SASE FOR SUPERHEROES

The Ultimate Integration eBook

perimeter 81

INTRODUCTION

perimeter 81

SASE stands for Secure Access Service Edge.

It's a new network security approach that is changing the way organizations secure the data, resources, and users present in their networks.

SASE software solutions provide organizations the opportunity to connect to a single secure cloud network as a service where they can gain access to physical and cloud resources. In the hands of IT, SASE security enables a more holistic and agile service for business networking and multilayered defense for organizations.

What makes SASE innovative and disruptive is the idea that as a combination of security tools becomes unified and streamlined, it enhances the overall productivity, security posture, and bottom line of any organization.

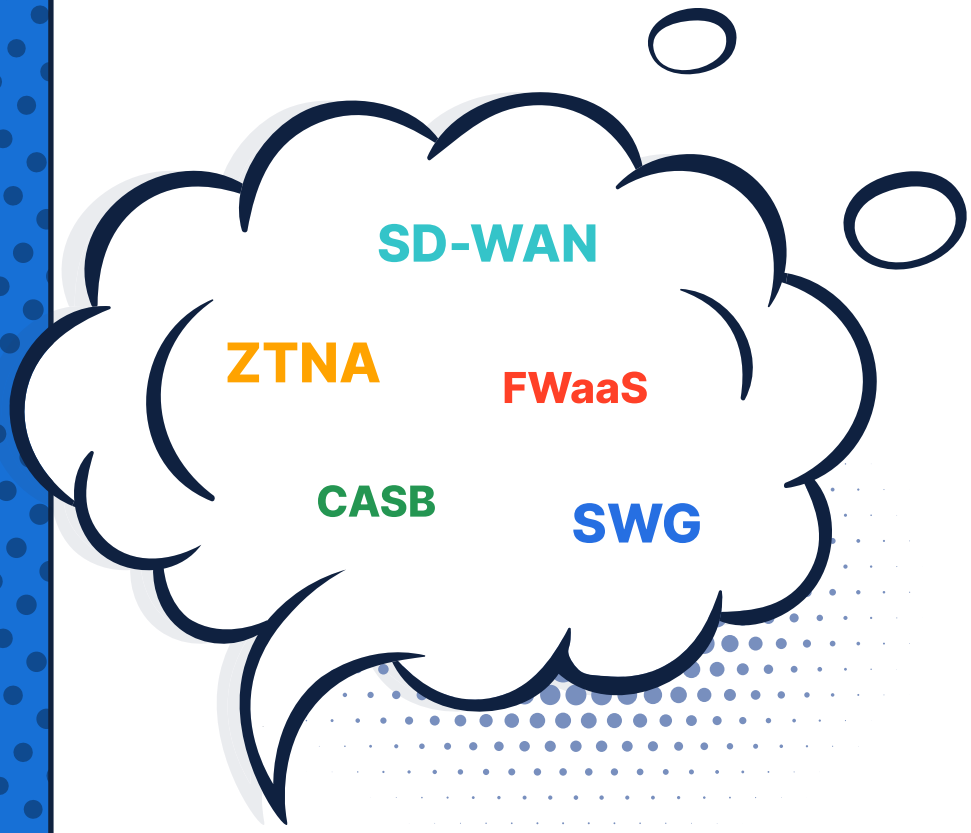
Due to the software-defined nature of its architecture, SASE lets IT set up and manage networks effortlessly from afar, and create custom user-focused access policies based on device, role, and other granular qualifiers. Plus, SASE includes monitoring and logging utilities, and total network visibility and access control from a centralized admin panel with no hardware or intense management required.

Moving from Site-Centric to User-Centric Security

Now more than ever, due to COVID-19 health concerns, businesses are required to enforce company-wide work-from-home policies. For many organizations, this new reality finds entire teams working remotely for the first time ever.

Remote work is now considered a key element of effective business operation due to results including greater agility, employee satisfaction and productivity, and reduced costs.

perimeter 81



So the key question is not what a site or organization's security profile is, but rather what is the security profile of a given employee inside or outside the office, no matter their location.

And because SASE integrates easily with cloud-based and local resources, IT can integrate sophisticated security ideas into every corner of the network, creating a more scalable security apparatus that can be instantly deployed to new departments and employees.

This e-book will help organizations understand the components of a SASE solution and how they integrate together.

