SecureCircle®

DATA SHEET

Traditional Data Security Fails to be Zero Trust

Data security tools are not providing enough value for their customers. The average total cost of a data breach in the United States is nearly $9million per the 2020 IBM Cost of Data Breach Report. That is a five % increase from 2019. 31% of data breaches in North America can be attributed to internal actors.

Per the Verizon 2020 Data Breach Investigations Report, 76% of companies that experienced breaches said remote work would increase time to identify and thus continue to increase costs to organizations.

What is Zero Trust Data Security

Zero Trust data security is a practice of never trusting users with data. For zero trust to be effective, data must be secured by default and not an exception. Never trusts the user with the data or giving them control. Instead, allow users to work with the data as if they're in control.

Data breaches and news headlines confirm Data Loss Prevention (DLP) solutions are broken. Customers like DLP because it seems easy. Three well-known steps: discover, classify, and protect. With DLP, chief information security officers (CISO) and other security teams feel like DLP casts a wide net.

Customers dislike DLP because it relies on users to be trusted, which creates security gaps that are hard to anticipate. Maintaining DLP is impossible because the DLP model creates rules to block behavior, so IT and security teams are constantly chasing the next unknown. Rule maintenance is a never-ending battle of finding new egress points in organizations. Let's review the three components of DLP.

Discover and identification of data that needs to be classified doesn't work because legacy DLP solutions rely on fragile pattern matching like a regex expression. Tiny changes to the pattern leave false positives and negatives that are not reliable.

DLP regex discovery may work for phone numbers and very static formatted data, but there is no pattern to match to locate 'top secret' data. 'Top secret' data could include intellectual property, internal finance and HR data, and more. DLP relies on users to discover this type of data.

Classify and tag data with labels so the protection systems can take the proper action. Tagging data in legacy DLP solutions only captures the data at the moment in time. DLP tags do not automatically update when the data changes. DLP requires tags to be added to file metadata. But most file types don't support the ability to add metadata to the file. This creates a dependency that DLP requires to function properly. It is the same reason these solutions can't support any file type or any application. So again, DLP relies on users to classify and tag data.

Protection of tagged data. Assuming the discovery and classification steps were correctly executed, data is protected by creating rules to block activity and transfers. Information is not protected by default. DLP depends on rules that either block (stopping the action or transfer), allow, or encrypt the data. Rules have to be created for every workflow possibility. When new applications are used, new rules must be created. When new functionality is added to existing applications, new rules must be created. DLP is an operational nightmare as security teams are in an endless battle to keep rules updated. Users will find ways to egress data. There are too many possibilities, and manual rule creation is error-prone at a minimum and deficient for most organizations.

DLP Zero Trust Data Security Litmus Test

- 🔴 Works with any file type
- 🔴 Keeps derivatives secure
- 🔴 Keeps data secured after access is granted

Alternatives to DLP include Secure Access Service Edge (SASE). SASE is a combination of Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), DLP, and SD-WAN to isolate applications, segment networks, and authenticate based on user permissions, authentication, and verification before giving access to resources that include data. Designed for a cloud world, SASE puts a perimeter around cloud services but still forces all data through one focal point, which has different performance, reliability, and security concerns. Data protection for SASE still relies on traditional DLP for data protection. Therefore, SASE has the same downfalls as traditional DLP.

SASE Zero Trust Data Security Litmus Test

- 🔴 Works with any file type
- 🔴 Keeps derivatives secure
- 🔴 Keeps data secured after access is granted

Another security option for organizations looking for Zero Trust data protection is Virtual Desktop Infrastructure (VDI). VDI was never designed as a security solution. VDI provides all the benefits of SASE by putting the user in the data center. The user is working with data but doesn't have control over the data. The data is always in the data center. VDI was designed for the local area network (LAN) world like a doctor's office or call center.

VDI is used by some organizations to protect the holy grail of data, which is source code. Source code is exceptionally challenging to secure because appeasing developers and not impeding their productivity or changing their workflow is always a concern for organizations. Developers are a tough audience to keep happy.

The downfalls of VDI is that the solution is costly, latent, decreases productivity, and user experience is not optimal. Still, it does check all the requirements for Zero Trust data protection. SecureCircle is able to deliver a Zero Trust data protection solution that allows organizations to control data without impacting how the user needs to do their job. Users aren't affected by reduced productivity or a change in the workflow, so they won't try to find ways to get around security because security is transparent.

VDI Zero Trust Data Security Litmus Test

- 🟢 Works with any file type
- 🟢 Keeps derivatives secure
- 🟢 Keeps data secured after access is granted

We have highlighted source code as the holy grail of data because source code has been complicated to secure. Still, SecureCircle protects data in other use cases such as (1) protecting SaaS data as it leaves the cloud application and (2) user-created content such as media, design, and office data.

Why Do Customers Choose SecureCircle?

- We remove users from the security process so you don't have to rely on users doing the right thing
- Transparent and frictionless to applications and users
- Reduce cost and complexity (one tool, protect by default persistently)
- Rapid deployment

SecureCircle persistently protects data by default. Data is secured at rest, in transit, and in use. Organizations grant workflows, applications, or users the ability to egress data from protection and create auditable events for compliance visibility. SecureCircle focuses on protecting not just devices or data but also the process and workflow around data creation, storage, and use.

SecureCircle tracks protected data, and when protected data is moved to new or unprotected files, the new file is automatically protected with the same permissions as the original data. Tracking data and not files allows SecureCircle to allow copy and paste and SaveAs functions while continuing to protect data as it moves. User, device, application, and network permissions can be changed in real-time since organizations never lose control of data regardless of where data is created, stored, or transferred.

SecureCircle Zero Trust Data Security Litmus Test

- 🟢 Works with any file type
- 🟢 Keeps derivatives secure
- 🟢 Keeps data secured after access is granted

Who is SecureCircle?

SecureCircle 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.

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

©2021 SecureCircle ® All Rights Reserved. All names, logos, and brands are property of their respective owners. All company, product and service names used are for identification purposes only. Use of these names, logos, and brands does not imply endorsement. SecureCircle is a registered trademark of SecureCircle LLC.