Brochure

A practical guide to implement SASE in 5 steps

Enterprise networks are undergoing a fundamental shift driven by cloud adoption, SaaS proliferation, hybrid work, and an evolving threat landscape. Traditional architectures built around centralized data centers, perimeter-based security, and static trust assumptions are no longer aligned with how applications are consumed or how users connect. As a result, IT architects are being asked to rethink not only connectivity, but also how security is embedded into the network by design.

Secure access service edge (SASE) provides a modern architectural model to address these challenges by converging networking and security into a cloud-delivered, identity-driven framework. This guide is intended to help IT architects and security teams understand what SASE delivers, why organizations need a structured SASE solution, and how to design and implement SASE in a pragmatic, phased manner. It focuses on architectural principles, real-world challenges, and best practices to support cloud-first, zero trust networking at scale.

A. Definition: what does SASE provide?

SASE is an architectural model that converges wide-area networking and security into a unified, cloud-delivered framework. Rather than treating connectivity and security as separate domains—often owned by different teams and enforced at different points in the network—SASE brings them together under a shared architecture, policy model, and operational approach.

At its core, SASE provides secure, optimized access to applications and data regardless of where users, devices, or workloads are located. It combines software-defined wide area networking (SD-WAN) for intelligent traffic steering with cloud-native security services such as secure web gateway (SWG), zero trust network access (ZTNA), cloud access security broker (CASB), and Data Loss Prevention (DLP). These capabilities are delivered from globally distributed points of presence close to users and cloud platforms, rather than from centralized enterprise data centers.

For IT teams, SASE represents a shift away from topology-driven design toward policy-driven design. Access decisions are no longer based primarily on IP addresses or network location, but on identity, device posture, application context, and risk. This approach aligns the network with modern usage patterns, where SaaS, public cloud, and hybrid work dominate traffic flows. When implemented correctly, SASE delivers consistent security, improved application performance, simplified operations, and greater architectural agility.

B. Network teams challenges and the benefits of SASE

IT teams face increasing pressure as enterprise environments become more distributed, cloud-centric, and dynamic. Architectures designed around centralized data centers and static perimeters struggle to meet modern requirements. A common issue is traffic backhauling, where branch and remote-user traffic is routed through centralized locations for inspection. This increases latency, degrades application performance, and inflates bandwidth costs, particularly for real-time collaboration and SaaS workloads.

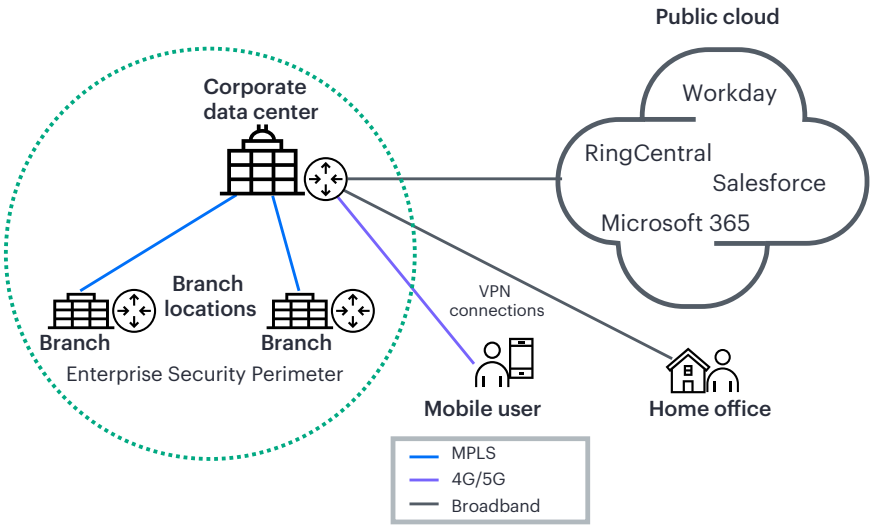

Figure 1. Legacy architecture based on routers and firewalls, where all traffic is backhauled to the data center results in very slow and unpredictable application performance

Operational complexity is another major challenge. Over time, organizations have accumulated separate platforms for routing, WAN optimization, firewalls, VPNs, web security, and cloud security. Each platform introduces its own policy model, management interface, and telemetry. Maintaining consistency across these systems is difficult, and troubleshooting often requires manual correlation across multiple tools.

Security posture also suffers from fragmentation. Branch offices, campuses, remote users, and cloud workloads are frequently protected by different security stacks, leading to inconsistent enforcement and visibility gaps. Implicit trust based on network location remains common, even though users and devices now connect from virtually anywhere.

