revenera™

COMPLIANCE INTELLIGENCE

Building and Expanding a $20M Revenue Recovery Program

Leading PLM developer transforms pirates and abusers into paying customers, and develops reliable knowledge for worldwide audits

An engineering design software provider with customers throughout North America and Europe built a successful new compliance program from scratch.

CHALLENGE

- Strengthen intellectual property protection by detecting piracy in the company's flagship product
- Converting pirate users to paying customers
- Actively pursuing audits to verify contract compliance wherever overuse may exist, worldwide

SOLUTION

- Implement detection strategy, rapidly deploy Compliance Intelligence
- Build collaborative processes to leverage data without compromising existing relationships
- Leverage Compliance Intelligence-based data and knowledge more widely, worldwide

BENEFITS

- Built a $20M/year revenue recovery operation that delivered one new 7-figure deal per quarter
- Gained reliable knowledge about patterns of piracy and overuse that now supports a highly-profitable complementary auditing strategy
- Increased the number of transactions associated with piracy and misuse from 300 in 2014 to more than 700 in 2017

Challenges quantifying the impact of piracy and finding the right approach to address it

Our customer's PLM products integrate people, process, and system management, helping companies accelerate time to market, increase productivity and quality, improve product development, and cut costs. A global leader, it serves over 35,000 customers worldwide, earning $1+ billion in annual revenue.

The company knew pirates targeted its software, and strongly suspected that piracy impacted sales. But it did not understand the extent, nature, or financial impact of these attacks, and could not respond effectively.

Sales opportunities were dying on the vine even though customers were still active, and suspicious behavior was often identified by technical support teams during support conversations. Identifications of apparent piracy were unpredictable and incomplete, because the company only discovered them when infringers interacted with it. So, too, the company had no way to quantify piracy or misuse that scaled across company's facilities.

Since no compliance practice then existed, sales teams were asked to handle apparent infractions. But sales teams were rarely trained for these types of contentious issues. They worried that data might be incorrect, and were concerned about alienating customers. Product management was also reluctant to launch compliance engagements that might prove unwarranted. The result: most infractions went unresolved.

To begin planning a more effective response, the company established a new anti-piracy team. Its team quickly discovered that piracy groups were cracking licensing and activation controls in an average of 32 days, with revenue losses beginning soon after. The consistent failure of protection mechanisms led them to refocus on detecting piracy, and treating detections as leads for a compliance team to engage separately.

Decision-makers concluded that starting with an audit-based compliance program would be too invasive and would require extensive software asset management skills the company didn't possess at the time. So, too, building and maintaining a "phone home" system with the capabilities it needed would be cost prohibitive.

Capturing and acting on piracy data would require complex workflows, highly configurable reporting, strong security, and flexible support both for specialized systems sold by sales teams and simpler products sold online. Software wouldn't be enough: the company needed a partner with experience and skills to monitor new cracks, ensure proper detection, and help transform detections into sales.

Compliance data drives new license revenue

Revenera addressed the company's detection, data collection, reporting, and analytics requirements in one turnkey solution. The company found Compliance Intelligence easy to embed, had virtually no impact on licensed customers. Revenera's Salesforce.com integration ensured secure access to piracy data, and its flexible, intuitive dashboard easily integrated with the company's existing CRM system—streamlining management of piracy-related leads throughout the sales process.

> *"Based on our customer dynamics, release cycle, and the need for further piracy information, we decided to pursue a strategy of detection, rather than prevention—and it has worked exceptionally well."*
>
> **—VP OF PRODUCT DEVELOPMENT**

The company deployed Compliance Intelligence within weeks. Then, cautiously and incrementally, it began capturing data, pursuing pirates, and learning from experience:

- The legal team quietly began to collect data. To assess opportunities, it began contacting carefully-chosen “non-customer” pirates.
- As their knowledge grew, legal and sales teams gradually widened contacts with pirates in North America.
- Legal and sales established procedures to safeguard relationships, handle objections, revise licenses, protect privacy, and escalate through appropriate channels to enforce compliance.
- In connection with a major upgrade, the company extended its program to most North America piracy data. Within six months, revenue recovery soared.
- The company rolled out Compliance Intelligence throughout Europe, with similar results.
- As sales grew confident in compliance processes and Compliance Intelligence data, it assumed primary responsibility for detecting piracy to generate revenue.
- With compliance revenue growing rapidly, more compliance expertise was needed, so the company hired a Compliance Director. Over time, the company began moving key products to a subscription model that generated lower payments but offered a more reliable revenue stream. The compliance team knew that there would be challenges adopting the new subscription model, since an annual subscription fee was nearly half the value of a perpetual license. During the first few years of implementing its subscription model, the company settled infringements using Perpetual and Subscription models, seeking to understand the impact of using Subscription licensing in each region, and tracking its success.

Revenera best practices recommend that software companies require two years of subscription payments as part of all settlements. On its own, the customer validated that Revenera best practice was the optimal approach for its own subscription-based recoveries. As it has moved towards a 100% subscription model, it has also begun requiring two-year contracts for all compliance transactions.

Through all these phases of developing its compliance systems, the company gained extensive experience with the processes, security, infrastructure, and privacy/GDPR methodologies it and Revenera had established for capturing and using compliance data. Based on its experience, it also had growing confidence in its understanding of piracy’s effects and the value of compliance initiatives. Reflecting this confidence, it was now ready to implement new programs aimed at enforcing licensing and monetizing overuse based on additional misuse patterns worldwide.

Compliance Intelligence was already validating "word of mouth" piracy reports from APAC whistleblowers and resellers, accurately profiling pirates and developing strong cases for raids. But the company had learned so much from Compliance Intelligence data that it could also confidently audit many customers where outright piracy did not exist, but indications of potential license infractions were present.

The compliance team built an audit methodology designed to identify misuse patterns such as out-of- territory use, where software was purchased in one region and used inappropriately in another.

In some cases, audit candidates possessed both instrumented and non-instrumented products. Since the telemetry gave strong indications of overuse in products instrumented with Compliance Intelligence, the company could be confident that it had good reasons for requesting an audit. Compliance Intelligence instrumentation also helped validate whether the customer was reporting completely and truthfully during the audit.

Building on success

Within 120 days of deployment, Compliance Intelligence began generating large numbers of actionable leads in the US; by the third quarter after deployment, revenue recovery for its flagship product soared from $90,000 to $1 million. The same explosive growth was soon replicated in European markets. Through these and other anti-piracy initiatives built on Compliance Intelligence data, the company grew revenue recovery to $20M, driving several seven-figure enterprise deals.

A small anti-piracy program that had begun in the legal department migrated to sales, grew, and worked so well that the company built a full-fledged compliance department. The team grew from three practitioners to upwards of 20—reflecting its consistently high return on investment. Meanwhile, the number of transactions associated with monetizing piracy kept growing: 300 in 2014, 500 in 2015, 615 in 2016, and more than 700 in 2017.

The company is currently adding more products to the anti-piracy program. Now, the customer's growing subscription program is supported by a strong anti-piracy compliance program and a "trust-but-verify" audit program. It can select the right compliance approach for each type of misuse, limiting invasive interactions while protecting shareholder IP.

NEXT STEPS

Learn more about Compliance Intelligence.

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**