NEXTLABS®

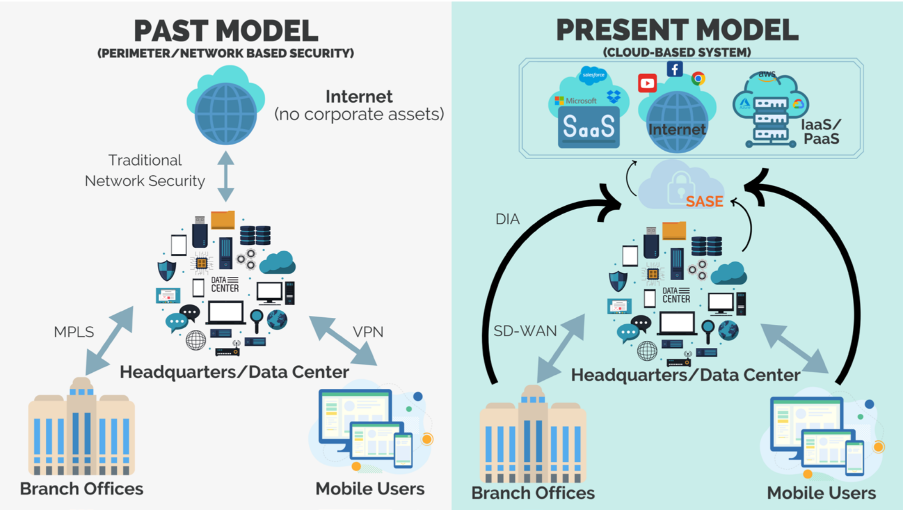
White Paper

The Next Frontier of SASE

Secure Access Service Edge (SASE) is a model introduced by Gartner in 2019 to combine network and security capabilities as a service, based on the identity of device or entity, and real-time context. The model works to streamline network access and improve the adherence to security and compliance policies.

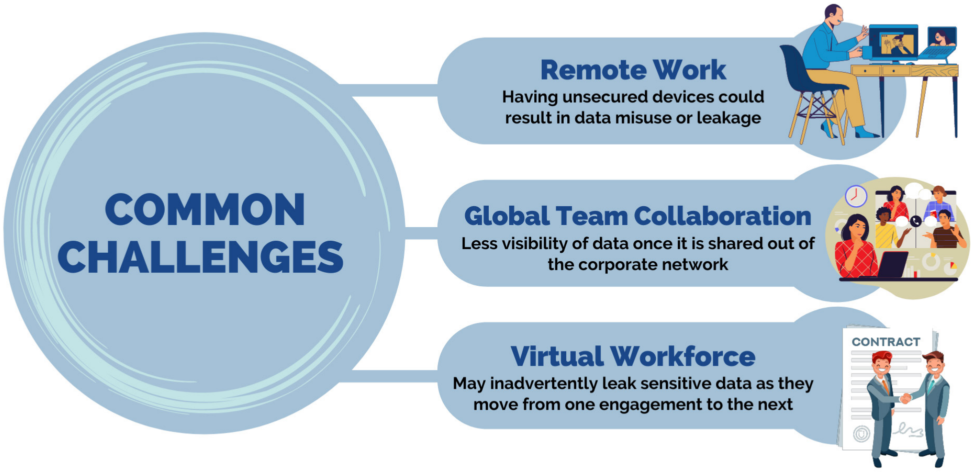
Before the internet revolution 20 years ago, the majority of applications were located at the headquarters (HQ) or data center of the organization, so network traffic was mainly between these locations and branch offices. In these past network settings, organizations would only need to secure the network and security access at the HQ or data center, which would allow data to be protected at the corporate edge.

In the current context, however, there is an increase in the adoption of cloud-native applications and SaaS. Organizations have started to move away from centralized cloud infrastructures to enable access to data outside of consolidated data centers due to the increase in cloud applications and remote work. This changes the dynamic of traffic whereby the network architecture distributes data across various devices, causing there to be less visibility on the data outside of the corporate network. As decentralization shifts the workplace, organizations need to secure the network and security not only at the HQ and data center, but also from a variety of locations for different users at the cloud-edge.



