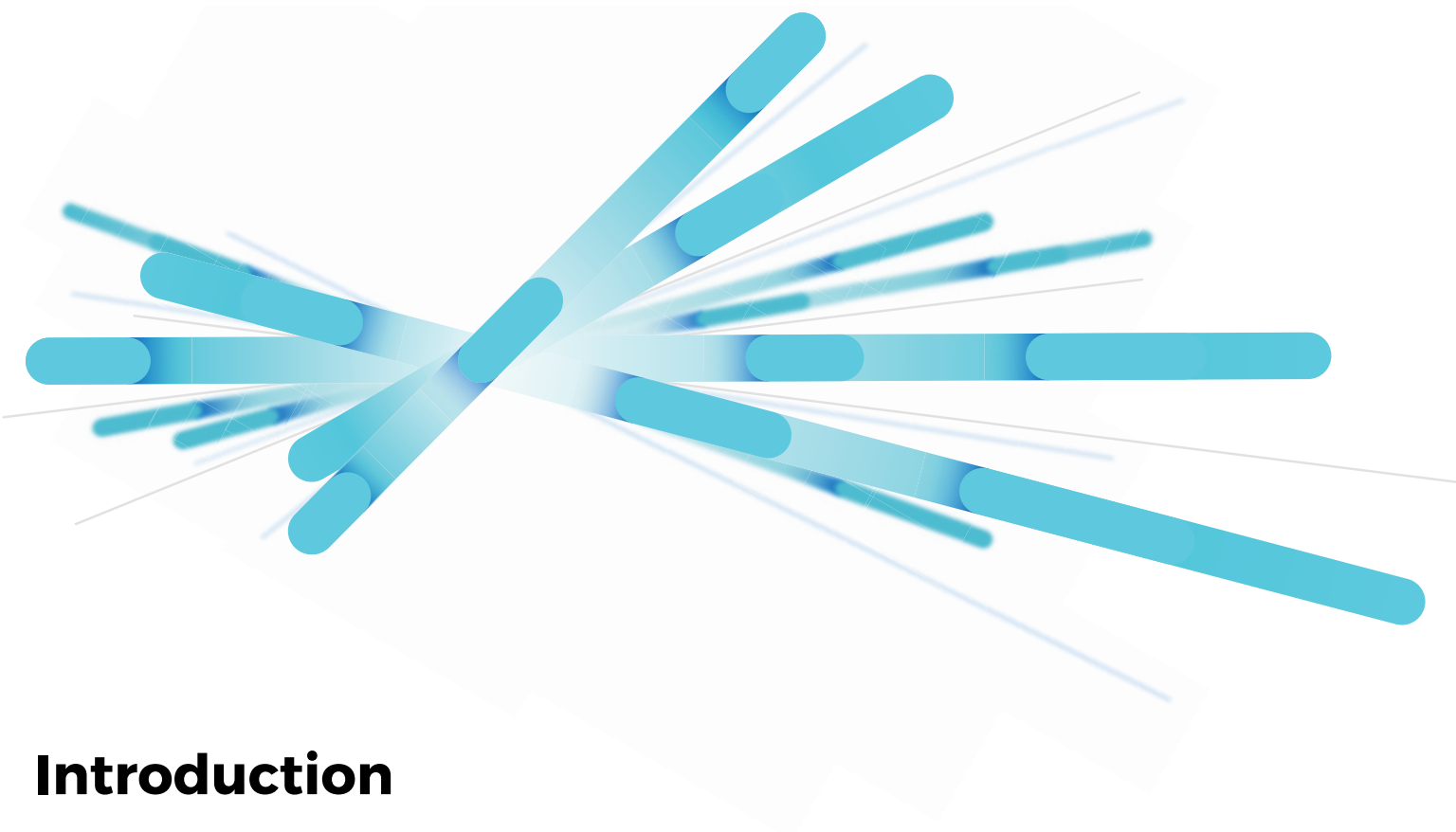




# **THE 10 TENETS OF AN EFFECTIVE SASE SOLUTION**

# Table of Contents

3	Introduction
4	Tenet 1: Software-Defined Wide-Area Network
5	Tenet 2: Virtual Private Network
6	Tenet 3: Zero Trust Network Access
7	Tenet 4: Quality of Service
8	Tenet 5: DNS Security
9	Tenet 6: Firewall as a Service
10	Tenet 7: Threat Prevention
11	Tenet 8: Secure Web Gateway
12	Tenet 9: Data Loss Prevention
13	Tenet 10: Cloud Access Security Broker
14	How Prisma Access by Palo Alto Networks Can Help
15	Conclusion



