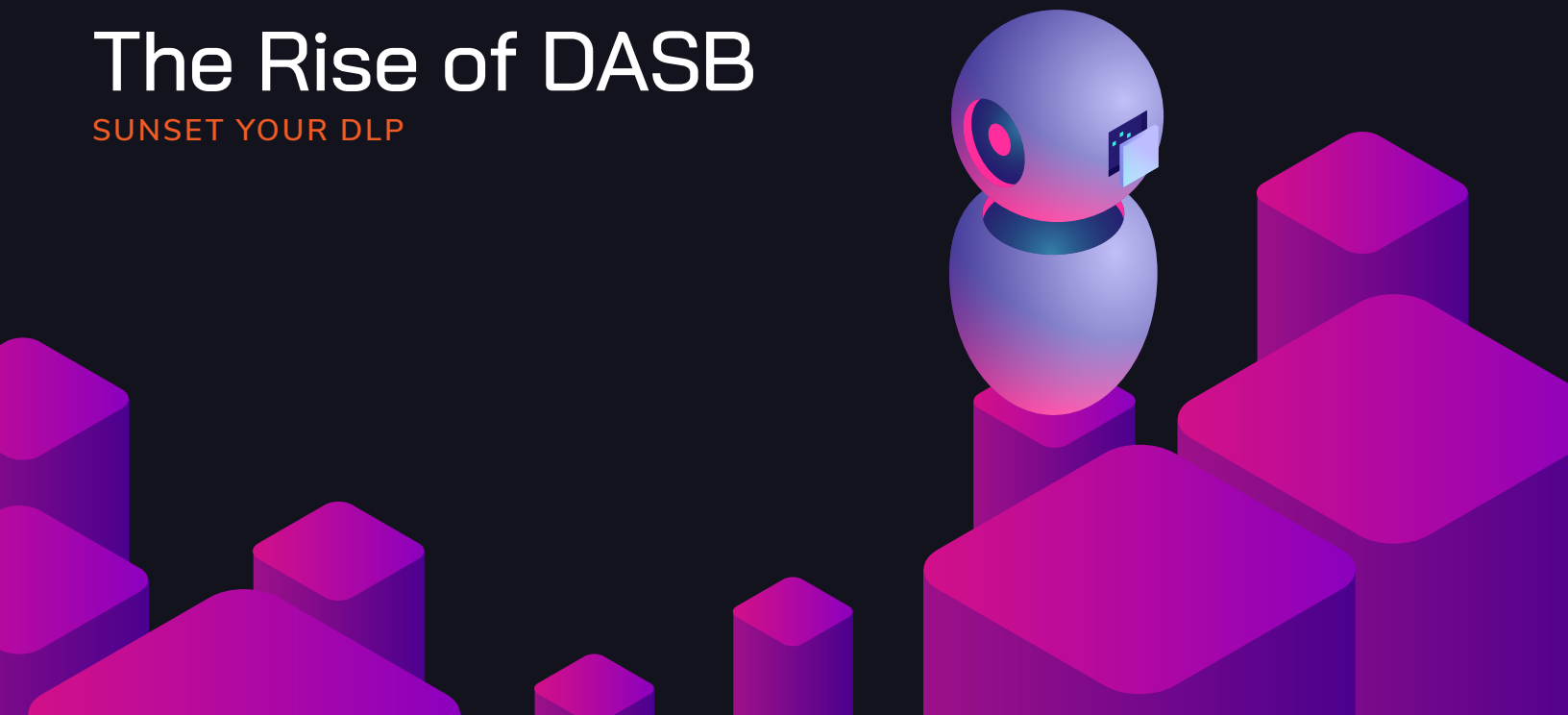
WHITE PAPER

SecureCircle®

The Rise of DASB

SUNSET YOUR DLP



Data loss prevention (DLP), the antiquated data protection model, takes a 'manage by rule' approach where all data flows freely unless the security team has written a rule to specifically protect the data. Rules come in many forms – discovery and classification rules that determine what data is sensitive, rules that dictate what applications, versions and file types can be used based on DLP limitations, and rules that determine what end-users can do with the data (copy, share, etc.). Unfortunately, there is tremendous effort for security teams to devise all the rules that apply, now and in the future, and align with business units before and during implementation, and ongoing. Managing by rules is also a tremendous burden on employee productivity as more and more restrictions are imposed on their daily workflows. And despite all this effort,, DLP is still highly error prone. Enterprises, even after investing considerable dollars, time and effort trying to implement and operationalize DLP, still are victim to data breaches.

