SecureCircle®

WHITE PAPER

Zero Trust Data Protection

ON ENDPOINTS

SECURECIRCLE.COM

SecureCircle®

Zero Trust Data Protection

ON ENDPOINTS

Contents

Introduction

Modern cloud services and web-hosted applications have matured over time and have implemented elevated in-cloud security controls to meet the security concerns of enterprises. However, the modern security controls provided by cloud applications and services stop short of protecting data as it leaves its online location and moves to end user devices, which is where many enterprises tell us their data is most at risk.

SecureCircle takes a unique approach to helping enterprises deliver cloud data security by persistently encrypting the data as it leaves the cloud service and moves to end user systems without any limitations on applications. Using SecureCircle, enterprises retain control of this data without impacting user experience or productivity and extend the protection of the cloud data beyond the limits of services onto end user systems.

As enterprises invest heavily in cloud infrastructure and web hosted applications, the requirements for data security become increasingly challenging to manage. For many enterprises the focus on securing networks and server infrastructure has lost relevance when the most valuable data is hosted in a variety of public cloud services, web applications, and online storage repositories. In this new model user endpoints are biggest risks for cloud data loss.

This whitepaper outlines the SecureCircle approach to modern data security and how SecureCircle can be leveraged to secure and control data as it is moved to endpoints regardless of data type or where the data is sourced.

Modern Data & Threats

Enterprises that are concerned with data security are generally looking to protect one or more of the following categories of data from ransomware exfiltration, accidental dissemination and malicious bad actors:

- Intellectual property such as source code, designs or product information
- Corporate data such as financial statements, employee information or M&A content
- Customer data such as subscriber information or personal identifiable information (PII)

Businesses that implement SecureCircle can protect all types of data against modern threats by securing the data itself as it is generated and limiting which users, devices and processes have access to data when it is stored in unstructured files, regardless of where that storage resides.

SecureCircle Protection

SecureCircle encrypts bytes inside of files regardless of file type so you retain access control to the data within them. This unique approach is completely application and file type agnostic.

SecureCircle is transperant to end users regardless of the applications they use to access and create data.

Operating Systems

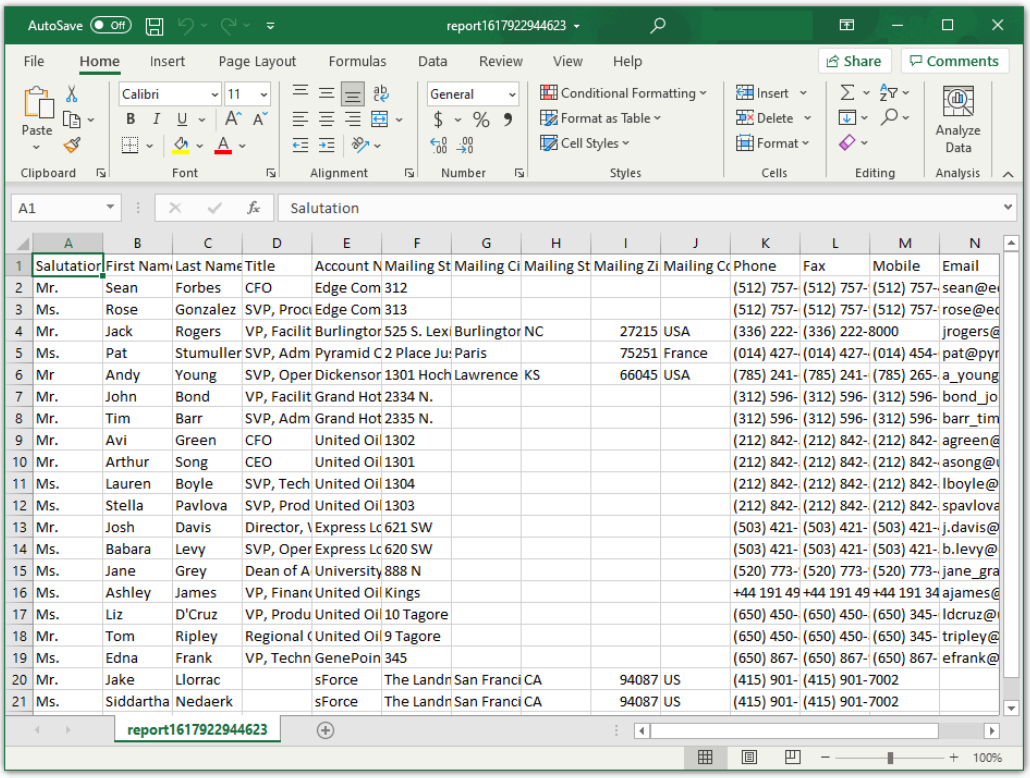
SecureCircle supports Windows, Mac and Linux platforms including desktop, server and public cloud operating systems.

