Business white paper

HPE aruba networking

Unified SASE with Zero Trust powers the digital enterprise

HPE GreenLake

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, with the rise of hybrid working, organizations must ensure that applications are directly and securely accessible at any time, from any location using any device.

Today's corporate networks were never designed for the cloud-first world and fall short on addressing the cybersecurity challenges of digital transformation and hybrid working. 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 increased cybersecurity threats.

Therefore, the strategic imperative is to adopt a more intelligent, highly automated unified SASE architecture that allows organizations to achieve even greater simplicity, operational efficiencies, and cost-savings. 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 and hybrid working. 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 increased cybersecurity threats.

Deliver cloud security with Security Service Edge (SSE)

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 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.

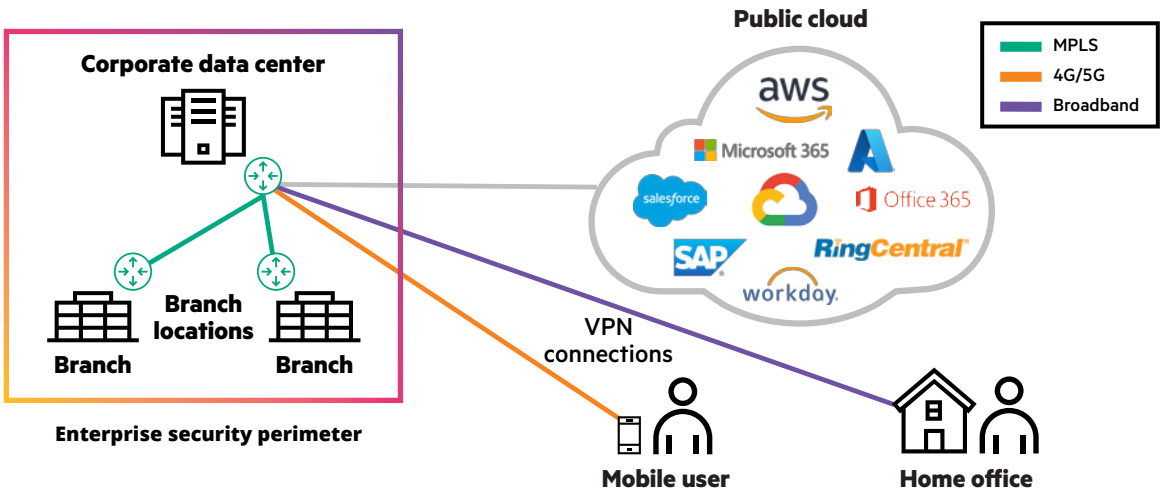

Figure 1. Traditional enterprise WANs and perimeter-based security approaches were not designed for the cloud. Backhauling all application traffic from branch locations to the data center impairs performance and delivers inconsistent user experience.

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 Zero Trust network access (ZTNA), secure web gateway (SWG), and cloud access security broker CASB). 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.