SecureCircle's data access security broker (DASB) flips the 'manage by rule' approach on its head and 'manages by exception'. Instead of investing effort building a dubious set of rules that identify data and attempt to protect every potential threat vector, DASB takes an expansive approach. This is possible because DASB is completely transparent to the end-user, there is no need to modify any application and DASB does not impose any workflow restrictions. As a result, any data can be protected, without having to manually discover, classify or ask end-users to label the data. With this approach, DASB bypasses the limits of DLP.

In this article, we examine the differences between the traditional data protection technology stack centered on DLP, and contrast it with SecureCircle's DASB, highlighting use cases derived from recent real-world breaches.

The Unfortunate Case of DLP

By default, DLP allows a file to flow freely, unless it has been specifically identified as sensitive and a rule exists to block what the user is doing to/with that file.

Some types of sensitive information can be programmatically detected such as credit cards and social security numbers that follow a predictable structure, however this is highly error prone. First, the security team must invest a lot of time in developing static pattern matching rules. Information like credit cards can take many different forms in practice, so even writing dozens of detection rules still may not catch them all, and block lots of unwanted information in the process. For example, DLP might encounter this telephone number (819661820893) and identify it as a credit card number, a false positive. An outgoing email attachment with this telephone number might be blocked causing a slowdown in the business where none is warranted. This interference with normal business operations is one of many major downsides of DLP. The more aggressively the security team adds and updates rules to regulate sensitive data, applications and user actions, the more often false positives occur, resulting in employee backlash. Employees complain and attempt to circumvent the DLP tools altogether.

DLP also fails to detect sensitive information that has been slightly altered, allowing it to pass freely, a false negative. For credit cards, classic exfiltration bypass is to spell out the credit card number ("eight one nine six..."), change the credit card number to Wingdings font, or re-write it as Roman numerals. It is easy to think up ways to get past DLP's pattern matching.

Credit card numbers and SSNs aside, the vast majority of valuable IP and personal data do not have obvious markers that a machine can automatically detect (source code, trade secrets, internal designs, M&A activity, health information, the list goes on). The result is that DLP ends up focusing on the smallest, most obvious subset of sensitive information like credit card numbers, while reams of truly sensitive data is left entirely unprotected.

To make matters worse, the implementation of DLP is laborious, lengthy, and highly restrictive. DLP forces the business to require specific applications, versions and specific file types based on DLP limitations, for example, a specific version of Microsoft Office, Adobe, or a specific engineering application. However, if the supported version of the application is discovered to have a security vulnerability, it can't be upgraded or downgraded to a secure version until the DLP environment is updated to work with that new version. Well-intentioned employees and partners are thus penalized having to work with DLP, meanwhile malicious actors still easily bypass DLP's attempts at protection. Depending on the DLP vendor and what rules have been set, a user who has read access to a file might simply breach the data by converting it to a different file type, saving as a different file name, copy/pasting the data, or taking a screenshot of the data. With DLP, security teams need to think through every exfiltration pathway and explicitly build a rule for each one – this requires a tremendous amount of manual time and effort and is extremely error prone.

As a result, security teams are simultaneously criticized from the executive suite and the business for not protecting data effectively and under pressure from the executive suite and the business to get out of the way of usability and productivity. Fed up organizations resort to setting DLP to "monitoring mode", silently logging accesses and shares of data, however not making any attempt to stop breaches. At this point, all sensitive and personal data is unprotected and flows freely inside and outside of the organization. There is no application control/process restriction. Data is fully vulnerable to malware, breaches, and bypasses logs.

In recent years, companies have explored alternative ways of detecting sensitive information, such as asking employees to manually classify their data. This can take the form of every employee in the company filling out a small form every time they send an e-mail or save a file, a major investment in time. However, your colleagues are not security professionals, and their incentive is to get their work done, so the accuracy of their classification is in doubt. Since insiders are known to be the largest threat vector, giving employees the power to classify whether data is sensitive or not is handing insiders the keys to the kingdom. In practice, classification ends up being a crutch to enable the most obvious DLP scenarios, and usually only on newly created data, while years of valuable data already housed in the enterprise remain unclassified and therefore unprotected and unaudited. A more recent trend attempts to apply machine learning to detect sensitive data, requiring a huge investment in training the algorithms, with a lot of hype, however little measurable gain has been reported to date.