SASE addresses these challenges by unifying networking and security into a single architecture. By enabling direct, secure access to cloud applications, it eliminates unnecessary backhauling and improves performance. By centralizing policy definition and distributing enforcement, it facilitates consistent security across all locations. By integrating visibility across network and security layers, it simplifies operations and improves response times. For IT teams, SASE provides a scalable and resilient model aligned with cloud-first strategies.

C. Why organizations need SASE

SASE is not simply a technology refresh; it is an architectural and operational transformation. Historically, network and security teams operated independently with different tools, priorities, and success metrics. In a SASE architecture, these boundaries dissolve. Traffic steering decisions affect security outcomes, and security controls directly influence application performance and user experience. Without shared ownership and governance, SASE initiatives risk becoming fragmented or inconsistent.

SASE establishes architectural principles, reference designs, and deployment standards that align teams around a common vision. It enables organizations to prioritize use cases, sequence deployments, and verify that SD-WAN, zero trust and cloud security initiatives reinforce one another. For IT teams, this represents a shift from designing static topologies to defining adaptive, policy-driven systems aligned with long-term business goals.

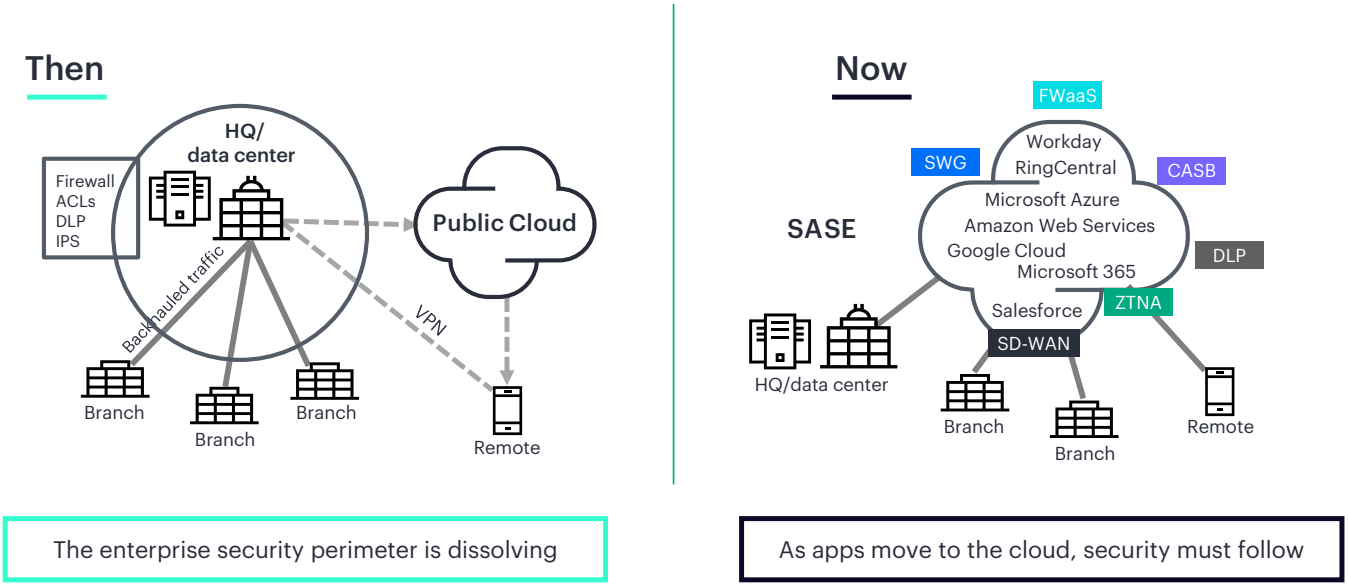

Figure 2. Moving applications to the cloud compels transformation of the network and security architecture

D. Methodology: steps to successfully implement SASE

1. Creating a cloud-first architecture with SD-WAN

The foundation of any SASE architecture is a modern, cloud-first SD-WAN. As most enterprise traffic is destined for SaaS and public cloud platforms, SD-WAN enables intelligent, application-aware steering at the edge. First packet identification allows applications to be identified immediately, enabling policies to be enforced from the start of the session rather than relying on static port-based rules, and intelligently steer traffic to the cloud directly from the branch. Trusted cloud application traffic, such as UCaaS traffic, is sent directly to the internet, while other internet-bound traffic is sent to an SSE (security service edge) solution for further inspection. Data center-hosted application traffic is routed to the headquarters or data center.