## Introduction

With increasing numbers of mobile users, branch offices, data, and services located outside the protections of traditional network security appliances, organizations are struggling to keep pace and ensure the security, privacy, and integrity of their networks and, more importantly, their customers.

Today, many of the current technologies on the market are built upon architectures that were not designed to handle all types of traffic and security threats. This forces organizations to adopt multiple point products to handle different requirements, such as secure web gateways, firewalls, secure VPN remote access, and SD-WAN. For every product, there is an architecture to deploy, a set of policies to configure, an interface to manage, as well as its own set of logs. This creates an administrative burden that introduces cost, complexity, and gaps in security posture.

To address these challenges, secure access service edge (SASE) has emerged. SASE (pronounced “sassy”) is designed to help organizations embrace cloud and mobility by providing network and network security services from a common cloud-delivered architecture. A SASE solution must provide consistent security services and access to all types of cloud applications (e.g., public cloud, private cloud and SaaS) delivered through a common framework. By removing multiple point products and adopting a single cloud-delivered SASE solution, organizations can reduce complexity while saving significant technical, human, and financial resources.

This e-book will help you to understand the 10 tenets of an effective secure access service edge.

## Tenet 1: Software-Defined Wide-Area Network

### What Isn't Working

Companies are embracing software-defined wide-area network (SD-WAN) to connect branch offices to the corporate network and provide local internet breakout as an alternative to costly MPLS connections. The challenge with SD-WAN, however, is how to combine security with the SD-WAN fabric, which leads to the need for multiple overlays.

### The SASE Way

In a SASE solution, SD-WAN edge devices can be connected to a cloud-based infrastructure, rather than physical SD-WAN hubs located in data center or co-location facilities. This enables the interconnectivity between branch offices without the complexity of deploying and managing physical SD-WAN hubs.

### Key Takeaway

SD-WAN should be something you are already considering or have already adopted into your organization's network infrastructure as a way to securely connect and control access to branch offices and remote employees. SASE creates a unified framework for SD-WAN services and other solutions to connect to, providing a single point of view and simplified management solution to protect your network.

**“Gartner predicts that spending on SD-WAN will surpass spending on traditional branch routers by 2022.”**

– Gartner

## Tenet 2: Virtual Private Network

### What Isn't Working:

Organizations rely on virtual private networks (VPNs) to provide a secure encrypted connection for mobile users and branch offices to access corporate data, applications and internet access. There are many types of VPN services, from IPsec VPN to SSL VPN, clientless VPN, and remote access VPN, which all require a connection to a VPN gateway. VPNs are not optimized for access to the cloud, resulting in no security or access control when users disconnect to reach cloud apps or services.

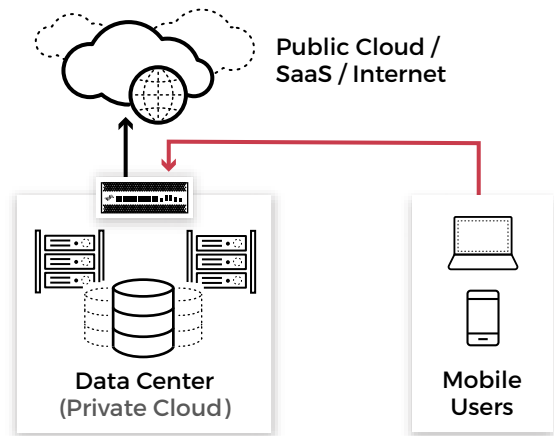
### The SASE Way

A SASE solution encompasses VPN services and enhances the capabilities to operate in a cloud-based infrastructure in order to securely route traffic to the public cloud, SaaS, internet or private cloud apps. In an IPsec VPN example, you can create a site-to-site connection to a cloud-based infrastructure from any IPsec-compatible device located at a branch or retail location via a branch router, wireless access point, SD-WAN edge device, or firewall. Mobile users employ an always-on IPsec or SSL VPN connection between their endpoint or mobile device, and a SASE solution ensures consistent traffic encryption and threat prevention.

