BUSINESS PAPER

BEST-OF-BREED SD-WAN AND SASE WITH ZERO-TRUST POWER THE DIGITAL ENTERPRISE

aruba
a Hewlett Packard Enterprise company

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 short on addressing the cybersecurity challenges 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, the proliferation of IoT devices has significantly increased the attack surface exposing organizations to growing cybersecurity threats.

Therefore, the strategic imperative is to adopt a more intelligent, more secure, highly automated software-defined wide area network (SD-WAN) that can be seamlessly integrated with cloud-delivered security services to form a best-of-breed Secure Access Service Edge (SASE) architecture. SASE must be augmented with identity-based, zero trust security to enforce segmentation such that users and IoT devices can only reach destinations on the network consistent with their role in the business.

Since WAN and security transformation 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.

Today's corporate networks were never designed for the cloud-first world and fall short on addressing the cybersecurity challenges of digital transformation. It is critical that enterprises not only secure applications in the cloud but also protect users connecting to these applications. At the same time, the proliferation of IoT devices has significantly increased the attack surface exposing organizations to growing cybersecurity threats

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

Traditionally, all application traffic from branch locations would be backhauled over private MPLS services to the corporate data center for security inspection and verification (see Figure 1). This architecture made sense when applications were hosted exclusively in the corporate data center. But with applications and services migrating to the cloud, this traditional network architecture falls short, mainly because it impairs application performance and delivers an inconsistent user experience as traffic destined for the internet first goes through the data center and the corporate firewall before reaching its destination.

Furthermore, with an increasing number of employees working outside of the corporate network and connecting directly to cloud applications, traditional perimeter-based security is 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.

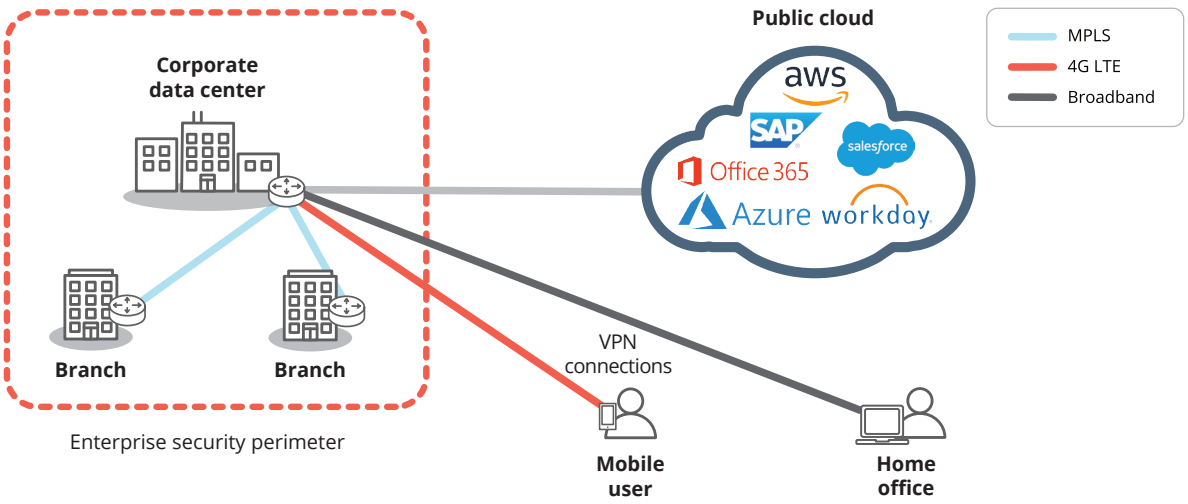

Figure 1: Traditional enterprise WANs and perimeter-based security approaches were not designed for the cloud. Backhauling all application traffic from branch locations to the data center impairs performance and delivers an inconsistent user experience.

In 2019, Gartner coined the term SASE, or Secure Access Service Edge for a framework that combines SD-WAN with cloud-delivered Security Service Edge (SSE) functions including secure web gateway (SWG), firewall-as-a-service (FWaaS), cloud access security broker CASB) and zero trust network access (ZTNA). Previously, these were each unique and dedicated functions, but can now be delivered from the cloud in a unified manner as shown in Figure 2.

