Solution Brief

Secure Access Service Edge (SASE) Or Zero Trust?

What is SASE?

SASE architecture combines networking capabilities to enable connectivity for any user, from any device, from any location, with security capabilities to enforce the organization's security policies on that access. SASE results in a secure access platform that enables as organization to securely support a modern, mobile, and cloud-based workforce.

The SASE architecture is designed to enable the enforcement of security at the network level (similar to traditional firewall or IPS solutions). Other approaches do not rely on a network for security enforcement, but rather on SaaS vendor capabilities or endpoint-based enforcement. Other approaches might also lack capabilities (at best) or (at worst) might be unsecure, such as BYOD or hosted applications with minimal security controls.

The SASE architecture allows uniform security enforcement across all corporate resources and user activities, regardless of the endpoint or SaaS vendor capabilities. This architecture also enables visibility into users' actions, which is a mandatory requirement for detection, forensics, and compliance.

What should you consider when evaluating a SASE architecture for your business?

Overview

In this brief, we will focus on the capabilities required to enable the Zero Trust model to secure your corporate data, what SASE components support that model, and what you should consider when evaluating a SASE architecture for your business.

How Do SASE and Zero Trust Work Together?

In order to successfully implement a Zero Trust model for the data in the modern enterprise, which is spread across SaaS, IaaS, and PaaS and hosted and on-premises environments, the SASE architecture must satisfy several requirements.

Because the Zero Trust model is enabled around data controls and visibility into corporate resources the two main components that provide this capability are the Cloud Access Security Broker (CASB) solution, which is used to access SaaS resources, and the Zero Trust Network Access solution (ZTNA), which is used to access IaaS/PaaS and hosted/on-premises resources.

These two solutions should allow you to control users' activities based on user context, device context, health, location, and other data. However, this is harder than it sounds. Most of the VPN and remote access solutions today are still focusing on network access, providing a true/false verdict on a full network access request (VPN connect event) by a user.

Restricting access to specific resources based on user and device risk, status, and role is not the only requirement; the visibility into the user's actions and the data being accessed is also critical to a successful implementation of a Zero Trust model.

To enable the implementation of the Zero Trust model, both CASB and ZTNA solutions must have the ability to provide Layer7 (application layer) visibility, allowing the control of user's actions (uploading, downloading, modifying content, and so on), providing integration with DLP (as the data is visible to these solutions), and giving full visibility into users' actions for detection, forensics, and compliance.

These solutions should also be able to integrate with your existing IAM investments, such as your directory services (Azure AD or Okta) and MFA, and they should be able to provide built-in capabilities such as user entity behavior analytics (UEBA,) sandboxing, and anti-malware features.

What is Zero Trust?

Zero Trust is a term that was coined in 2010. This term refers to an approach where nothing, including the corporate network, users, or devices, should be trusted. The Zero Trust model assumes that each of these entities could be breached and used to steal sensitive data.

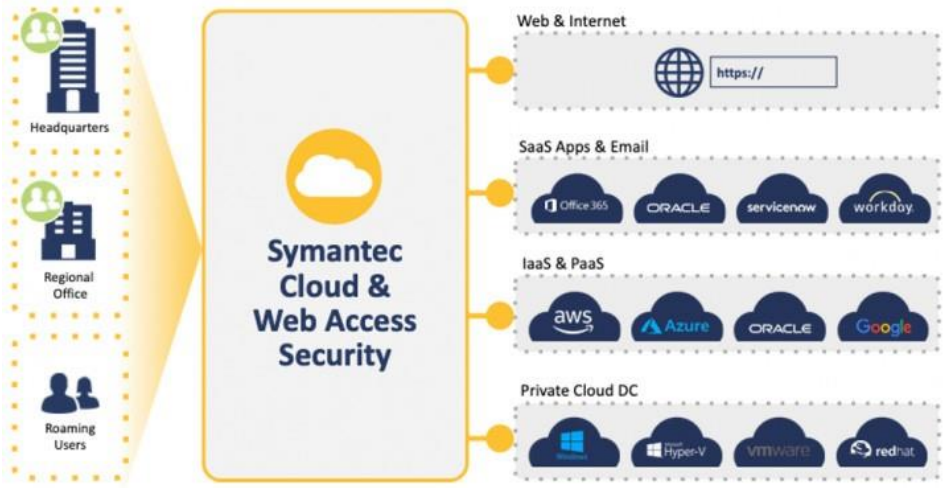
The Zero Trust model puts the data at its center and references multiple controls, which are involved in determining whether a specific entity should be allowed access to a specific resource or data. These controls also allow visibility into the users' activities to enable detection and should provide behavior analytics to determine the risk the user poses to the resources and data. In other words, the data that the controls provide helps to determine the risk that an account has been compromised. These controls focus on the identity of the client (user or service), the device, and the data (workload or network). For example, the following set of controls are common to the Zero Trust model:

- Risk score of the user
- Authentication method (FIDO, MFA, and so on)
- Organizational role
- Device risk and status (managed as compared to unmanaged)
- Location
- Data context (confidential, PII, PCI, and so on)

How Does Symantec Support SASE and Zero Trust?

Symantec offers CloudSOC, a market leading CASB solution enabling secure access to SaaS resources and Secure Access Cloud, an innovative ZTNA solution. These solutions enable secure access to on-premise, hosted, and IaaS-based or PaaS-based resources

Both solutions provide the ability to enforce access and activity controls based on the context of the user and the device, built-in integration with Symantec DLP, and the ability to integrate with all leading directory service and IDaaS solutions. These two solutions, combined together, provide Layer7 secured connectivity to corporate resources anywhere, while enabling the controls and the visibility required by the Zero Trust model. With the addition of the Secure Web Gateway solution, Symantec offers a comprehensive SASE platform, while helping you to drive the implementation of a Zero Trust model in your organization.



What Next?

As enterprise organizations shift to a modern architecture centered around cloud and mobile, they require a modern security architecture to securely leverage their new investments.

The SASE architecture is becoming the modern architecture of choice for many enterprise business, because it allows both security and connectivity. In turn, the Zero Trust model is the security model of choice, one that should be supported and implemented by the controls available in the SASE architecture. Therefore, it is critical to evaluate the capabilities of the vendors of your SASE architecture for their ability to implement a Zero Trust model. SASE and Zero Trust are *not* mutually exclusive. On the contrary, they are complimentary to each other; and one should be used to enable and drive the other.

For more information, please visit out site at
broadcom.com/products/cyber-security

Symantec
A Division of Broadcom

Braxton-Grant TECHNOLOGIES

For product information and a complete list of distributors, visit our website at: broadcom.com

SED-SASE-Zero-SB100 June 22, 2020

For more information, visit www.braxtongrant.com or contact us at 443-545-2052.
Braxton-Grant Technologies, Inc.
1340 Charwood Road Suite I
Hanover, MD 21076