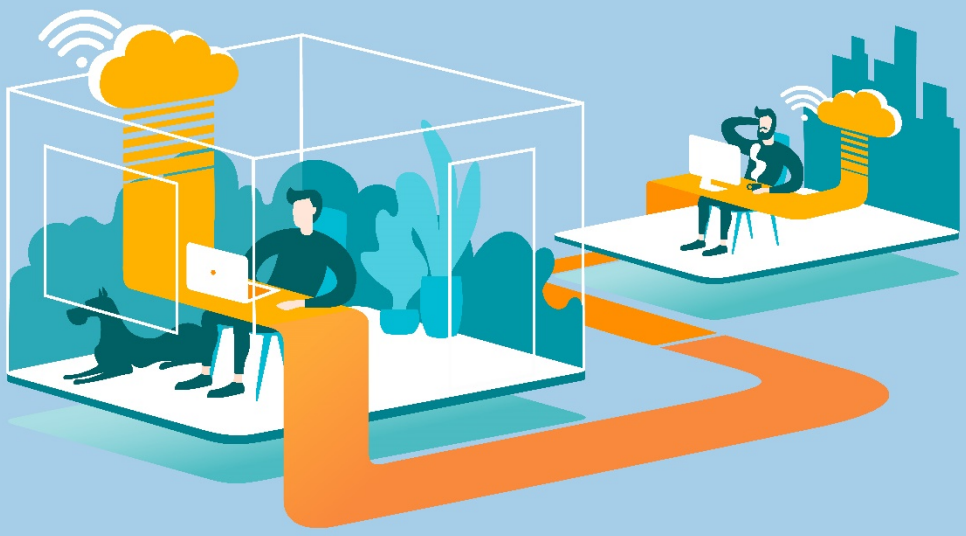
CIO ACADEMYASIA

Enabling Digital Transformation and Cloud Migration with SASE Technology

A research primer published by CIO Academy Asia

MARCH 2021

In partnership with bitglass



Introduction

The COVID-19 pandemic has rapidly accelerated the shift of workloads to the cloud, combined with a massive increase in remote work.

Companies are struggling to keep their cloud estates and endpoints secure as continuous change, disruption, and persistent threats create gaps in security postures.

Often, security controls are not designed for the dynamic, distributed, and virtual nature of cloud environments, and widely dispersed remote working. Companies tend to react to cloud security challenges by adopting multiple point solutions to plug gaps and address varying needs, including Cloud Access Security Broker (CASB) technology to secure SaaS traffic, and Secure Web Gateway (SWG) technology to secure web traffic. Each solution needs to be configured and managed — this creates complexity and risk. Failing to apply any setting correctly can prove to be disastrous.

Companies also commonly discover that their cloud security controls are not fit for purpose. Cloud security solutions are often unable to scale across an expanding number of people and devices, located outside the traditional enterprise perimeter.

Companies need full visibility across their cloud resources. They need to deploy a single set of policies which can be managed and configured on a single dashboard. They also need an integrated set of tools.

These requirements can now be addressed by Secure Access Service Edge (SASE) technology. A SASE solution can enable rapid cloud adoption and remote access, by offering security services from a common cloud-delivered architecture, using the same policies and a single dashboard.

This paper uses inputs from discussions with technology decision makers across ASEAN. It highlights some of the main security challenges faced by companies in ASEAN as they seek to leverage cloud technology. It will focus on:

- The cloud and remote working security gaps created by the pandemic
- The ways of addressing cloud security gaps, particularly by using a zero-trust approach to security
- SASE technology as a cloud adoption enabler, and solution to cloud security concerns
- Key SASE considerations.

AUTHORS

P. Ramakrishna
CEO
CIO Academy Asia

Andrew Milroy
Principal Advisor
CIO Academy Asia

Pandemic Highlights Cloud and Remote Working Security Gaps

The rush to the cloud and remote working has created some sizeable security gaps including misalignment of security policies with new technology architectures, misconfigured clouds, weak identity and access management and insecure APIs.

Remote working and pandemic restrictions, across ASEAN, have led to companies accessing an increasing number of applications, including SaaS, PaaS, and IaaS, from multiple public clouds. Companies' primary focus has been on ensuring that employees have access to these resources — often at the expense of security.

Traditional Network Perimeter is Inadequate

The traditional network infrastructure model of centralised corporate datacenters secured by on-premises network perimeters, doesn't work today. Data that once resided in datacenters is increasingly found in the cloud, on SaaS applications, and on endpoints.

Traditional security controls struggle to deploy sufficient automation to provide the real-time visibility required to instantly detect, monitor, and secure changes within clouds. The dynamic nature of the cloud makes integration with traditional security solutions difficult — or impossible. Every time, there is a change in cloud service requirement, a new security gap can emerge.

