perimeter 81

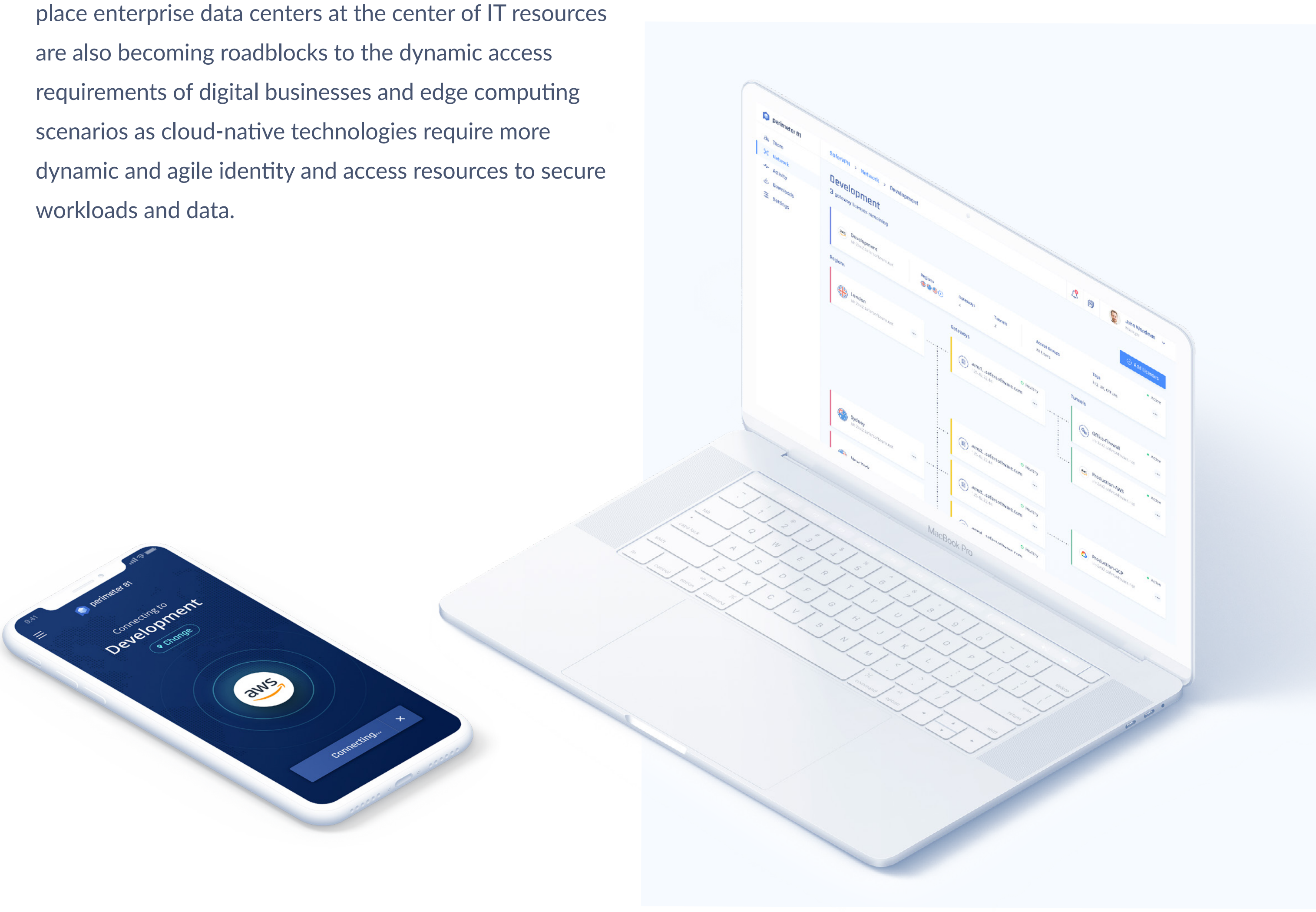
Why Your Organization Needs to Adopt the SASE Model

Introduction

As organizations continue to drive compute workloads to the cloud and mobile devices proliferate, edge computing is changing access requirements with billions of connected devices requiring cloud services and on-premises resources. At the same time, more users, devices, applications, services and data are being generated and located outside of an organization than inside.