### Key Takeaway

No matter which type of VPN service you use in your organization, a SASE solution provides a unified cloud infrastructure to connect to, instead of backhauling to a VPN gateway at corporate headquarters. This dramatically simplifies the management and policy control needed to enforce least-privileged access rules.

**Before: Remote access VPN is not designed to support cloud applications**



**After: Use cloud infrastructure to connect users to both cloud apps and the data center**

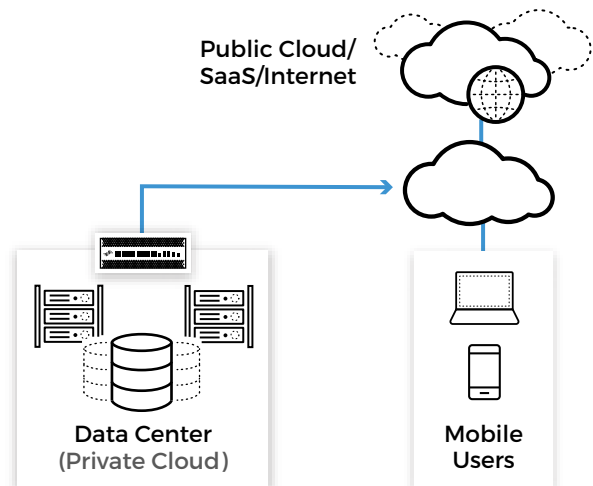


Figure 1

## Tenet 3: Zero Trust Network Access

### What Isn't Working:

As seen in Figure 2, companies still lack the necessary security protections and policies needed to adequately protect their users and data. Zero Trust network access (ZTNA) is a key part of the Zero Trust philosophy of “never trust, always verify,” developed by Forrester to identify the need to protect data. ZTNA requires users who want to connect to the cloud to authenticate through a gateway prior to gaining access to the applications they need. This provides an IT admin the ability to identify users and create policies to restrict access, minimize data loss, and quickly mitigate any issues or threats that may arise.

Many ZTNA products are based on software-defined perimeter (SDP) architectures, which do not provide content inspection, thus creating a discrepancy in the types of protection available for each application. In terms of consistent protection, the organization must build additional controls on top of the ZTNA model and establish inspection for all traffic across all applications.

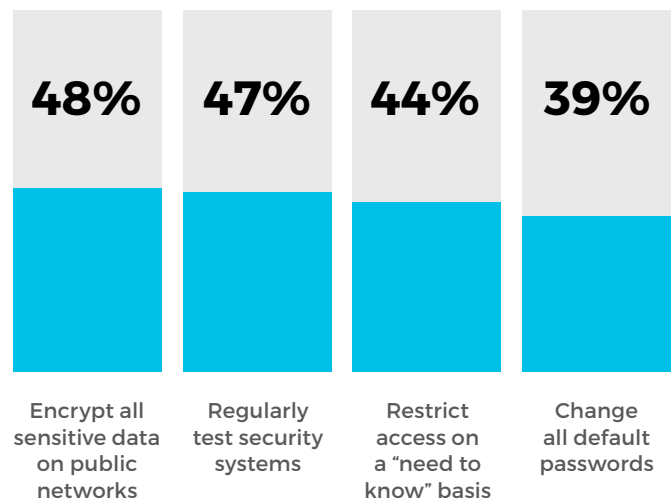
### The SASE Way

SASE builds upon the ZTNA key principles and applies them across all the other services within a SASE solution. By identifying users, devices, and applications, no matter where they are connecting from, policy creation and management is simplified. SASE removes the complexity of connecting to a gateway, by incorporating the networking services into a single unified cloud infrastructure.