Misconfiguration of Clouds and Inconsistent Controls can be Disastrous

Across ASEAN, the rapid deployment of workloads to the cloud is often a major burden for security teams. Growing 'operational sprawl' adds to security complexity, and can hinder business processes. Within multicloud environments, incompatibility issues frequently emerge as users move between clouds. For example, the security services and controls in a Microsoft Azure cloud may not be aligned with the controls required for an AWS cloud, or for other kinds of deployments such as on-premises or private clouds. Inconsistent controls across multicloud environments are having an increasingly negative impact, on business performance.

Cloud misconfiguration is highlighted as a major risk for companies in ASEAN. IaaS solutions typically require extensive configuration to make sure that they work properly. Often, the need to configure IaaS solutions in line with a company's desired security posture is overlooked, potentially leaving data, public facing. Incorrect configuration can result in storage offerings such as AWS S3 being exposed. Access to this data can easily be indiscriminately granted to anyone who tries to access it, which can have a devastating impact. Repairing misconfigurations is an essential part of data leakage prevention and is critical to ensuring that cybersecurity posture is effectively managed.

Addressing Cloud Security Gaps

As companies migrate to the cloud, it is critical to stay ahead of threats. A zero-trust approach can equip companies with the resilience they need as they transform and migrate workloads to the cloud. Basically, a zero-trust strategy establishes a "never trust, always verify" approach to everything the company does.

Zero-trust involves consistent visibility, enforcement, and granular access control that can be delivered on endpoints, or through the cloud, to manage access and prevent data loss.

It involves moving defenses from static, network-based perimeters to focus on users, assets, and resources. Trust is no longer granted to assets, user accounts based on their physical or network location, or asset ownership. Authentication and authorization must be performed before every session to a company resource is established.

The recent SolarWinds Sunburst attack highlighted the need for a zero-trust approach to security. Companies need robust processes to mitigate these risks, including clear identification of dependencies and accountabilities.

Security needs to be baked into coding

Security needs to be part of application design. Baking security into the process of coding, builds much greater agility into security. The widespread use of cloud-native technologies including containers, serverless and microservices enables the continual integration and continuous delivery of updated code without impacting the performance of an application.

In addition to baking security into code, companies need a set of policies, procedures, and technologies that work together to protect cloud-based systems, applications consumed from private data centers, IaaS, PaaS and SaaS, data, and infrastructure. From authenticating access to filtering traffic, cloud security must be configured to the company's exact needs.

Cloud Security Posture Management (CSPM) Mitigates Cloud Misconfiguration Risk

Companies can use CSPM tools to identify and remediate costly and potentially harmful misconfigurations. CSPM tools can crawl IaaS instances in search of inconsistencies with defined custom benchmarks, as well as established security standards such as the Payment Card Industry Data Security Standard (PCI DSS). Uncovered misconfigurations can then be categorized and displayed, illustrating how a company's cybersecurity posture is changing.

Companies also need to understand the necessary remediation steps to address discovered issues, and to ensure the correct configuration of IaaS instances. This can be a time consuming and costly process. Companies must consider working with cybersecurity solution providers that can uncover misconfigurations, perform remediation, and repair misconfigurations automatically.

Cloud security requires alignment with the agile nature of the cloud, visibility of data analytics and adherence to compliance and governance standards. By making these requirements part of a security strategy together with a zero-trust approach, companies can gain operational transparency and consistency which earns trust – while ensuring that security posture is optimised.

SASE as a Cloud Adoption Enabler

With increased remote working, users need to be able to connect to resources from anywhere forcing companies to provide network access and a secure, route to the internet without impacting performance.

SASE is designed to enable the delivery of an integrated set of network and security services in a consistent way. This enables digital transformation, cloud migration, edge computing and remote working.

More specifically, SASE solutions integrate security and networking into one cloud solution. Instead of having multiple discrete services, it offers the following as a unified solution:

- Zero-trust network access
- Virtual private networks
- Software defined WANs
- Firewall as a service
- Secure web gateway
- Data loss prevention
- Cloud access security broker

Figure 1 – SASE Model

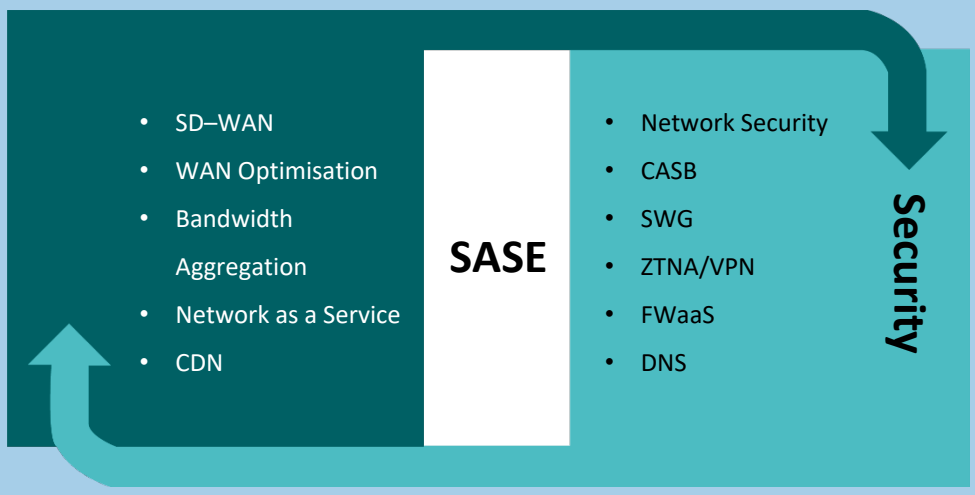


Figure 1 illustrates the SASE model.

