SECURECIRCLE

# Securing Virtual Perimeters

*"When it comes to effective data security,*
*the most successful solutions are transparent"*

SecureCircle

# *"With More Than 100,000 Cyber Attack Incidents per Day, The Time to Adapt Is Now"*

## Introduction

Data Security is at the forefront of every corporate agenda, not only are outside security breaches a threat but the threat from inside is of equal risk – overall attacks number over 100,000 per day. An effective data security platform must protect, equally, from both internal and external threats; this is where many data security solutions fall short.

With more than 70% of enterprise data taking the form of unstructured data, the ever-increasing task within the enterprise to Secure, Manage, Audit & Track unstructured data has becoming arduous at best.

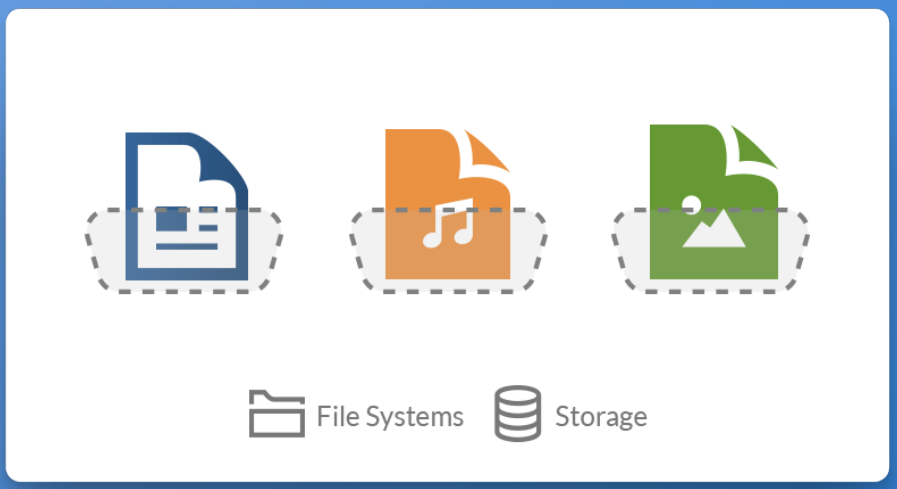
There are many solutions that protect the perimeter by building higher walls; however, in today's *Perimeter-less Enterprise,* this approach to safeguarding critical data is met with end user resistance. A more advanced and comprehensive approach to transparently securing business critical data is the key to protecting IP within the modern enterprise.

Whether it is product designs, financial information, patient records, trade secrets or any other intellectual property that drives your business, the need to prevent loss is paramount.

Data silos are constantly evolving and are growing beyond the traditional data center. With distributed data sets that live everywhere, from the data center, cloud to employee devices such as desktops, laptops, tablets and phones (BYOD), it is now increasingly more complex and challenging to account and secure sensitive data within the enterprise.

Traditional protection techniques to keep files within network-based perimeters lose their effectiveness as the growth in consumer-based connected devices (BYOD) increase within an organization. To make things even more difficult, IT Organizations are expected to deliver solutions that make collaboration a simple task for individuals. The balance between securing data and productivity has long been difficult to achieve. Striking the balance between the right level of security and ease-of-user experience (productivity) is at the crux of this ever-important challenge.

SecureCircle delivers a solution that is both secure and transparent to the end user, keeping data safe while not requiring end users to change their behavior with regards to file interaction and collaboration. There are no policies to create, manage and maintain. There are no behavioral modifications that users need to adopt. It's tight security with control and productivity at its best. Additionally, Enterprises should ensure that trusted employee's today, do not have access to misuse critical information that belongs to the company, knowingly or unknowingly. SecureCircle has solved this age-old hurdle. Because Files are always in an encrypted state, we mitigate an employee's ability to misuse critical data. We will explain this in more detail.




***File Virtualization** / Encrypted, Trackable, Retractable and Portable*

SecureCircle

# *Secure Virtual Perimeters Deliver Visibility and Control*

At the core of SecureCircle is a Patent-Pending Virtual & Portable Encrypted File System (EFS) and Similarity Detection Technology that are designed to transparently protect files through their entire life cycle. A SecureCircle protects data in all the forms it takes throughout the entire collaboration process, from publishing to retirement, regardless of file type.

Our Encrypted File System is built on virtualization technology that transparently containerizes each file so they are always encrypted with 256 bit AES, even when file content is being accessed or modified. At no time does the content leave the virtual container (EFS). Files of any type can move between Windows, Mac, Linux, iOS and Android while retaining the highest level of protection, visibility and control, without sacrificing end user freedom.

SecureCircle

**Completely Transparent** – Our File Virtualization adds a protective, invisible layer on top of any existing file system. This core piece of technology allows both users and applications to interact with secured files in the same way they would with unsecured files. The virtualization process does not change any file attributes, file names or file extensions nor does it change the contents of the file. The file is 100% unchanged and is hash-identical.

