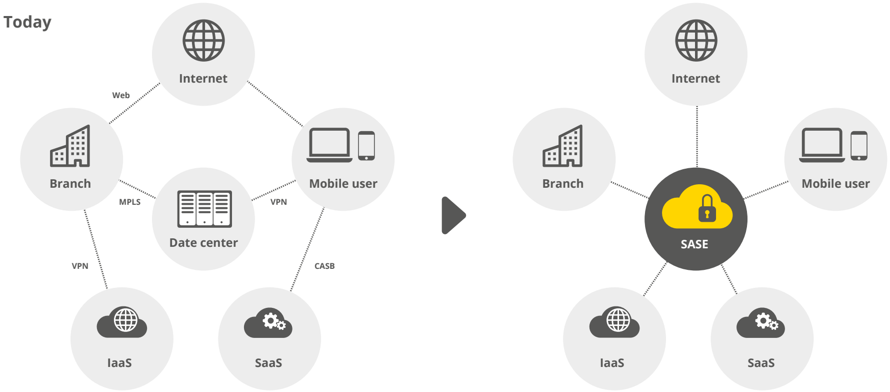
DTS
Secure Access Service Edge (SASE)

Secure Access Service Edge (SASE)

The traditional network perimeter is disappearing. Conventional security measures assume that applications and users are located within the organization's network perimeter. This assumption no longer holds true today. Enterprise data is increasingly being moved to the cloud, employees are working remotely more often and digital transformation initiatives require IT organizations to be agile in order to take advantage of new business opportunities. So the traditional network perimeter is dissolving and new models for access control, data protection and threat protection are needed.

Here, Gartner uses the Secure Access Service Edge (SASE) concept as a way of protecting digital business transformation through a secure, cloud-based, software-defined access solution. It combines network and security services in a unified, cloud-based platform to protect users, applications and data everywhere. We enable you to implement this concept, tailored to your requirements. So that your company can position itself flexibly and securely for the future.

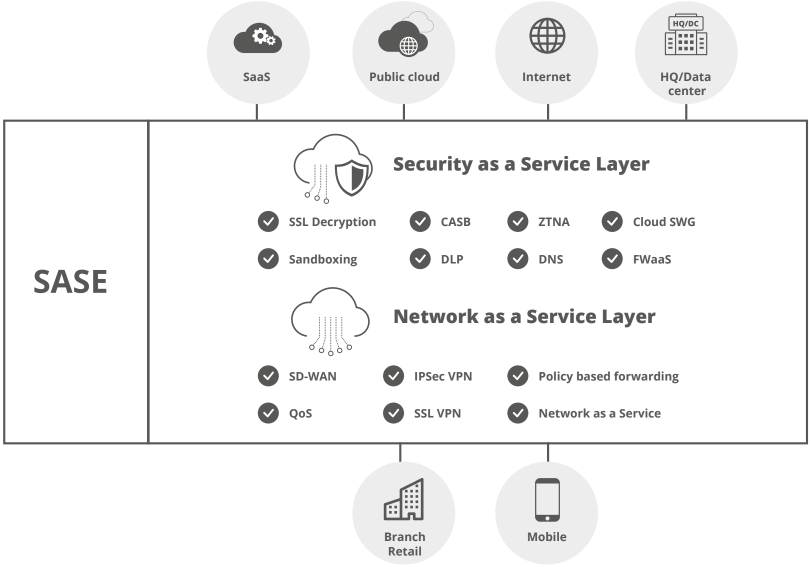
- Greater entrepreneurial agility & speed
- Better network performance & less complexity
- Consistent transparency & security to defend against cyber attacks in hybrid environments
- Cost savings by using a single platform instead of purchasing & managing multiple individual products
- Consistent enforcement of zero-trust security policies, regardless of whether users are on or off the corporate network
- 24/7 support through Elite ASC in German & English
- More than 10 years of Palo Alto Networks expertise and numerous certified experts for conceptual design & implementation
- Managed services support, e.g. for reviews of the platform, VM-Series PaaS for PoPs that cannot be addressed by Prisma Access, health checks, etc.
- End-to-end platform & service from a single source



Palo Alto Networks Prisma Access provides modern enterprises with powerful networking and security services designed specifically for cloud-based infrastructures. Designed to prevent cyber attacks effectively and efficiently. To do so, it is not enough simply to block threats from the internet. All incoming and outgoing data traffic must be monitored. Prisma Access protects all traffic at all ports and to and from all applications.

Prisma Access is based on a shared cloud infrastructure that provides multiple protection for branch offices and mobile users from over 100 locations in 76 countries. Dedicated cloud instances enable enforcement of customized security policies and provide each company with the assurance that its own confidential traffic is isolated from the data streams of other clients at all times.

Security mechanisms specifically address threat prevention and credential theft protection, web filtering, sandboxes, DNS security, DLP and next-generation firewall policies based on user, application and host information profiles. Unlike traditional software-defined perimeter or proxy solutions, Prisma Access thus provides network **services and security functions for all applications. This ensures that your policies are enforced consistently across the enterprise.**


SaaS
Public cloud
Internet
HQ/DC
HQ/Data center
SASE
Security as a Service Layer
SSL Decryption
CASB
ZTNA
Cloud SWG
Sandboxing
DLP
DNS
FWaaS
Network as a Service Layer
SD-WAN
IPSec VPN
Policy based forwarding
QoS
SSL VPN
Network as a Service
Branch Retail
Mobile