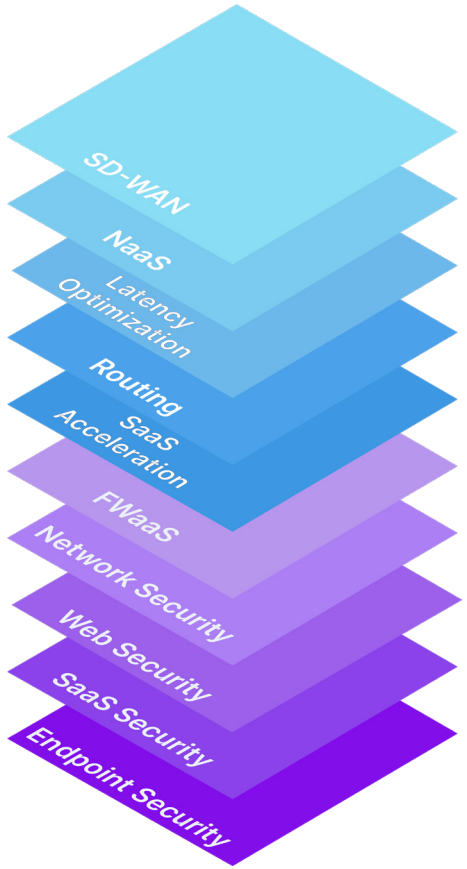
WHAT IS SASE?

perimeter 81

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.

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. This includes SWG, CASB, FWaaS and ZTNA with WAN capabilities (i.e., SDWAN) to support dynamic secure access to organizational assets.



The three main use cases of SASE include Zero Trust remote access enabling users to access internal resources, Internet security for user or branch connections to the Internet and/or SaaS, and finally, branch office to branch office interconnectivity.

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.

A single, integrated SASE solution combines the various vital networking and security tools that many IT teams still consume separately, and puts them on the cloud.

A varied stack of products – like a firewall, VPN, and 2FA solution, for example – can be effective at securing a network and "locking the door" against hackers, but not ideal.

Unification of common, crucial networking and security ideas inside one cloud-hosted administration panel eliminates much of the effort that IT expends configuring many products to work together. When an organization has a growing number and variety of employees and business resources, one streamlined solution is best.

"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."

- **Andrew Lerner, Gartner Research**
  Vice President

perimeter 81

Integrating SASE Components

Gartner believes that SASE offerings will provide policy-based “software defined” secure access from an infinitely flexible network fabric.

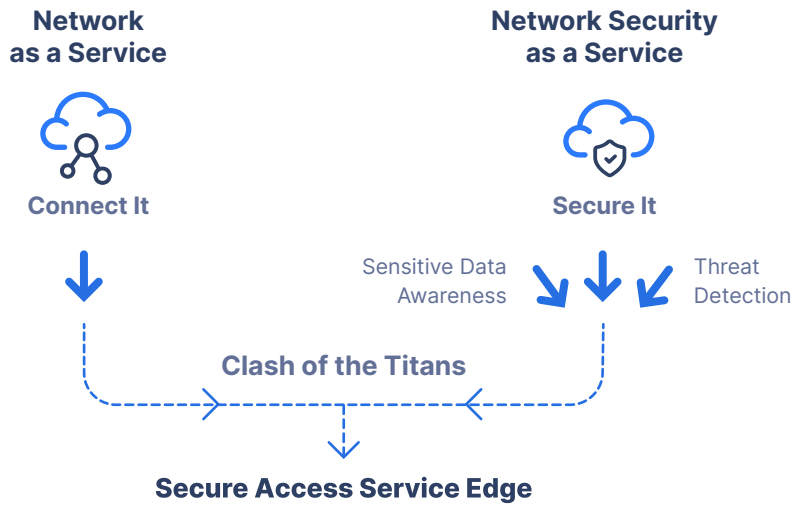
Integrating SASE components into the network fabric will also enable enterprise security professionals to precisely specify the level of performance, reliability, security, and cost of every network session based on identity and context.

A single, unified SASE solution combines stand alone services offered in a streamlined package that has never ever existed in this form before.

