# SASE

## SECURING THE CLOUD NETWORK ARCHITECTURE

WHITE PAPER

ManageEngine
AD360

# Table of contents

# The migration to the cloud

The rapid adoption of cloud services by businesses across the world has been one of the major shifts in the tech world over the last few years. Up until the advent of the cloud, businesses relied upon on-premise data centers that were owned and run by the organizations themselves. Since the advent of the COVID-19 pandemic, the adoption of cloud computing has increased steadily. This is mostly because the cloud has various advantages over traditional data centers like cost-effectiveness, high scalability, and improved performance.

Businesses are updating their data platforms to make them compatible with modern applications while also shifting their data to the cloud. A study by Deloitte states that cloud and data modernization are highly interrelated and reinforce each other.

## 1.1 The need for cloud-based network security and access

The traditional network architecture routes all endpoints through the enterprise data center. This process is suitable only for the on-premises workplace model where all the users are located and connected within the enterprise perimeter. When the same process is stretched to meet the access requirements of the remote users, it often results in issues and complexities at the edge of the network, that is, the users' endpoints. Also, because these network structures are run manually, they're not easy to automate. This reduces the flexibility, agility, and ability to scale up the network beyond the enterprise perimeters.

The increased user dependency on SaaS applications during this remote era has also resulted in organizations shifting to cloud-based services for data storage. This means data is being moved from traditional data centers to clouds in huge numbers. The dynamic access requirements of organizations are majorly hindered by the functioning of the on-premises data center as the hub of the network security architecture.

As users continue working remotely or work from both the home and office, they move in and out of several networks and work on multiple devices, thinning the boundaries between their work life and personal life. This eventually leads to employees letting down their guard in terms of cybersecurity and leads them to unsecure practices. Due to limited and outdated security functions, traditional network architectures are not well suited to guard employees devices from current cyberthreats.

Therefore, there is an urgent need for a unified, robust approach towards network security that is cloud-based and can be implemented uniformly irrespective of user location.

## 1.2 The rising issues with cloud security

It is currently estimated that 94% of all enterprises use some form of cloud services and 48% of businesses store their critical data and resource in clouds. The global cloud service market is expected to reach 623.3 billion dollars by 2023.

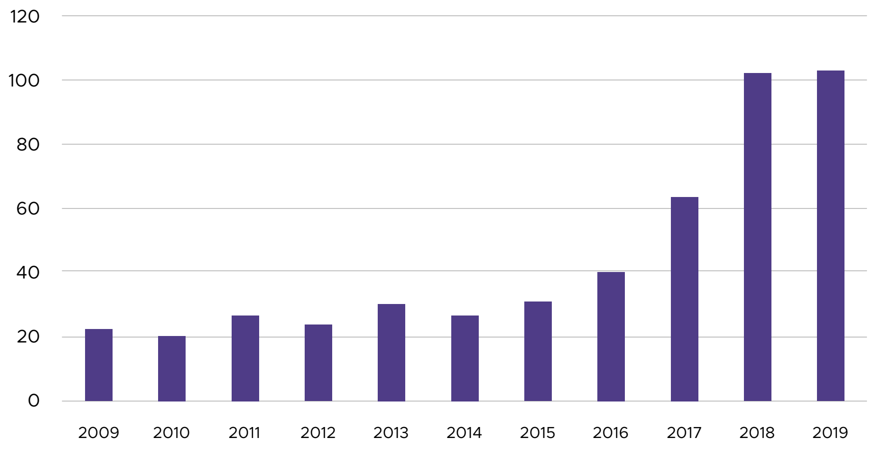
The following cloud computing statistics highlight the significance of the rapidly growing cloud industry:

- The value of the global cloud computing market is estimated to increase from 371.4 billion dollars in 2020 to 832.1 billion dollars by 2025.
- By 2025, there will be over 100 zettabytes of data stored in the cloud, which equals 1 trillion gigabytes of data.
- Currently, 94% of enterprises use some form of cloud service for their business operations.
- 48% of businesses store highly sensitive data on a cloud platform.

