SecureCircle®

WHITE PAPER

Reducing Insider Threat

SECURECIRCLE.COM

SecureCircle®

Compliance and Visibility

Contents

Introduction

Your organization is inundated by "Insiders" maliciously or unintentionally using authorized access to exfiltrate data. We call this an "Insider Threat."

- Inside" - Anywhere your data resides -- on premise file shares, public or private cloud storage, removable media, even carrier pigeons.
- "Threat" - Anyone, internal or external, maliciously or unintentionally, trying to breach data.

Colleagues continue to be the most significant threat to data. While using unauthorized tools or unapproved workflows may seem innocuous, these activities lead to significant loss of data and control. Limitations on the size of email attachments may cause frustrated employees to use less secure methods of data migration, such as moving data from one device to another, copying data to USB drives, or using unauthorized applications.

Similarly, employees may use unapproved file sync and share solutions, such as Box or GoogleDrive to collaborate internally and externally more easily, bypassing IT-approved solutions that involve more complex and time-consuming elements such as VPNs. These well intentioned behaviors create data vulnerabilities that can't be ignored.

- 59% of employees voluntarily or involuntarily take confidential data with them whendeparting an organization.[1]
- Up to 43% of data breaches are caused by insiders putting data at risk. [2]
- 73% of companies confirm insider attacks are becoming more frequent. [3]
- 29% of all businesses had reported accidental disclosures by insiders as their single largestsource of lost data – bigger than either software vulnerabilities or outright theft. [2]
- The average cost of a data breach in the U.S. is $8.19 million. [4]

Mitigating Insider Threat

To effectively mitigate the insider threat, organizations must adopt a data security approach that features persistent data protection, easy to manage access control policies, and an auditable trail of every action taken on data. They must also have the ability to protect new derivatives and ensure that access control persists no matter where data is created, consumed, stored, or modified. SecureCircle's Data Access Security Broker (DASB) is the only solution capable of delivering these requirements in an entirely transparent way, while not adding operational overhead for the business, IT staff, or users.

SecureCircle's Data Access Security Broker (DASB) is the only solution capable of delivering these requirements in an entirely transparent way, while not adding operational overhead to the business, IT staff, or users.

- DASB moves access control policies from the storage system of the data to the data itself – from device/file-centric to data-centric.
- DASB access control works with local and remote storage systems, as well as cloud file storage, without requiring any change to applications.
- Access is granted to users, devices, processes, and/or applications without ever releasing control. Access control persists no matter where the data is created, consumed, stored, or modified.
- DASB's patented DerivativeWorks™ analyzes the DNA structure of all data, comparing protected data to newly created pieces of data and extending the same access rights.Your organization can protect new derivatives and clean up 'sins of the past.'
- Data protected by SecureCircle is exempt from mandatory Data Breach Notification laws in all 50 states, as well as those related to HIPAA, FINRA, SEC, and PCI.

Case Study: Inadvertent Insider Threat

1. Accountant Jenny has access to your organization's financial documents, which are protected by DASB.
2. She shares documents with her colleague Frank, who works in sales and has access to the protected data.
3. Frank copies the protected quarterly financial data and pastes it into a sales presentation.
4. DASB Derivative Works detects protected DNA in this new presentation and automatically extends the same access rights -- meaning only the people who could already access the protected financial data can access the presentation.
5. Frank sends the presentation to a client, not realizing that the financial data is confidential.
6. The client has not been extended access to the protected financial data within the presentation. When he opens the file he sees gibberish, ensuring that sensitive data remains secure within your organization.

Navigating the Paradigm Shift in Data Security

Historically, data has been protected while held within the perimeter of a firewall. Today, with the Cloud, SaaS, & BYOD, your data escaped or never resided in the perimeter, leaving sensitive data vulnerable.

It's not surprising that data breaches occur to enterprises, in all industries, seemingly daily. Data is used and generated everywhere. Data powers embedded applications, smartphones, cars, web browsers, refrigerators, HVAC systems, and toilets.

The infrastructure of these platforms consists of client server systems and cloud services, and the platforms are powered by your data flowing in and out of them. The increasing rate of data breaches points to data, replacing humans, as the most valuable asset within an enterprise.

SecureCircle's data-centric DASB enables you to control this asset, retaining control of your data without impacting applications, overhead, workflows, or end user experience. DASB is the only solution that empowers you to enable secure access and satisfy various data security compliance requirements.

[1] Deloitte, Insider Threats: What every government agency should know and do, 2016
[2] Absolute, https://www.absolute.com/en/solutions/insider-threat, 2017
[3] Securonix, Insider Threat Report, https://www.securonix.com/resources/2019-insider-threat-survey-report, 2019
[4] IBM, Cost of a Data Breach Report, https://www.ibm.com/security/data-breach, 2019

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