



Combating Software Piracy with Intelligence

Large PLM Software Vendor Chooses V.i. Labs' CodeArmor® Intelligence to Quantify Piracy and Generate Piracy Leads to Recover Revenue

Background

A leader in Product Lifecycle Management (PLM) and CAD/CAM/CAE software solutions has over 35,000 customers worldwide with product revenues approaching \$700M a year. The company was aware that its software was being pirated, but did not know the extent or how widely it was actually being used by organizations where revenue could be recovered. The company had active legal and license compliance programs to reduce software piracy and was concerned with piracy rates outside of the United States. Given its emphasis on growing revenue in emerging markets and the knowledge that its software was a target of piracy groups, the company formed an anti-piracy team made up of license compliance, product management, and development representatives to evaluate additional technologies to prevent software piracy.

"We decided to pursue a detection versus prevention strategy based on our customer dynamics, release cycle, and the need for further piracy information."

— EVP, Software Solutions

Challenges

The organization uses Acresto FLEXnet (formerly Macrovision) for its license management system. Although the company had worked to secure its implementation of license management, the piracy groups consistently bypassed licensing and activation controls using binary patches – meaning that subsequent releases would also be subject to this threat vector. The company originally pursued protection technology to secure the company's licensing technology against reverse engineering and extend the time it took piracy groups to crack their software. However, several other factors contributed to pursuing a detection and piracy lead generation strategy instead of applying software protection:

Lack of data – Although piracy group activity was evident, there was no data to quantify the number of businesses actually *using* its software illegally.

Existing piracy leads process – The company had some success with internal and external legal services such as Business Software Alliance (BSA) programs and manual piracy leads from hotlines and whistleblower programs. As a result, the company felt that forensic evidence from actual pirated software installs would add leads and accelerate revenue recovery efforts.

Customer risk – The company has more than 35,000 customers and a large partner ecosystem and felt that software protection could introduce technical challenges.

Mature product and market – The company had a mature product line and was concerned that preventing piracy on a current release would not stop the use of its still highly functional previous releases.

Solution Evaluation

After weighing the technical risks as well as the lack of current data on pirated software use, the anti-piracy team decided on a detection strategy over prevention – especially given the maturity of the products and the number of customers using them. The organization evaluated adding an internally-developed piracy detection and reporting capability, but ran into several limitations:

- **Creating a data collection and reporting system** – based on experience from previous attempts to build “phone home systems,” building the data reporting capability in a way that the legal and sales organizations could filter the data and build reports was cost prohibitive.
- **Piracy detection and stealth operation** – The team felt that they had limited knowledge to develop these capabilities and would rather leverage commercial alternatives and companies with security experience.
- **Lead management and reporting** – collecting piracy data and acting on it required workflow, configurable reporting, and a secure method to view and act on data. The team felt it was cost prohibitive to build this internally.
- **Multiple products** – The company has multiple products that are targeted by piracy groups and therefore a commercial off the shelf solution would be easier and more cost effective to implement compared to a custom designed solution.

Solution and Implementation: CodeArmor Intelligence from V.i. Labs

The anti-piracy team chose V.i. Labs as its partner to implement piracy detection and reporting into the company's major product line and provide additional piracy analysis services.

V.i. Labs' CodeArmor Intelligence solution was selected for the ease in which it could be integrated into current products, its ability to stealthily report data, and the fact that it provided a turnkey system to meet the detection, data collection, and reporting requirements. Because the solution would only trigger reporting when a tampered version of the software was actually used, the CodeArmor Intelligence process minimized any impact to the existing licensed customer base.

CodeArmor Intelligence's integration with Salesforce.com met the requirements for a secure method to access piracy data as well as a flexible interface to report and create dash boards on piracy use. In addition, because of CodeArmor Intelligence's gateway architecture, the group felt that the data could eventually be integrated with their own internal CRM system with minimal effort.

The product management and development team was able to integrate and test the CodeArmor Intelligence capability into their flagship product within 30 days. Within 120 days after general release of their software, over 1,500 reports of infringements were being collected daily and that number is steadily growing. After reviewing the data, the piracy team saw immediately actionable leads and the legal team has begun acting on them. In addition to leads generated by the piracy group crack releases, the reporting indicated that 30 percent of the data was generated from individual end users who have been replicating the binary patch process and have been using the software unlicensed far prior to the actual releases by the piracy groups.