Traditional network security architectures that typically place enterprise data centers at the center of IT resources are also becoming roadblocks to the dynamic access requirements of digital businesses and edge computing scenarios as cloud-native technologies require more dynamic and agile identity and access resources to secure workloads and data.

With numerous cybersecurity and network security solutions offered across a highly segmented market space, too many security services and categories are complicating what should be an integrated approach to an organization's network security environment. The entire cybersecurity vendor community needs to come together and provide a holistic approach to cybersecurity, and this is where the concept of Secure Access Service Edge or SASE comes in.



The Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE), pronounced "sassy," is a new cloud-based network security model proposed by research firm Gartner that combines multiple network technologies delivered as a service including SWG, CASB, FWaaS and ZTNA with WAN capabilities (i.e., SDWAN) to support dynamic secure access to organizational assets. This new model allows IT security teams to easily connect and secure all of their organization's networks and users in an agile, cost-effective and scalable way.

"Essentially, SASE is a new package of technologies including SD-WAN, SWG, CASB, ZTNA and FWaaS as core abilities, with the ability to identify sensitive data or malware and the ability to decrypt content at line speed, with continuous monitoring of sessions for risk and trust levels," says Gartner Research Vice President Andrew Lerner.

Gartner also believes that SASE offerings will provide policy-based "software defined" secure access from an infinitely flexible network fabric through which enterprise security professionals can precisely specify the level of performance, reliability, security, and cost of every network session based on identity and context.

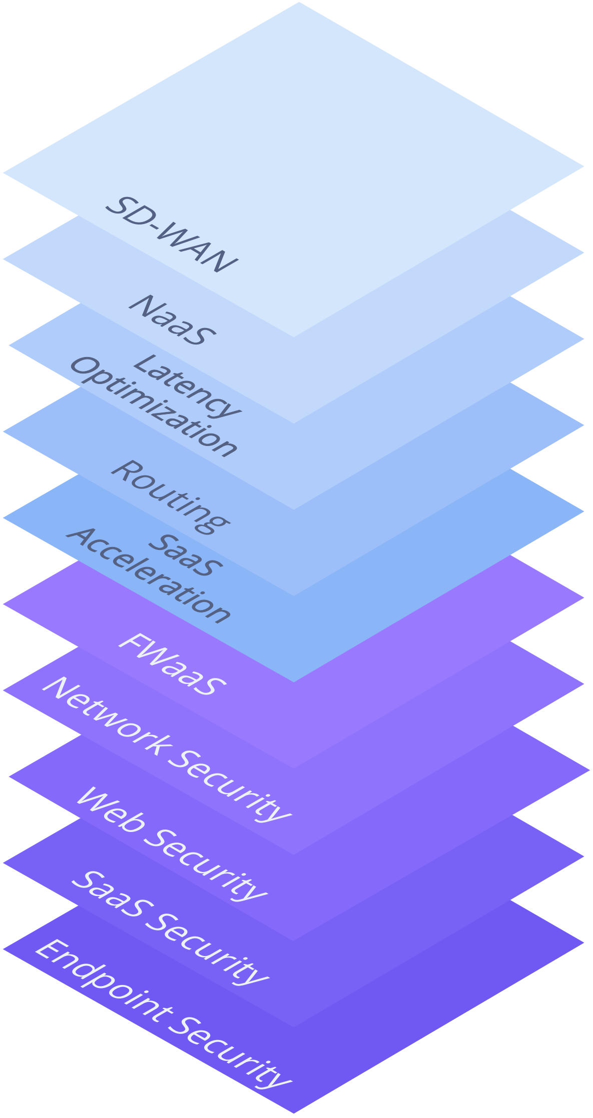


Figure 1. SASE Convergence

1 https://blogs.gartner.com/andrew-lerner/2019/12/23/say-hello-sase-secure-access-service-edge/

Benefits of SASE and Use Cases

SASE enables the delivery of integrated secure network security services that supports digital business transformation, edge computing, workforce mobility and identity and access management. In addition to improved security and network performance, key benefits include increased user and IT staff productivity, operational efficiency, cost reduction and new digital business scenario enablement. Additionally, cloud-based SASE offerings enable organizations to update their security solutions against new threats and establish policies more quickly for agile adoption of new security capabilities.

