SecureCircle Data Access Security Broker (DASB) concepts and benefits

DASB: What is a Data Access Security Broker?

Is data protected while it is held within the perimeter of a firewall? The answer to this question has historically been "Yes". While for a time this was true, with the Cloud, SaaS, & BYOD, your data has escaped or never resided in the perimeter, leaving sensitive data vulnerable. A new approach to protect data is required for organizations to control their data and map to modern compliance requirements.

Applications running on endpoints or in the cloud require access to data and this access has been controlled by the storage systems where the data resides. Endpoint applications are either on a local or remote file system (i.e., NTFS, AFS, SMB, NFS) and cloud applications like Spark or Tableau, are on cloud file systems (i.e., S3 Bucket, HDFS). In any situation, if access is granted and the data is moved off of the storage system, control over that data is lost forever. Data can be encrypted on the storage system, but applications must be modified to manage encryption keys and decrypt the data, contrary to what applications are designed to do, access data. When a key is issued, the control over access is lost and the data can be accessed by any person or any process that has the key.

SecureCircle's Data Access Security Broker (DASB) moves access control policies from the storage system of the data to the data itself – from device-centric to data-centric. This access control works with local and remote storage systems, as well as cloud file systems, without requiring any change to applications. Access is granted to applications without losing control, and this access control persists no matter where the data is moved. Data can

DASB Eliminates
• Data Breaches

DASB Never
• Compromises Control
• Impacts end-users
• Changes business workflows or applications

DASB Supports
• Any Application
• Any File Type
• Any Device

Control that is never compromised while enabling access.

Protection that follows your data no matter where it is created, consumed, stored, or modified.

Audit of every action that happens to data; everything is an auditable event.

be migrated from on-premise to cloud or from cloud-to-cloud and remains protected in all states: at rest, in transit, during migration, at the new storage location, and even in-use. If data is moved, applications only need new paths or endpoint URLs, and can continue to read and write data as if nothing else has changed. This is because the access control follows and protects the data and doesn't affect the application.

SecureCircle's DASB works by inserting a transparent layer between the read and write processes of applications and their storage systems. For cloud storage systems, the broker is implemented using Cloud Functions in AWS, Azure, or GCP. These functions are managed services that dynamically scale with the workload accessing the data. Access to the storage systems through the DASB is identical to that of the storage system. If data protected by SecureCircle is accessed by an authorized user, device or process, the access control policy will allow the user, device, or process to read decrypted bytes. If data protected by SecureCircle is accessed by an unauthorized user, device or process, the access control policy will not allow the user, device, or process to read decrypted bytes, only encrypted bytes get accessed.

As the data breaches to enterprises occur at a rapidly increasing clip, it is obvious that the most asset within these enterprises is their data. In addition to legacy client-server systems, potentially sensitive data is now used and generated everywhere. Data powers your embedded applications, smartphones, cars, web browsers, refrigerators, HVAC systems. The infrastructure of these platforms consist of cloud services. These cloud services are powered by your data flowing in and out of them. SecureCircle's DASB is the only solution that will empower you to enable secure access, without giving up control to your data with no impact to applications, workflows, or end user experience.

SecureCircle is the first Cloud-Delivered Data Access Security Broker

Let's chat about how SecureCircle can help map your compliance requirements. Call or email us now. 408-827-9100 info@securecircle.com

About SecureCircle

SecureCircle's Data Access Security Broker (DASB) eliminates data breaches and mitigates insider threats, with no impact to the end-user experience and no modifications to applications and workflows. Data is always protected at rest, in-transit, and in-use; no matter where it is created, consumed, stored, modified, or shared. Headquartered in Silicon Valley, SecureCircle delivers the world's first data-centric protection for a zero-trust world.

SecureCircle®

SecureCircle.com
4701 Patrick Henry Drive
Building 19, Suite B,
Santa Clara, CA 95054
408-827-9100