HPE

Article

Evaluating SASE: five use cases to protect, secure, and modernize

As applications, users, and data continue to move beyond the traditional network perimeter, many organizations are evaluating how they connect and protect their environments. Cloud adoption, SaaS usage, and hybrid work have changed traffic patterns and access requirements, often exposing the limits of architectures built around fixed locations, backhauled traffic, and disconnected tools.

SASE is increasingly part of that evaluation. Rather than treating networking and security as separate disciplines, SASE brings them together through a cloud delivered approach designed to support modern access patterns and security needs.

SASE is not an all-or-nothing decision. Many organizations approach it as a journey, adopting capabilities over time based on their priorities, existing infrastructure, and risk posture. The following use cases reflect common points along this journey. They highlight how organizations evaluate SASE in practical terms, by addressing immediate challenges while building toward a more unified networking and security model over time.

1. Modernizing branch connectivity for a cloud-first world

Branch networks were originally designed for an era when most applications lived in the data center and traffic followed predictable paths. Today, cloud and SaaS applications dominate traffic patterns, and backhauling data through centralized infrastructure can introduce latency, complexity, and unnecessary cost, especially across distributed branch locations.

Modernizing branch connectivity with a secure SD-WAN enables organizations to adapt to these cloud-first realities. By consolidating networking and security functions at the branch and applying centralized, application-aware policies, organizations can optimize performance for cloud and SaaS traffic while maintaining consistent controls across locations. This approach reduces reliance on legacy branch architectures and provides a more flexible foundation for integrating broader SASE capabilities over time.

What this enables

- Direct, optimized access to cloud and SaaS applications from branch locations
- Simpler branch designs by consolidating routing, security, and connectivity functions
- Improved application performance through application-aware traffic steering
- Greater operational efficiency when managing distributed branch environments

2. From VPN to ZTNA: securing access for hybrid work

As hybrid working is becoming the norm, many organizations are assessing how remote users access private resources. Traditional VPN-based access models were designed for environments where applications lived in the data center, and users worked from predictable locations. In today's cloud-first environments, these models can introduce performance bottlenecks and grant broader network access than is necessary for most users.

ZTNA shifts access decisions from the network to the identity. Rather than placing users onto the network, ZTNA enforces identity and policy-based access at the application level, supporting least privilege principles across employees, contractors, and third -party users. This approach enables organizations to provide secure access to private applications without exposing the underlying network or relying on VPN tunnels designed for a different era.

What this enables

- Application-level access instead of broad network connectivity
- Least privilege policies based on user identity and context
- Consistent access controls for remote, on-premises, and third-party users
- A practical starting point for organizations rethinking secure access in cloud-first environments

3. Applying consistent security across users, web, and SaaS

Securing access to private applications is only part of the challenge. As reliance on cloud services and SaaS applications becomes increasingly common, security controls must extend beyond private application access alone. Users interact with the internet and SaaS platforms from a wide range of locations and devices, making it difficult to maintain consistent visibility and policy enforcement using traditional, perimeter-based tools.

A unified SSE (security service edge) approach, adding SWG (secure web gateway) and CASB (cloud access security broker) capabilities to ZTNA, applies security policies consistently across user access, web traffic, and SaaS usage. By managing these controls together rather than as isolated tools, organizations can reduce policy gaps, improve visibility into user activity, and enforce protections more uniformly as environments become more distributed. This model helps security teams address web-based threats, manage SaaS risk such as shadow IT and data loss, and apply least privilege principles without adding unnecessary operational complexity.

What this enables

- Consistent policy enforcement across users, web traffic, and SaaS applications
- Improved visibility into web activity and SaaS usage
- Safer internet browsing and protection against web-based threats
- A scalable security foundation for cloud-first environments

4. Protecting IoT and unmanaged devices with universal ZTNA

IoT and edge devices remain one of the most persistent security gaps in modern environments. Many are unmanaged, difficult to patch, and unable to run endpoint agents, making it challenging to apply traditional zero trust controls consistently. As these devices increasingly connect to enterprise networks and cloud services, they expand the attack surface in ways that user-centric and perimeter-based security models were never designed to address. Universal ZTNA extends identity-driven access controls beyond users to include IoT and other unmanaged devices, using profiling, segmentation, and global policies to limit what each device can access.

AI-powered NAC strengthens this approach and helps protect unmanaged devices and IoT, by improving device visibility, behavior analysis, and continuous trust validation across environments. Once authenticated, IoT traffic can be segmented, isolating it from mission-critical application traffic. Also, because many IoT devices generate internet and cloud traffic for activities such as updates and telemetry, integrating SWG capabilities with secure SD-WAN enables organizations to protect these devices without installing an SSE agent on each one. This approach expands web security to all devices and provides protection against harmful websites, through functionalities like URL filtering. Together, these capabilities help organizations close IoT security gaps while applying consistent zero trust protection across users, devices, and traffic.

