CASE STUDY

# Reducing Piracy and Growing Revenue with Stronger Customer Relationships

## A customer-centric approach to piracy based on compliance analytics data

### CUSTOMER

Leading global provider of simulation software for electrical, fluid, and mechanical engineering

### MARKET

Over 40,000 customers worldwide, more than $800M in annual revenue

### CHALLENGE

Convert pirates to paying customers, while building customer relationships instead of straining them

### PROGRAM OWNER

Executive management

### SOLUTION

Use Compliance Intelligence data to thoroughly understand infringements and infringers, and successfully convert them to purchase

### RESULTS

- Generated nearly 130 new settlements in one year
- Expanded to EMEA markets with one of Revenue Services, earning $3M USD in the first eight months

## Revenera Customer

Our customer builds state-of-the-art software used by electrical, fluid, and mechanical engineers to simulate large scale engineering problems and create more successful designs. Using this software, engineers can predict how their product designs will work in the real world, optimizing performance and cost as their products are manufactured and then used in customer environments. Our customer's installed base of more than 40,000 companies includes most of the world's largest industrial firms, as well as many midsized and smaller companies. Every day, its products drive innovation in sectors ranging from aerospace to chemicals, heavy machinery to health.

## The Customer's Challenge

Our customer determined that software piracy represented a significant threat to revenue. Cracked implementations of it's high-value flagship products were in widespread distribution; meanwhile, sales representatives and channel partners pointed to specific accounts and prospects where business was being lost to piracy. Going forward, our customer faced a major strategic decision: should it attempt to protect its software, or focus on detecting and monetizing piracy?

The company's developers had already spent four years working with hardening technologies. The results weren't promising. It could typically protect a new software version for three to six months before safeguards were circumvented by crackers and unauthorized software was widely distributed. As management concluded, if its software were desirable enough, crackers would find a way to render protections meaningless: there could be no absolute protection from piracy. The company's prior experience also made it skeptical of claims that hardening would have minimal impact on legitimate customers' user experience.

Our customer had an additional problem, its customers were engineers who'd recently come from academic environments where piracy was ubiquitous. Even if not all of them were comfortable pirating software, they all knew how easy it was to do.

Facing such odds, the company decided not to divert valuable time and resources to a well-intentioned hardening strategy that would inevitably fail. Those resources would be dedicated to creating new, high value features—and the company would focus its anti-piracy strategy on detection and monetization.

In doing so, the company needed to protect its customer relationships and its reputation at all costs. Several principles would drive its program. First, the compliance team's mandate would not be to generate revenue directly. Rather, it would gather and develop intelligence about activities in its marketplace, share that information with sales, and collaborate with sales to use that information: both for the company's long-term benefit, and for the long-term benefit of infringing organizations. Second, the company would start by assuming that piracy was the result of an individual's bad decision, and that it wasn't corporate policy to turn a blind eye to piracy. It aimed to help honest customers stay honest. Third, its goal would be solely to sell its software, not to seek penalties or damages; and it would litigate only in the most extreme circumstances.

## The Solution

For this strategy to succeed, the company needed rock-solid detection data—and for that, it turned to Compliance Intelligence. As the company's technical experts gained confidence that Compliance Intelligence would capture the data it needed, its business decision makers performed a detailed ROI analysis, and concluded that Revenera's solution would likely pay for itself after generating even a small number of successful leads.

The company quickly embedded Compliance Intelligence in two key products. Meanwhile, its compliance and sales teams worked together to build lead management processes to be triggered by the thousands of infringement "pings" it was now capturing from Compliance Intelligence every day.

The company developed a blueprint for success: one that combines Compliance Intelligence data with a well-articulated set of processes for revenue recovery.

## The Results

The company started with a single product, closing 16 new deals in its first year: more than enough to pay for its investment in Compliance Intelligence. The following year, it closed 25 new deals. Then, it deployed Compliance Intelligence into additional products, and closed deals with nearly 130 new prospects. As it scaled up its use of Compliance Intelligence data, it maintained a very high conversion rate: worldwide, 75% of cases that progress to a customer contact lead to new revenue.

As the customer's business has grown organically and through mergers, it has extended its use of Compliance Intelligence with an enterprise license, and integrated it into six key products. Concurrently, its compliance team grew from two individuals to a decentralized organization, reflecting growing confidence that it could recover more money without significant risk to either its brand or its customer relationships.

Building on its success in North America, the customer wanted to expand its compliance program into other regions, but did not have local resources. For assistance, it turned to Revenue Services. Collaborating with Revenue Services, the company now uses Compliance Intelligence data to recover revenue in many additional markets. These include EMEA markets where the company didn't have compliance staff or couldn't support local languages.

The company's turnkey arrangement with Revenue Services follows the same strict rules designed to protect and nurture customer relationships. Through a Force.com dashboard, Revenue Services prepares detailed information about infringers based on the data Compliance Intelligence is generating, and the company's regional sales managers approve every lead Revenue Services pursues.

The company pays Revenera only when a sale is closed—and, in the first eight months of this relationship, Revenue Services has used Compliance Intelligence data to close $3,000,000 in new business. In addition to growing compliance revenue without increasing overhead, Revenue Services provides valuable expertise in privacy law and IP management.

## Successful Lead Management Blueprint

- Infringement data worth pursuing is vetted and triaged by compliance team.
- Leads that won't result in revenue, such as infringements from Chinese state-owned universities, are discarded.
- Starting from Compliance Intelligence data, compliance analyzes infringing companies: the extent and locations of abuse, working environment, geopolitics, likely motivation, and other factors.
- The company reconciles Compliance Intelligence data against its own CRM database, often discovering prospects that earlier chose not to purchase.
- Compliance presents the full picture of the infringement to sales.
- If sales determines that pursuing an infringement will irrevocably damage a customer relationship, it is not pursued.
- If the teams agree to move forward, compliance builds a complete narrative report of the infringement.
- The company contacts the infringer's senior management, presents an offending IP address, and asks the executive to investigate and resolve the situation. The company stresses that it isn't seeking damages, but wants to serve needs that exist at the infringer's organization.
- Many companies immediately admit to the illegal usage and agree to negotiate payment. Occasionally, a customer acknowledges only a small, possibly inadvertent infringement.
- If necessary, compliance can often demonstrate far more extensive infringement. At that point, the prospect usually agrees to resolve the infringement quickly.

**NEXT STEPS**

Turn Software Piracy into Revenue

LEARN MORE >

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**