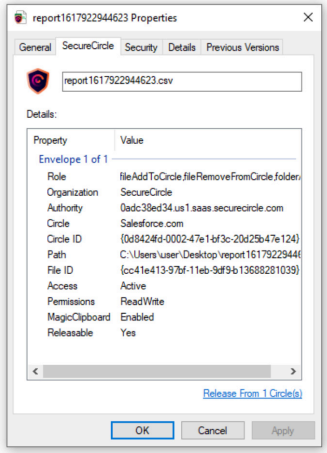
Encryption Enforced Access Control

SecureCircle is a cloud to agent service that secures data as it's created allowing enterprises to take control of their data regardless of where it is transferred or stored. As data moves from structured formats into unstructured files the data stored within the files is automatically and transparently encrypted, which creates a layer of security that provides persistent protection and access control to the data.

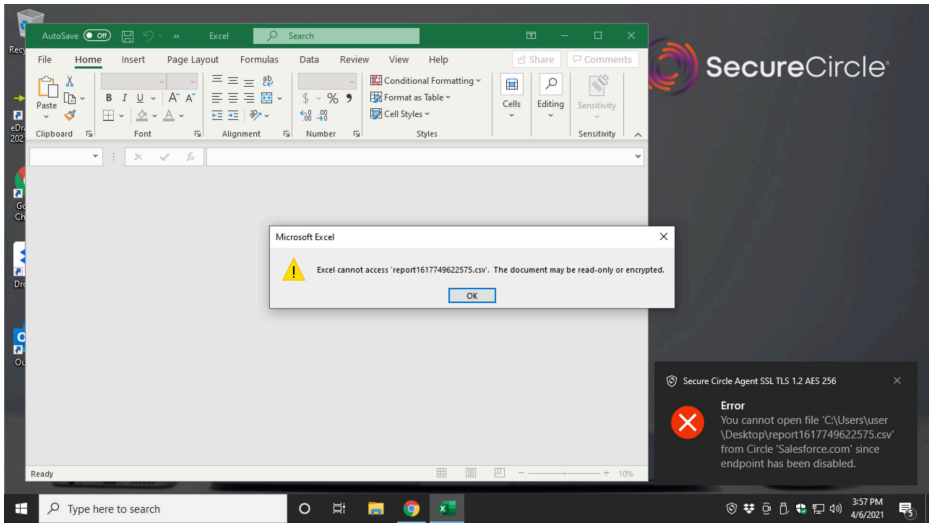
SecureCircle's transparent encryption approach is implemented through a low level driver, which means any legitimate user is not impacted by the encryption and works with the data stored within files. However, any attempts to access the data by an illegitimate user or process will be unsuccessful, as an unencrypted version of the data will not be accessible.

Once data has been secured (encrypted) by SecureCircle, not only is access limited to legitimate users only, acces may also be limited to specific processes and actions. For example, you can choose to restrict whether or not a privileged user is allowed to copy content from one application to another. These security controls allow enterprises to retain control and visibility of data even when access to content within files has been allowed, granting access does not relinquish control of data.





Transperant Encryption
SecureCircle encryption is completely transparent to authorized users when they are working with secured files



Access Denied
Only allowed users, on allowed devices, with allowed processes can read data that is secured by SecureCircle. Access to data can be revoked at anytime, which stops any user or processes from reading the encrypted data within secured files.

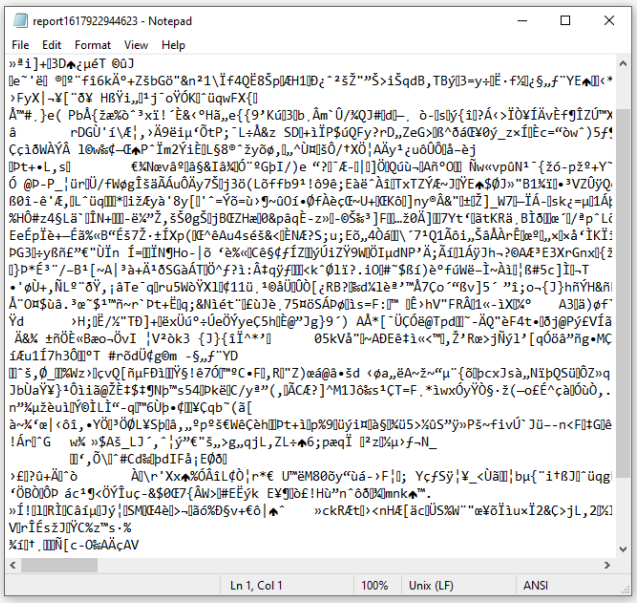
Process Level Protection for File Data

To ensure data is kept secure from unauthorized access and dissemination, SecureCircle can be configured to limit which processes read decrypted bytes of any secured file. Typically, only end-user applications and other security tools will be able to read the decrypted view of content on behalf of any user. Any application or process that moves data such as Windows Explorer, Mac Finder, email clients, and web browsers will not be allowed to directly read secured bytes, which means any files that are moved by those processes are always kept encrypted, keeping data secure wherever it goes when these processes move the data.