Some early adopters of SSE 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 Security Service Edge solutions and SD-WAN eliminates the cost and complexity associated with managing multiple on-premise firewalls but still requires 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. Advanced SD-WAN capabilities integrated with modern cloud-delivered security services ensures consistent policy enforcement and access control for users, devices, applications, and IoT. This enables enterprises to enforce compliance, prevent downtime and mitigate the risk of data compromise associated with a security breach.

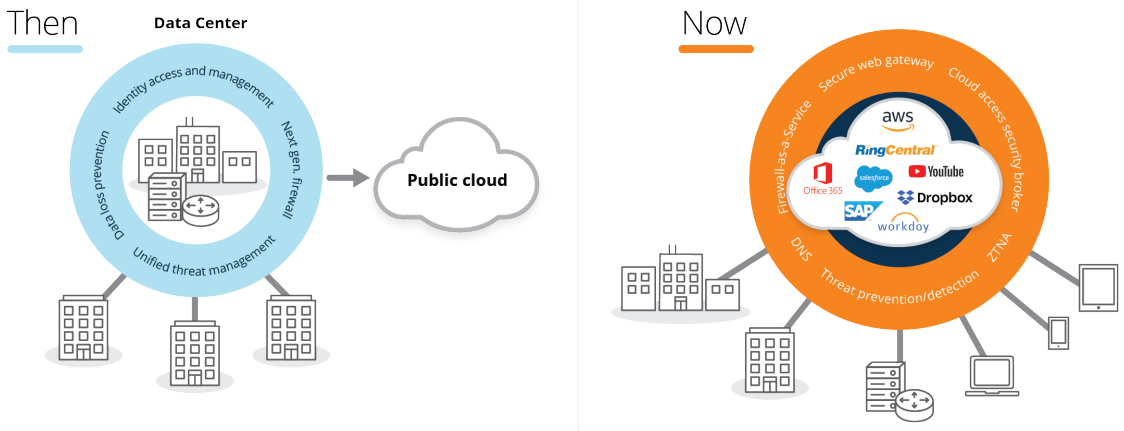

Figure 2: In the past it was all about securing the enterprise data center where applications were exclusively hosted. Now that applications have moved to and are being delivered from the cloud, enterprise perimeter-based security is becoming increasingly ineffective. It is imperative to think differently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

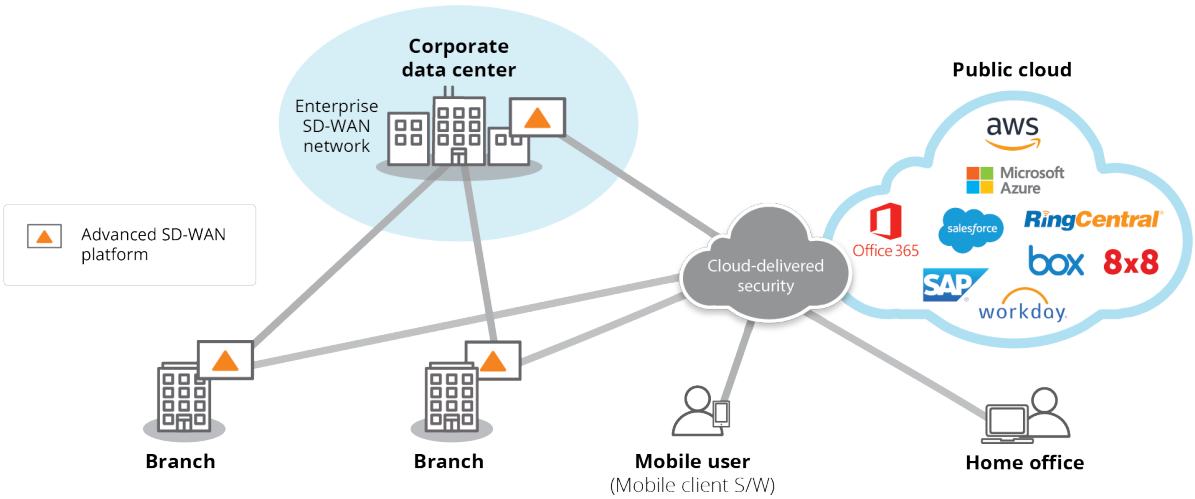

Figure 3: An advanced SD-WAN provides enterprises with a secure cloud on-ramp. Branch office locations can use broadband connections and adaptive internet breakout to directly connect users to cloud applications, optimizing application performance and user experience. Combining advanced SD-WAN and cloud-delivered security creates a secure access service edge (SASE) ensuring that users, devices, and applications are always secure.