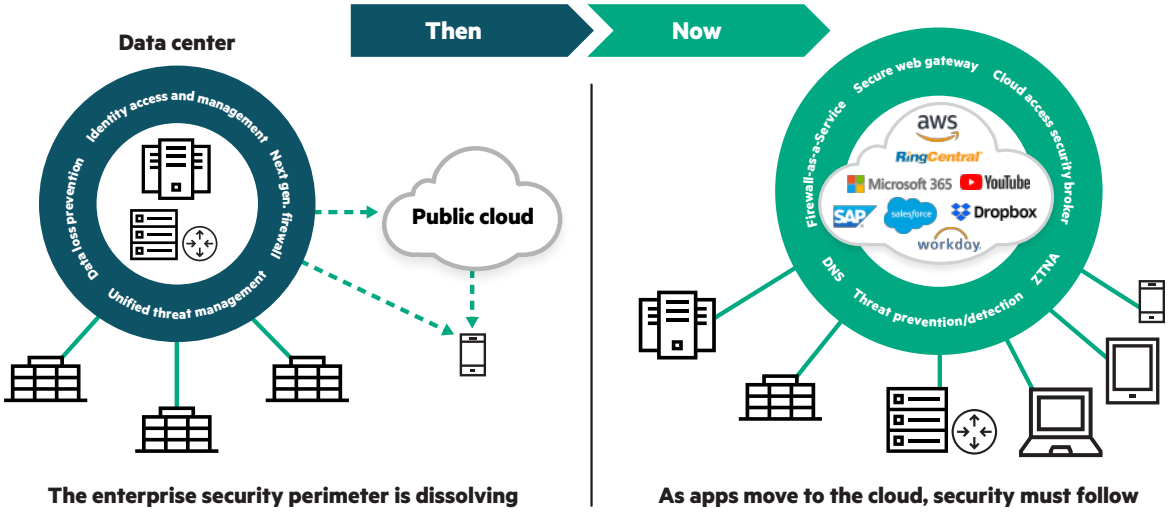

Figure 2. In the past it was all about securing the enterprise data center where applications were exclusively hosted. Now that applications have moved to and are being delivered from the cloud, enterprise perimeter-based security is becoming increasingly ineffective. It is imperative to think differently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

Unlike VPN, ZTNA (Zero Trust Network Access) ensures least privilege access and application-level network segmentation based on user identity. This approach allows users to access only the necessary resources, protecting data from cyber threats by masking private resources from the internet. ZTNA enables remote workers to connect securely from anywhere, using any device and network. Additionally, organizations can seamlessly onboard third-party users onto their network without the need to install a ZTNA agent on their laptops. Third-party users can simply log in to a ZTNA web portal using their own credentials. Once authenticated, they can conveniently access the specific applications they require while preventing access to other applications or services. Moreover, advanced ZTNA solutions offer numerous Points of Presence (PoPs) instead of just a few VPN concentrator geo-locations. This ensures minimal latency and an enhanced quality of experience for users.

To safeguard organizations against web-based threats like malware, ransomware, phishing, and other cyber security risks, a Secure Web Gateway solution (SWG) intercepts web traffic between users and websites. SWG performs various security inspections, including URL filtering, malicious code detection, and web access control. By establishing policies that restrict access to specific categories of websites, such as adult content, gambling platforms, and high-risk sites, organizations can maintain a secure and productive browsing environment for their users while mitigating potential legal, reputational, and security risks.

As more sensitive data is hosted outside the enterprise security perimeter in cloud applications, both sanctioned and unsanctioned, organizations face significant challenges in terms of data security and protection. Cloud Access Security Broker (CASB) plays a vital role in identifying and detecting sensitive data within cloud applications. It monitors user activity in granular detail, including application access, timestamps, and downloaded files, to prevent data loss and safeguard the organization against data exfiltration. CASB also enables organizations to enforce robust security policies, such as authentication and Single Sign-On (SSO), and restricts users from utilizing unauthorized cloud applications, thereby reducing the risks associated with shadow IT.

Unified SASE reduces complexity and facilitates deployment

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.

However, not all SASE solutions are created equal. Some SASE vendors offer multiple point solutions that are loosely integrated or require routing between different vendor Point of Presence (PoPs), resulting in potential drawbacks such as latency, performance issues, and management overhead.

On the other hand, single-vendor SASE solutions, encompass all the fundamental capabilities of SASE, tightly integrated and centrally managed. These solutions help organizations reduce complexity and facilitate deployment, while improving security posture, user experience, and cost efficiency.

Unified SASE solution provides SSE capabilities including ZTNA that enforces least-privilege access to hybrid workers, SWG to protect against malicious web traffic and CASB to ensure sensitive data remains protected while preventing data from being lost.

SD-WAN is the foundational component of this unified SASE architecture optimizing the connection between branch offices and headquarters by combining multiple links such as MPLS and broadband internet, and intelligently steering application traffic to the cloud. This results in enhanced application performance and user experience. Some advanced SD-WAN also includes a built-in next-generation firewall that lets organizations safely remove physical firewalls, as well as routers, in their branch offices.

To facilitate this transformation, organizations have the flexibility to begin their SASE journey by securing remote workers with Zero Trust Network Access (ZTNA) or by addressing application performance issues in branches using Software-Defined Wide Area Networking (SD-WAN). The choice depends on prioritizing specific use cases based on business and security goals.