Cloud on-ramps extend the WAN fabric into major IaaS platforms such as AWS, Microsoft Azure, and Google Cloud™. This simplifies connectivity, improves resilience, and achieves consistent policy enforcement across on-premises and cloud environments. For IT teams, this step transforms the WAN from a transport mechanism into a strategic enabler of cloud adoption.

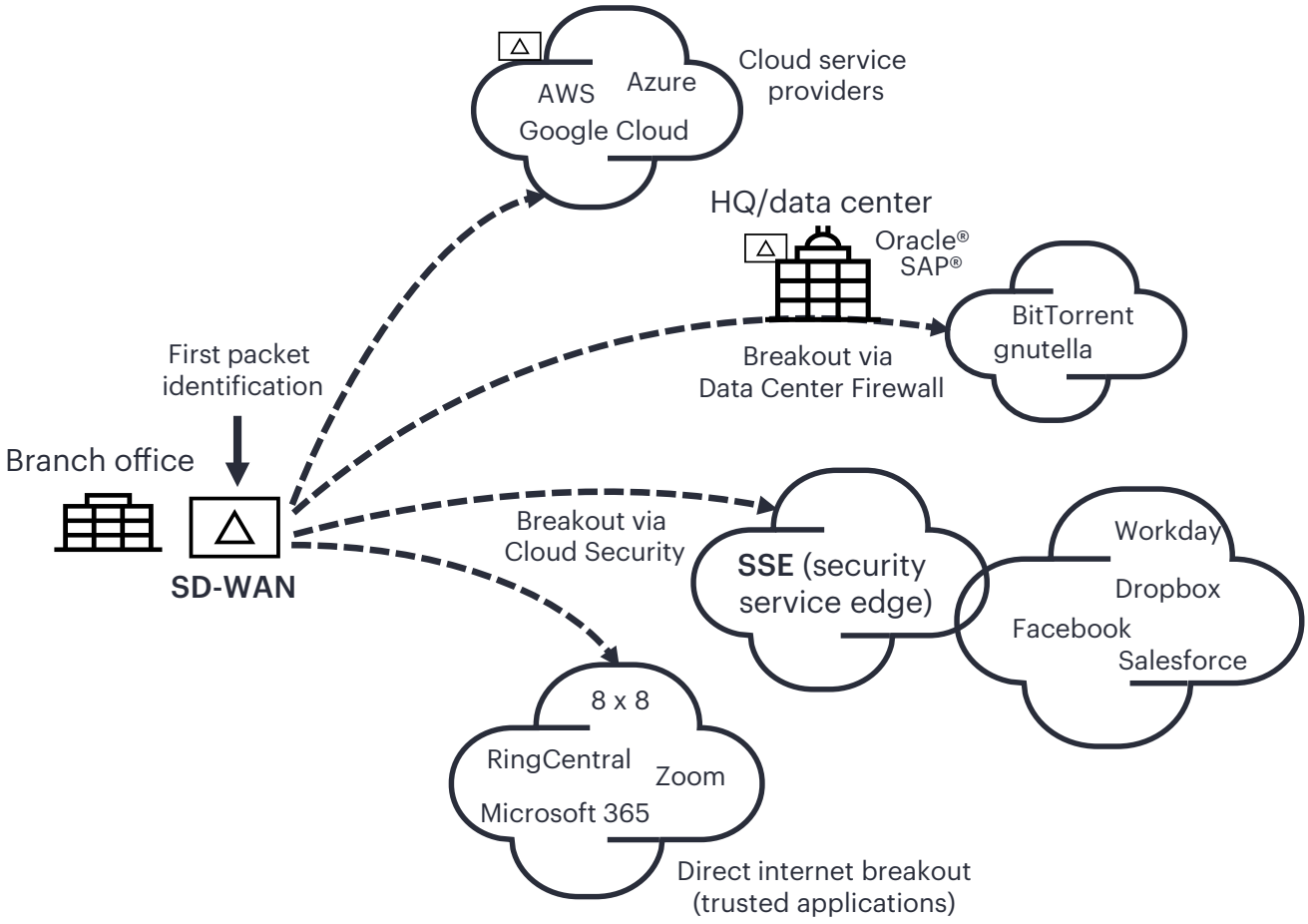

Figure 3. Intelligently steer traffic from the branch to the cloud based on first-packet identification

2. Consolidating branch equipment and protecting all devices with SWG

With a cloud-first SD-WAN foundation in place, organizations can significantly simplify and modernize their branch architectures. Many branches still rely on a combination of legacy routers and standalone firewalls that were designed for static, perimeter-based networks. These devices are often complex to manage, expensive to maintain, and poorly aligned with modern traffic patterns dominated by SaaS and cloud applications.