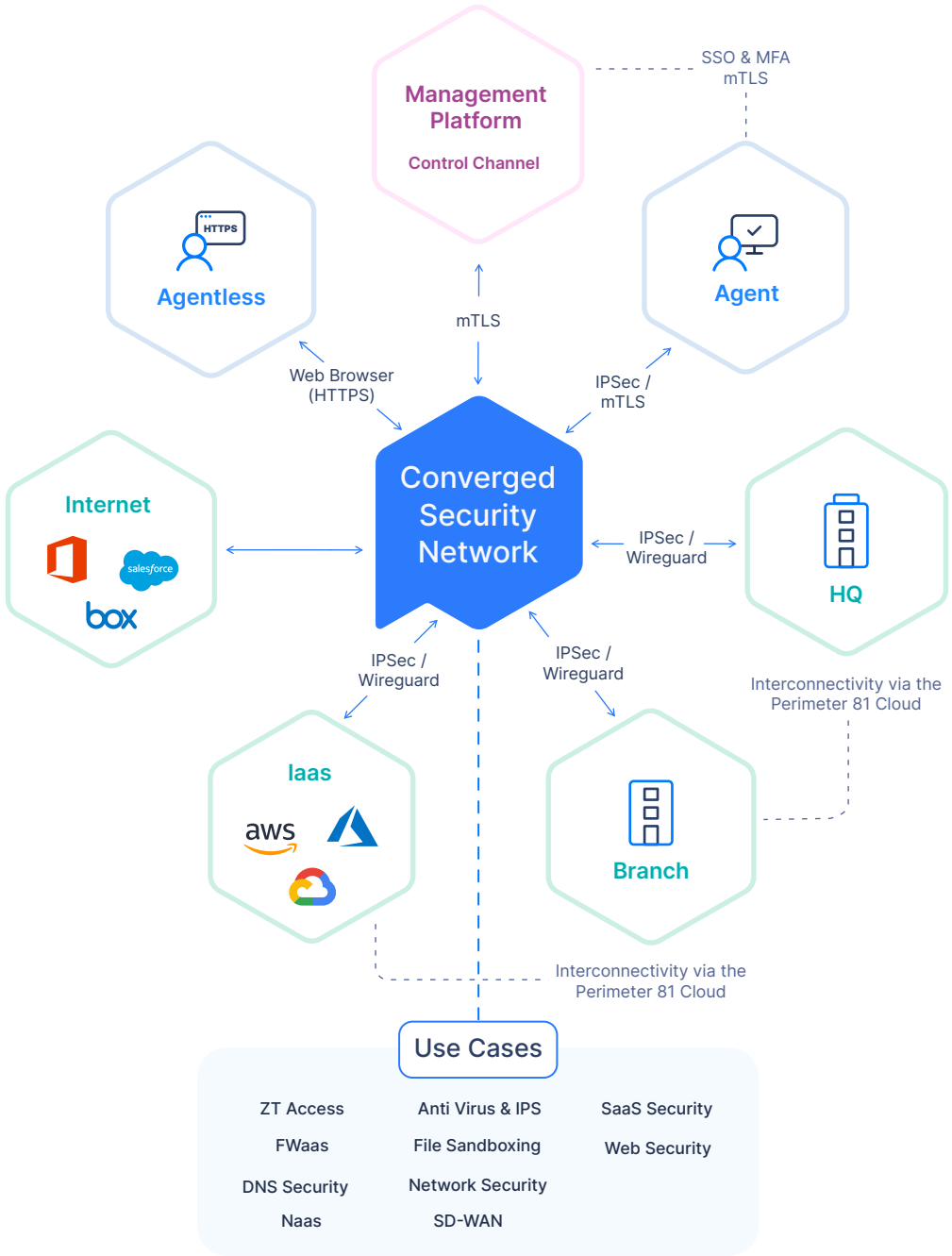
This combination of SASE components and functions each contributes a crucial building block of the overall security fabric.

Next, we detail the essential services and technologies that make up the core of a SASE configuration.

Secure Access Service Edge Convergence



Source: Gartner, The Future of Network Security Is in the Cloud, MacDonald, Orans and Skorupa, 30 August 2019



The core SASE components of today include:

SD-WANaaS

(Software-Defined Wide-area Network)

Multi-Regional Cloud Edge Network

Firewall as a Service (FWaaS)

Zero Trust Network and Application Access

SaaS Security (CASB)

Secure Web Gateway (SWG)

Cloud Sandboxing

Encrypted Tunneling

DNS Filtering

perimeter 81

SD-WANaaS and Multi-Regional Cloud Edge Networks

An SD-WAN, also known as a software-defined wide-area network as a service, is a virtualized network that is abstracted from datacenter or branch office hardware to create an easily configurable and scalable overlay wide area network distributed across local and global sites.