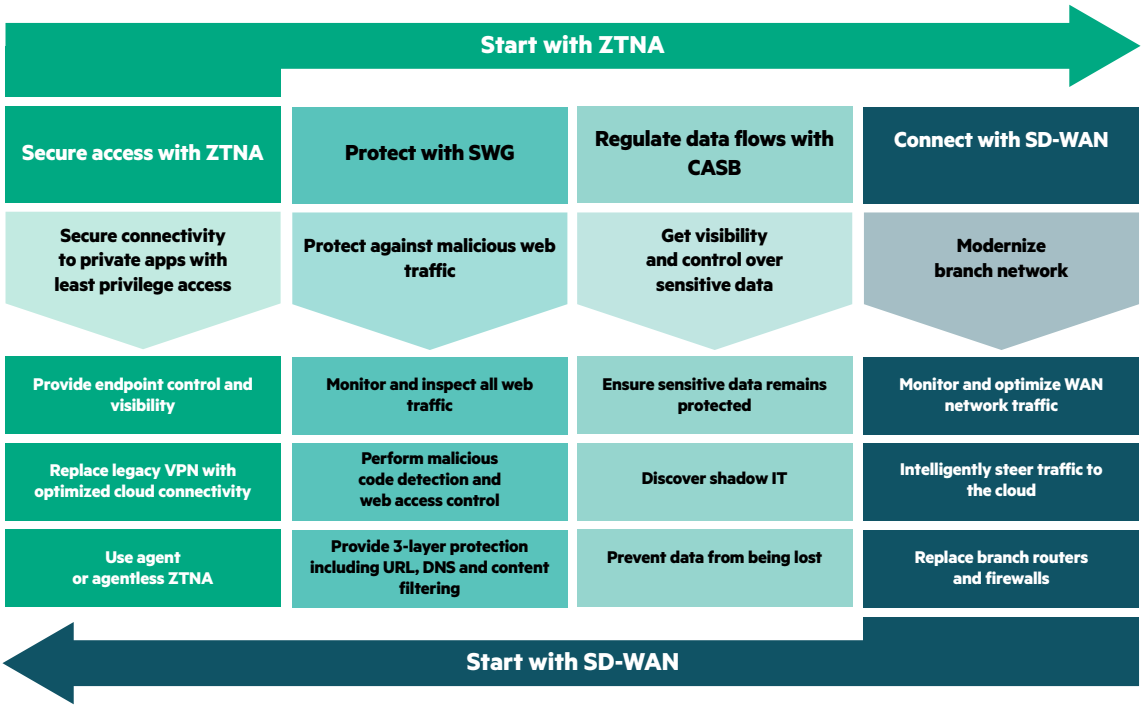

Figure 3. Begin your SASE journey with ZTNA or SD-WAN

With unified SASE, enterprises can accelerate their journey to SASE with a single platform combining SD-WAN and SSE for a simpler adoption and a faster deployment of SASE. This ultimately enables enterprises to build a consistent security architecture that blocks the impact of cyber attacks while increasing business agility and reducing complexity.

Modernizing branch network with SD-WAN

To connect branch offices, implementing an SD-WAN solution can optimize network performance by combining multiple links, such as MPLS, Internet, and 5G. Advanced SD-WAN solutions utilize techniques like Path Conditioning to mitigate the effects of dropped and out-of-order packets commonly experienced with broadband internet and

MPLS links. This ensures a performance similar to private-line connections over internet links, allowing organizations to reduce their dependency on MPLS and easily establish new branches.

Some early adopters of SSE solutions implemented 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.

As shown in Figure 4, using an advanced SD-WAN solution tightly integrated with SSE services, 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 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 tightly integrated with SSE 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.