A SASE architecture identifies users and devices using policy-based security and delivers secure access from the network to the application or data. Since SASE is about establishing secure access to network, enterprises' secure access should not stop at the network, but should also extend to enable secure data access. This is because users do not simply require access to the network, they also need access to data.

In today's digital environment, according to IDG, more than 60% of companies run the majority of their applications in the cloud. Additionally, a report by IDC predicts that by 2025, nearly 60% of the world's data will be stored in cloud. Given, data and applications are central to core business processes, it is essential for companies to secure access to data and applications on the cloud. This provides the underlying argument for extending SASE to secure access to data and applications in the cloud.


COMMON CHALLENGES
Remote Work
Having unsecured devices could result in data misuse or leakage
Global Team Collaboration
Less visibility of data once it is shared out of the corporate network
Virtual Workforce
May inadvertently leak sensitive data as they move from one engagement to the next
CONTRACT

Moreover, the following common challenges make it highly important for enterprises extend SASE to protect data and
applications:

- **Remote working** – Data security can be compromised as workers have other unsecured devices such as printers and storage drives which could result in data misuse or leakage.
- **Global team collaboration** – Data is being shared across different teams, suppliers, and partners who can be located across the world, this poses a major challenge to visibility once shared outside the corporate network.
- **Virtual workforce** – Virtual employees may inadvertently leak sensitive data into and out of the organizations as they move from one engagement to the next.

In these situations, it is imperative for organizations to realize that what matters most in the network environment is its data. Especially with ever-changing security dynamics, it is important to properly secure data access; protecting the organization's data in its multi-cloud environments from unauthorized access, usage, changes, or theft.

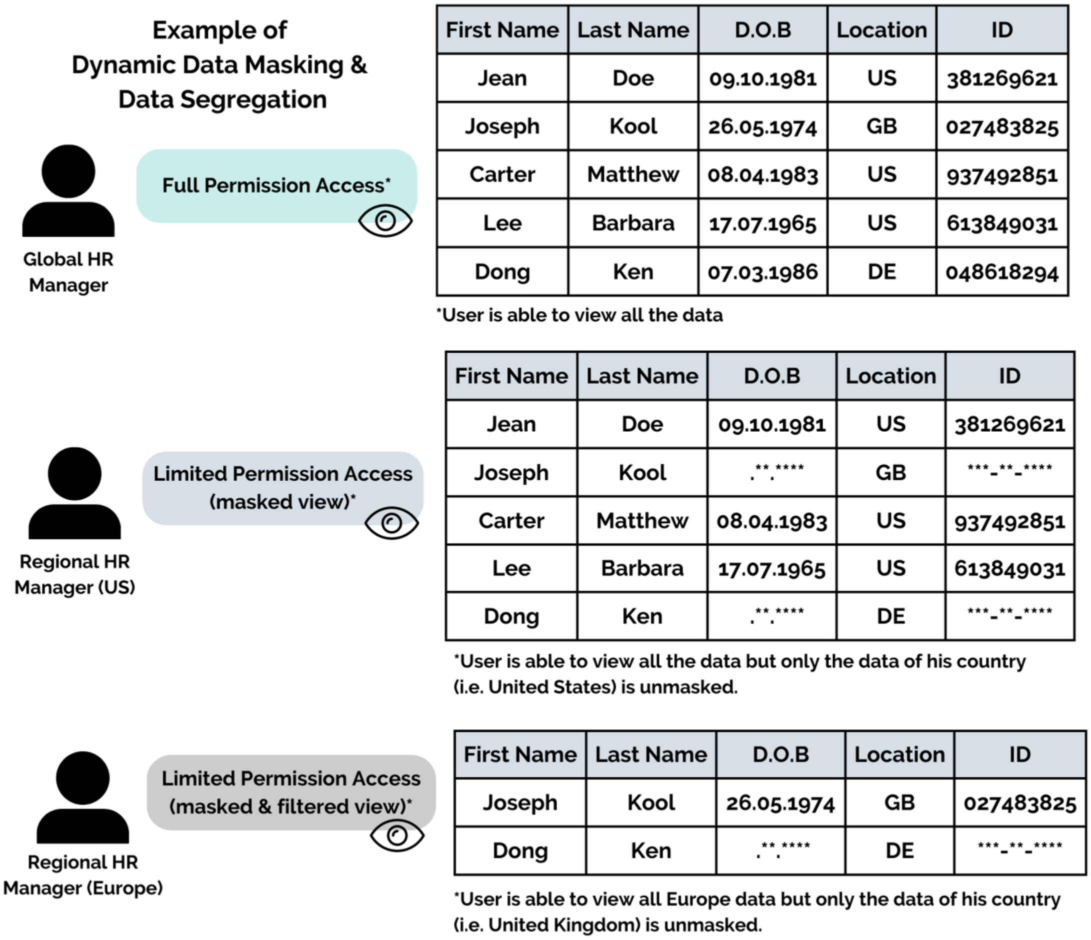
As reported by Gartner, by 2025, more than 85% of organizations will adopt cloud computing, and will not be able to maximize digital strategies without cloud-native applications and technologies. This drives the need to extend SASE to data resources in a multi-cloud environment to safeguard data with the data access service edge (DASE) approach.