### Key Takeaway

A SASE solution should incorporate ZTNA concepts for protecting applications as well as apply other security services for the consistent enforcement of data loss prevention (DLP) and threat prevention policies. This is because access controls, in and of themselves, are useful for establishing who the person is, but other security controls are also necessary to make sure their behaviors and actions are not harmful to the organization. It is also necessary to apply the same controls across access to all applications.

### Only 12% of companies had all four basic protections in place



**Figure 2**

Which of the following match your organization's security policies? [Verizon Mobile Security Index 2019 report](#)

## Tenet 4: Quality of Service

### What Isn't Working:

As organizations transition from MPLS to SD-WAN using broadband services, they are finding that the service quality varies. Quality of service (QoS) establishes bandwidth allocation assigned to particular apps and services. Businesses rely on QoS to ensure their critical apps and services perform adequately, for example medical equipment or credit card processing services. If these systems were to get bogged down due to lack of bandwidth, this would severely impact business operations and sales. QoS prioritizes business-critical apps, based on ranking system, so you can choose which apps and services take precedent over others.

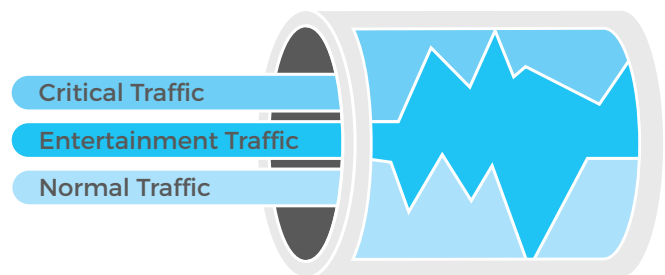
### The SASE Way

QoS is an important step when you begin migrating from MPLS. A SASE solution incorporates QoS services in the cloud, allowing you to easily mark sensitive applications, such as VOIP, as high priority over general internet browsing and entertainment apps.

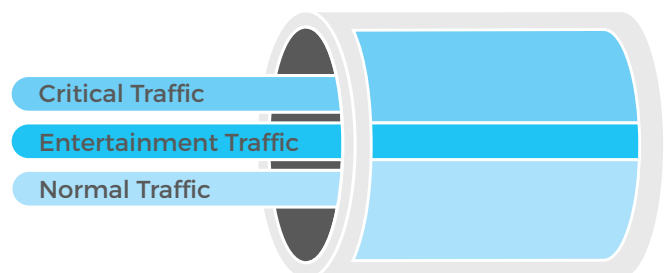
### Key Takeaway

QoS is immensely important for businesses of any size. Managing the QoS traffic and allocation doesn't need to be difficult. SASE enables you to dynamically shape traffic based on the policies that prioritize critical application requirements. Make sure your SASE solution contains QoS capabilities.

**Bandwidth without QoS Control**



**Bandwidth with QoS Control**



**Figure 3**

## Tenet 5: DNS Security

### What Isn't Working:

Every organization uses Domain Name System (DNS) to translate a domain name into an IP address. DNS is an open service, and by default it does not have a way to detect DNS-based threats. As a result, malicious activity within DNS can be used to propagate an attack.

### The SASE Way

DNS security protects your users by predicting and blocking malicious domains while neutralizing threats. A SASE solution embraces DNS security features by providing consistent security across the network and users, no matter their location.

### Key Takeaway

Your SASE solution should contain DNS protections, delivered within the cloud environment as part of the network access. DNS security should be built-in, rather than bolted-on, to the solution your branch offices and mobile users use to connect to the internet. The DNS Security provided in your SASE solution should leverage a combination of predictive analytics, machine learning, and automation to combat threats in DNS traffic.