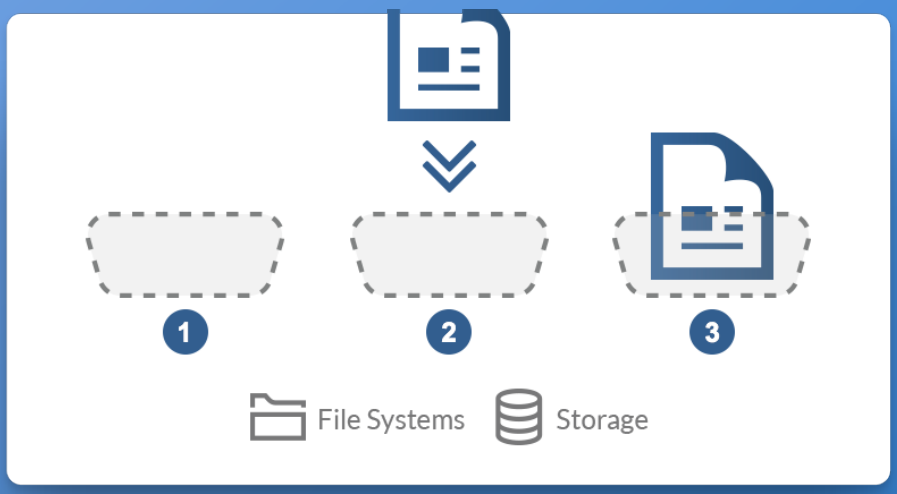
**Always Encrypted** – As the protection travels as part of each file, the files themselves are always encrypted as they move between devices and storage services, including Cloud. From the moment they are created, to the time they become dormant, inactive or retired, the files are encrypted. Even as users interact with the files content (read/write, copy/paste), the container itself remains in an encrypted state. This is how we are able to protect an organization from internal misuse of critical data.

**Always Tracked** – Each containerized file carries a unique Circle ID that is used to identify the group of "Trusted Devices" that have access to the containers content – the actual file. Each time the container is accessed, authorization is checked; meaning, only trusted devices can see and use the file, regardless of where the file resides or where it is transported.

**Always Retractable** – Because the transparent container is always encrypted, files can be disabled regardless of their location by disallowing access to the containers decryption keys. So regardless of what device the files are located on, render them useless by removing the device from the SecureCircle.

**Always Portable** – Secure Circle's File Virtualization is cross-platform, file-type agnostic and is permanently bound to the file it is protecting. This means that regardless of the transport means, the location or the device used, unstructured data is only accessible by those who are active members of the Circle. So today, an employee can be part of the Circle, the moment their device is removed from the Circle, they no longer have access to the files. If they copy them to another device, such as a USB stick and try to open the files on their computer at home, they cannot because the files are useless without the corresponding encryption keys.

**Derivative Work Protection** – Our Similarity Detection allows users complete flexibility in how they want to work with unstructured data, just as they do today. SecureCircle's ability to identify binary or digital "DNA" within each file allows data to move freely between files but guarantees that all derivative work is containerized in real-time. These derivatives are only accessible by devices within the SecureCircle. There is tremendous power in having the ability to automatically protect derivative work.

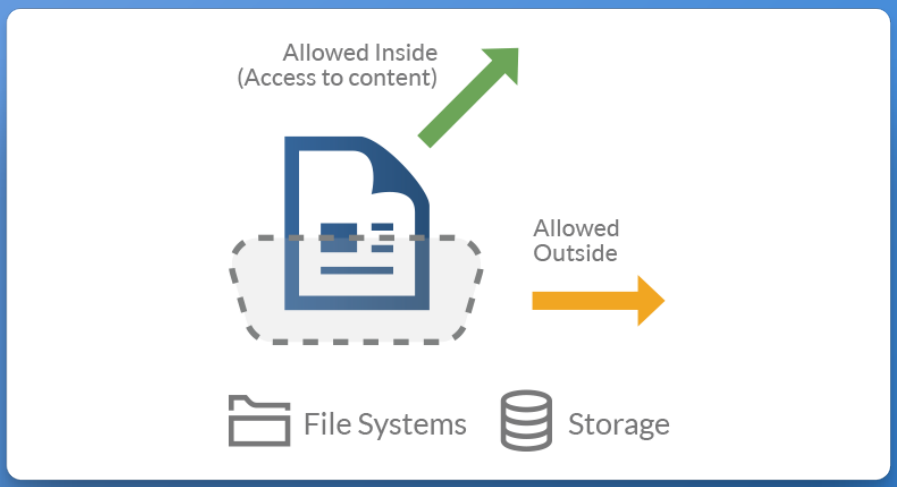



*Once the file is in the protected state described above, authorized devices and processes can access and modify it's content as if the file itself was still in its original state however, the content will always remain containerized. Any attempts to move the content into a non-containerized state will transparently be met with a new container.*

SecureCircle

## *How Does The Transparent Container Work?*

- ✓ A Transparent Encrypted Container is provisioned in real-time for new and derivative files.
- ✓ The contents of the file are put into the Container and are now protected regardless of their location.
- ✓ The Container is always seen as the original file by authorized processes (applications) and users.




SecureCircle

# Two Levels of Access Deliver Transparent Portability

SecureCircle monitors each request to a containerized file to make sure that trusted users and authorized processes have fast and uninterrupted access to contents of the container.

For all processes that are not granted access (not white listed) to the data inside the container, they will access the encrypted bytes of the container itself. This means that the container can be copied moved to any type of storage using standard means such as a copy operation, mail attachment or instant message service. Typically, applications that copy and move files such as Windows Explorer, Mac Finder, Chrome and Safari are not white listed. Containerized files are free to move just like any other file; however, they are only accessible by those authorized processes and users.

## Delivering Transparent Protection

SecureCircle enables organizations to transparently secure and protect critical data. We enable our customers to adopt cloud services and BYOD without putting sensitive business information at risk. Our solution automatically protects sensitive information at the point of creation and does not change the way users collaborate and share files. Businesses can protect intellectual property and meet regulatory compliance requirements without burdensome policy management and end-user adherence.