BEST OF BREED SASE PROVIDES FREEDOM OF CHOICE

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 SASE 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.

An advanced SD-WAN solution tightly integrates with multiple SSE vendors, offering the freedom of choice to select best-of-breed vendor solutions that unify SD-WAN and cloud-delivered security using automated orchestration. With best-of-breed SASE, enterprises build a consistent security architecture that blocks the impact of cyberattacks while increasing business agility and reducing complexity. This ultimately enables enterprises to achieve a multiplier effect on their existing and ongoing investments in cloud applications and services.

SECURING ENTERPRISE IOT WITH A ZERO-TRUST APPROACH

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. The manner in which IT tackles the growing mobile device security challenge is to deploy a zero-trust network access (ZTNA) solution based on the zero-trust model. A ZTNA solution works by installing an endpoint agent on a user device such as a laptop, tablet, or mobile phone.

That software agent ensures traffic from the device is directed to a cloud-delivered security service before being directed towards a SaaS application or IaaS provider. However, unlike tablets and smart phones, ZTNA software agents cannot be installed on IoT devices since they are agentless; they do not support installation of third-party software agents. 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.

An advanced SD-WAN supporting a zero-trust architecture dynamically segments the network and applies least privileged access principles, enabling enterprises to reduce the risk associated with breaches when deploying IoT devices. It ensures that users and devices only communicate with destinations consistent with their role based on identity, access rights and security posture. It orchestrates end-to-end segmentation spanning the enterprise LAN-WAN-LAN and LAN-WAN-Data Center/Cloud resulting in consistent and automated security policy enforcement with greater visibility. With end-to-end segmentation, enterprises can create isolated segments for IoT device traffic. An independent security policy may be defined for each segment defining the security policies to enforce for the device traffic. Since traffic in one segment is isolated from traffic in all other segments, it prevents any unauthorized access. Even if a threat were to appear, its impact is contained to the segment in which it emerged.

Let's look at an example. In a remote site where agentless IoT devices such as PoS and HVAC systems are installed (Figure 4 below), an advanced SD-WAN platform identifies applications used by the devices uniquely. A system policy intercepts PoS traffic and directs it to the corporate data center where the credit card transaction processing application is hosted. Existing firewall security services deployed within the data center in this example are applied. On the other hand, HVAC system policies segment and direct the HVAC traffic to the cloud-delivered security service for additional security inspection before reaching the IoT control center hosted in the public cloud. Since IoT traffic is isolated according to business policy, a breach in the HVAC segment does not compromise or put at risk credit card and personal data in the PoS segment. Segmentation also helps organizations in meeting PCI (or other) compliance mandates for their business. As shown in this example, a comprehensive security deployment with an advanced SD-WAN platform can better safeguard today's dynamic enterprises in their transformation journey as they embrace IoT's benefits.