It's also an application of Software Defined Network (SDN) technology that is more reliable and scalable than VPN-based WAN solutions because it takes a software-based approach to building and extending enterprise networks beyond the core SDN.

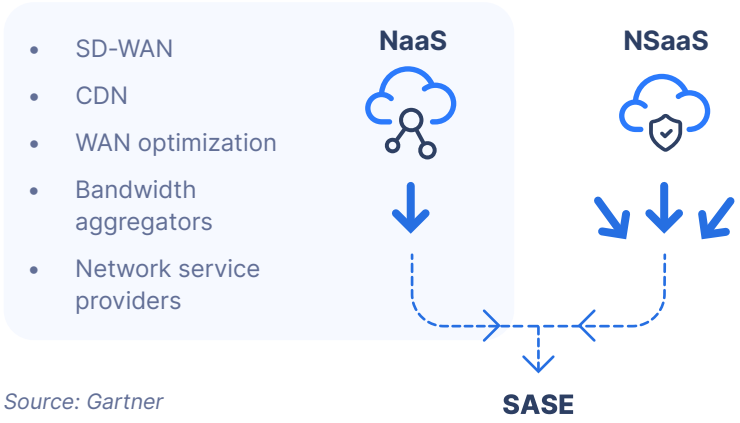
The challenge with SD-WANs, however, is that the virtualized network "fabric" may not always include the security and access controls that organizations require to protect their networks across multi-cloud environments.

By combining Secure Access Service Edge or SASE solutions with SD-WAN technology, organizations can deploy flexible and scalable comprehensive security functions across their virtualized networks both locally and globally.

SD-WANs can also be used to deploy multi-regional cloud edge networks that position compute resources close to end users where they reduce network latency and expedite services to generate greater value.

Multi-cloud requirements for SD-WAN platforms include branch-multi-cloud connectivity to scale enterprise applications across major cloud providers, and consistent application performance with security policies based on end user and group profiles.

Secure Access Service Edge Convergence

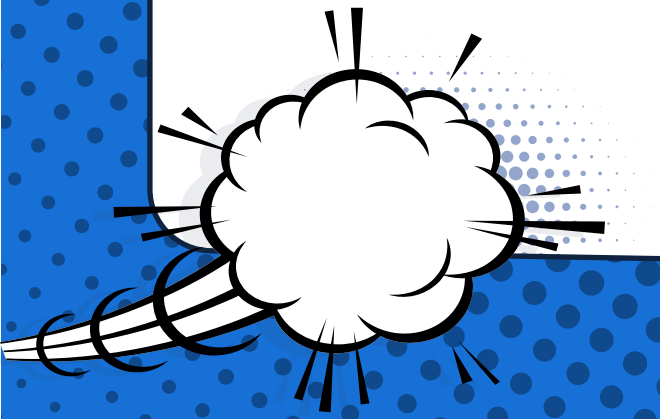


Source: Gartner

Zero Trust Network Access

Zero Trust networking is a security model that removes the idea of trust for all users on a network. This means a Zero Trust Network Architecture (ZTNA) provides privileged network access and policy-based segmentation while also constantly monitoring all individuals on the network, regardless of their status or role. ZTNA internal networks are made up of different levels of “trust boundaries” that should be segmented according to sensitivity.

The Zero Trust security model is an approach to combining operational rigor and new security capabilities to protect organizations from credential theft, network- based attacks, and unauthorized access to sensitive data. By monitoring the network via centralized management capabilities, network visibility can be enhanced to detect unknown threats, or support compliance reporting.



Firewall as a Service (FWaaS)

A Firewall as a Service or FWaaS protects an organization’s site-centric networks from potential threats by filtering out malicious traffic, while at the same time implementing modern security features for next-generation firewalls.

FWaaS is delivered as a cloud-based service or hybrid solution, both in the cloud and as on-premises appliance solution. It provides a more streamlined and flexible architecture that uses centralized policy management, enterprise firewall features and traffic tunneling to conduct web traffic inspections in the cloud.