> *According to IBM Data Breach Report 2021, the global average cost of a data breach is estimated at 4.24 million dollars.*

Data breaches cost organizations their money, negatively impact their public reputation, and can invite legal action as well. Although the shift in workplace models ensures business continuity during times of uncertainty, there is a massive rise in cybersecurity concerns.

Cyberattack incidents with $1M+ in reported losses



The above chart tracks the number of cyberattack incidents with more than 1 million dollars reported in losses between 2009 and 2019. A report by IBM states that the average cost of a breach at organizations with 81-100% of employees working remotely is 4.54 million dollars. With the increase in cloud adoption, security concerns involving the cloud also increase. Today, three out of four enterprises believe cloud security is a top concern for them.

To increase their defenses against such high losses, organizations need to deploy strict cloud security measures that are designed to secure the cloud platform and the data stored in it, like secure user and device authentication, data access control, and data privacy protection. Additionally, measures must also be implemented to protect the enterprise data from hackers, DDoS attacks, malware, and unauthorized user access.

## 1.3 A unified approach towards cloud security

With the increasing complexity of cybersecurity threats targeting clouds, it becomes impossible for a single security solution to counter them all. The worldwide shift to remote and hybrid workplace models has resulted in an increased number of possible attack surfaces that can be targeted by cybercriminals.

As security measures have evolved over the years, so have the types of threats. Today, there are vastly different cyberthreats with each targeting a different vulnerability. Different security measures work individually to defend against different types of threats. But a single cyberattack can be comprised of multiple attack types, forming a cyber kill chain.

For these types of attacks, each security measure can detect a certain aspect of the attack. To provide security against the entire cyber kill chain, all security measures need to work coherently. This way, even if one security measure fails in the initial levels (like the firewall), the next one can prevent further spread of the attack, thereby reducing the overall impact of the cyberattack, This can help in stopping the data breach from spreading further.

This highlights why a unified cybersecurity strategy comprised of multiple security solutions working together is the right approach towards cloud security.

# Secure Access Service Edge

Secure Access Service Edge (SASE) is a term coined and defined by Gartner in its 2019 report of *The Future of Network Security in the Cloud* by Gartner analysts Neil MacDonald and Joe Skorupa and later elaborated on in Gartner's 2021 report of *Strategic Roadmap for SASE Convergence.*

SASE implements a cloud-centric network architecture that manages user and device access by applying unified, policy-based organization security. It ensures secure access to the applications and resources on the cloud platform. Through SASE, organizations can deploy secure, uniform, policy-based access irrespective of the location of users or devices. Gartner has estimated that by 2024, at least 40% of enterprises will have explicit strategies to adopt SASE.

## 2.1 What is SASE?

SASE is a cybersecurity framework designed to converge network and security features in a cloud-based architecture that is distributed globally. It aims to deliver these features at the edge of the cloud network, that is, closest to the end user. SASE brings multiple security frameworks like software-defined wide area networks (SD-WANs), Zero Trust, and Firewall as a Service (FWaaS) together on a cloud-centered platform to ensure secure network access for users from anywhere.

## 2.2 Why SASE?

Gartner analysts have stated that SASE enables companies to operate during times of disruption by providing highly secure and uninterrupted access to any application or resources, regardless of the user location. This is because SASE focuses on identity-centric access management that is independent of the user, device, location, or network.