**82%**

Companies that experienced a DNS attack



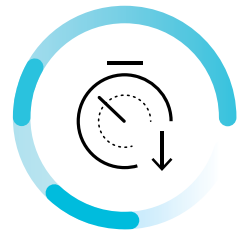
**9.45**

Average number of attacks per company



**\$1.07M**

Average damage cost



**63%**

Companies that suffered application downtime

Figure 4

[IDC 2019 Global DNS Threat Report](#)



## Tenet 6: Firewall as a Service

### What Isn't Working:

Firewall as a service (FWaaS) is a deployment method for delivering a firewall as a cloud-based service. FWaaS has the same features of a next-generation firewall, but it is implemented in the cloud. By moving the firewall to the cloud, organizations can benefit from cost savings by eliminating the need to install or maintain security hardware at branch and retail locations.

### The SASE Way

A SASE solution incorporates FWaaS into its unified platform, providing the same services as a next-generation firewall but as a cloud-delivered service. By encompassing the FWaaS service model within a SASE framework, organizations can easily manage their deployments from a single platform.

### Key Takeaway

A SASE solution should enable FWaaS capabilities in order to provide the protection of a next-generation firewall by implementing network security policy in the cloud. It is important to ensure your SASE solution does not only provide basic port blocking or minimal firewall protections. You need the same features a next-generation firewall embodies as well as the features cloud-based security offers, such as threat prevention services and DNS security.

“A company with 500 employees can expect to save on average 37% by using FWaaS solutions versus traditional hardware.”

— Secure Data

## Tenet 7: Threat Prevention

### What Isn't Working:

In today's world of small and large scale breaches, where ransomware attacks occur on a daily basis, threat prevention is key to protecting your organization's data and employees. There are a variety of threat prevention tools out there, from anti-malware and intrusion prevention to SSL decryption and file blocking, providing organizations ways to block threats. However, these point products require separate solutions, making management and integration difficult.

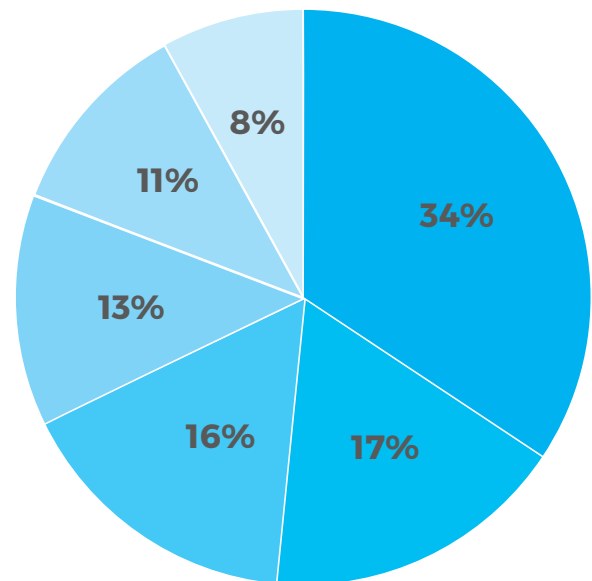
### The SASE Way

Within a SASE solution, all these point products and services are now integrated into a single cloud platform. This provides simplified management and oversight of all threats and vulnerabilities across your network and cloud environments.

### Key Takeaway

Stopping exploits and malware by using the latest threat intelligence is crucial to protecting your employees and data. Your SASE solution should incorporate threat prevention tools into its framework so you can react quickly and swiftly to remediate threats. Be sure to check the quality of threat intelligence that is being provided by the vendor. They should be gathering and sharing data from various sources, including customers, vendors and other related thought leaders, to provide continuous protection from unknown threats.

**Why Threat Detection and Response is More Difficult Today**



- The volume and/or sophistication of threats has increased, 34%
- The threat detection/response workload has increased, 17%
- The attack surface has grown, 16%
- The threat detection/response is dependent on many manual processes at my organization, 13%
- My organization uses numerous disparate threat detection/response tools, 11%
- My organization does not have the skills or appropriately sized cybersecurity staff, 8%

**Figure 5**

[ESG Master Survey Results: The Threat Detection and Response Landscape](#)

## Tenet 8: Secure Web Gateway

### What Isn't Working:

Organizations rely on secure web gateway (SWG) to protect employees and devices from accessing malicious websites. SWG can be used to block inappropriate content (e.g., pornography, gambling) or websites that businesses simply don't want users accessing while at work, such as streaming services like Netflix, for example. Additionally, SWG can be used to enforce acceptable use policy (AUP) before internet access is granted.