SASE reduces complexity and costs with the goal of consolidating secure access services from a single provider. By reducing the overall number of security vendors and solutions, the number of physical and/or virtual appliances will be reduced along with the number of agents needed for end-user and edge devices. As more SASE services are adopted in the long run, additional cost reductions will be realized through the further consolidation of vendors and security technology stack simplification.

SASE services will also let organizations make their applications, services, APIs and data securely accessible to third-parties such as partners and contractors, without the risk exposure of legacy VPN and demilitarized zone (DMZ) architectures.

Network performance can be increased with SASE solutions providing optimized traffic routing across global POPs (points of presence) for latency-sensitive apps such

- ✓ Complexity and cost reduction
- ✓ Ease of use and user transparency
- ✓ Zero Trust Network Access
- ✓ Enable new digital business scenarios
- ✓ Improved security
- ✓ Increased security staff effectiveness
- ✓ Improving network performance
- ✓ Low operational overhead
- ✓ Centralized policy management with local enforcement

as collaboration, video, VoIP, and web conferencing. Using policy controls and enforcement, users will be routed through SASE compliant high-bandwidth networks and peering partners.

The number of agents required on a device will be reduced with SASE compliant solutions such as Zero Trust Network Access to a single agent or device with streamlined access policies that do not require user interaction while at the same time providing a consistent access experience regardless of location and resource requested.

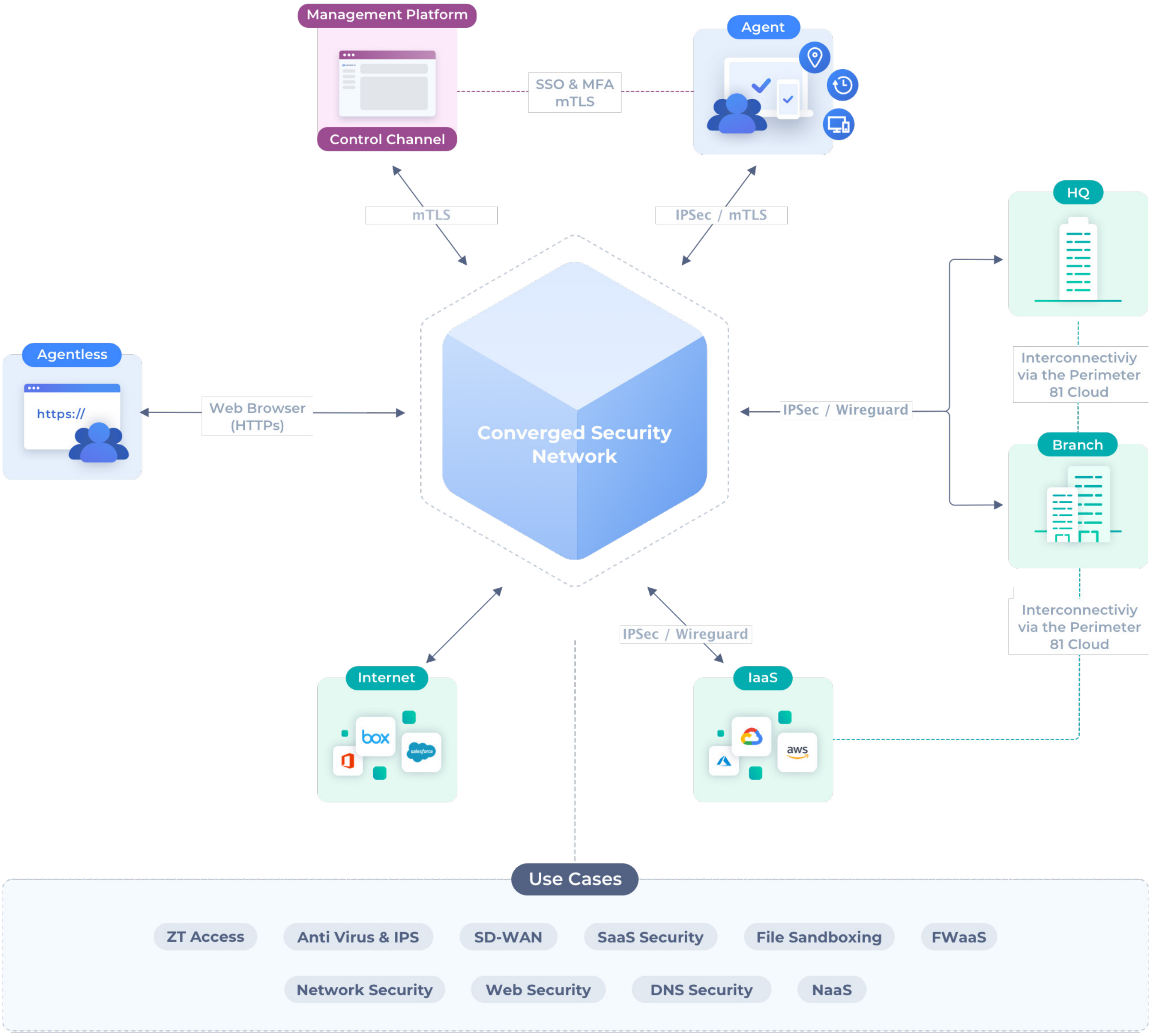
By providing zero-trust protection of user sessions seamlessly and consistently on and off of the enterprise network, SASE solutions will provide end-to-end encryption as well as web application and API protection (WAAP) services. Using Zero Trust Network Access, SASE solutions will also extend protection to endpoint devices for public Wi-Fi network protection to protect remote workers.