What is Data Access Service Edge (DASE)?

Applying SASE to secure data access in hybrid and multi-cloud environments utilizes concepts like DASE. With hybrid and multi-cloud architectures being the future for businesses, DASE will come into play to extend beyond the concept of SASE by securing data access using zero trust principles. DASE gives organizations the ability to enhance their security systems by controlling the access to data through dynamically enforced policies that protect resources over the network perimeter by enabling least privilege access.

DASE ensures that the access to data is not accessible by default, taking on a never trust, always verify approach. Leveraging on attribute-based access controls (ABAC) and dynamic authorization technologies, enabling policies to be validated in real-time based on their attributes. Examples of these attributes include user role, location, and device at the time of access. Assuming that threats can originate from inside and outside of the network, DASE evaluates risks and mitigates threats to data within the network and cloud. The authorization and access rights to an organization's data, applications, and sensitive assets, are granted dynamically in real-time using attribute-based rules and policies.

Organizations can control access to critical data through fine-grained data-level security controls to protect data. This can be done with dynamic data masking and data segregation techniques. Dynamic data masking prevents unauthorized access to sensitive data by applying policies to ensure that users can only view the fields on the record that they are granted access to, and the value of the other unauthorized fields will be masked. In contrast, data segregation ensures that data in records can be filtered such that authorized users can only view those which they have



Example of Dynamic Data Masking & Data Segregation

First Name	Last Name	D.O.B	Location	ID
Jean	Doe	09.10.1981	US	381269621
Joseph	Kool	26.05.1974	GB	027483825
Carter	Matthew	08.04.1983	US	937492851
Lee	Barbara	17.07.1965	US	613849031
Dong	Ken	07.03.1986	DE	048618294

*User is able to view all the data

First Name	Last Name	D.O.B	Location	ID
Jean	Doe	09.10.1981	US	381269621
Joseph	Kool	.**.****	GB	***-**-****
Carter	Matthew	08.04.1983	US	937492851
Lee	Barbara	17.07.1965	US	613849031
Dong	Ken	.**.****	DE	***-**-****

*User is able to view all the data but only the data of his country (i.e. United States) is unmasked.

Regional HR Manager (Europe)
Limited Permission Access (masked & filtered view)*

First Name	Last Name	D.O.B	Location	ID
Joseph	Kool	26.05.1974	GB	027483825
Dong	Ken	.**.****	DE	***-**-****

*User is able to view all Europe data but only the data of his country (i.e. United Kingdom) is unmasked.

