Solution Brief

Symantec
A Division of Broadcom

Data Loss Prevention:

Essential Building Block for the Secure Access Service Edge

Challenge

Have you ever wonderered why phishing and all its variants never go out of style? To a bad actor, an end user who is comprimised by phishing is worth their weight in gold, opening the door to troves of personally identifiable information (PII) and intellectual property (IP). That is why data loss prevention (DLP) is an essential weapon in the defensive arsenal of cyber security.

Opportunity

The prevention of end-user data loss is undergoing profound change. The prevalence of mobile users, and the increasing reliance on cloud-based services, has rendered traditional cyber security strategies obsolete.

Formerly, if the network perimeter was protected, the interior was presumed to be safe. No more. It is not possible to trust an end-user once he or she has gained access to the corporate network. In our opinion, to address this new reality now and in the future, you need to leverage Secure Access Service Edge (SASE). SASE is a cloud-delivered cyber-security architecture developed by Gartner.

Users and data are everywhere. You need data loss prevention to be everywhere, too.

The SASE Approach to Data Loss Prevention

At Symantec, we are pursuing a data-centric approach to cloud security that leverages SASE to take data loss prevention everywhere that users, devices, applications, and data live.

By converging DLP with our cloud and web security services, such as Secure Web Gateway (SWG), Cloud Access Security Broker (CASB), and Zero Trust Network Access (ZTNA), we can intelligently inspect content at the secure access service edge without backhauling traffic bound for SaaS, IaaS, or the internet, to a centralized data center.

One of the benefits of this approach is that it allows security teams to readily detect sensitive data movement and consistently and logically apply data protection policies closer to the resources being accessed, while eliminating unnecessary latency.

This approach also allows them to quickly remediate exposed data, at the point that it was created or used, through inline and API-based controls.

A SASE security provider should effectively identify and classify sensitive data in encrypted traffic streams, apply a consistent set of policies to data at rest and data in motion across cloud and web services, and deliver a single-pass content inspection architecture from the cloud.

SASE addresses the limitations of legacy security architectures that are fragmented between on-premises and cloud resources, and shifts security controls to wherever the users, devices, applications, and data are located.

How Do Get There From Here?

SASE is poised to transform security, and warrants consideration by enterprises, because it can enable security teams to support the needs of digital business transformation and mobile workforces.

By adopting SASE, you can build on many of your existing security investments, such as DLP, Cloud Access Security Broker, and Secure Web Gateway.

Benefits

SASE addresses the shortfalls of traditional hub-and-spoke architectures by moving traffic inspection and policy enforcement to where modern users, applications, and data reside: outside of the enterprise.

By applying SASE principles, organizations can address data loss by identifying sensitive data across any connection, regardless of where the user or the user's device is located, what the user is accessing, and where the resource being accessed is located. In other words, security goes to the traffic rather than traffic going to the security.

How Do Get There From Here? (cont.)

Gartner recommends that organizations, "avoid SASE offerings that are stitched together," and "evaluate the integration of the services to be orchestrated as a single experience from a single console, with a single method for setting policy."

With that goal in mind, Symantec offers the core technologies needed to enable SASE:

- **Data Loss Prevention (DLP)**
  DLP monitors sensitive data movement across an organization and prevents accidental or malicious exfiltration of data in motion, data at rest, and data in use.
- **Cloud Access Security Broker (CASB)**
  CASB is a policy enforcement point that sits between cloud consumers and cloud service providers, applying security policies as cloud resources and data are accessed.
- **Zero Trust Network Access (ZTNA)**
  ZTNA, also known as a software-defined perimeter, limits access and grants least privilege rights to users for both cloud resources and on-premises resources through a trust broker.
- **Secure Web Gateway (SWG)**
  SWG inspects web traffic flowing from remote users to the internet, and enforces network security policies to filter malicious websites and content.
- **User and Entity Behavior Analytics (UEBA)**
  UEBA monitors behavior during sessions and identifies anomalies and excessive risk.

When you integrate these technologies so that they complement each other under the SASE umbrella, you gain a firm foundation for your organization's cyber-security now and in the years ahead.

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

Symantec
A Division of Broadcom

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

SED-DLP_EssBB_SB100_0622 June 22, 2020