Secure SD-WAN platforms allow organizations to consolidate branch infrastructure by replacing legacy routers and firewalls with a single, integrated solution. Modern secure SD-WAN includes a next-generation firewall directly at the branch edge, enabling security controls to be enforced close to users and devices. These capabilities typically include intrusion detection and prevention systems (IDS/IPS), distributed denial-of-service defense (DDoS), URL filtering, and microsegmentation to reduce lateral movement and limit blast radius.

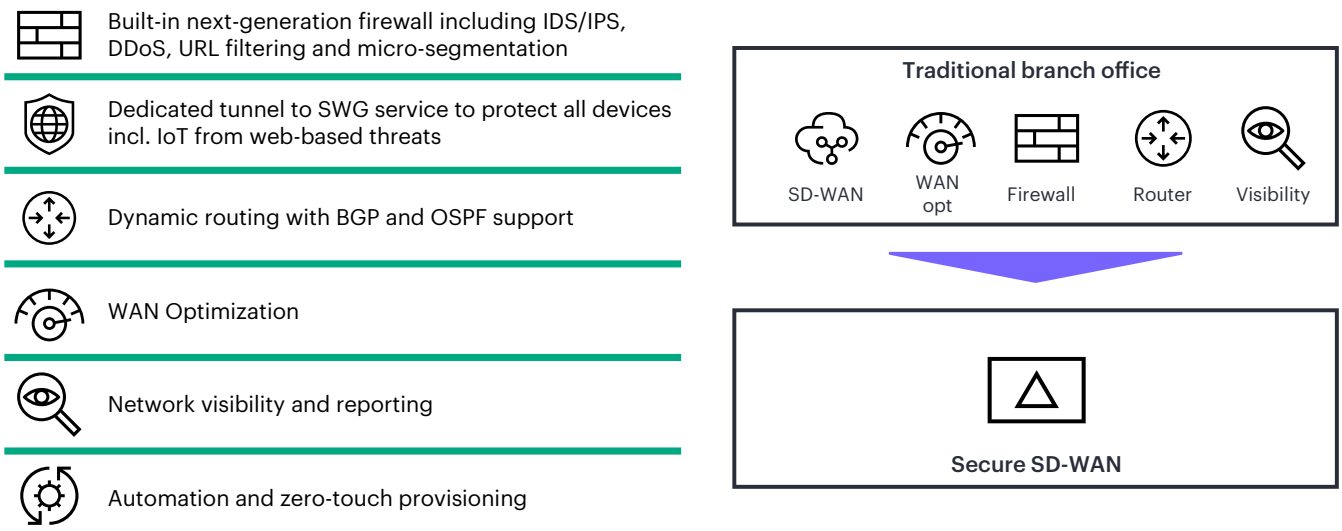

Figure 4. Consolidate branch equipment including firewall and router into one single solution

Organizations can extend protection further by integrating SWG services. SWG inspects all web-bound traffic for threats and policy compliance, performs deep content inspection including HTTPS decryption, detects zero-day malware and phishing attacks, analyzes files in sandbox environments, and enforces DLP policies. Advanced SD-WAN platforms can even establish a dedicated SWG tunnel from the branch to the SASE cloud, protecting all devices—including unmanaged IoT and guest devices—without requiring an SSE agent on every endpoint.

3. Implementing zero trust everywhere with universal ZTNA

A mature SASE architecture applies zero trust principles consistently across all environments, not only for remote users but also within branches, campuses, and data centers. This concept is often referred to as universal ZTNA, which extends zero trust from remote access into on-premises networks and cloud environments. Rather than assuming trust based on network location, universal ZTNA ensures that every user, device, and connection is continuously verified and grants access only to the specific applications and resources they are authorized to use.

Traditional VPNs stand in sharp contrast to this model. VPNs were designed to extend the corporate network perimeter to remote users, effectively placing users “on the network” once authenticated. This creates several risks. If a user’s credentials are compromised, attackers can gain broad network access. VPNs also enable lateral movement, allowing threats to spread across the internal network once inside. From a performance perspective, VPNs often introduce unnecessary latency by backhauling traffic through centralized gateways, even when users are accessing nearby SaaS or cloud services. As a result, VPNs struggle to deliver low latency and consistent performance for modern, cloud-first applications.

