SecureCircle®

DATA SHEET

DASB

Microsoft Office365

Data Access Security Broker

SecureCircle Presents the New Model of Data Protection

SecureCircle eliminates data breaches and mitigates insider threats. SecureCircle's enables organizations to protect all or a subset of your data, allowing your organization to ensure the security, visibility, and control of unstructured data from internal and external threats, regardless of format or storage location.

We are confident in making this bold statement because we have proved it within organizations, ranging from banking and legal to semi-conductor and SaaS, across the globe—allowing these companies to adequately secure data in today's cloud-first, zero-trust or other environments.
This new model of data protection is SecureCircle's Data Access Security Broker (DASB), which uses the concept of a Circle to define access rights.

- A Circle is a grouping of users, devices, and data.
- Devices and users can belong to as many Circles as needed.
- Data belongs to a specific Circle.
- Only authorized users and devices can access data within the Circle.
- Users or devices that do not belong to the Circle cannot access data within the Circle.
- DASB ensures data remains protected at rest, in transit, and in use without alteration to the data or its storage location.

Unlike existing technologies, DASB acts as a transparent layer between the read and write processes of applications and their storage systems.

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. Grant applications access without losing control. Access control persists no matter where the data moves.

Data can 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. As data moves, applications only need new paths or endpoint URLs to read and write data as if nothing changed. The access control follows and protects the data and doesn't affect the application

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.

Secure data in Office365 environments

Office 365 can provide centralized management of content in the cloud, but it can't protect documents which locally saved, such as preventing unauthorized access or re-distribution of files. SecureCircle's DASB extends the centralized access protection to the data regardless of its location. Data-centric protection enables security to follow the file.

Content-based MagicDerivative™

DASB protects more than the file; DASB protects the content of the file, the actual data. DASB's patented similarity detection engine understands the digital DNA (dDNA) of a protected file. dDNA found in another file is automatically protected. Protection follows the content even with SaveAs , Copy-n-paste, or manual reconstruction of the data. Adjust the sensitivity of the MagicDerivative at any time to determine your threshold for automatic protection.

The content-based MagicDerivative™ provides complete protection to the content inside your files, whenever authorized users access the data in your Office 365 environment. Office365 users work with files protected with SecureCircle's DASB the same way files are stored and shared today.

- Files are always protected. Persistent protection encrypts files at rest, in transit, and in-use.
- Transfer and store protected files via existing tools such as email, USB, and cloud such as OneDrive and SharePoint Online.
- Users open and edit files using the same applications. File names or extensions are never changed.
- Any file type can be protected.
- Access control by user, device, application, and network location.

Administrators manage SecureCircle centrally.

- SecureCircle integrates with Active Directory. Manage access rights using the same user groups that already exist
- Only applications in the SecureCircle's Allowed List have access to the contents of the file. Applications not in the Allowed List can only move the file.
- Management is real-time, and permissions are revocable at any time.
- Set off-line access rules.
- Output detailed geolocation enabled logs with IP address, application, success/failure, time of access, and much more to Security Incident and Event Management (SIEM) for real-time monitoring and compliance reporting.

To Learn More

Contact your DASB expert at sales@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