

Case Study: Clipboard, Processes, and Temporary File Protection SDK for DLP Product (India)

Areas: Data Leakage Prevention (DLP), Data Security, Security Application protection, Encryption

Client: India-based (NDA protected name)

Project started: 2010

Duration: 18 person-months, 11 calendar months.

The Situation:

The DLP (Data Leakage Prevention) solution market is highly competitive, and it is rather hard to enter it with something really new. One of the India software market leaders accepted this challenge and started development of the new DLP system. When basic architecture was developed, the company initiated research of the ways to increase competitive benefits of the solution, create additional data protection levels and program self-protection modules.

The idea to engage external experts was good in several aspects. First, it would allow the team to use the new expertise and get independent valuation of the solution. Second, it would allow the company to conduct development simultaneously in 2 teams thus reducing product time to market.

The Problem:

The company specialists composed the list of possible vulnerabilities and corresponding solutions to discuss with expert team and then implement. It was decided that general solution would be an SDK as this format was the most suitable for the development team and was a universal tool to deal with a wide range of tasks.

A team of IT Security experts with wide expertise was required. The company's managers met Apriorit team at the RSA conference. After several discussion sessions, Apriorit profile was discovered to be perfect for this project.

Work started with the research and discussion of the vulnerabilities and solutions list. After the joint discussion sessions, the working direction list was created and pilot project task was formulated.

The Solution:

Three main tasks were stated:

1. Analyze and block start of some processes during the application work (application self-protection, additional data protection).
2. Prevent copying data via system and application clipboard (clipboard protection).
3. Encrypt all temporary files created by such applications like MS Word and others, on driver level.

The first one, besides implementing process monitoring and blocking, was a pilot project aimed to try Apriorit team and perform basic research to describe the general work scope. Team for that task was composed of 1 Developer, 1 Quality Assurance Specialist and Project Manager. The project was estimated and successfully finished in 3 person-months.

After the teams had analyzed the results of the first stage, the client approved plans for the next stages of SDK development.

Project team was extended up to 3 Developers, which specialized in Driver Development, and 2 Quality Assurance Specialists; team work was coordinated by the Project Manager. Team was working on the 2 subsequent project stages simultaneously.

While the pilot task mainly required the team to apply neatly its expertise, two other tasks were more challenging.

Thus, the complicacy of clipboard protection task was that besides the system clipboard, a number of applications, e.g. MS Word, use its own custom clipboard with a specific architecture. Developers were to create a universal tool and provide smooth work with any clipboard having “hidden” the specifics of its functioning into SDK. This task was successfully implemented in 6 person-months.

Temporary file encryption discovered to be the most challenging task in terms of technology. Initially, it was planned to implement redirection of files to the encrypted storage and providing applications with the file images. After in-depth research had been finished and the client and Apriorit specialists had discussed this task, the new technical approach was proposed for the client’s consideration. It was encryption/decryption of the files for the specified applications on the fly using dynamic keys. This approach enabled to significantly shorten the terms of the solution development and, at the same time, improve its reliability at the architecture level. Thus, the development according to the initial approach was estimated in 2 person-years; and team managed to implement the proposed one in 8 person-months.

The really challenging aspect of this task was to create as universal tool as possible, while there are a lot of application that create temporary files. Quality Assurance team created extensive compatibility test plans, which included both popular and specific applications, in particular those working on the Asian market. In sum, team checked SDK compatibility with 707 various applications; at the same time, they were gathering statistics about various program behavior, formulating general and specific rules about how various applications work with various files.

To provide as universal and configurable tool as possible, the detailed rule system was created. Using the combinations of these settings, developers could apply the SDK to virtually any application working with data.

One more challenging aspect was to turn on/off the runtime encryption depending on the type of the file currently processed by the data application (temporary data file, or, for example, configuration file). Meanwhile, the application was to work as usual, providing all available functionality. To resolve this task, an intellectual system of rules was created; it classified the files to be used and made a decision to turn on or do not turn on the encryption for a file, basing on the gained application behavior knowledge.

It was not also a trivial task to integrate all developed functions into one SDK and synchronize their work.

After the SDK had been deployed, Apriorit team continued working with the client specialists helping them to configure the system for the particular tasks.

The Impact:

The project took 18 person-month and was completed in 11 calendar months. Developed SDK was integrated to the DLP product that enabled to create advanced protection and some unique security features, which are to become a strong competitive advantage of the product on the market.

What's next?

Get the **free estimation** of time and effort for your project! After initial research, we'll provide you with the basic task dropdown and estimates indicating approaches and tools we can use to save your budget.

All we need is a brief project description sent to the info@apriorit.com with "RFP" mentioned in the subject.

Apriorit Inc.

Headquarters

Plehanova str. 34B,
Dnipropetrovsk, Ukraine
49000

Phone

+380 (50) 340 1747

Web

info@apriorit.com
www.apriorit.com

The logo for Apriorit Inc. features the word "apriorit" in a lowercase, sans-serif font. The letters "a", "p", "i", "o", and "r" are green, while the letters "i", "o", "r", "i", and "t" are orange. The "i" and "o" in the second half of the word are slightly larger and more prominent.