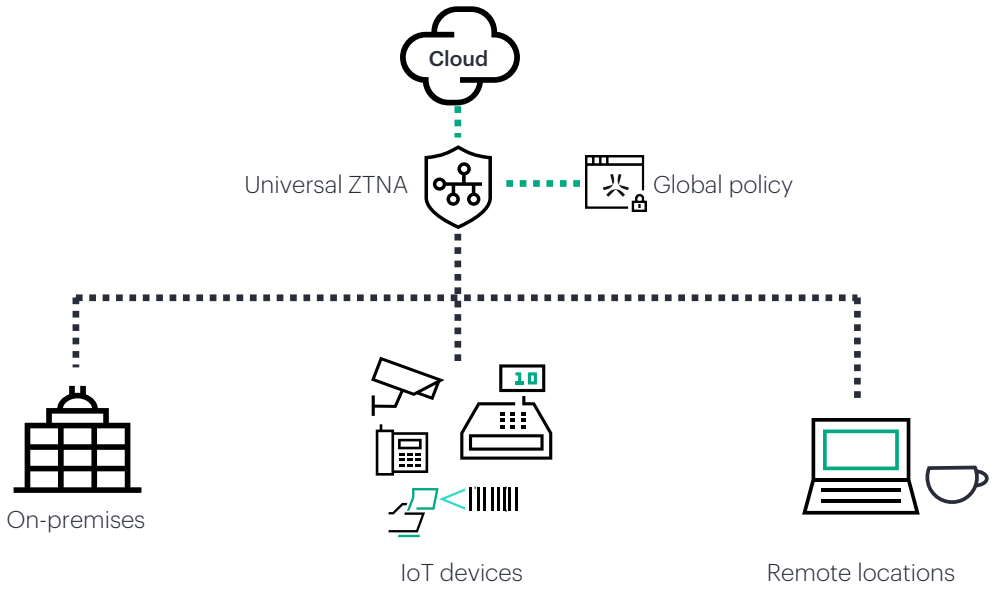

Figure 5. Universal ZTNA extends zero trust principles on-premises by combining ZTNA and NAC

ZTNA addresses these limitations by replacing network-level access with application-level access. Users connect only to the specific applications they are authorized to use, and applications are never directly exposed to the internet. Access decisions are made dynamically based on identity, device posture, and contextual signals, and are continuously re-evaluated throughout the session. Because ZTNA enables direct access to applications without forcing traffic through centralized VPN concentrators, it significantly reduces latency and improves user experience, particularly for SaaS and cloud-hosted workloads.

To fully realize zero trust, ZTNA must be complemented by Network Access Control (NAC). NAC provides visibility and control over devices as they connect to the network, whether those devices belong to employees, contractors, guests, or operational environments. Modern, AI-powered NAC solutions use machine learning to perform continuous device profiling and observability, analyzing network behavior to accurately identify device types and roles. This approach works across all devices, including unmanaged endpoints and IoT systems, which often lack traditional security agents and represent a growing attack surface.

By applying machine learning to network traffic patterns, AI-powered NAC can classify devices automatically, detect anomalous behavior, and adapt policies in real time. This deep observability allows organizations to understand not just who is connecting, but what is connecting and how it behaves over time. When combined with role-based policies and microsegmentation, NAC verifies that devices are placed into the appropriate trust zones and can communicate only with authorized services.

Microsegmentation is a critical component of this architecture. Rather than relying on broad network zones, microsegmentation enforces fine-grained policies between users, devices, and applications. This limits lateral movement and significantly reduces the blast radius of a compromised account or device. Even if an attacker gains access, their ability to move within the environment is tightly constrained by zero trust policies.