By providing process level control, SecureCircle can help protect against many modern data security threats such as accidental dissemination, bad actors and ransomware exfiltration. Below is a visual example of how the notepad process on Windows can be either allowed or disallowed access to secured data within a .csv file.

Data Access Allowed

In this case the notepad process has been set to data access enabled, allowing it to read the decrypted view of content in the secured



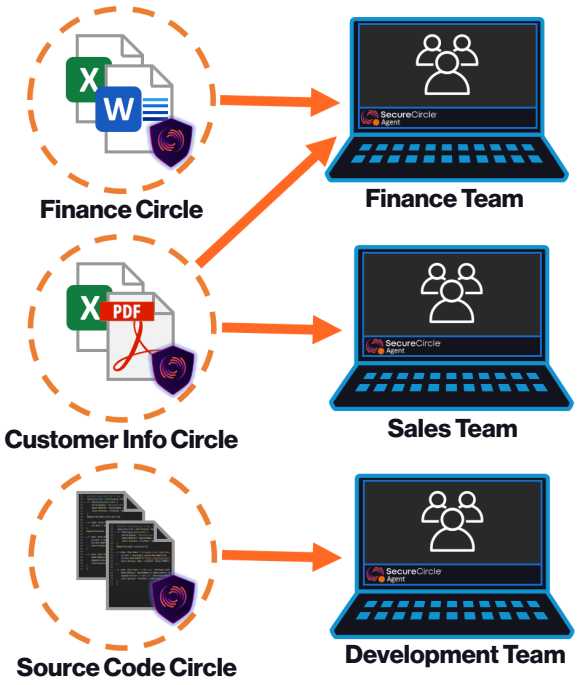
Data Access Disabled

In this case the notepad process has been set to data access disabled, the process can not read the decrypted view of the secured bytes

Managing Data Access with Circles

To simplify the management of data security at scale, SecureCircle allows the creation of circles, a logical grouping of files that need protection. As files are secured by automated rules, SecureCircle encrypts the bytes inside each file and the files becomes a member of a Circle specified by the rule. Circles provide a simple mechanism to securely segment data, regardless of where the data is sourced or stored.

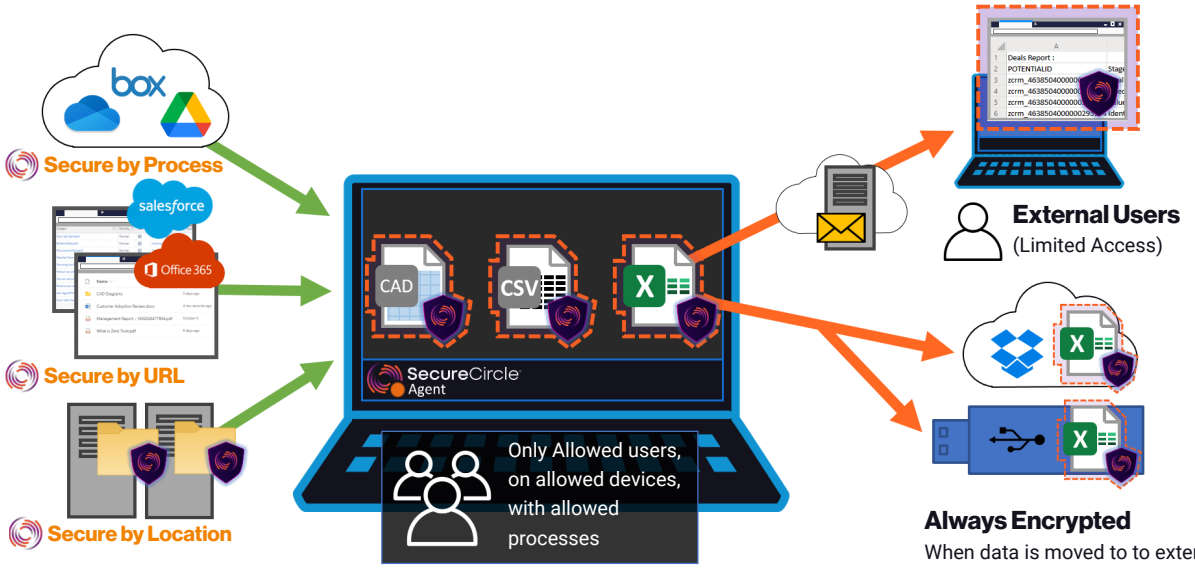
Users and groups within the enterprise can be granted access to Circles to ensure they can access the decrypted content without the user needing to change their day to day processes. Since Circles are a very flexible construct, we see many different approaches implemented in enterprise environments. Often enterprises will create unique Circles for each type of data they are looking to protect. In the example below we have created 3 Circles “Finance”, “Customer Info”, “Source Code”. Users can be members of one or more Circles depending on the data they are entitled to have access to.



Securing Cloud Application Data on Endpoints

Modern cloud applications have security controls that help enterprises control who can access what aspects of the application within the browser. However, most cloud applications allow authenticated users to pull information to their endpoint devices for internal use. The data that is exported from cloud applications is often important business data such as sales information, product pricing, employee information, intellectual property and sensitive customer information.