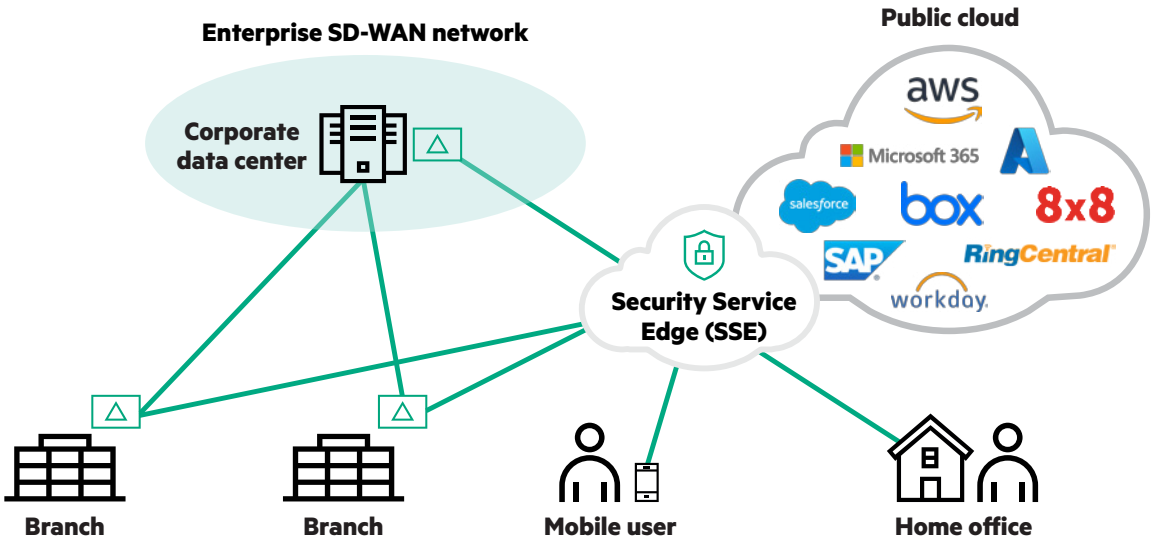

Figure 4. An advanced SD-WAN provides enterprises with a secure cloud on-ramp to directly connect users to cloud applications. Combining advanced SD-WAN and SSE creates a unified SASE solution, ensuring that users, devices, and applications are always secure.

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.

A secure SD-WAN with a built-in next-generation firewall and supporting a Zero Trust architecture, dynamically segments the network and applies least privilege 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 IP camera systems are installed (Figure 5 below), a secure SD-WAN platform identifies applications used by the devices uniquely. The POS terminal traffic is isolated/segmented from the IP camera traffic, which prevents the threat of lateral traffic movement. Even if a hacker compromises the IP camera system, the danger is contained only in that segment and does not affect the POS traffic. Segmentation also helps organizations in meeting PCI DSS (or other) compliance mandates for their business. As shown in this example, a comprehensive security deployment with a secure SD-WAN platform can better safeguard today's dynamic enterprises in their transformation journey as they embrace IoT's benefits.

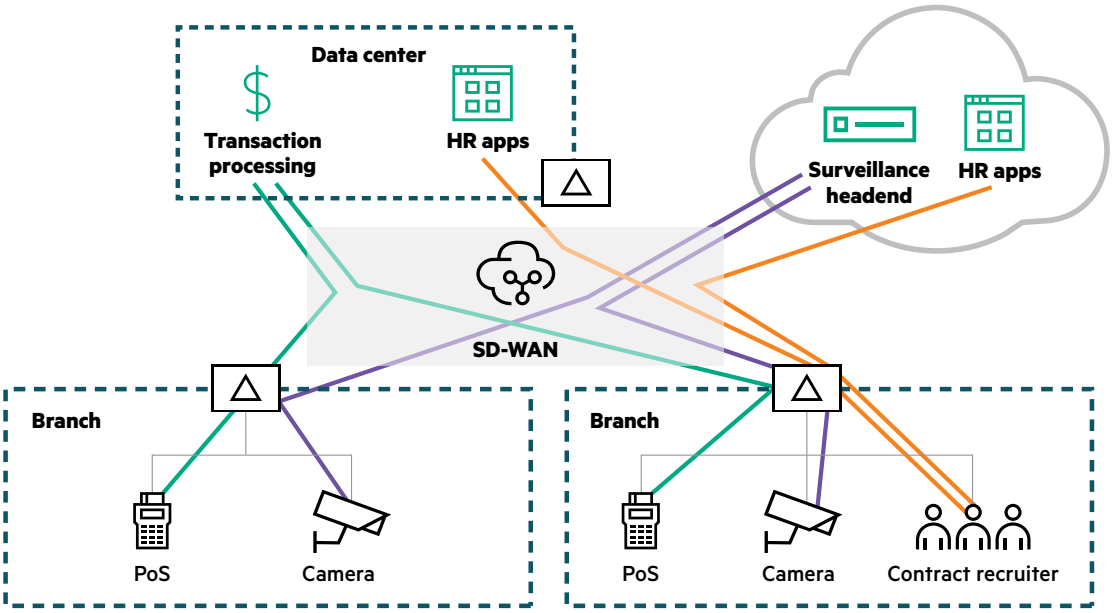

Figure 5. IoT endpoints are multiplying and pose new risks for security breaches. By using a secure SD-WAN platform, enterprises can protect IoT devices by implementing a Zero Trust architecture and dynamically segment the network.

