with user and device identity and role-based policy enforcement, enabling zero trust dynamic segmentation.

With zero trust dynamic segmentation, traffic in one segment is isolated from traffic in all other segments. This fine-grained segmentation prevents any threat of lateral traffic movement. Even if a threat were to appear, its impact is contained to the segment in which it emerged. Moreover, with a unified stateful zone-based firewall, enterprises can secure remote sites and IoT devices from any potential incoming threats by blocking them.

For example, as shown in Figure 4, a fine-grained segmentation policy can prevent IoT security cameras from accessing credit card transactions or HR applications. Zero-trust dynamic segmentation helps enterprises isolate any potential security threats by device type, role, and application while assisting them in meeting industry compliance requirements such as PCI, HIPAA, and SOX.



	Camera	Surveillance Headend	POS Terminal	POS Terminal	Transaction Processing	HR Applications
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
POS Terminal	✗	✗	✗	✓	✗	✗
Transaction Processing	✗	✗	✓	✓	✗	✗
Contract Recruiter	✗	✗	✗	✗	✗	✓
HR Applications	✗	✗	✗	✗	✓	✓

Figure 4: Zero Trust dynamic segmentation allows users and devices to only communicate with destinations consistent with their role in the organization. For instance, the POS terminal traffic (grey) and the IP Camera traffic (blue) are completely isolated/segmented from each other, preventing any threat of lateral traffic movement.

BEST OF BREED SOLUTIONS ENABLE ENTERPRISE AGILITY

With the constantly evolving approaches to delivering network security and the intricacy of building complex networking solutions, it is important to evaluate best-in-class security and network solutions from vendors that have proven experience and focus. It is unrealistic to find a single vendor that can deliver best-in-class capabilities across both domains and enterprises shouldn't be forced to compromise with basic capabilities on either side.

With security being a top-of-mind concern due to a continuously evolving threat landscape, enterprises must retain the agility to quickly and cost-effectively adopt new security solutions without being locked into a single vendor solution. Having an independent network solution provides enterprises with the assurance and peace of mind to select and deploy the cloud security solutions that best align to their evolving business and security requirements.

By having the freedom of choice to select best-of-breed vendor solutions that unify SD-WAN and cloud-delivered security using automation, enterprises gain increased business agility and speed, while reducing complexity and cost by building a consistent security architecture that blocks the impact of cyberattacks. This ultimately enables enterprises to achieve a multiplier effect on their existing and ongoing investments in cloud applications and services.

WAN TRANSFORMATION IS CRITICAL FOR DIGITAL TRANSFORMATION SUCCESS

In addition to all the benefits of migrating to a modern cloud-delivered security architecture, there is tremendous value in transforming the WAN for today's cloud-first enterprises. Traditional router-centric WANs were never designed for the cloud. Enterprises must modernize their WAN architecture and rethink how to best architect their branch networks to improve the performance and security of cloud applications. Enterprises are increasing the use of cloud and SaaS, with a focus on delivering the highest quality of experience to users.

WAN transformation encompasses providing a more efficient path and better experience between users and the cloud. As described previously, adoption of adaptive internet breakout to cloud-hosted and SaaS applications directly from branch locations not only optimizes available bandwidth, but also reduces any latency that can negatively impact user productivity.

Many organizations are transforming their network edge and embracing SD-WAN to connect branch locations using broadband internet connections. SD-WAN provides application-driven intelligent path selection across multiple WAN links (MPLS, broadband internet, LTE, 5G etc.) based on centrally defined policies. The benefits of SD-WAN include:

- Providing cost-effective delivery of business applications
- Improving application performance, availability and end-user Quality of Experience
- Satisfying requirements of the modern branch/remote sites or locations
- Accommodating SaaS and cloud-based applications and services
- Improving branch IT efficiency through automated service provisioning

MEETING THE DEMANDS OF APPLICATION SLAS

This directly results in greater enterprise productivity and business agility. Enterprises need a high-performance network, built on a highly available foundation that can support business critical applications reliably. Security must never be an afterthought. The ability to support micro-segmentation capabilities and granular policy enforcement provides enterprises with the ability to secure their WAN, meet compliance requirements and defend against breaches.

Enterprises need the agility to spin up new branches and dynamically adjust policy and security rules. The ability to propagate policy context is a critical requirement for branch automation. This makes the concept of an advanced SD-WAN solution, very attractive and can help enterprises eliminate the need for multiple appliances performing dedicated security functions and in turn, simplify and consolidate — or "thin" — their branch WAN edge architecture. An advanced SD-WAN edge platform enables enterprises to transform their WAN by unifying SD-WAN, routing, firewall, IDPS, segmentation, and WAN optimization in a single centrally managed platform.

Centralized SD-WAN orchestration and an application-specific approach ensures the priorities of the business are always reflected in the way the network behaves. Unifying the orchestration of network and security policies ensures that QoS and security are consistently applied and enforced to applications — or classes of applications — regardless of how or where they are being accessed. Application performance and security can be dictated by top-down business policies, not bottoms-up technology constraints.

An advanced SD-WAN continuously monitors the state of the network and applications, detects changing conditions and triggers immediate, automated real-time responses to eliminate the impact of brownouts, blackouts and security threat events. Furthermore, automating cloud platform connectivity with integrations via application programmable interfaces (APIs) simplifies IT operations, providing enterprises with timely access to cloud-delivered security services, IaaS and SaaS.

