SecureCircle®

DATA SHEET

Effective Data Security

VIA AN OPT-OUT PRINCIPLE

Most organizations accept that cybersecurity is a business risk, not solely the responsibility of IT. This acceptance is crucial for the risk of data loss in particular, as this is the most material exposure to businesses. Cultural decisions need to be considered to ensure data protection.

Industry statistics prove that most data breaches (60%) are insiders within the business or attackers who were able to become native within the IT environment. Therefore, the traditional approach of enforcing controls and tools to manage data risk restrict business operation and quickly reach maximum effectiveness that falls short of addressing the business risk.

It is essential that any security solution achieves a balance between control and risk mitigation; business agility and user freedom is maintained. Without the former, the challenge persists; without the latter, users find ways around controls that are perceived as restrictive or inhibit productivity.

The security market has seen numerous tools that partially address the data loss challenge, each with its limitations:

Disk Encryption	Doesn't protect against common issue like email exfiltration, malware, hackers or users uploading data to the cloud
Cloud Access Security Broker (CASB)	No local security or protection of locally-created data. Users forced to login through a gateway for cloud applications.
File Encryption	Management overhead for encryption keysl decrypted during use removes all protectionsl no alerting or auditing of decryption.
Informatin Rights Management (IRM)	Limits useable applications; curtails productivity; only works on specific file extensions; files still decrypted during use.
Data Loss Prevention (DLP)	Numerous egress points and devices need to be managed; file access not logged or audited; DLP changes file names and extensions; data only encrypted on egress and subject to malware and malicious actors.

Even with many of the above tools deployed, users may still bypass restrictive or undesired controls by sending data to personal e-mail, copying data into an e-mail body, or moving the data to a cloud service.

Opt-In vestus Opt-Out

Most attempts to address the data challenge assume an opt-in approach: the user opts to be secured, agrees to abide by a policy, and we trust they won't bypass the controls and protection in place – either accidentally or deliberately.

However, time again this cultural approach fails and in these cases the response by the business is reactive: we know only after the event if suspicion exists (if we know at all) and is costly and time-consuming to prove evidentially that a crime was committed.

Opt-Out reverses this approach – the principle is that the security is thereby defaulted; a user can send data to any location but needs to consciously make that decision, which creates a forensically sound record of each action.

This approach secures each piece of file data across the whole business through a method invisible to both users and applications. All data is encrypted and secured whenever and wherever it is – in transit, at rest, and in use. Access is governed by the existing identity management system within the business, leveraging the groups and department privilege that pre-exist. To gain access to data a user has to be employed and within active directory, and the user has to be on an authorized machine to access the data (with Bring Your Own Device (BYOD) or Contractors' devices easily included). When a user leaves the organization, any access to data is revoked, irrespective of where it is, through the simple act of excluding a previous identity. All the data that is secured is no longer accessible, and all the data the user has sent insecurely is auditable and evidenced.

When a user wishes to share data with any third-party, they may either send the data encrypted or make a conscious decision to transfer the data unencrypted. To unencrypt, a user needs only perform two mouseclicks – however, this activity is recorded, and thus the visibility of data movement is auditable and forensically sound; we can verify this exact data left, when, from where.

As cultural maturity evolves, this opt-out model can be modified to incorporate segregation between HR, Finance and Sales teams, or for specific project purposes - such as the executive team looking at an M&A. In each case, data pertinent to a specific team or role may only be accessible by an appropriate member. In the latter example of highly sensitive M&A data, further precautions would prevent all external sharing, perhaps allowing an exception for external legal counsel.

The Principle

The principle of this approach means that company data can exist in any location, in any cloud service, or wherever it is sent, and it is secured and protected. Further, whatever derivative is created from the data (such as a copy-and-paste function of Excel data) is equally, automatically, secured, and protected. In short, only authorized identities and machines can un-encrypt and access company data - and the company owns the authorization.

Under this principle, data protection is achieved with security, visibility, and control, in a way that is transparent to users and the organization, with the ability to audit and retract as needed.

To Learn More

Contact your Data Access Security Broker expert at sales@securecircle.com or 408-827-9100

What makes SecureCircle Special

SecureCircle	Others
Protects the data. The data is protected no matter where it is including temporary files such as those created by MS Word.	Only protects the container of data. If data is copied outside of the container (copy/paste, save as) the data is unprotected.
Transparent to end-users. No impact on their workflow or tools.	File names are changed. Workflows are interrupted. Added security is clunky and awkward to use.
Allow/deny any process from accessing the data.	Limited application support. Often requires SDK, plugins, or other manual integration efforts.
Compatibility with your storage, wherever it is, be it external or Cloud Storage. No impact on how you copy, move, or store data.	Support for targeted solutions with limitations and workflow restrictions.
Support for Windows, Mac, iOS, Android, Linux	Select platforms. Difficult to support BYOD and mobile platforms. Mac and Linux environments particularly challenging.
Protected data can be searched and indexed without any changes to the application.	Protected files are unreadable by outside utilities such as Finder in OSX and search.
Support for Virtual Desktop Infrastructure (VDI)	No support for VDI
No impact to direct media (SSD/HDD) IO performance.	Performance impacts users due to applications userspace performance
Native operating system support.	Loss of functionality such as icons & file previews. Noticeable performance impact when reading or writing to protected files.
Fully compatible with BYOD culture	Restrictions on devices, operating systems, applications & file-shares. Operational burden shifts to the IT team.
Easily deployed. Protect-by-default is easier than classifying and selectively rollings things out.	Often cumbersome to deploy.
Easily managed. Works with any application or process with granular controls that are easily configured by the policy.	Requires granular rulesets on data flows. Many dependencies on SDKs and plugins for application integration.

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.

SecureCircle.com

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