Protect branches from external threats with a secure SD-WAN

With the digitalization of enterprises, the risk of cyber attacks 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 SASE, a secure 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 defense 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 or 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.

A secure 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 and reduce hardware footprint. 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.

Virtual instances of SD-WAN solutions can even be deployed in cloud service providers like AWS, Microsoft Azure, and Google Cloud, establishing a resilient connection from branch offices to the cloud. This optimized connection not only enhances performance but also ensures end-to-end segmentation, allowing users to access cloud applications according to their assigned roles.

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

The benefits of a unified approach to SASE

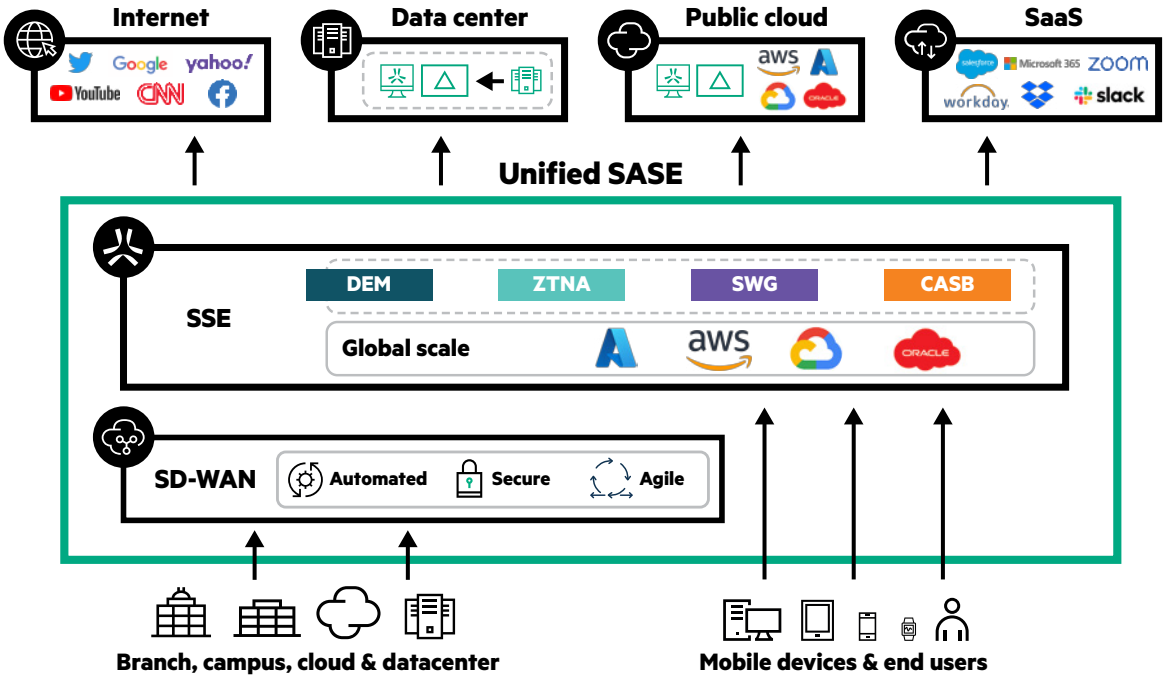

Figure 6. Seamlessly deploy a unified SASE architecture

Unified SASE solutions provide a comprehensive and tightly integrated platform that combines all the core capabilities of SASE. This integrated approach offers numerous benefits, including improved security posture, seamless deployment, enhanced user experiences, and greater cost efficiency.

By unifying security posture, unified SASE reduces the attack surface and enhances threat detection and response times. Universal security policies and centralized access controls are applied across all traffic and locations, minimizing vulnerabilities, and providing consistent security policies.

Unified SASE streamlines network and security operations by eliminating the need for managing multiple networking and security appliances. This reduces costs, resources, and skills, allowing IT teams to focus on core tasks. Centralized management systems provide visibility, configuration, monitoring, and troubleshooting capabilities, improving overall operational efficiency.