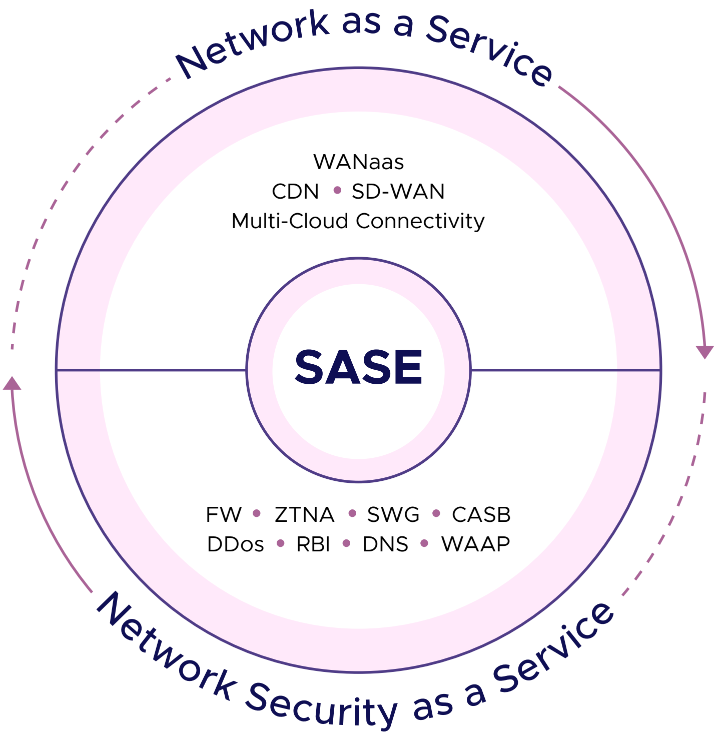
Managing security through identities is a core component of SASE. Additionally, SASE ensures a seamless network experience for all users by shifting network traffic from the enterprise data centers to the public cloud. Real-time routing optimizations factors in network congestion and determines the fastest network path.

This way, network traffic is routed as close to the end user as possible, reducing the chances of end users experiencing network latency. This also reduces the back-hauling of network traffic to the enterprise data centers. As SASE is globally distributed, all the users across edges experience the networking and security functions consistently.

SASE uses the least privilege access method. In the least privilege access method, users' access to resources and the functions enabled for them is highly restricted and monitored. The idea is to ensure that only required users should have the access to designated resources. Using this method, all authorization requests are approved on a need-to-know basis. Additionally, a centralized security policy is defined by the organization to ensure secure access to the network at all times. This policy is enforced to verify and grant access privileges based on the user identity. SASE defines a common framework for mandating this policy across all users, devices, and networks. When threats evolve and the SASE service provider adapts to this new threat, the security changes are replicated across all endpoints. SASE also guarantees the network system's viability by ensuring local access to critical network services. This acts like a backup to ensure business continuity in case of any disruption in WAN connectivity.

## 2.3 SASE: The convergence

SASE converges network and security services and delivers them from a globally distributed cloud-centered platform. According to Gartner, SASE capabilities will be deployed as a service based on the user identity in a real-time context to enable a continuous risk analysis throughout the access period. Along with that, a unified organizational security and compliance policy will be defined for continuous risk assessment during each user session.



## 2.4 Network as a Service

SASE implements the idea of *Network as a Service* by bringing together multiple standalone network solutions on a single, integrated cloud-platform.

The SASE network architecture is globally distributed with decentralized access. This means the enterprise network must be extended globally to reach all the users and provide uninterrupted secure access.

SD-WANs, FWaaS, data masking, secure web gateways, remote browsing isolation, and content delivery networks are some of the network solutions that are implemented in SASE.

### i. SD-WAN

An SD-WAN creates a virtual network architecture with centralized software access that uses the internet to securely connect end users to the required applications. As defined by Gartner, the characteristics of an SD-WAN are:

- Supports multiple connection types
- Ability to do dynamic path selection
- Provides a simple interface for managing the WAN
- Supports VPNs

Traditional WANs are hardware-oriented and function using routers. They manage network traffic by sending data through the central data center located on the enterprise perimeter for security control. Since this highly restricts the flow of data in terms of geographical boundaries and is not compatible with the upcoming cloud technology, the traditional WAN system is not well-suited for cloud-based operations.

With an SD-WAN, data, applications, and resources are hosted in the cloud. The SD-WAN deploys software-defined centralized control over the network architecture through which it not only securely connects the networks but also chooses an intelligent path for the flow of data across the WAN. This delivers a high-quality user experience and improved network performance.

## ii. Data masking

Data masking is a process of securing sensitive data by replacing the original, confidential data with a faux version of the data. This process is also known as data obfuscation or data anonymization. The faux data is created by shuffling or substituting the letters, numbers, or characters from the original data in a way that it cannot be reverse engineered. This prevents the risk of exposure to sensitive data. Even in case of a data breach, the data remains meaningless and cannot be misused. It also reduces the possible risks when confidential data is shared to third-party service providers.

