SecureCircle™

USE CASE

Source Code Protection

End Source Code Theft

Protect your IP

The Customer

A publicly traded Cyber Security Company (CSC) located in Silicon Valley, with 50+ in-house software developers and 100+ contract developers from several 3rd party consulting firms. CSC is also a Gartner Magic Quadrant leader, with over 3,000 customers in more than 80 countries.

The Challenge

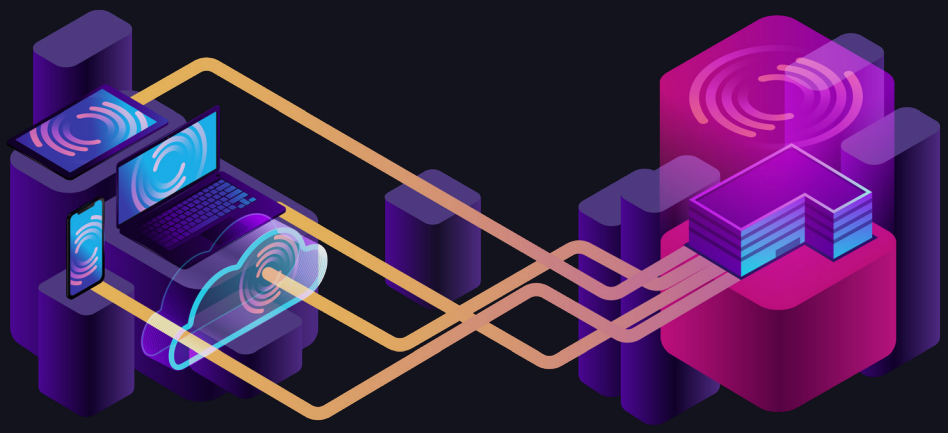
The initial challenge was how to ensure that CSC's source code that is checked-out onto developers machines from their GitHub Enterprise repository was not stolen or lost. Even though it was met with much resistance from their developers, CSC adopted a costly virtual desktop infrastructure (VDI) solution as a way to prevent loss of source code. Despite these measures, source code was still stolen. The scale of the source code theft is still unknown.

The Solution

CSC adopted SecureCircle's Data Access Security Broker (DASB). Now, they transparently protect all of their source code that is checked-out onto developers machines without impacting developer productivity. Upon check-out of any source code, the source code is automatically encrypted and transparently accessible to any IDE and development tools used by the developers. For the first time, the developers check-out repositories on their own device and work using the most effective and developer-friendly tools, applications, and workflows. And CSC has persistent access control over source code on the local machine.

Prior to DASB, engineers were limited by VDI; they struggled with simple tasks like taking screenshots, copying/pasting, and collaborating on code. With DASB, they complete assignments in their preferred way, ensuring greater engagement and efficiency. Upon check-in of source code, encryption is released to allow the internal repository tools, such as diffmerge, to continue to operate as expected.

DASB addressed CSC's challenges, ensuring source code is never lost or stolen.



DASB addressed additional CSC's concerns, including ensuring source code can only be sent to the approved company repository. This eliminated the risk of data leaking into unapproved and unmanaged repositories/locations that are vulnerable to hackers and CSC's competitors.

To further protect against accidental or intentional data breaches, DASB also transparently protects any modification or recreation of data - in this case, CSC's source code - that has been protected by DASB. The content-based MagicDerivative™ understands the data DNA of protected content. When data DNA is found in another file, regardless of how the protected data ended up in this other file, that file is automatically extended the same protections and access policies as the original data.

The Outcome

CSC is now protected against source code theft; they have full protection of all source code and derivative works. Any action taken on protected data is tracked and becomes an auditable event. The costly VDI software is no longer used, resulting in cost savings from significantly lower licensing and decreased operational overhead. Source code is accessible from any approved device and by any approved process, allowing developers to focus only on features and functionality. This has resulted in improved morale and productivity among internal and external developers, as well as considerable cost savings for CSC.

About SecureCircle

SecureCircle's Data Access Security Broker (DASB) eliminates data breaches and mitigates insider threats, with no impact to the end-user experience and no modifications to applications and workflows. Data is always protected at rest, in-transit, and in-use; no matter where it is created, consumed, stored, modified, or shared. Headquartered in Silicon Valley, SecureCircle delivers the world's first data-centric protection for a zero-trust world.

SecureCircle™

SecureCircle.com

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