At SecureCircle, we help our customers protect their web-hosted application data as it moves from trusted cloud applications to user endpoints by targeting the source cloud applications as the context for our data security policies. When data is exported from the cloud application to a file on the endpoint the data within the file is automatically encrypted and a data policy is immediately applied that restricts who or what can access a decrypted view of the data within. At this point, data is only consumable by allowed users, on allowed devices, with allowed processes. If the data is moved off the device, it remains encrypted and secured regardless of where it is stored.



Security Rules (Triggers)

Below is a list of SecureCircle context and content based security triggers that can be used to automatically secure data as part of cdata policy (circle):

Secure by URL

This security trigger targets data based on the originating web location that data was sourced from. More details on how this can be leveraged to secure web app data is available in the Securing & Controlling Cloud App Data section below.

Secure by Process

This security trigger can be used to automatically secure any data that is written by a specific process on the endpoint. For example, when Microsoft OneDrive is installed on the endpoint, all data that is written to the endpoint from a Sharepoint location in the cloud can automatically be secured as it is written on the endpoint. This means all Sharepoint data that moves to the endpoint can be kept secure.

Secure by Location

For businesses that have folder structures either locally or on file servers (SMB), Secure by Location can be used to automatically encrypt and secure all data in that location. The security will stay with the data even once it has been moved out of the location that was defined. In this situation, SecureCircle uses the fact that data traverses the location as a trigger to secure the data.

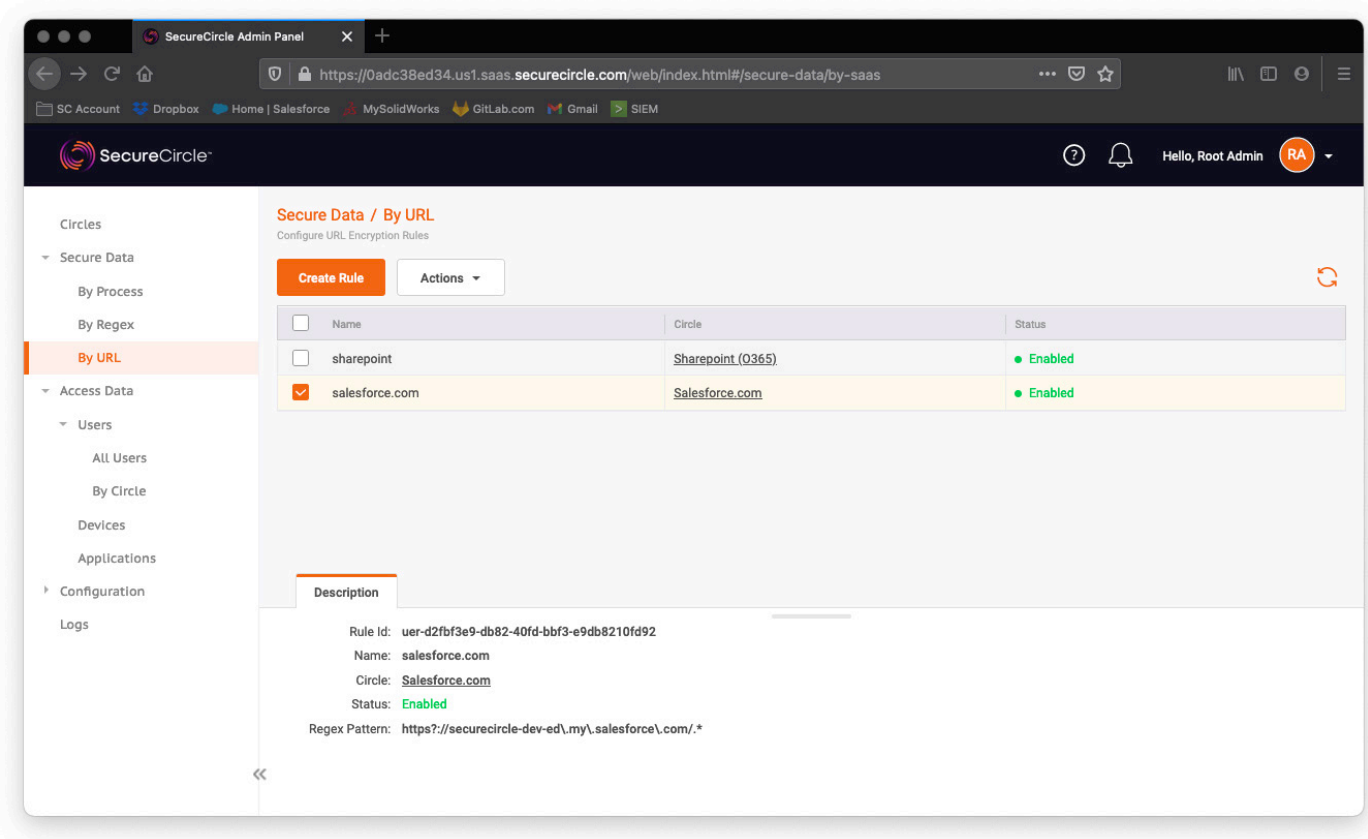
Secure by regular expression

This allows SecureCircle to secure data based on its content. For example, this can be configured to secure files that contain specific data such as PII or PHI.

