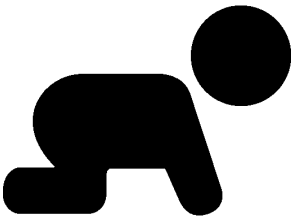
SecureCircle Deployment Guide

SecureCircle delivers a Zero Trust Data Loss Prevention solution that mitigates data breaches and ransomware. End users operate without obstacles, while data is continuously secured. Instead of relying on complex reactive measures, data is persistently secured in transit, at rest, and even in use.

How to get started with SecureCircle?

Once customers understand the values of SecureCircle, their attention focuses on implementation. This guide covers SecureCircle's recommended deployment process. The deployment consists of three steps that map to our crawl, walk, run philosophy for success.



Crawl

Deploy SecureCircle Agents

Organizations start deploying the SecureCircle agents to all devices that may be authorized to access secured data in the future. This process should be similar to how the organization installs and updates antivirus, EDR (Endpoint Detection Response), or any other software application. Agents are available for Microsoft Windows, Apple MacOS & iOS, Linux, and Android.

Customers deploy using MDM (Mobile Device Management) tools such as Microsoft Intune, Jamf, and VMware Workspace ONE to deploy agents. Customers can use any provisioning tool, including Windows GPO (Group Policy Objects) or email.

SecureCircle recommends deploying a few agents initially and checking for compatibility with other security solutions during this stage. Occasionally, customers will need to add SecureCircle to the allowed exception list antivirus or EDR solutions. Check the SecureCircle documentation website for additional details.

Walk

Identify Initial Data Set and Monitor

Once the SecureCircle agents are installed, initial data sets are identified and ingested in order to monitor workflows and application usage. Customers can add additional data sets to monitor at any time.

Customers should configure their SIEM (Security Information and Event Management) or log reporting tool at this time to collect all the monitoring data such as:

- Unknown regulated data
- Actual access to highly confidential data
- Unknown applications, malware, or shadow IT threats
- List of all potential application egress points

The initial data sets can be:

- Regulated data categories such as PII (Personally Identifiable Information), PCI (Payment Card Industry), and PHI (Protected Health Information). SecureCircle suggests these categories are selected.

- SaaS location such as Saleforce.com, Workday.com, or any URL where sensitive data originates
- Specific folders on endpoints or central file servers

During this stage, the SecureCircle agent will secure the data in the initial data set, but data will be allowed to egress off the device without security. All applications will be enabled to access secured data. SecureCircle will log all access to secured data into reports viewable in a SIEM such as Splunk.

The SIEM reports will show interaction with the initial secured data set by users, devices, applications, and more. Reports will show many files SecureCircle was able to detect PII, PHI, PCI. The goal of this step is to monitor and collect data.

Run

Apply Security

Finally, organizations will enable their security policies based on the data collected in step 2. Organizations can roll policies out in phases or all at once.

Apply security policies to users, devices, data sources, data types, applications, networks, and more. (examples below)

- Users: associate all users from the engineering AD (Active Directory) group to the engineering Circle.
- Add additional data sources: secure all data downloaded from Saleforce.com and only allow users from the 'Sales' group in Active Directory or OKTA to access the data.
- Add additional data sources: automatically secure source code from GitHub and only allow users from the 'Engineering' group to access the data.
- Update data categories: select data sets to secure when detected, such as PII, PCI, and PHI.
- Applications: based on the populated list of applications that accessed secured data in step 2, decide which applications will have access to secured data in production. Carefully review applications that can transfer data off the endpoint, such as email clients, browsers, file transfer, file sync, cloud storage, or any application that can directly move data to the cloud.
- Application: select any applications in which all output will be automatically secured regardless of content, such as Excel or git.exe
- Network: Create advanced policies for inbound and outbound data transfer. Network rules are applied per application.

Employees will continue their work without any change to their workflow.

Deploying legacy DLP takes months to set up and requires significant resources to upkeep. With SecureCircle, companies see value within days or weeks. Since SecureCircle's security is transparent, there is no training needed for employees. Ongoing maintenance doesn't require creating new and updating existing DLP rules. SecureCircle policies only need to change when data egress policies need to change. SecureCircle Zero Trust data security for endpoints doesn't impact users and workflows and protects data by default.

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

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