The purpose of data masking is to secure confidential data while providing an alternate data set that can be used in cases where there is a need for data similar to the original data in terms of characteristics. Some instances where masked data is used are software testing processes, training, and sales demos. Data masking is also used in data sanitization. At times, deleted files can be recovered and possibly lead to data breaches. If the original data is masked before deletion, it becomes useless even if retrieved post deletion.

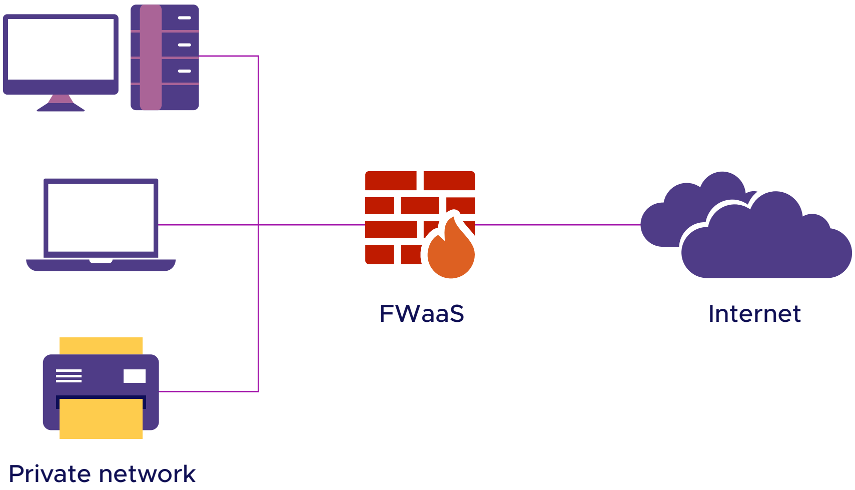
## iii. FWaaS

A firewall acts as a security system that prevents unauthorized access to the network. It monitors all incoming and outgoing network traffic and applies the organization’s security policies to authorize access requests. Traditional firewalls were deployed in on-premises data centers where all the applications and data were stored. Here, firewalls acted as the main access checkpoints and functioned within a predefined network perimeter. However, with the advent of cloud technology, applications are hosted on third-party networks and the traditional idea of the network perimeter no longer exists.

In FWaaS models, firewalls become a part of the cloud-based infrastructure. Similar to traditional firewalls, the FWaaS is positioned in between the organization’s network and the internet to analyze network traffic and secure the network from inside and outside threats.

However, FWaaS works on a unified organizational security policy which is continually applied to all the websites, networks, applications, and users to ensure the security of the network. Since FWaaS works using cloud-centric operations and software-defined control, it is highly cost-effective and can be scaled easily to suit dynamic organizational requirements. It also provides complete visibility and software-defined control over the organization's network.

## How FWaaS works



### iv. Secure web gateways

A secure web gateway (SWG) is a security solution that prevents the entry of unsecured traffic into the enterprise network to protect it from malwares and viruses. SWGs prohibit access to malicious websites as defined by the organizational security and regulatory policies.

Traditional network infrastructures route access to applications and resources through enterprise data centers. In the remote working era, the enterprise network becomes decentralized as users connect from different locations, networks, and devices. To secure remote employees, their network traffic is backhauled to the data centers, which results in latency and reduced network speeds.

Additionally, remote employees are increasingly adopting cloud-based services and platforms. Since most of the cloud services are web-enabled, web traffic keeps increasing. This is why it becomes crucial to increase the network perimeter to all endpoints to secure the enterprise network from cyberthreats without impacting the end-user experience.

When users access websites using SWGs, they do not directly access any website. The SWG is added to the web browser and it performs additional functions like URL filtering, inspection of malicious content, and web access control before delivering the web content to the user. SWGs block access to certain websites based on organizational security policies and ensure a safe internet experience. They also help prevent unauthorized data access and transfers.