Known as Next-Generation Firewalls (NGFW), these solutions include technologies not previously available in traditional firewall products. This includes intrusion prevention systems (IPS) that detect and block cyber attacks; deep packet Inspection (DPI) that inspects data packet headers and payload information, versus just the headers and helps detect malware and malicious data; and finally, application controls.

perimeter 81

Secure Web Gateway (SWG)

Secure Web Gateway (SWG) solutions provide advanced, cloud-delivered or on-premises network security services that protect user devices against malware infections from web-surfing activities and enforce organizational security policies. They filter unwanted malware from web-requested traffic and enforce corporate and regulatory policy compliance.

Secure Web Gateways must include URL filtering, malware detection and filtering, and application controls for web-based applications. This includes apps such as instant messaging (IM) and Skype. Data leak prevention is also a characteristic of Secure Web Gateways.

Cloud Access Security Broker (CASB)

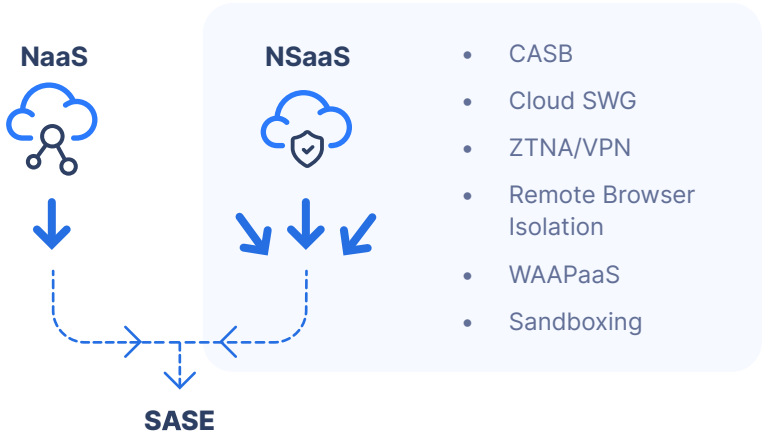
Cloud Access Security Brokers (CASBs) are security policy enforcement points that ensure policy compliance between cloud service customers and cloud service providers.

A CASB is a tool or service that also manages and tracks an organization's and cloud provider's compliance. CASBs help organizations to mitigate cloud service risks, audit cloud resource access, enforce security policies and meet strict compliance regulations.

CASBs may include firewalls for malware prevention, user credential authentication checks, Web Application Firewalls (WAFs) to protect against malware at the application level, and Data Loss Prevention (DLP) services to prevent users from sending sensitive information outside of an organization.

perimeter 81

Secure Access Service Edge Convergence



- CASB
- Cloud SWG
- ZTNA/VPN
- Remote Browser Isolation
- WAAPaaS
- Sandboxing

Source: Gartner

Cloud Sandboxing

Traditional appliance-based sandboxing solutions are normally deployed on-premises and only protect users when using an organizational network. They allow traffic through a network while inspecting suspicious files but may not be able to completely inspect SSL traffic because of hardware limitations. Moreover, attackers are exploiting hardware limitations to distribute malware.

Cloud Sandboxing provides full SSL traffic analysis and real-time threat detection, without the need for expensive hardware. Cloud Sandboxes scan unknown files for zero-day exploits and advanced persistent threats both on and off the network versus DNS filtering that automatically blocks malicious domains that are identified with real-time analysis and global threat intelligence.

perimeter 81

Encrypted Tunneling

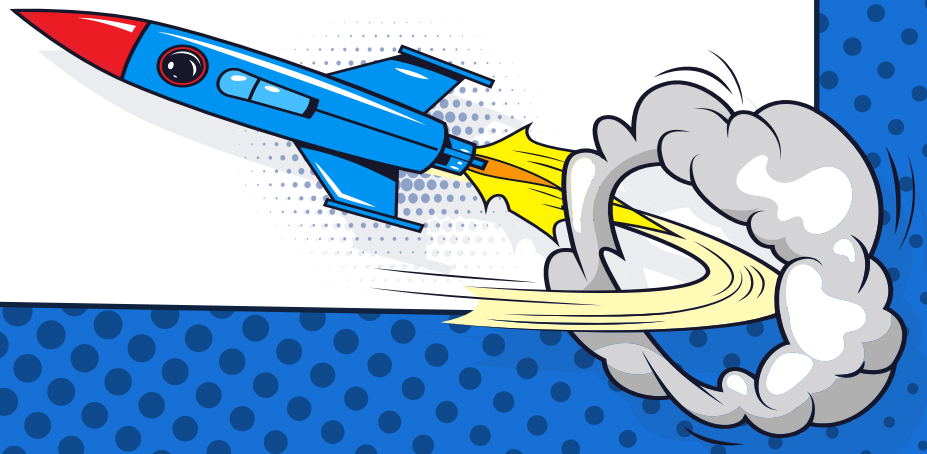
Remote Access enables network security and compliance for organizations that have transitioned to the public cloud or hybrid cloud environments using WireGuard,or Internet Protocol Security (IPsec), the secure network protocol suite that authenticates and encrypts data at the IP Packet Layer. IPSec Site-to-Site tunneling enables IT administrators to create secure communication links between two different networks located at different sites.