SASE allows companies to eliminate a complex and fragmented set of physical and virtual solutions by providing one integrated cloud-native solution. This removes the cost of the appliances, and reduces network complexity. It offers much lower latency, greater visibility across assets and centralized control.

SASE is also essential for the development of a zero-trust approach to security. In addition to addressing many of the challenges associated with hybrid clouds and remote working, a zero-trust approach plays a significant role in mitigating third-party risks.

Current digital transformation and cloud migration projects are placing unnecessary risks on companies. SASE and a zero-trust approach to security are the best ways in which companies can mitigate the increasing risk they face.

When selecting a SASE solution, companies must make several considerations. The most important considerations relate to performance, visibility, zero-trust network access (ZTNA), and CASBs.

Some Key SASE Considerations

There are a growing number of SASE solutions available today. When choosing a solution, it is important to consider options that protect data wherever it resides and wherever it moves. It is also important to select a solution that enables digital transformation and does not negatively impact the performance of any application or business process. Some of the most important SASE issues for consideration are:

- Uptime and availability. Few companies can afford outages or sluggish performance which slows business activity. A scalable and simple architecture is an important foundation for high availability. Companies must focus on SASE solutions that are elastic, auto-scaling, and resilient for the highest levels of availability. Companies should seek 99.99% uptime as a minimum.

- Secure Web Gateways. Applications are often accessed through remote access VPNs, but when users access cloud applications, they are typically disconnected from VPNs —increasing risk. SWGs provide secure internet access when users are disconnected from VPNs. A major challenge with SWGs is that they are usually set up standalone without coordinating workflows, or integration with security infrastructure in the company. This causes increased complexity as companies often have insufficient visibility across all point products. Companies must select a SASE solution which provides SWG in the cloud as part of a unified platform. This gives greater visibility and increased control over web access while enforcing security policies that offer protection to users, from malicious websites.

- ZTNA architecture. ZTNA is commonly endpoint-initiated. In other words, the endpoint or end user is initiating access to a resource. This approach is difficult or impossible to implement on unmanaged devices because of the need to install software locally. Customer, partner, and supplier endpoints cannot be directly managed. Alternatively, companies can have ZTNA that does not require agents. A ZTNA broker can initiate the connection between endpoint and the resource. This approach is ideal for unmanaged (BYOD) devices and for partner and customer access. Given the increasing need to engage digitally with customers and suppliers as well as the growth of remote working, this approach is becoming increasingly attractive.

- The shared responsibility model. Internal security teams typically maintain some responsibilities for security as applications, data, containers, and workloads move to the cloud, while the provider takes some responsibility, but not all. Companies in ASEAN are often unsure about their level of responsibility and have not adjusted to a transparent shared responsibility model. This can leave huge gaps in security, particularly regarding access controls and alignment of security posture across clouds and on-premises resources. Companies need a multi-mode CASB that offers end-to-end protection for data in any cloud service and on any device. Corporate data needs to be protected in real-time across enterprise resources. This entails granular data protection, zero-day threat protection, strong identity and access management, and full visibility. If these four components of CASB are in place, companies can lower risk substantially.

Summary

As companies become digitally enabled and rapidly migrate workloads to the cloud, they must make their systems, services, APIs, data, and processes accessible from any location, at any time, and from any device. Adequate security tools are needed to enable this.

Few companies in ASEAN have controls in place that are fit for purpose. Security solutions face challenges in scaling across an expanding number of people and devices located outside the traditional enterprise perimeter.

Indeed, ASEAN companies are starting to acknowledge that their physical network and security infrastructure must evolve to protect an increasingly perimeter-less environment. They need full visibility across their resources. They need to deploy a single set of policies which can be managed and configured on a single dashboard. SASE solutions are the answer — enabling digital transformation and cloud adoption by offering security services from a common cloud-delivered architecture, using the same policies and a single dashboard.

ASEAN companies increasingly share resources and engage digitally with partners, suppliers, customers, and employees who sit outside the traditional network perimeter. It is not possible to manage all their devices — so agentless ZTNA will progressively become the preferred option.

Importantly, SASE solutions need to enable digital transformation and cloud migration without negatively impacting business performance. SASE solutions must include uptime guarantees, offering the highest levels of availability. A minimum of 99.99% uptime is recommended.

This research primer is prepared by CIO Academy Asia

www.cioacademyasia.org

For partnership opportunities, please contact:
David Chin
Head of Relations
CIO Academy Asia
david@cioacademyasia.org

CIO ACADEMYASIA