### v. Content delivery network

A content delivery network (CDN) is a set of servers that is widely distributed geographically to quickly load web content. This is achieved by bringing the web servers closer to where the users are physically located. Traditional enterprise data centers use caching to enable faster loading of web content. In caching, multiple copies of the files used to access the web content are stored temporarily at the enterprise data centers to reduce the loading time of websites and browse faster. In a CDN, the cache content is stored in proxy servers closer to the user's location. This means caching is expanded far beyond the organizational network perimeter using a CDN.

Traditional data centers operate using a central server that stores all data. Data transfer from the central server to user devices is a time-consuming process that often results in network congestion when multiple users try to access large amounts of data from different locations. A CDN prevents this by moving the storage of web content closer to each user to enable quick loading of web content each time. The remote work era has resulted in users working and accessing data from different corners of the world. A CDN ensures reduced website loading time, reduced usage of bandwidth, reduced network costs, and consistent content delivery for all users irrespective of their locations.

### vi. Remote browser isolation

Remote browser isolation (RBI) is an advanced cybersecurity measure that provides security for the organizational network infrastructure and resources while the user is browsing the internet. Through RBI, each user's browsing activity is secluded from the organization's network infrastructure. Essentially, any possible threats that may enter the network during the browsing session are isolated and have no means to enter the enterprise network perimeter. The possible attack surface remains limited to the user's browser.

RBI works by implementing a remote browser, held virtually on the cloud, each time a user accesses a web page or a web application. At the end of each browsing session, the virtual browser network is erased. This means that if any malware had gained access during the browsing session and was downloaded to the browser, it will be deleted, keeping the network secure and eliminating the possibility of a data breach through the browser.

With cloud-based applications and resources, there is a continuous need for users to stay connected to the internet. This opens up organizations to cyberrisks, as most cyberattacks target users through their browsers using clickbait or fake advertisements. When a user's browser connects to a website, hackers get access to the user's device and perhaps the entire network as well. Usually, firewalls are deployed to block the potentially risky websites, but attacks are getting increasingly sophisticated and it becomes almost impossible to block every new malicious site. RBI enables continuous secure browser access and closes pathways to prevent any risky web content from entering the organization's network.

## 2.5 Security as a Service

SASE implements the idea of *security as a service* by bringing together multiple network security solutions on a single, integrated cloud platform.

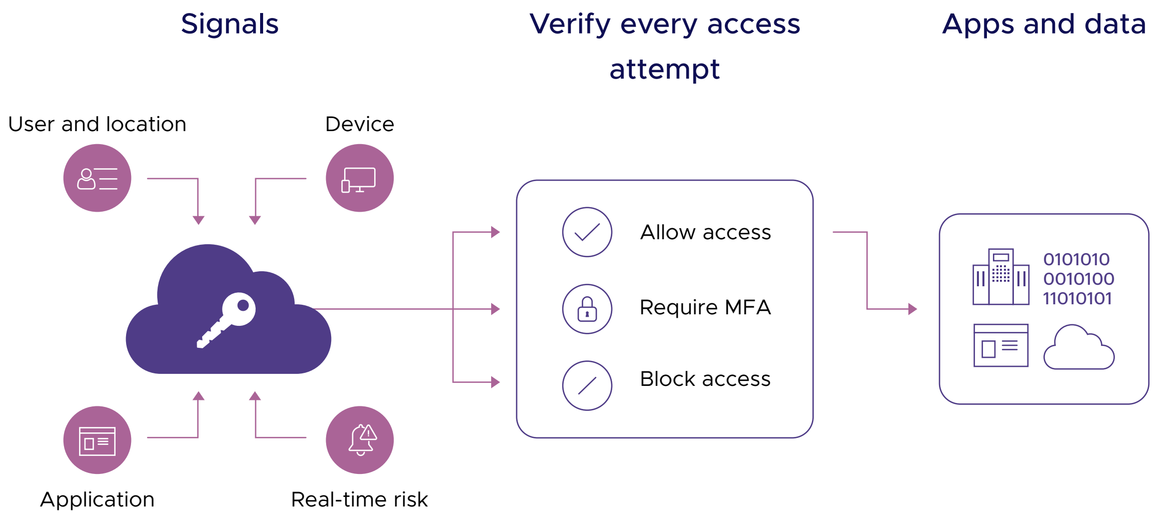
SASE security solutions must ensure that each user endpoint is secure by extending the secure perimeter globally. Zero Trust, user and entity behavior analysis (UEBA), cloud access security brokers (CASBs), and web application and API protection are some of the network security solutions that are implemented in SASE.

