SecureCircle®

DATA SHEET

Data Access Security Broker

MOVE BEYOND DLP'S FAILURES

DLP (Data Loss Prevention) solutions haven't stopped data breach growth. IBM reports the average total cost of a data breach reached $3.86 million USD in 2020. DLP solutions only block or encrypt data that tries to leave the endpoint. Hackers have used malware and ransomware like the Palmerworm to take advantage of the lack of security. Data security should focus on persistently securing data wherever it goes. Data should be secured regardless of location. Which means data must be secured by default.

Another large security gap for DLP is internal users will find ways to work around any security solution that impacts their ability to work effectively. Workarounds are possible because DLP requires an extensive library of rules and policies which need to be continuously updated. Security administrators play whack a mole with new applications, SaaS vendors, and more.

SecureCircle's Data Access Security Broker (DASB) addresses DLP's faults. Data is securedwithout impact to users and workflows while securing data by default. SecureCircle is transparent to users and workflows. Users continue to use the same applications without any knowledge an additional security layer is active. There is no change in file names or extensions, and SecureCircle has no limit to file size. Because of the transparent nature of security, SecureCircle can secure all data by default.

SecureCircle is transparent to users and workflows. Users continue to use the same applications without any knowledge an additional security layer is active. There is no change in file names or extensions, and SecureCircle has no limit to file size. Because of the transparent nature of security, SecureCircle can secure all data by default.

SecureCircle corrects the failures of DLP

- DASB doesn't require extra discovery or classification tools.
- Users are entirely unaware security is in place since there is no change to user workflow.
- DASB's secure by default posture allows aminds to focus on exception policies only.
- SecureCircle's security continues regardless of data location.

DLP Pain Points:

Discovery & Classification

- DLP requires additional tools, such as Discovery and Classification, to work. Relying on other products increases cost and complexity.

Operations

Operatoinal success can be measured by the amount of friction introduced into the work environment on users and administrators.

- Because DLP is so complicated, companies often hire DLP deployment consultants to configure the DLP to work correctly. The Symantec DLP version 15.5 Administration Guide is 2560 pages.
- Companies never operationalize DLP within a company because DLP requires so much maintenance. Admins must continuously create and update new rules to cover policy changes, additional applications, additional cloud/SaaS applications, etc.
- Companies either continue paying their DLP consultant to maintain their solution, or the effectiveness of DLP begins to degrade.

Failed Architecture and Technology

- DLP doesn't secure data on the endpoint. Instead, DLP tries to limit data egress from the endpoint. By doing this, users are blocked from everyday tasks such as copying data to the USB drive. For files and workflows that can't be emailed due to size, portable drives and cloud storage may be the only option to transfer large files and data sets DLP security coverage is limited to a small set of business applications and file formats.
- DLP requires users to be an active participant in the security process. Users do not have an interest in doing this. They will secure the least amount of data because it makes their work easier. Also, even diligent employees will make mistakes.
- DLP is based solely on regex pattern matching, which is very fragile. Creating lots of data escapes.
- Specific vendors such as Symantec have limited cross-platform support.

Many companies adopt Zero Trust security frameworks, but these companies use DLP solutions that can never be called Zero Trust. Zero Trust DLP solutions must secure the data by default. That is not how legacy DLP works.

SecureCircle's Zero Trust DLP for Endpoints

SecureCircle introduced Data Access Security Broker (DASB) to bring Zero Trust DLP for endpoints to the market. DASB does not require extra discovery or classification tools. Besides regex and manual classification, SecureCircle can automatically secure data based on location, such as a file server, a folder, specific SaaS applications, and URLs. SecureCircle removes users from the security workflow. Users are entirely unaware security is in place since there is no change to user workflow.

Instead of managing every possible workflow with DLP, DASB's secure by default posture allows admins to focus on exception policies only. Policies only need to be created for egress rules to release data from protection. One example could be when a user uploads files to specific SaaS applications or cloud storage. In this case, the SaaS application takes over securing the data during transfer to the cloud.

For companies that utilize a centralized identity platform, SecureCircle integrates, so admins do not manage extra authentication. Typically, Active Directory groups map directly to SecureCircle policies.