What this enables

- Visibility into IoT and unmanaged devices through profiling and behavior analysis
- Segmented access policies that limit device reach and reduce lateral risk
- Consistent zero trust enforcement for devices that cannot run agents
- Web threat protection for IoT traffic without adding endpoint complexity

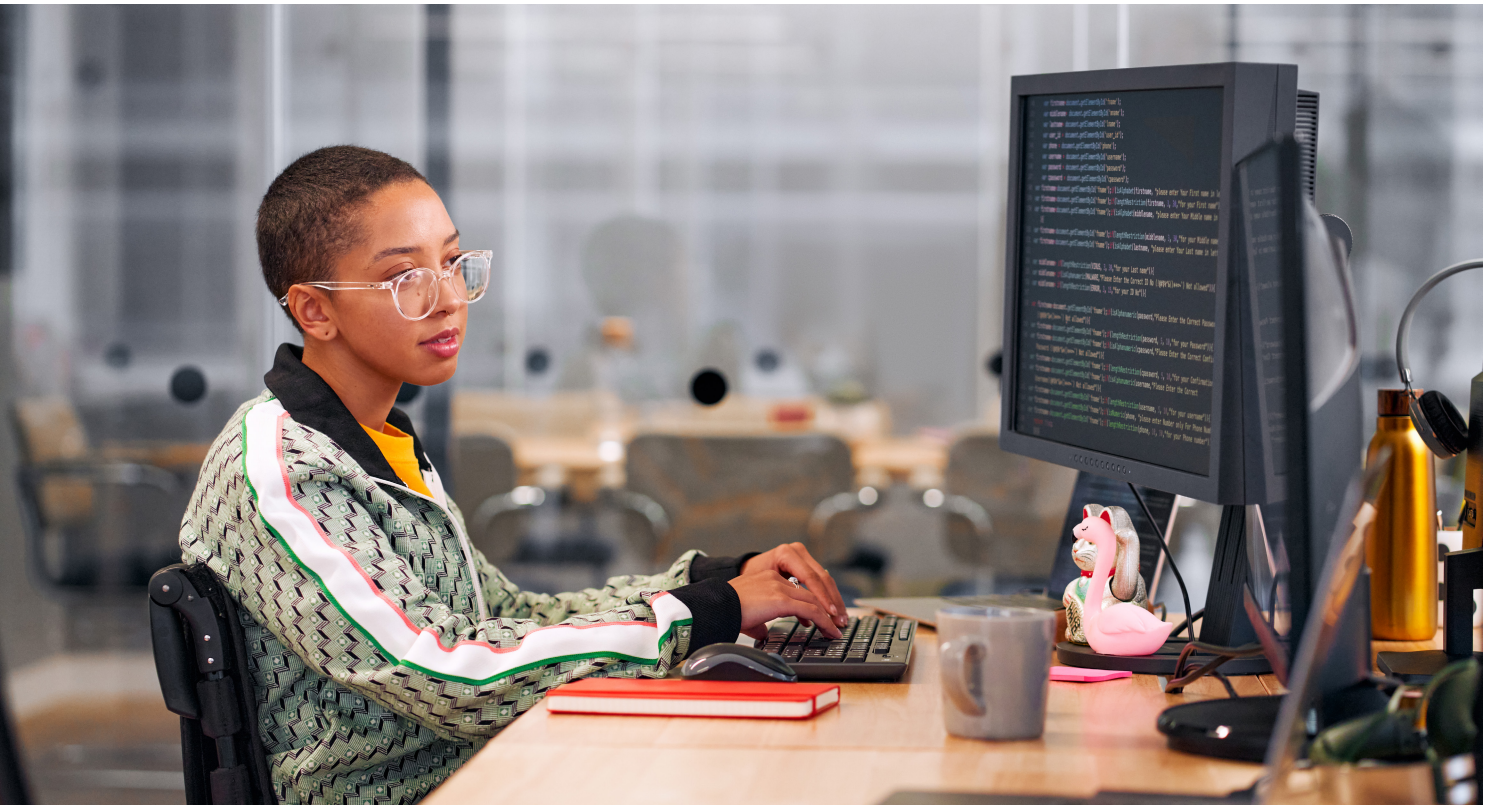
5. Bringing access, security, and connectivity together with unified SASE

Managing access, security, and connectivity as separate initiatives can introduce unnecessary complexity. Disconnected tools, overlapping policies, and manual integration efforts often slow down deployment and make it harder to maintain consistency as environments expand. Over time, this fragmentation can increase operational overhead and limit an organization's ability to adapt to new requirements.

A unified SASE architecture brings these capabilities together under a single, cloud-delivered model. By aligning secure access, web and SaaS protection, and modernized branch connectivity, organizations can simplify how changes are introduced and managed across users, applications, and locations. This unified approach supports faster adoption, reduces integration effort, and helps teams operate with greater confidence as their environments continue to evolve.

What this enables

- Simpler adoption of SASE capabilities without stitching together multiple platforms
- Reduced operational overhead through unified management and policy models
- Faster rollout of changes across users, applications, and locations
- A cohesive architecture that scales without adding unnecessary complexity



Supporting Your Journey to Unified SASE

Organizations evaluating SASE often approach it as a journey rather than a single, all-at-once initiative. By addressing access, security, and branch modernization first, and then bringing those capabilities together through a unified SASE architecture, organizations can build a foundation that supports flexibility, consistency, and long-term scalability as requirements continue to evolve.

Throughout this journey, HPE is positioned to help at every stage. Our AI-native unified SASE platform integrates SD-WAN, SSE, and NAC into a single, identity-driven architecture. And leveraging AIOps, the platform delivers advanced observability and authentication, providing organizations with real-time visibility and ongoing trust validation for users, devices, and applications, even across third-party environments.

Organizations can now move forward with confidence, whether they are taking their first steps toward SASE or looking to unify capabilities they already have in place.

Learn more at

HPE.com/networking

Visit HPE.com

Chat now

a00158357ENW

HEWLETT PACKARD ENTERPRISE

hpe.com