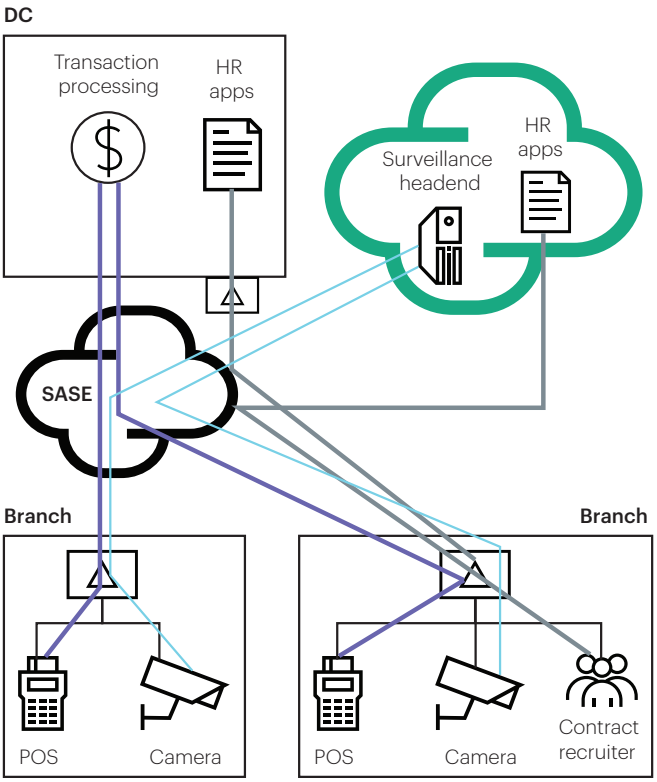

Figure 6. Segment the network with granular policies to restrict lateral movement and safeguard critical traffic from unauthorized access

4. Securing SaaS access with CASB and DLP

As SaaS applications become the primary way employees access business services and collaborate, organizations face growing challenges around visibility, control, and data protection. While IT teams may approve a set of sanctioned SaaS applications, employees frequently adopt additional cloud services on their own to improve productivity. This results in widespread use of unsanctioned SaaS applications, creating shadow IT and significantly increasing the risk of data exposure.

Shadow IT is particularly problematic because sensitive corporate data is often uploaded, shared, or synchronized with SaaS applications that have not been evaluated for security controls, data residency, or compliance requirements. Personal data, healthcare information, payment card data, or intellectual property may be stored in services that lack appropriate safeguards, creating risks of data leakage and regulatory non-compliance.

CASB capabilities address these challenges by restoring visibility and control over SaaS usage. CASB provides insight into both sanctioned and unsanctioned SaaS applications, enabling organizations to detect shadow IT, assess application risk, and enforce access and usage policies. Once policies are defined, CASB enables consistent enforcement across users and locations.

DLP strengthens SaaS security by monitoring how data is used within cloud applications. Integrated with CASB, DLP tracks user activities such as uploads, downloads, sharing actions, and data transfers. It enables organizations to identify sensitive data, apply classification rules, and prevent unauthorized disclosure or exfiltration.

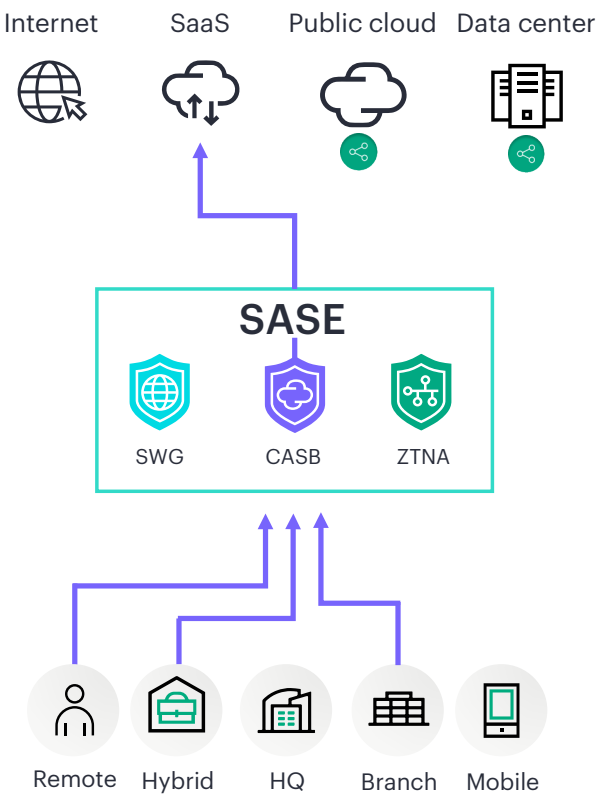

Figure 7. CASB provides visibility and enforces security policies, such as access control, data protection, and threat prevention across cloud and SaaS applications

Together, CASB and DLP help organizations meet regulatory requirements such as GDPR, HIPAA, and PCI DSS. They provide visibility into where regulated data is stored and accessed, enforce controls that limit unauthorized sharing, and support audit and reporting obligations. Within a SASE architecture, CASB and DLP extend security beyond the network into the application and data layers, where risk increasingly resides.

5. Monitoring and streamlining operations with AIOps

As SASE environments become more dynamic and distributed, operational complexity can shift from infrastructure management to data interpretation. Modern SASE platforms generate vast amounts of telemetry across networking, security, and user experience domains. Without automation and intelligence, extracting actionable insights from this data becomes a bottleneck for operations teams.