Market Update

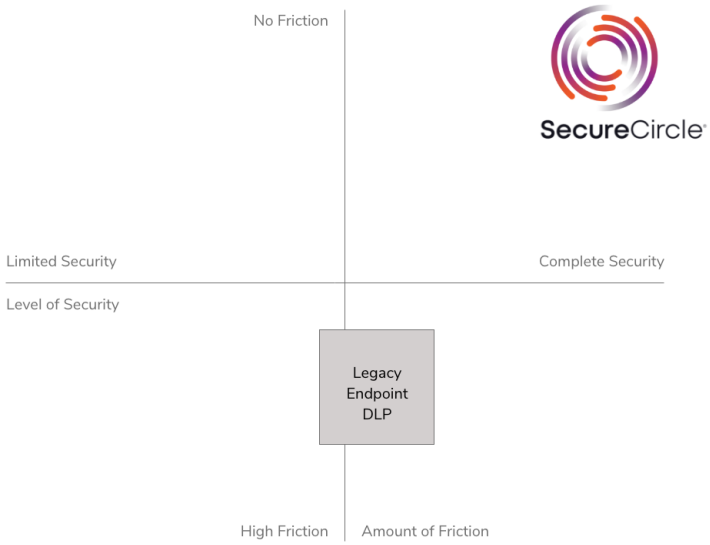
Market Analysts predict the DLP software market to continue to grow at 23.59% CAGR between 2020 and 2025. At the same time, IBM reports the average total cose of a data breach reached $3.86 million in 2020.

DLP is the right solution, but why aren't data breaches getting smaller and less often.

With SecureCircle, users are unaware of additional security unless they attempt to access data without proper permission. Users can work with any application and file type allowing DASB to secure data in complex use cases such as securing source code and media creation. SecureCircle creates a solution for securing data from accidental and malicious insiders as well as external threats.

Unlike DLP, which only tries to secure or block data transfer when data leaves the endpoint, SecureCircle continues to secure data regardless of location. If a user sends an email with a secured attachment, the recipient will receive the secured file. If the recipient is authorized, they can access the data within the file. Unauthorized users will not be able to access the secured contents. SecureCircle supports endpoints using Windows, Mac, Linux, iOS, and Android.

Security versus Friction



Endpoint DLP

High Friction: Admins need to create and maintain a massive list of DLP rules. Admins cannot keep up with changes in the network, endpoint applications, etc. so over time, more and more holes are introduced. DLP asks users to be part of the classification process. Users are also limited to the applications and file types that can be used.

Moderate Security: The fundamental security model is flawed since data is not secured by default. Security is only applied when data attempts to egress from the device. Ransomware and malware take advantage of this because once the malicious application is running on the device, the application can try many methods to get data off the device.

Data Access Security Broker - Zero Trust Endpoint DLP

No friction: DASB is completely transparent to users. Users continue with the same workflow as before. Admins integrate with existing authentication solutions and manage exception policies only. Exception policies do not change often.

Complete Security: Data is secured by default, including at rest, in transit, and even in use. When secured data is transfered off the device, the data remains encrypted and only authorized users will be able to access the content. This allows for use of cloud storage and file sync and share to be used as secure transport methods.

Legacy DLP vs. Zero Trust DLP for Endpoints Comparison

	Legacy DLP[1]	SecureCircle DASB Zero Trust DLP for Endpoints
Types of Files Protected	Supports specific application and file formats only. Three hundred file types supported. Scripting language available to help support applications not supported by default.	Support for all applications and file formats without any customization or modification. No limit to file size. Files are never renamed, and extensions remain the same.
Time to Value	Months & Years	Hours & Days
End-User Experience	Obtrusive	Transparent
Operational Overhead	Dedicated resources and laborious training	Minimal time and training
Technology Dependancies	Discovery & Classification	None
Management Mode	Users Opt-In to security	Users Opt-Out of security to remove data from protection
Policy Management	Endless, extensive rule management required	Simples ingress and egress rules to set and forget
Data Alwa Encrypted on Endpoint	No	Yes
Perimeter less control (control of secured data beyond the endpoint)	Manage by edge/perimeter	Yes, full control regardless of data location
Always Trackable	No	Yes
Real-time Monitoring, Reports, Audits	No. Only monitoring for data egress policies	Yes. Output detailed geolocation enabled logs with IP address, application, success/failure, time of access, releasing security, file system events, and much more to a SIEM for real-time monitoring and compliance reporting.

What data can we help you secure?

At SecureCircle, our goal is to deliver truly frictionless security for our customers' most valuable data. We focus on securing data persistently and transparently to deliver business value for our customers. We are always looking for ways to help improve our customers' data security.

References: IBM Cost of Data Breach: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

[1] Based on Symantec DLP 15.5 Administration Guide

SecureCircle.com

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