### The SASE Way

SWG is just one of the many security services that a SASE solution must provide. As organizations grow and add more and more remote users, coverage and protection becomes more difficult. A SASE solution moves SWG into the cloud, providing protection in the cloud through a unified platform for complete visibility and control over the entire network.

### Key Takeaway

A SASE solution includes the same security services in a SWG, allowing organizations to control access to the web and enforce security policies that protect users from hostile websites. It is important to remember that SWG is just one service of the SASE solution. Other security services like FWaaS, DNS security, threat prevention, DLP, and CASB should be included.

Over 500,000 Unsafe Websites Detected by Google since July 2019

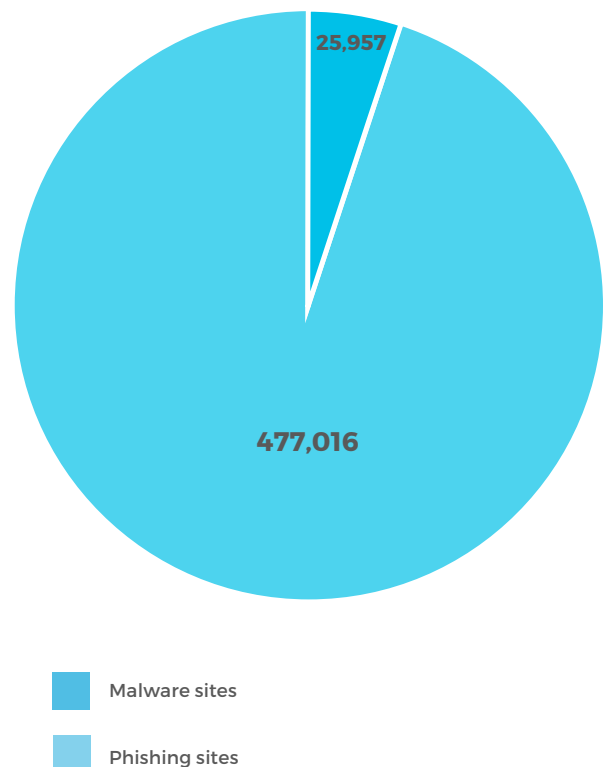


Figure 6

[Google Transparency Safe Browsing Report](#)

## Tenet 9: Data Loss Prevention

### What Isn't Working:

Data loss prevention (DLP) tools protect sensitive data and ensure it is not lost, stolen or misused. DLP is a composite solution that monitors data within the environments where it is deployed (such as network, endpoints and cloud) and through their egress points. It also alerts key stakeholders when policies are violated. Due to compliance requirements from HIPAA, PCI, GDPR, etc., DLP is a crucial solution needed for data security and compliance. Legacy DLPs rely on old core technology initially designed for on-premises perimeters and subsequently extended and adapted to cloud applications. Loaded with features, disjointed policies, configurations and workarounds, DLPs have become very complex, difficult to deploy at scale and too expensive. Digital transformation and new data usage models demand a fresh approach to data protection.

### The SASE Way

Through the SASE approach, DLP becomes one cloud-delivered solution centered around the data itself, everywhere. Same policies are consistently applied to sensitive data, at-rest, in-motion and in-use, regardless of its location. In the SASE architecture, DLP is not a standalone solution anymore, but is embedded in the organization's existing control points, thus eliminating the need of deploying and maintaining multiple tools. With SASE, organizations can finally enable a comprehensive data protection solution that relies on a scalable and simple architecture and allows effective machine learning by leveraging access to global traffic.

### Key Takeaway

DLP is a necessary tool to protect sensitive data and ensure compliance throughout the organizations. To this end, the SASE solution must include this core capability. With SASE, DLP is an embedded, cloud-delivered service used to accurately and consistently identify, monitor and protect sensitive data everywhere across networks, clouds and users.

“Gartner estimates that by 2021, **90%** of organizations will have implemented at least one form of integrated DLP, up from **50%** in 2017.”