Using consistent SASE policy controls will enable content inspection for sensitive data identification or malware "at line speed" based on user and device across any network or cloud resource, globally. In addition, policy controls allow for distributed enforcement points close to cloud resources and user devices for local decision making where needed.

Finally, SASE can increase the effectiveness of IT and network security staff by eliminating the need and time to set up physical infrastructure letting them focus on cloud-based business, compliance, and application access requirements.

Perimeter 81 and the SASE Approach

Perimeter 81's SASE platform combines network and security functions into one unified network security service solution. The cloud-native offerings fall under the SASE network and endpoint security solutions managed and delivered through the Perimeter81 platform to provide user centric network and policy management for organizations of all sizes.



The global, multi-region and multi-tenant Perimeter 81 cloud network provides a comprehensive set of secure network capabilities that includes SaaS security for Office 365, Google Drive and Dropbox as well as a Firewall as a Service (FaaS) to protect an organization's site-centric networks from potential threats, while implementing modern security features of a next-generation firewall.

Cloud Sandboxing analyzes unknown files for zero-day exploits and advanced persistent threats both on and off the network and DNS Security automatically blocks malicious domains that are identified with real-time analysis with global threat intelligence.The Perimeter 81 platform also predicts and stops malicious domains containing algorithm-based malware payloads with instant enforcement.

For complete endpoint security, Perimeter 81 delivers multiple endpoint protection capabilities, including Wifi protection, next-generation malware protection and support for visibility into encrypted traffic. With endpoint compliance, Perimeter 81 scans for security feature updates including Firewalls, Antivirus, Windows patches and malware for a more secure network and threat-free network.

Perimeter 81's Zero Trust Network Access (ZTNA) provides policy enforcement and protection by isolating applications and segmenting network access based on user permissions, authentication, and verification. The platform's comprehensive software-defined perimeter (SDP) solution offers simple cloud migration security, seamless least privilege access to resources and secured access to cloud environments including IaaS and PaaS.

About Perimeter 81

Perimeter 81 is a cloud-based, Secure Network as a Service provider, driven by the mission to transform secure network access for the modern and distributed workforce. Built from scratch based on input from security leaders needing a change from legacy VPN technology, Perimeter 81's user-friendly interface, unified management and seamless integration with major cloud services, allows employees to securely access on-premise and remote resources, and gives companies of all industries and sizes the power to be fully mobile and confidently cloud-based.

Contact Us

https://www.perimeter81.com

+1-646-518-1997

Request a Free Demo

Follow Us

in f ▶ Blog

perimeter 81