### i. Zero Trust

Zero Trust is a security framework that entirely removes the idea of trust from the organization's security policy. This means that, by default, no user, device, or network is trusted and everything is verified before authorization requests are granted. The verification of each user, device, and network that tries to access organizational data and resources is done irrespective of their location, whether within or outside the organizational network perimeter.

Usually, organization-approved devices are trusted by default which often results in breaches and attacks when someone else uses the device for attacks or while they are connected over insecure public networks. With Zero Trust, every device has to go through authorization processes to ensure security each time access is granted.

Zero Trust uses the least privilege method, that is, users are given only as much access as they need. To deploy the least privilege method, user roles and their requirements must be carefully analyzed before granting them permission for different data sets and resources. This way, access to sensitive data and resources is highly limited. This minimizes the exposure to the sensitive data and keeps track of access requests granted over time.



The idea of zero trust is to prevent both insider and outsider threats. Hence, it becomes important to monitor and verify each user and device. In zero trust, data and resources on the network are divided into separate unique zones based on their level of confidentiality and sensitivity. Through this, access to such crucial data is limited and even in case of breach in other zones, this data remains safe from possible breach.

### ii. UEBA

UEBA analyzes the behavioral pattern of users and devices to detect suspicious behavior and possible threats. UEBA creates large data sets of user and device behavior over the enterprise network and, based on occurrence, frequency, and other characteristics, categorizes behaviors as typical and atypical.

Using this baseline, UEBA engines are able to identify any deviation from the norm as suspicious behavior, which can indicate a potential cyberthreat. UEBA also makes use of artificial intelligence and machine learning to identify these typical behavior patterns. On detection of atypical behavior, it sends out real-time alerts to the security team to check for possible threats and prevent them from causing a breach. UEBA is a security measure that has the ability to detect even non-malware based cyberattacks, as it works on the basis of behavioral patterns.

The analytic component of UEBA detects anomalies using different approaches like stat models, machine learning, and threat signatures. Additionally, UEBA can identify possible insider threats. Based on the organization's security policy, a UEBA solution can detect and report on user behavior that violates organizational policies. For instance, users copying or moving data into local USB devices can be detected, and if users try to view files or folders that are not relevant to their job responsibilities, administrators will be notified.

### iii. CASB

As defined by Gartner, a CASB is on-premises or cloud-based software that is positioned between the cloud service provider and the cloud service users to enforce the organizational security policies while using the cloud platform. Since cloud services are often delivered by a third party, a CASB ensures that there are no security gaps and all security policies are deployed across all the cloud environments like SaaS, Platform as a Service, and Infrastructure as a Service. Additionally, it also provides visibility and control into the cloud-based applications using which security policies can be created for cloud operations.

As organizations become increasingly dependent on cloud services, CASBs are necessary to protect sensitive data and enable secure cloud usage that falls within the organizational security principles. The CASB acts as a policy enforcement entity, as it brings together multiple security policies to create a unified policy that is deployed across all cloud-based functions. Through this, security is delivered irrespective of the user's location or network, so each user, device, network, and location is monitored consistently.

A CASB brings control over the cloud network through organization-defined security policies. It performs multiple functions like authenticating users' credentials and authorizing access to only the necessary resources. It deploys firewalls to ensure security at the application level rather than at the network level, which ensures a higher degree of security. It prevents data loss by not permitting sensitive data sharing outside the organization.

### iv. Web application and API protection

Web applications are increasingly becoming the targets for cyberattacks. When an attack is launched on a web application, the attackers gain access to the stored data and are also able to move into other parts of the network. This is a huge threat to the entire network architecture and other applications and resources on the same network.

With users working remotely, web applications and APIs are accessed using public networks. In case of a breach, this can lead to access to sensitive data. Traditional security solutions do not tend to web applications, as they are a relatively new adaptation and require advanced security solutions.