Configuring "Secure by URL" to Protect Web App Data

With SecureCircle, data being exported from cloud applications such as Salesforce, Jira, and Service Now can be targeted based on source URL. This means that no specific integration is required to secure data as it leaves a given web application. This functionality is referred to as "Secure by URL" and provides a broad level of support for both cloud and internally hosted web applications. For many enterprises this provides assurance that all current and future applications can be protected, regardless of data type or where the application is hosted.

To configure security for a specific web application, a single rule can be created within the "Secure Data > By URL" section of the SecureCircle admin console. The rule includes a name (description), URL Regular expression, and a Circle. The example below shows how a simple rule can be created to protect all data that is exported out of SalesForce.com onto a user endpoint.



Below are the basic settings that need to be configured to create a Secure By URL rule

1. **Rule Name -** A description of the rule for administration

2. **Regex Pattern -** This regular expression pattern is used to identify the URLs that this rule will apply to. For example, `https?://securecircle-dev-ed\.my\.salesforce\.com/.*` is an example of a from the above screenshot which will ensure that all data exported from SecureCircle's internal SalesForce.com account will be automatically secured as it is exported to the endpoint

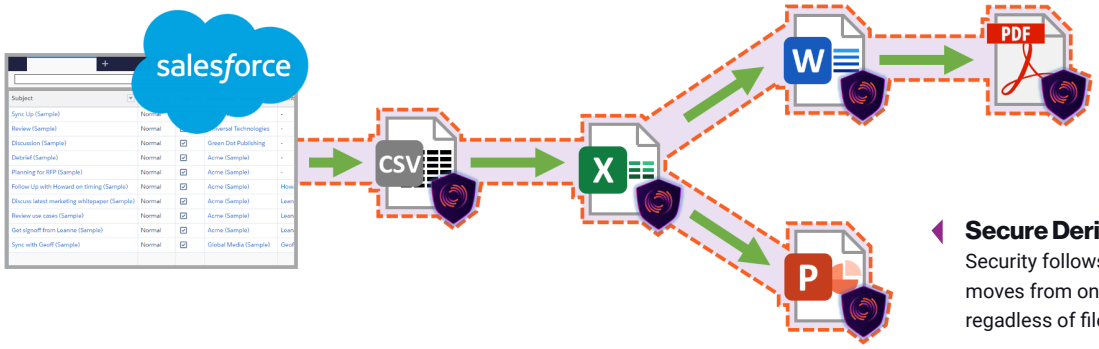
3. **Circle -** A Circle is a logical grouping of data. In the example above, all the data that is exported from SalesForce.com will become encrypted and secured as part of a Circle known as "SalesForce.com"

Once data is exported onto end user systems, the above rule will ensure that if that data has been downloaded from SalesForce.com into any type of file on the endpoint, it will be encrypted and the file and its contents will become part of the "SalesForce.com" circle.

A circle is a logical grouping of data that requires protection, which includes an access policy. Users and Groups can be added to a circle, which will allow them access to any data that has been secured as part of that circle.

Keeping Derivative Data Secured

When data has been secured by SecureCircle on an endpoint, SecureCircle creates binary DNA for that data known as a fuzzy hash. By creating DNA for all secured data on an endpoint, SecureCircle can automatically detect when a new file is created that has binary similarity to existing data. This means that SecureCircle can extend the protection of a data security policy to any new files that are created from existing files that have been protected. Therefore, not only is data secured when it is downloaded from a given cloud application, but any derivative of that data can also be protected with the same policy, allowing for ongoing protection of data as it moves between files.



Secure Derivatives
Security follows the data as it moves from one file to another regadless of file type

Securing Cloud File Services (One Drive, Box and Google Drive)

Cloud file repositories such as Google Drive, One Drive, and Box, have become widely adopted as an alternative to traditional file services, as they provide a convenient way to share file data within organizations that doesn't require traditional storage infrastructure and can be accessed from anywhere.

There are 2 ways data can be accessed from most modern cloud file repositories. Firstly, data can be manually exported from the service to the user endpoint from a web browser. Secondly, data can be automatically pushed (sync'd) back and forth between the cloud service and the user endpoint by a software sync agent such as OneDrive, Google Drive or Box Sync.

To secure files that are manually pulled down through the browser or by an export feature in the web application itself, a "Secure by URL" rule is used to ensure all files that move to the endpoint are kept secure.

To keep data secured that is written to the user endpoint by a software sync agent, a "Secure by Process" rule targets the sync agent and secures all files that it writes to the user endpoint.