AIOps addresses this challenge by correlating telemetry end-to-end and applying machine learning to detect anomalies, identify root causes, and surface meaningful insights. Beyond traditional dashboards, advanced AIOps platforms enable operators to interact with the environment using natural-language queries, allowing them to ask questions such as why application performance degraded, which users are impacted, or whether a security policy change introduced latency.

This natural-language interaction significantly streamlines operations by reducing the expertise and time required to investigate issues. AIOps also helps simplify configuration by recommending policy adjustments, validating changes before deployment, and automating routine tasks. During incidents, AI-driven troubleshooting accelerates mean time to resolution by guiding operators directly to the most likely causes and corrective actions.

For IT architects, AIOps transforms SASE from a complex, interconnected architecture into an operationally manageable platform, enabling proactive operations, faster troubleshooting, and continuous optimization. The result is lower operational overhead, improved reliability, and a more resilient security posture at scale.

E. What are the best practices for a SASE project?

Implementing SASE is a multi-year transformation that affects architecture, security posture, operations, and organizational alignment. Success depends on clear architectural intent, strong collaboration, and disciplined execution.

— **View SASE as a modern network architecture with built-in security.**
Treat SASE as an architectural foundation for cloud-first networking, not a collection of security tools. Embedding security into the network fabric supports SaaS, hybrid work, and cloud adoption without recreating legacy perimeters.

— **Avoid trying to do too much too soon.**
Adopt a phased approach instead of a big-bang migration. Start with cloud-first SD-WAN, then layer security and zero trust capabilities to reduce risk and deliver incremental value.

— **Establish a core SASE team with clear roles and responsibilities.**
Create a cross-functional team spanning networking, security, cloud, and operations. Clear ownership for architecture, policy, and operations provides consistency and faster decision-making.

— **Work closely with the security team from the start.**
SASE blends networking and security, making early alignment essential. Collaborate on zero trust principles, threat models, and compliance requirements to balance performance and protection.

— **Set up an executive board to define direction and monitor progress.**
Executive sponsorship provides strategic guidance, resolves cross-team dependencies, and keeps the program aligned with business priorities.

— **Ensure KPIs reflect both operational and strategic goals.**
Move beyond uptime metrics to include application performance, user experience, security effectiveness, and operational efficiency.

— **Set quantifiable objectives early.**
Define measurable goals such as reduced latency, faster branch deployment, or improved MTTR to enable accountability and data-driven decisions.

— **Use dashboards tailored to each stakeholder.**
Provide role-specific visibility for operations, security, and executives so insights translate into action.

— **Implement a communication plan to share the SASE vision broadly.**
Clearly explain the rationale, benefits, and roadmap to build alignment and drive adoption across the organization.

Conclusion

SASE represents more than the adoption of new technologies; it is a shift toward a modern network architecture with security built in from the ground up. By combining cloud-first SD-WAN, zero trust access, SaaS and web security, and AI-driven operations, SASE enables organizations to deliver secure, high-performance access wherever users, devices, and applications reside.

For IT architects, success with SASE depends on treating it as a long-term architectural evolution rather than a point solution. A phased implementation, strong collaboration with security teams, clear governance, and measurable objectives are essential to realizing its full value. When approached correctly, SASE simplifies complexity, strengthens security, improves user experience, and provides a scalable foundation for future cloud and digital initiatives.

Successfully implement SASE with HPE

HPE provides a fully integrated zero trust platform that unifies a single-vendor SASE solution with advanced, AI-powered NAC capabilities. This platform enables organizations to enforce a universal ZTNA model.

HPE integrates secure SD-WAN, cloud-native SSE services, universal zero trust, and AI-driven operations into a single platform. This enables IT architects to implement SASE pragmatically, delivering secure, high-performance access aligned with cloud, SaaS, and hybrid work realities while remaining adaptable to future requirements.