– Gartner

## Tenet 10: Cloud Access Security Broker

### What Isn't Working:

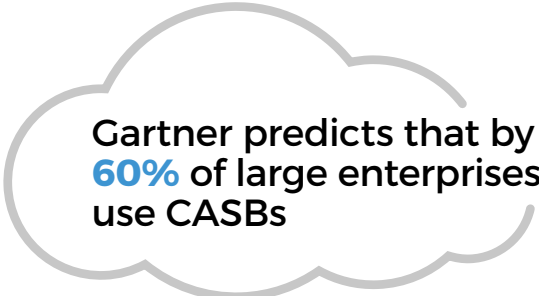
Many organizations depend on cloud access security brokers (CASBs) to provide visibility into SaaS application usage, understand where their sensitive data resides, enforce company policies for user access, and protect their data from hackers. CASBs are cloud-based security policy enforcement points that provide a gateway for your SaaS provider and your employees.

### The SASE Way

CASB should be another security feature that is part of your SASE solution, creating a single platform for stakeholders to manage security controls. A SASE solution helps you understand which SaaS apps are being used and where data is going, no matter where users are located.

### Key Takeaway

Your SASE solution should incorporate both in-line and API-based SaaS controls for governance, access controls, and data protection. Also called a multi-mode CASB, the combination of in-line and API-based CASB capabilities also provide superior visibility, management, security, and zero-day protection against emerging threats.



Gartner predicts that by 2022, **60%** of large enterprises will use CASBs



Up from the **20%** that used them at the end of 2018.

# How Prisma Access by Palo Alto Networks Can Help

Prisma™ Access is the industry's most comprehensive SASE solution, providing organizations the ability to deliver protection from the cloud, while reducing capital costs and cutting the overhead normally associated with deploying security at scale. Prisma Access delivers the networking that organizations need in a SASE architecture designed for all traffic, all applications, and all users.

Rather than creating single purpose technology overlays that are normally associated with point

products, Prisma Access uses a common cloud-based infrastructure (see Figure 7) that delivers multiple types of security services, including advanced threat prevention, DNS security, DLP, FWaaS, SWG, and CASB to be combined with networking services, like SD-WAN, VPN, ZTNA, and QoS.

Prisma Access eliminates many sources of complexity that are normally associated with the deployment of different types of point products.