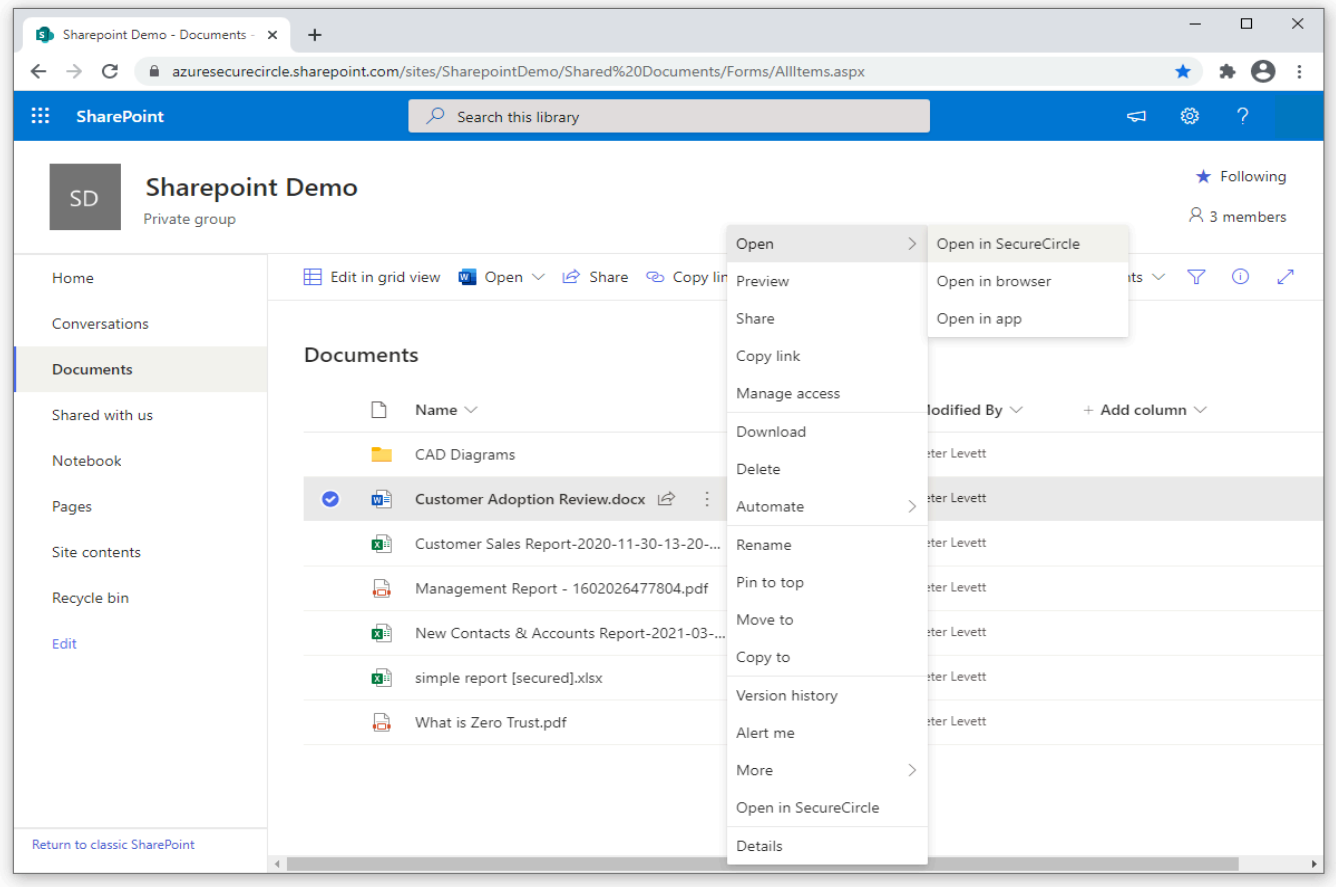
By combining the 2 rules outlined above, all the data that moves from the cloud file service will be kept encrypted and secured on the end user system, and will remain secured if it is moved to an unsanctioned location.

Securing File Sync & Share
Files are secured as they moves to the endpoint via web download and sync software by combining "Secure by Process" and "Secure by URL"

Accessing Secured Data in Office 365

For many enterprises keeping data in a secure format while stored within cloud services provides additional protection in the event that the cloud service provider is ever compromised. The challenge with keeping file data encrypted in the cloud can impede the ability for users to leverage in-cloud features. For example, some enterprises want the ability for their users to edit content in the browser directly using the Microsoft Office 365 online.

SecureCircle has specific integrated functionality that allows users to access content through the in-browser Word, Excel or Powerpoint applications, whilst keeping the data encrypted and controlled by a given SecureCircle policy. The data within these files can only be accessed by sanctioned users and the data is never accessible in an unencrypted format in the cloud service itself, reducing exposure in the event the files themselves are accessed by unauthorized parties.