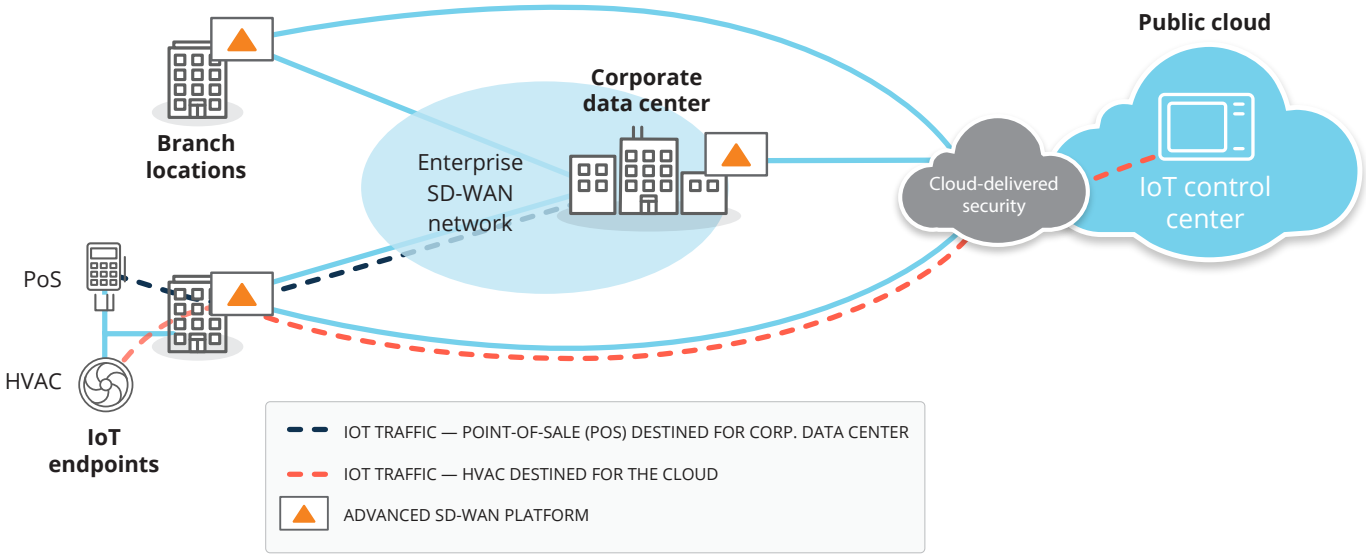

Figure 4: IoT endpoints are multiplying and pose new risks for security breaches. With an advanced SD-WAN platform, enterprises can protect IoT devices by implementing a zero-trust architecture and dynamically segment the network. As shown in the diagram, all PoS transaction data from the branch is destined to the enterprise data center, whereas the HVAC traffic is routed to an IoT control center in the cloud.

PROTECT BRANCHES FROM EXTERNAL THREATS WITH AN ADVANCED SD-WAN

With the digitalization of enterprises, the risk of cyberattacks has significantly increased over the last decade. In traditional router-based network environments, branch offices have stacked a multitude of networking and security equipment, but this equipment is difficult to configure, maintain, and keep up to date with the latest threat information. Remote sites also lack experienced IT staff exposing them to potential security breaches.

In addition to protecting cloud operations with best-of-breed SASE, an advanced SD-WAN solution can protect branch offices from malicious threats. It is built with a next-generation firewall that includes threat defense capabilities such as intrusion detection and prevention (IDS/IPS) and DDoS to protect branch offices from malicious threats.

A signature-based IDS system typically monitors network traffic to find patterns that match a particular attack signature. When an intrusion is detected, the sensor provides actions such as drop, inspect, and allow traffic. Intrusion prevention systems can operate either in strict mode or performant mode. In strict mode, the traffic passes through the sensor so that the traffic is immediately blocked when an intrusion occurs. In performant mode, a copy of the traffic is sent for analysis, providing more efficiency without impacting network performance. An intrusion is blocked after its detection. Depending on its security requirements, organizations can choose between the strict or performant mode.

An advanced SD-WAN can also dynamically detect DDoS attacks such as protocol attacks, ICMP floods, SYN floods, and IP spoofing attacks. After detecting abnormal network behavior, the solution limits the number of requests using actions such as rapid aging, drop excess, and block source. Additionally, it can route the traffic over unaffected network links in case of a DDoS attack ensuring business continuity.

By integrating advanced networking and security capabilities into one single SD-WAN solution such as routing, WAN optimization, and next-generation firewall, organizations can greatly simplify their network operations in branches. Additionally, security policies can be automatically pushed to branches from a central location with zero-touch provisioning facilitating the configuration of network and security policies. New branches are set up quickly and easily, and security policy changes can be automatically distributed to hundreds or thousands of branches in minutes while minimizing errors.

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, 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, WAN optimization, segmentation, and branch security 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. SASE, or Secure Access Service Edge 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.