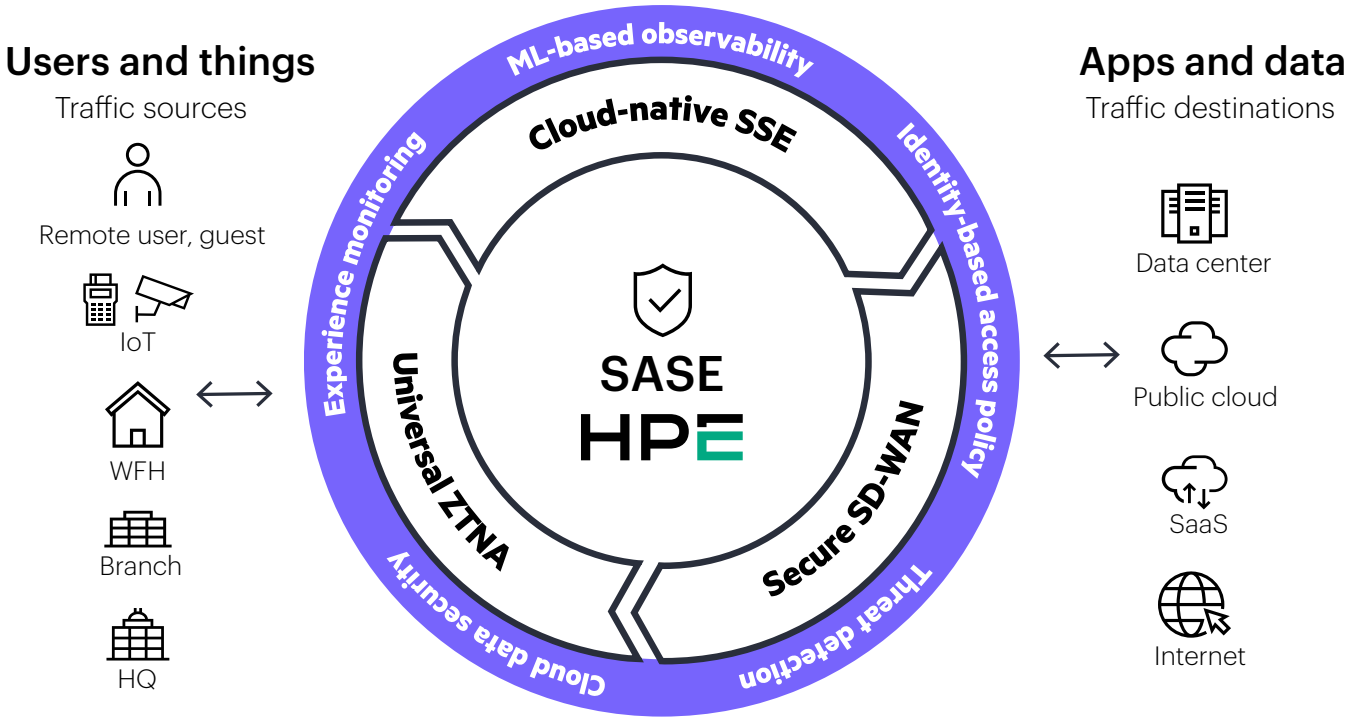

Figure 8. HPE provides a fully integrated zero trust platform that unifies a single-vendor SASE solution with advanced, AI-powered NAC capabilities

HPE Networking SASE provides a unified, cloud-first foundation for modern networks by overcoming the limitations of traditional router-based architectures.

Using first-packet identification, EdgeConnect SD-WAN intelligently steers traffic directly to the cloud to reduce latency and improve user experience. Business Intent Overlays translate business and security requirements into policy-driven networking, while Path Conditioning and optional WAN optimization deliver private-line performance over standard internet links, reducing reliance on MPLS. AppExpress continuously monitors experience for mission-critical applications and dynamically selects the optimal path using real-time and synthetic telemetry. Native integration with AWS, Microsoft Azure, Google Cloud, and connectivity partners such as Equinix and Megaport enables resilient multicloud networking.

At the branch, integrated next-generation firewall capabilities—IDS/IPS, Adaptive DDoS protection, URL filtering, and role-based segmentation—simplify security, while deep SWG integration extends malware protection and web filtering to all devices, including unmanaged IoT, without agents.

Cloud-native SSE unifies ZTNA, SWG, and CASB under a single policy engine and UI, enforcing policies once and everywhere with single-pass inspection at each point of presence. Combined with AI-powered NAC, the SASE architecture gains deep device observability and machine-learning–based profiling across all endpoints, enabling universal ZTNA enforcement based on both user and device context.

Delivered at global scale across more than 500 hyperscaler-powered edge locations with smart routing and fast failover, the platform achieves consistent performance and security worldwide. AI-driven AIOps and the SASE Copilot further streamline configuration, troubleshooting, and operations through generative AI, improving efficiency and resilience at scale.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

© Copyright 2026 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Google Cloud is a registered trademark of Google LLC. Azure and Microsoft are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. SAP is the trademark or registered trademark of SAP SE or its affiliates in Germany and in other countries. Oracle is a registered trademark of Oracle and/or its affiliates. All third-party marks are property of their respective owners.

a00158270ENW

HEWLETT PACKARD ENTERPRISE

hpe.com