Open in SecureCircle
Files that have been secured with SecureCircle can be access and edited within the browser. The files are always encrypted inside Sharepoint

Collaborating Externally with Secured Data

For most enterprises, end users need to share sensitive data with external parties and potential risks of exposure when sharing data is a common concern. When data has been secured by SecureCircle, data can only be accessed by external parties when it is shared by sanctioned methods.

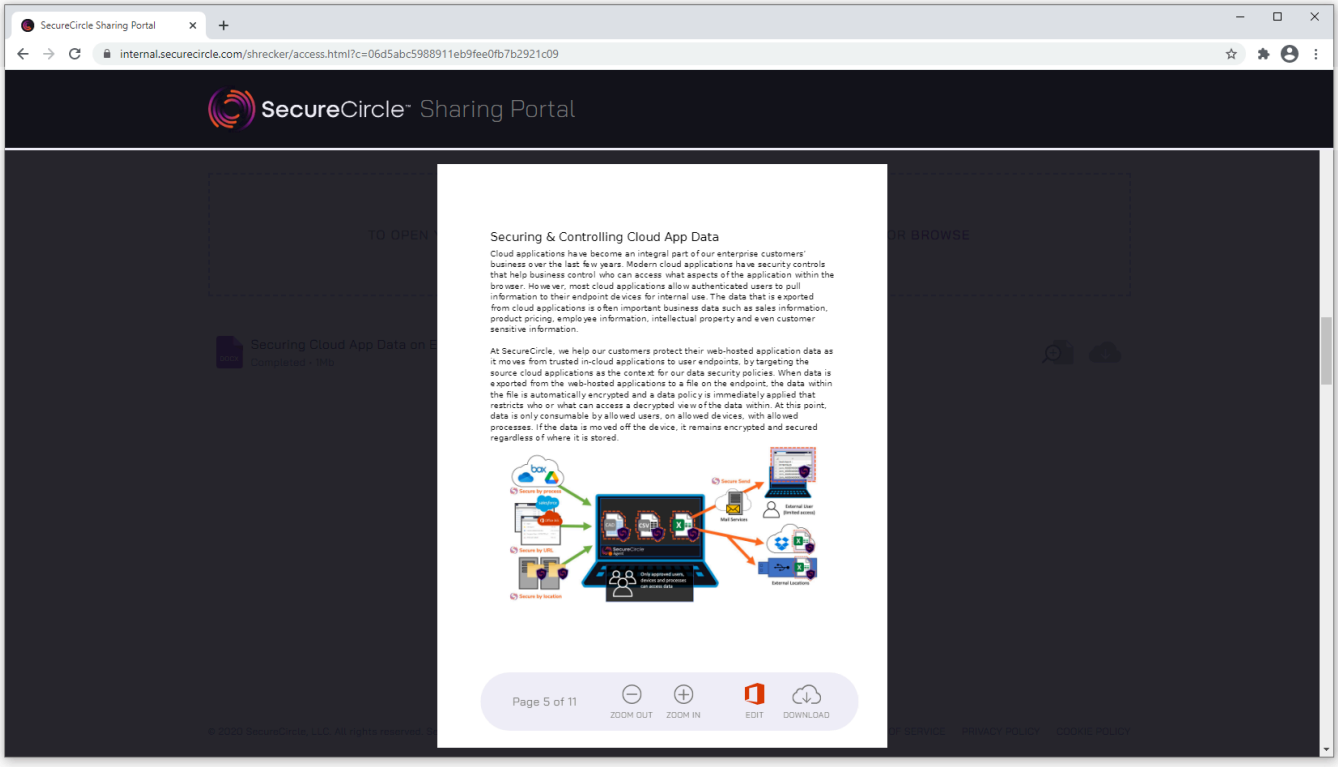
The ability to provide simple and effective methods to share secured data greatly increases the rate at which enterprises can secure data, without compromising end user productivity.

Secure Send Files Externally

To allow users to share files externally without releasing control of data, a Secure Send policy can be configured which allows secured data to be sent to external parties over email.

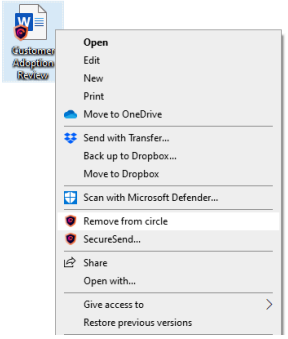
Secure Send allows an internal user to send a secured file, and the recipient of that file will be able to either download the file or access its contents. Limits can be set on which email address or domains data can be sent to, how many times the file can be accessed, or the length of time a file can be accessed for.

In addition to the limits that can be set on access to files shared via Secure Send, it is also possible to revoke access to files at any time. This is ideal in situations where data has been accidentally sent to the wrong party or access needs to be retracted due to change of circumstance.