By creating the IPSec Tunnel, gateways can securely connect to local networks or cloud services. Establishing a virtual tunneled connection with IPsec between network resources and an external device and user requires two main components: remote access client software and secure network access gateway.

DNS Filtering

DNS filtering allows administrators to block network users from navigating to web page URLs with their Internet browser. The process filters out malicious websites and allows access to approved ones is accomplished with IP and URL restriction tools that block traffic on an individual basis or by category (gambling, social networks, etc.).

When restricting a URL with DNS filtering features, the DNS Resolver does not resolve the website associated with its unique IP address. Instead, it will display a custom message notifying users that their access to the page is restricted. Accordingly, DNS filtering is crucial for productivity and protection as well.



THE BENEFITS OF SASE

perimeter 81

SASE enables the delivery of integrated secure network security services that support digital business transformation, edge computing, workforce mobility and identity and access management.

Key benefits include:

- Complexity and cost reduction
- Network performance improvements
- Ease of use and visibility
- Improved security
- Zero Trust network access
- Centralized policy management

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.

As more SASE services are adopted in the long run, additional cost reductions will be realized through security technology stack simplification.

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'S SASE APPROACH

perimeter 81

Perimeter 81's SASE platform combines network and security functions into one unified solution. The cloud-native offerings fall under the SASE network and endpoint umbrella. Managed and delivered through a single dashboard, Perimeter81 provides user centric network and policy management for organizations of all sizes.

Perimeter 81's Secure Access Service Edge (SASE) platform offers:

- Complete visibility
- Precise segmentation
- A user-centric experience
- Increased security
- A highly scalable solution
- Simple transition to cloud environments

The global, multi-region and multi-tenant Perimeter 81 cloud network provides a comprehensive set of secure network capabilities for SASE configurations.

This includes SaaS security for Office 365, Google Drive and Dropbox as well as a Firewall as a Service (FWaaS) to protect an organization's site-centric networks from potential threats.

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.

Perimeter 81's Zero Trust Network Access solution provides policy enforcement and protection by isolating applications and segmenting network access based on user permissions, authentication, and verification. For complete endpoint security, Perimeter 81 also delivers multiple endpoint protection capabilities, including Wifi protection, next-generation malware protection and support for visibility into encrypted traffic.

perimeter 81

Conclusion

As cloud-native technologies require more dynamic and agile identity and access resources to secure workloads and data, solutions like SASE are becoming critical for smarter networking and stronger security.

Moreover, traditional network security architectures that typically place enterprise data centers at the center of IT resources are becoming roadblocks to the dynamic access requirements of digital businesses and edge computing scenarios.

SASE solutions remove these roadblocks with Secure Web Gateways, URL or DNS filtering, VPN-like tunneling with IPSec, cloud sandboxing, Cloud Access Service Brokers, Firewall as a Service, multi-factor authentication technologies

The key to SASE is combining all of these utilities and serving them as a single product through the cloud.

About Perimeter 81

Perimeter 81 is a leading Secure Access Service Edge (SASE) provider that has taken the outdated, complex and hardware-based network security technologies, and transformed them into one unified, scalable and easy-to-use software solution — simplifying secure access for the modern and distributed workforce.

Perimeter 81 is headquartered in Tel Aviv, the heart of the startup nation, and has offices in New York and California.

The company's clients range from small businesses to Fortune 500 corporations across a variety of sectors, and our partners are among the world's foremost integrators, managed service providers and channel resellers.

To learn more visit www.perimeter81.com
or follow us on LinkedIn.

CONTACT US

perimeter 81

www.perimeter81.com

+1-929-57-59307

Request a Free Demo