Web application and API protection (WAAP) is a cloud-based service that contains multiple security components with different levels of security. WAAP is deployed at the outer edge of the enterprise network as a measure to protect web applications by monitoring and analyzing the incoming traffic.

# Zero Trust and SASE: Better together

Zero Trust is a critical part of SASE, as it amplifies the core idea of SASE: the need for a unified network and security process that is independent of any other factors like network perimeters and user devices,. Zero Trust acts as an enabler for SASE, because it nullifies the idea of perimeter-based security practices and adds an additional layer of security.

The Zero Trust security framework assumes that any user, device, or network requesting access to connect to any enterprise resource could be a potential threat. Traditional network security places default trust on users within the organizational network architecture once they are authenticated at the initial entry. However, a Zero Trust approach removes any default trust assumptions, whether the user is inside or outside the corporate network. When integrated with SASE, the cloud-based nature of SASE allows Zero Trust to deploy complete security no matter where access is requested from, when access is requested, or how.

The Zero Trust approach is one of the main elements of SASE, as it implements unified authentication methods that require authorization each time access is requested with no exceptions. Zero Trust reserves software-defined access at the application level rather than at the network level, working independent of the user network or location. It also ensures that access is granted only to the authorized and authenticated users who were previously chosen to have access.

# Benefits of SASE

The goal of SASE is to deliver multiple network and security solutions through a single platform and reduce IT costs in the long run. As SASE eliminates backhauled network traffic, bandwidth costs are also reduced. Additionally, improved technology functions are delivered, like seamless remote access, secure global network scalability, and consistent user experience independent of location. SASE helps detect potential cyberthreats traffic at the network boundary itself and secures the organizational network perimeter across the world.

SASE implements a unified security policy through which the IT team gains complete visibility and control over all network processes. This results in efficient and quick resolution of any IT issues that may arise. Since SASE is cloud-centric, it can be deployed globally to reach each user endpoint and develop a highly secure, end-to-end connected network.

Since SASE has no central access but is globally distributed, it can manage network traffic and possible interruptions easily with minimal impact on user experiences.

# Challenges of SASE

Since the core idea of SASE requires all the network and security solutions to be delivered as an unified experience, many organizations will want a single vendor to deliver all SASE features as a single service. However, the SASE service provider may excel at some individual network and security frameworks while not offering the best services for others. Opting for a single vendor has a major disadvantage, as it limits access to the best vendors of individual function.

Additionally, handing over the entire network architecture to a single vendor is a highly risky decision. As SASE is an emerging market, the number of available vendors is minimal. With a SASE architecture running on solutions from a single vendor, enterprises are constantly exposed to the risk of a massive single point of failure. Since the entire network architecture and security measures are delivered through a single vendor, if there are any technical issues from the vendor's side, the entire system can fail at once.

# Roadmap to SASE implementation

The most important part of implementing SASE in enterprises is to strategize the migration plan according to the organizational requirements. SASE cannot be adopted by organizations overnight. It needs to be scaled gradually and with the lowest possible impact on everyday business processes.

The core idea of SASE is to converge multiple security and network functions together. This is why the people who are a part of those IT teams must be trained to work together as a single team. Along with the gradual adoption of SASE, the multiple IT and security teams should be integrated to fit long-term SASE requirements. The process of adding new technological functions and discarding outdated ones must be done in a synchronized manner without disrupting the functioning of the organization.

The deployment of these new processes will involve a significant financial investment as well, which must be considered in advance so that the budget can be allotted accordingly. Multiple SASE vendors should be assessed before choosing the one that fits the business requirements well. Since SASE cannot be deployed in organizations overnight, it's important to set explicit time-oriented goals, which must be continually assessed and followed throughout the migration.

As stated by Gartner, “SASE enables companies to operate during times of disruption and provides highly secure, high-performance access to any application, regardless of user location." The complete shift to a SASE-based platform model will take significant time. Along the way, there will be numerous disruptions and difficulties while moving away from traditional network security and access management. But SASE is no longer an option; it's a necessity. As organizations move into a dynamically changing world, SASE is crucial for efficient network security operations and improved cybersecurity.

# About AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote    ⤓ Download