Unified SASE is highly scalable to quickly adapt to changing business needs, and support digital transformation initiatives such as hybrid work, cloud migration, IoT and OT initiatives. It also provides multiple points of presence for geographically distributed organizations.

User experience is also enhanced with unified SASE. High-performance, low-latency connectivity is guaranteed by automatically routing traffic through the fastest access paths, avoiding unnecessary backhauling to the data center.

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 and facilitate hybrid working. Unified SASE, or Secure Access Service Edge moves the industry in this new direction by offering a holistic approach to network and security, resulting in seamless deployment, improved security, increased efficiency, and enhanced user experience. As shown in Figure 7, it is important that enterprises consider both WAN and security transformation as they architect a unified SASE solution.

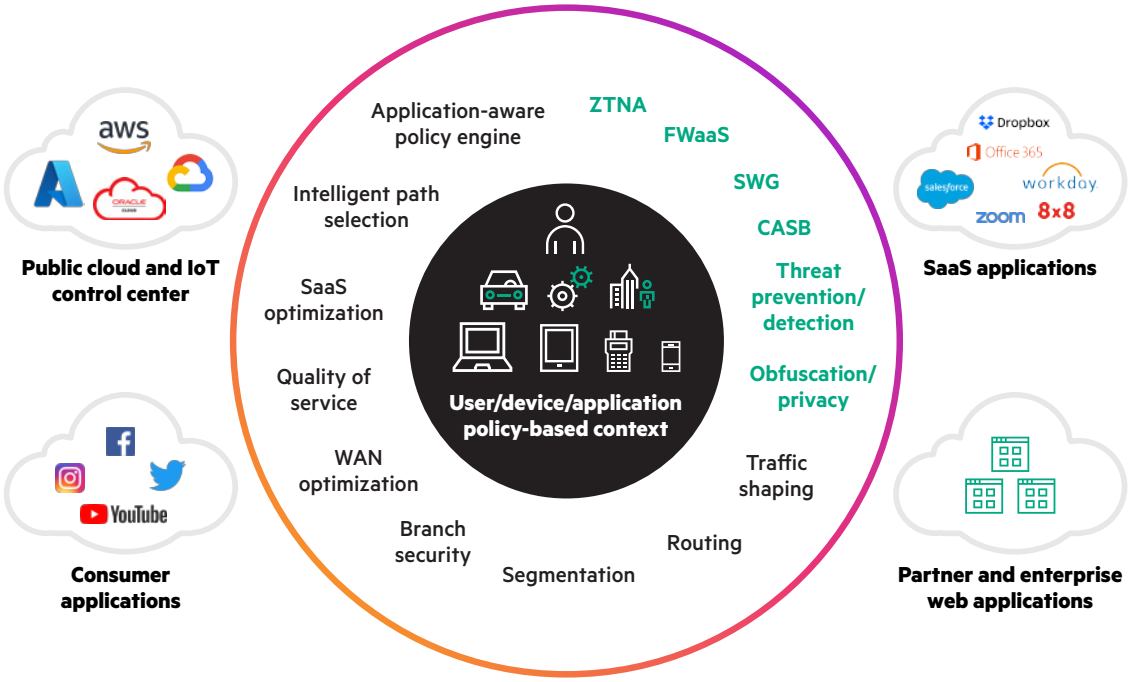

Figure 7. SASE is needed to support the enterprise's digital transformation initiatives, i.e., cloud-first strategy and hybrid workforce needs. In a unified SASE architecture, comprehensive WAN capabilities work in conjunction with network security functions to support digital enterprises' dynamic, secure access needs for users, devices, and applications.

Additionally, with the proliferation of IoT devices, unified 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.

A secure 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.

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 and facilitate hybrid working.

As enterprises continue to make substantial investments in the cloud, considering the requirements for both WAN and security transformation will put them on the path to delivering the highest quality of experience to users, while tackling today's cybersecurity challenges. Unified SASE will ultimately enable enterprises to accelerate their journey to WAN and security transformation, protecting their digital assets and achieving a greater efficiency through reduced complexity, cost reduction and seamless deployment.

Learn more at

arubanetworks.com/solutions/sase/

Visit **ArubaNetworks.com**

Make the right purchase decision.
Contact our presales specialists.

Contact us

Hewlett Packard Enterprise

BWP_Unified-SASE_RB_020524 a00110932enw