An advanced SD-WAN platform provides the ability to seamlessly connect to a variety of best-in-class cloud security services, delivering a best-of-breed SASE architecture. Ultimately, no single SASE 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 SASE. By doing so, enterprises can avoid being locked-in to proprietary single vendor solutions or having to settle for basic features and capabilities.

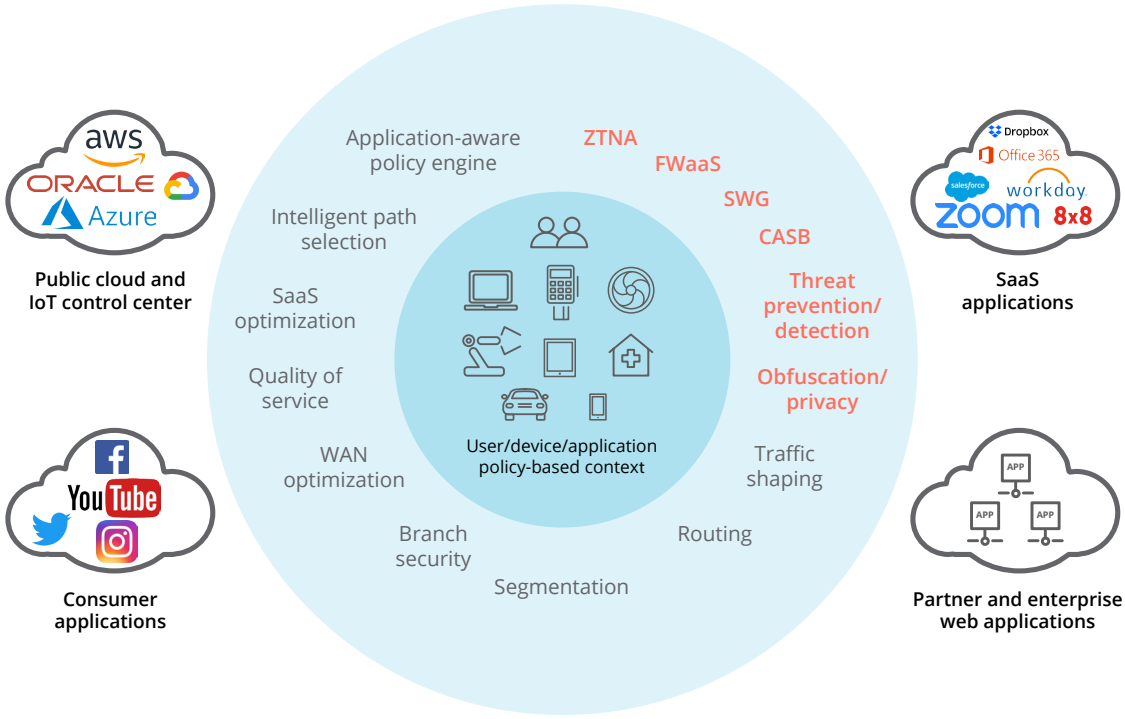

Figure 5: A secure access service edge is needed to support the enterprise's digital transformation initiatives, i.e., cloud-first strategy and workforce mobility needs. In a robust SASE architecture, comprehensive WAN capabilities need to work in conjunction with comprehensive network security functions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

Additionally, with the proliferation of IoT devices, SASE must be complemented with a zero trust security framework that dynamically segments the traffic based on identity, so that users and IoT devices can only reach network destinations consistent with their role in the business.

An advanced SD-WAN can support the foundational security functions required at the branch by integrating a next-generation firewall with IDS/IPS capabilities and complement cloud-delivered security to deliver seamless end-to-end security policy enforcement across the entire enterprise. This enables enterprises to simplify their network infrastructure with the opportunity to transition to modern, cloud-first secure 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, while tackling today's cybersecurity challenges. Embarking on a thoughtful, no compromise WAN and security transformation journey will ultimately enable enterprises to protect their digital assets and achieve a multiplier effect from their existing and ongoing cloud investments.

aruba
a Hewlett Packard Enterprise company

BP_Successful-WAN-and-Security-Transformation_RVK_080422 a00110932enw

Contact us at www.arubanetworks.com/contact