Right-click “Remove from Circle”

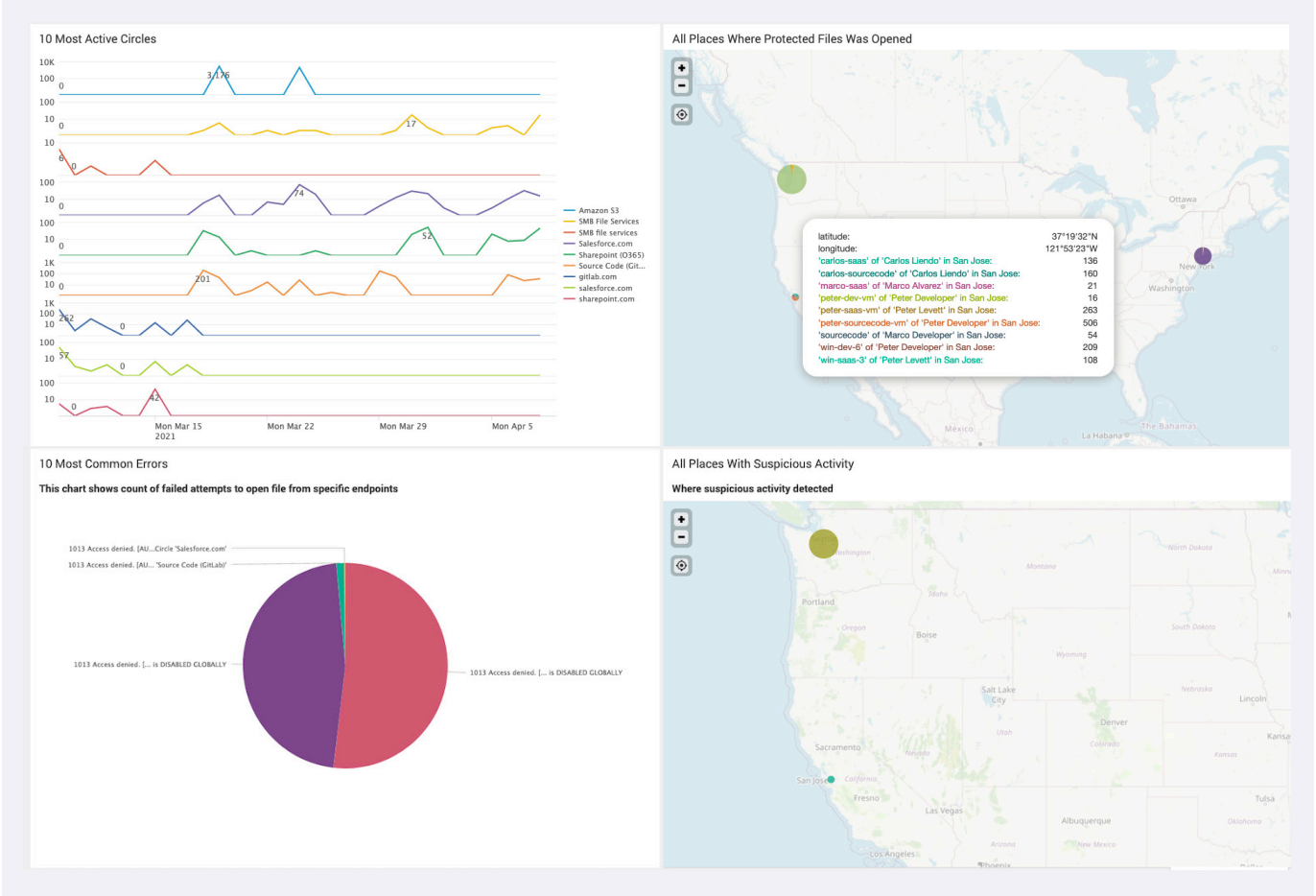
In some cases, users can be given the ability to manually remove a file from a Circle (decrypt), by right-clicking on a given file and selecting the “Remove from Circle” context menu option. In this situation, the security is removed and the decryption event is logged centrally, for reporting. At this point the file can be sent by any means to an external party.



Maintaining Visibility and Auditability

To assist with audit and compliance requirements, SecureCircle logs all events that take place against secured data. Each operation that takes place is logged and can be sent to a log aggregation (SIEM) for processing, visualization and reporting.

When data is accessed, the endpoint location, user, and process are all logged. Any denied event is also logged to ensure that suspicious attempts on data are identified and can be investigated.



Conclusion

For many enterprises, legacy data security approaches have limited their ability to deliver security without impacting productivity. SecureCircle's focus is to deliver data security that raises protection against existing and potential future threats, without compromising user experience or operational burden on IT and security professionals.

As cloud-based applications grow in the enterprise, securing data as it moves from cloud to endpoint becomes the simplest and most effective solution to securing enterprise data from modern security threats.

About SecureCircle

SecureCircle's Data Access Security Broker (DASB) delivers a SaaS-based cybersecurity service that extends Zero Trust security to data on the endpoint. At SecureCircle, we believe frictionless data security drives business value for our customers. Instead of relying on complex reactive measures, we simply secure data persistently in transit, at rest, and even in use. End users operate without obstacles, while data is continuously secured against breaches and insider threats.

SecureCircle.com

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