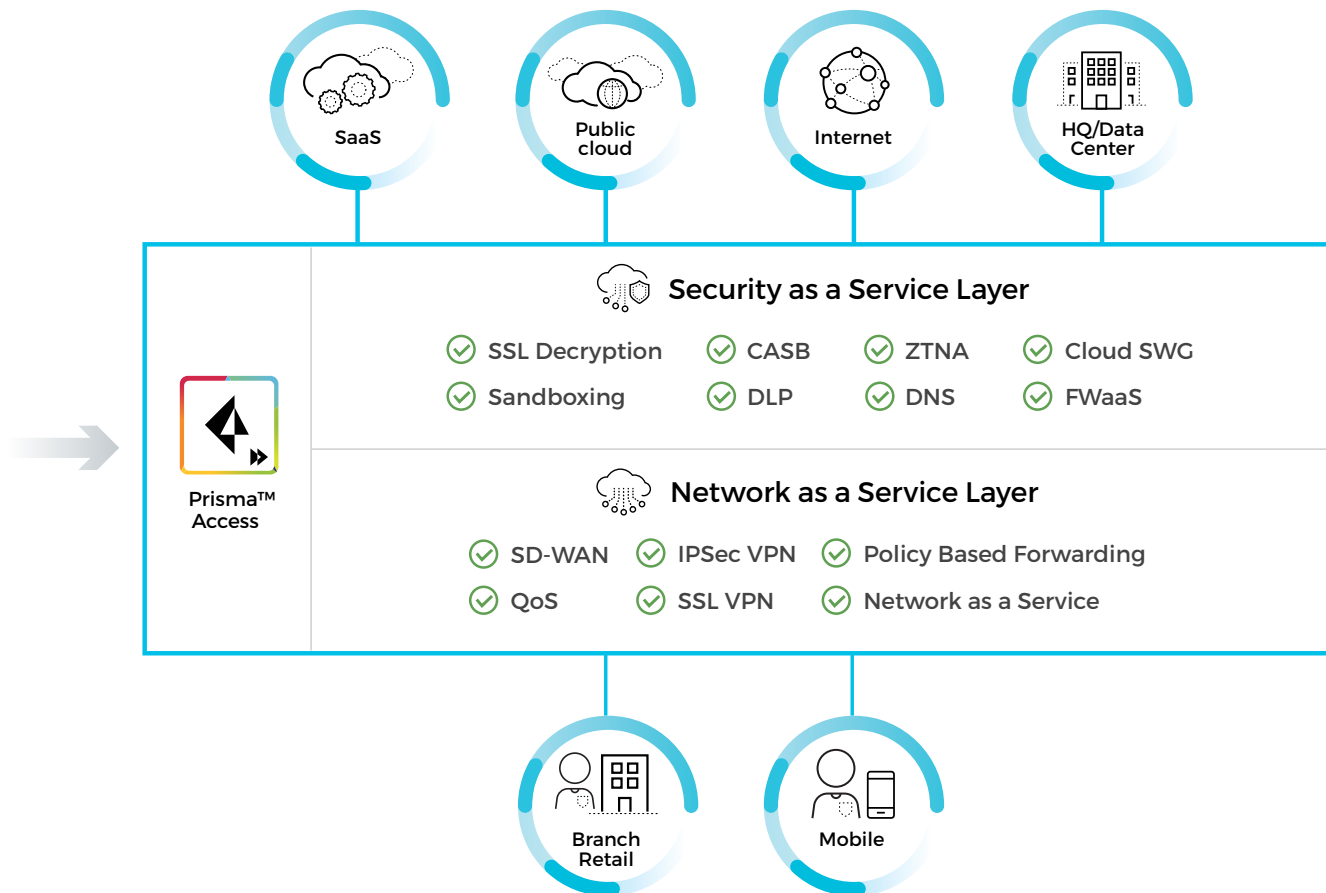


Figure 7

# Conclusion

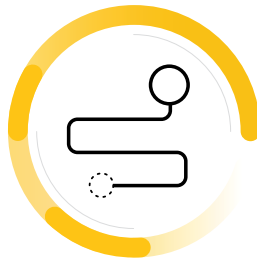
As your business grows and you continue on your cloud journey, we encourage you to consider a comprehensive solution for Secure Access Service Edge, such as Prisma Access, to solve your networking and

networking security needs. The top three strategic benefits your business will realize from SASE are outlined below:



## Business Agility and Speed

- Embrace digital transformation using a modern cloud-based network and security infrastructure.
- Organization can grow, expanding to new locations regionally and globally to capitalize on new initiatives.
- Streamlined operations increases competitive advantage, reduces costs, and increases profits.



## Reduced Complexity

- Eliminate unnecessary, limited use of point products.
- Operate from the cloud to cut operational complexity and cost.
- Avoid logistical issues with shipping, installing, and upgrading hardware.



## Consistent Security Designed to Stop Cyberattacks

- Consistent security policy strengthens the organization's risk profile.
- Provides full visibility and security for all traffic.
- Delivers protection to users in any location.

In short, a successful SASE solution delivers a holistic view of your entire network while providing

superior protection and performance from a single, unified, cloud-delivered platform.

[Learn more about Prisma Access](#)

# About Prisma by Palo Alto Networks

Governed access plus pervasive protection for data, applications, hosts, containers, and serverless—this is the proper foundation for the journey to the cloud. With a comprehensive cloud security suite, Prisma helps our customers secure every step of their journey.

Prisma provides unprecedented visibility into assets and risks, consistently securing access, data, applications, and modern workloads, regardless of location. The suite helps customers deploy and adapt quickly with speed and agility as well as control operational costs and reduce complexity with a radically simple architecture.

Prisma is the most complete cloud security suite for today and tomorrow.

To learn more, visit our website:

[www.paloaltonetworks.com/cloud-security](https://www.paloaltonetworks.com/cloud-security)