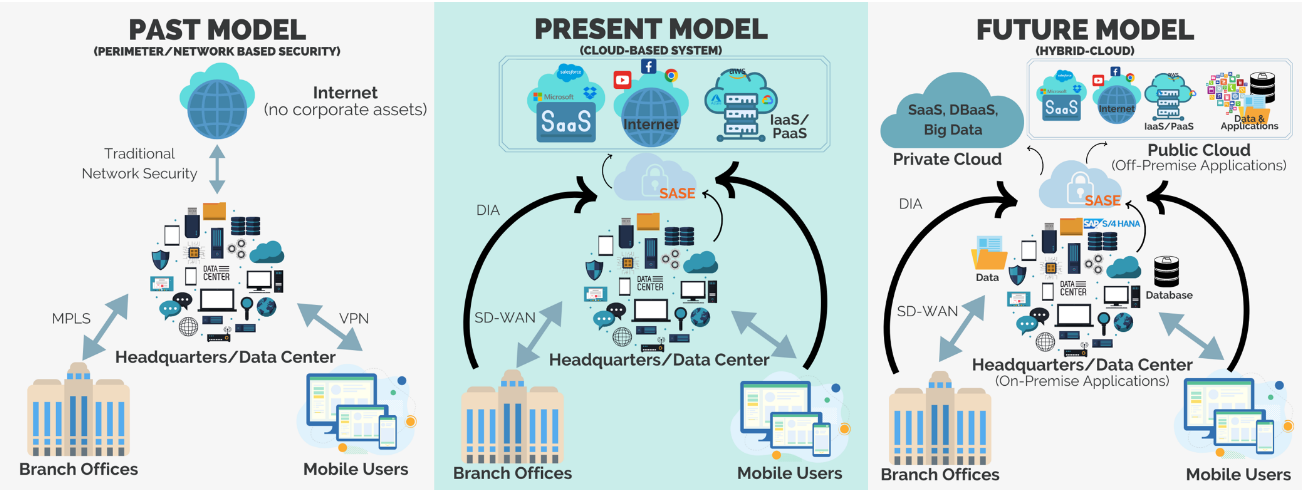
Why is DASE significant?

Safeguarding data in dynamic environments can be rather complex but there are several aspects which DASE can help organizations to ensure data security. To avoid data breaches or contamination, organizations can protect sensitive data at the service edge using data access level enforcement system, as mentioned above.

With the increase in virtual and remote workforce, various stakeholders are geographically distributed which makes it difficult and expensive to physically or manually control access to systems with sensitive data. In order for users to get access to data in an efficient manner, it is vital to automate policies for data protection to simplify and streamline the risk assessment process. This will allow data to be protected continuously as policies can be directly managed by the administrator. In doing so, organizations can embrace automation to scale, as it is more repeatable, and less error prone enabling the handling of a high volume of data while meeting ever-changing requirements. With this, critical information can be shared, and secure collaboration can be established between employees and external partners, increasing business agility and scalability. Additionally, this flexibility can benefit in cases such as sanctions. When a sanction is imposed or revoked, the variables of the data will need to be changed to comply with the given sanctions. With DASE automation, it enables organizations to simplify their response to new regulatory requirements.

Through the application of DASE, organizations can quickly react to changes in any business or regulatory environments, greatly increasing agility and flexibility, while enhancing secure access of data beyond the network.

The Next Frontier



As organizations move towards hybrid cloud environments, they will have to manage access to the network and data. The next frontier of SASE will not only be about establishing secure access to the network environment but will also be about protecting applications and data to support multi-cloud environments. In a diverse cloud computing environment, managing data security is critical since data and applications are stored in public clouds, private clouds, and on-premise databases, which can be at risk of data breaches. To address data protection needs, this future frontier will need an approach to protect data with DASE which ensures continuous protection for structured and unstructured data across all cloud computing environments.

Takeaways

In closing, as digital strategies continue to evolve with more data stored in hybrid cloud and multi-cloud environments, SASE needs to continue to evolve to cover device, network, data, and applications. As such, the next frontier of SASE will extend to secure access to continuously protect data and applications regardless of where it is with Data Access Service Edge (DASE).

- DASE expands the coverage of SASE to secure access to data with zero-trust principles.
- It gives organizations the ability to enhance their security systems by controlling the access to data through dynamically enforced policies that enable least privileged access.
- Utilizing attribute-based access controls (ABAC) and dynamic authorization technologies, DASE evaluates risks and mitigates threats to data within the network and cloud.
- Organizations can control access to critical data through fine-grained data-level security controls, such as dynamic data masking and data segregation techniques.
- Through the use of DASE and automation of data security controls, organizations can increase agility while easily reacting to new business or regulatory requirements.

To learn more, visit NextLabs Data Access Security to find out how DASE can support you in securing data access for various applications such as SAP S/4HANA, BigQuery, SAP HANA, Oracle, Microsoft and Azure SQL, and more.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www. nextlabs.com.