Given the amount of effort required of the security team to devise rules that detect sensitive data, and the overhead incurred by employees classifying their own data, using only prescribed applications and file types, the DLP approach ends up being opt-in to the least amount of data to be protected as possible. This is the old paradigm, this is DLP.

DASB – A New Data Protection Paradigm

DLP's protect by rule approach imposes limits at every turn – limits on what data can be protected, limits on file types, unwanted limits on application types and versions, limits on workflows. DASB's 'manage by exception'allows for a limitless approach where any data can be protected transparently, with no obstacles to protection or productivity. A truly Zero-Trust data protection program.

Limitless data protection - contrary to DLP's reductive approach of opting in to only the smallest subset of data to protect, DASB takes an expansive approach to data protection. We recognize that most, if not all, enterprise data contains sensitive or valuable information and this data should not be allowed to leak. DASB achieves persistent protection, delivering it completely transparently to end users. DASB protects any and all data without impact to the end-user experience.

DASB is based on a patented portable, virtual, encrypting file system that inserts a transparent layer between the read and write processes of applications and their storage systems. Access to the storage systems through DASB is identical to how the data is accessed today. If data protected by DASB is accessed by an authorized user, device or process, the access control policy will allow the process, device, user to read decrypted bytes. If protected data is accessed by an unauthorized user, device or process, the access control policy will not serve the process, device, user decrypted bytes, only encrypted bytes get accessed. As a result, users are not even aware of DASB's existence, unless they attempt to access data they should not be accessing.

Limitless productivity – DASB's transparency allows it to expansively protect all data. DASB imposes no limits on applications, versions, file types, file sizes, repositories, developer tools, workflows, or anything else in the environment, no matter how complex or enterprise-specific.

DASB can be implemented enterprise-wide, or with a phased approach, selecting the most important use cases first (source code, CRM, trade secrets, finance, PCI/PHI, etc.) and protecting all data related to those use cases. For data that is permitted to be shared externally, such as marketing material or sales quotes, role-based permissions allow users to securely collaborate with external stakeholders without giving up any control, protection, visibility or accountability.

Limitless control – with DLP, control is only persistent if the DLP rules have been configured to exactly the specific application, version, file type and migration path (copy/paste, file copy, cloud-to-cloud, etc.). These scenarios are almost impossible to configure in the required depth and nuance, resulting in workflow interruptions more than actual data protection. DASB moves access control policies from the storage system of the data to the data itself – from device-centric to data-centric. No matter where data is created, consumed, modified and stored, it is persistently protected by DASB. 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. This is because the protection and access control follow the data and any and every action that touches the data.

Let's look at four core data protection capabilities of DASB that make this limitless protection possible. These can be used individually, or in combination, to protect against data exfiltration, whether inadvertent or intentional.

MagicFolder™

With DASB, users or administrators can target a location to protect with MagicFolder. Any data within a magic folder is automatically and immediately protected. This includes all subfolders and directories. Any filesystem can be a magic folder – a user's desktop, documents folder, even C:\. File servers and everything within them can be magic folders. Even an Amazon S3 bucket, commonly involved in data breaches, is simply a cloud file system that can be protected automatically, as is any Azure Blob storage, Google cloud storage bucket , etc.

From there, any data that already exists in the folder, or is downloaded, dragged, copied, created, etc. in the folder is protected instantly and automatically.

Following the DASB paradigm with the ability to protect everything, most enterprises protect entire filesystems and storage repositories, opting out of protection for the very small subset of specific data that needs to be managed by an exception.

In the real world: The issue of S3 bucket security has come to a head in recent years with prominent data breaches affecting companies like Capital One, Uber, Accenture and the United States Department of Defense. These breaches keep happening for the same reasons, again and again. S3 buckets are convenient for collaboration, however are often misconfigured, leaving their contents open to the public. Victims of these high-profile breaches had DLP, yet no DLP rule successfully blocked the exfiltration pathway. Even worse, in several instances, the data had never been discovered and the enterprise only became aware when the breach was disclosed. In contrast, DASB would protect sensitive data automatically before it even reached S3, preventing the breach altogether.

