SecureCircle®

USE CASE

Source Code Protection

End Source Code Theft

Protect Your Intellectual Property

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

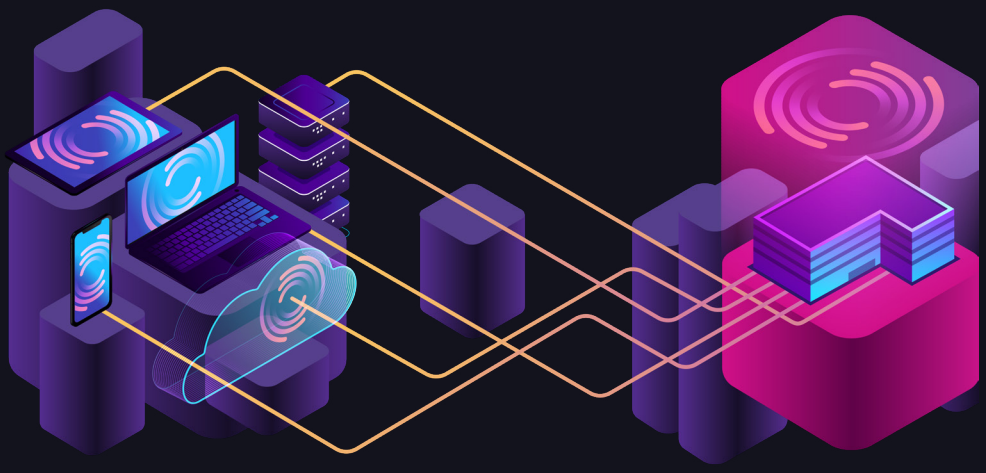
CSC needed to ensure that their source code was not stolen or lost. A costly virtual desktop infrastructure (VDI) solution, was implemented to prevent misuse and add accountability for developers working with source code. This was met with resistance from their developers. They were extremely limited by VDI. Developers struggled with simple tasks like copying/pasting, taking screenshots, and collaborating. Despite employing VDI and other defense in depth strategies, source code was still lost. The scale of misuse is still unknown.

The Solution

CSC adopted SecureCircle's Data Access Security Broker (DASB). Now, all of CSC's source code is protected, transparently, without impacting developer productivity.

Upon checkout of any source code, the data is automatically encrypted and transparently accessible to any development tool. For the first time, developers can check out code on their personal devices and work using the most effective and developer-friendly tools, applications, and workflows. CSC has persistent

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



access control over the data on any device it resides. CSC chose to release encryption upon check-in to allow internal repository tools, such as diffmerge, to operate as expected. With DASB, developers' complete assignments in their preferred method, ensuring greater engagement and efficiency.

CSC discovered that DASB was able to address other risks. DASB enforces that source code can only be transmitted to the approved company repository. This eliminated the risk of data leaking into unapproved and unmanaged repositories or locations that are vulnerable to hackers and CSC's competitors.

DASB protects any modification or recreation of data transparently. In this case, DASB discovered CSC's source code had been copied to numerous locations throughout the enterprise. DASB automatically applied the appropriate access control policies to the newly discovery data. SecureCircle's, content-based MagicDerivative™ understands the data DNA (dDNA) of protected data. When protected DNA is found in another file, regardless of how dDNA ended up in the file, that file is automatically extended the same protections and access policies as the original data.

The Outcome

CSC's source code can't be misused. Source code and derivative works are fully protected. Protected data is tracked, and any action is an auditable event. CSC realized considerable cost savings, in addition to, improved morale and productivity among the entire enterprise and external developers. VDI software is no longer used. This lowered license costs and decreased operational overhead. Source code is accessible from any approved device and by any approved process, allowing developers to more efficiently focus on business requirements.

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