Today's network requires end-to-end visibility, programmability, and automation to dynamically ensure performance, security, and the highest quality of experience required for multi-cloud environments. An intelligent WAN architected with best-of-breed SD-WAN and cloud-delivered security solutions advances digital transformation initiatives and enables enterprises to evolve and embrace timely new innovations without limiting their productivity and growth, all while minimizing exposure to security risks.

CONCLUSION

As modern cloud-first enterprises continue to migrate applications from the data center to the cloud, they must embrace WAN and security transformation to realize the maximum return from their cloud investments. Gartner coined the term SASE, or Secure Access Service Edge that moves the industry in this new direction. As shown in Figure 5, it is important that enterprises consider both WAN and security transformation as they architect a secure access service edge to enable a seamless experience.

Ultimately, no single vendor will have the ability to truly deliver best-in-class network and security technologies across a single platform. With the continuously evolving threat landscape, enterprises must retain the agility to quickly and cost-effectively adopt new security solutions. Enterprises are well-served to evaluate platforms that offer the freedom of choice to integrate best-of-breed network and security solutions. By doing so, enterprises can avoid being locked-in to proprietary single vendor solutions or having to settle for basic features and capabilities.

An advanced SD-WAN platform that supports integrated orchestration to connect to best-in-class cloud-delivered security services enables a best-in-class SASE architecture and brings new levels of automation to enterprises.

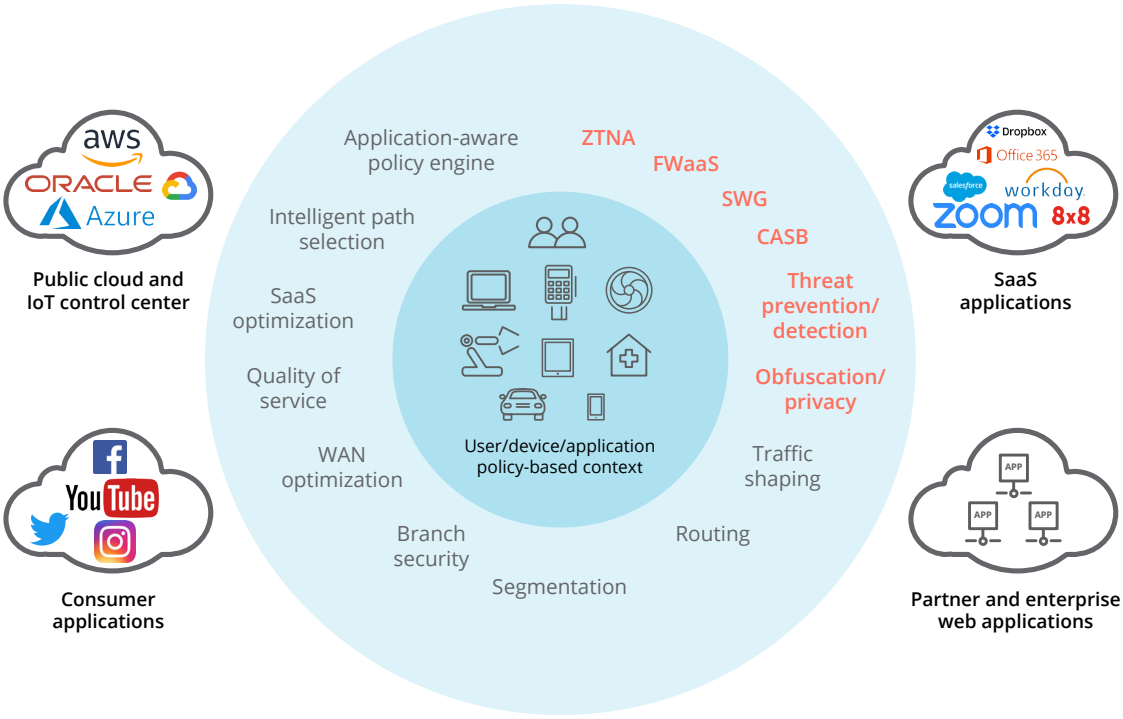


Figure 5: A secure access service edge is needed to support the enterprise's digital transformation initiatives, i.e., cloud-first strategy and workforce mobility needs. In a robust SASE architecture, comprehensive WAN capabilities need to work in conjunction with comprehensive network security functions to support digital enterprises' dynamic, secure access needs for users, devices, and applications.

It can support the foundational security functions required at the branch and complement cloud-delivered security to deliver seamless end-to-end security policy enforcement across the entire enterprise. This enables enterprises that are not yet ready to completely transform both their WAN and security architectures with the opportunity to transition to modern, cloud-first WAN architecture at their own pace, without compromise.

Finally, for enterprises that may not be ready to retire branch firewalls and move completely to a cloud-delivered security model, it is important to find an advanced SD-WAN platform that offers the freedom-of-choice to support leading third-party unified threat management (UTM) software solutions running as an integrated solution in branch locations.

This eliminates the additional cost and management complexity that would normally be incurred with separate dedicated firewalls, but it also provides enterprises with the flexibility to deploy best-of-breed solutions, ultimately offering a smooth migration to a cloud-delivered security model.

As enterprises continue to make substantial investments in the cloud, considering the requirements for both WAN and security transformation will ultimately put them on the path to delivering the highest quality of experience to users, increasing productivity and driving new revenue streams. Embarking on a thoughtful, no compromise WAN and security transformation journey will ultimately enable enterprises to achieve a multiplier effect from their existing and ongoing cloud investments.

BP_Successful-WAN-and-Security-Transformation_RVK_031122 a00110932enw

Contact us at www.arubanetworks.com/contact