Another real-world use case is protecting data generated by legacy client/server web applications. Legacy client/server web applications are notorious for having outdated data protection capabilities, yet enterprises often have entire lines of business built around them. Imagine a legacy CAD editor that produces an enterprise's key industrial designs, however the editor is no longer supported by the vendor. Or a home-grown content authoring tool that no longer has an in-house development team. These legacy applications are so entrenched in business workflows that changing to another application for security reasons is unrealistic. With DASB, MagicFolder protects the legacy web application's data folder, with the web application as the only process allowed to access that folder. This enables the encryption of data output by the legacy application, with zero change to the application, and no impact to any existing integrations or workflows.

MagicProcess™

With DASB, administrators can also specify a "magic process" from which any data that comes out of the process is protected or unprotected. This could be a web browser, Microsoft Word, Outlook, Adobe Acrobat – any process at all. Following the DASB paradigm with the ability to protect everything, enterprises set all processes to be protected by default. DASB also allows for protecting only certain processes to support specific protection use cases, for example making only the HR or accounting application a magic process.

In the real world: Source code has become one of the most valuable forms of intellectual property. However, we've seen numerous technology giants, including AWS, Tesla, Waymo, breached due to a single employee exfiltrating hundreds of thousands of lines of source code. Historically, source code protection was limited to when it was stored in a repository, however as soon as a developer takes code from the repository, DLP and other traditional tools are not configured to protect the source code or may fail to identify it altogether. Now with DASB, this breach is not possible as the tools to access the repository are made a 'magic process' and upon checkout of any source code, through any approved process, the source code is automatically and transparently protected.

Source code is a poignant example, however the use cases for magic process are far reaching, including the malicious employee who logs in to the company CRM and downloads all of the company's contacts or pipeline to a CSV file, or the external threat who compromises an internal account and attempts to download personal and financial data from the ERP. In all of these cases, DASB prevents the data breach.

MagicClipboard™

With DASB, enterprises control how data in the clipboard can be pasted. Users might be allowed to copy and paste from protected processes to other protected processes, or certain data can be copied from an unprotected source to a protected source under certain conditions, depending on the policy that is set.

In the real world: a too-often overlooked source of leaks is copy/paste of sensitive data to collaboration applications like Slack, Skype, or simply e-mail. This has led to headlines such as Beware! Slack leaks are the new email leaks[1] documenting the impact to The New York Times, Breitbart and Reddit through the "laughably simple means of copying and pasting internal conversations". Magic Clipboard protects against these leaks, where traditional technologies typically are not able to protect this increasingly common threat vector.

MagicDerivative™

No matter how careful a company plans and targets its data protection policies, some data is sure to be missed, either now or in the future. This is where DASB's MagicDerivative has your back. Whenever unprotected data is accessed, DASB's patented similarity detection engine understands the DNA of the data (dDNA) and looks for a match to dDNA that is already protected. If there is a match, MagicDerivative applies protection to this data automatically, with the same access policies as the originally protected data. This means that even if you did not ' discover' the sensitive data, or your colleagues create or import new sensitive data down the road, DASB will automatically recognize that data as sensitive and protect it.

In the real world: Large enterprises can have tens of thousands of servers or more, too many of which are unknown or contain unknown data. And we have all seen the infographics that show how fast 'new' data is being created. What of this data is sensitive and needs to be protected? What is relevant? And what is legacy and can be discarded? The market for data discovery tools is very active, yet the only thing those tools can do is minimally provide clues as to what data exists within a company's walls. However, MagicDerivative works with all data, even "unknown" data that has not been discovered or classified. MagicDerivative encounters company data as it's being accessed (when it's most vulnerable), and protects it automatically, whether the security team is aware of that data or not. Over time it spreads like a "benevolent virus", protecting all data with the correct policies, according to its dDNA.

MagicDerivative even works with non-text data such as images. If a user copy/pastes your protected photo into a PowerPoint file, the PowerPoint is recognized as having the same dDNA as the image and is automatically protected with the same access controls.

Putting It All Together

Breaches are happening at extraordinary rates, making it a matter of when, not if, your data will be exploited. 'Managing by rule' has proven to be ineffective and modern businesses demand a paradigm shifting approach to data protection.

With SecureCircle's Data Access Security Broker, data breaches are eliminated. End-users are none the wiser and business does not need to contort to the limitations of DLP.

To Learn More

Contact a DASB expert at info@securecircle.com

[1] (https://mashable.com/2018/02/16/slack-leaks-new-email-leaks/)

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