CASE STUDY

COMPLIANCE INTELLIGENCE

How a Top PLM Provider Built a $24 Million Compliance Program

Compliance that works: detection is succeeding where auditing and prevention failed

Leading global provider of Product Lifecycle Management (PLM) software generates and converts actionable piracy leads at both current customers and new prospects.

CHALLENGE

- Generate and convert actionable piracy leads at both current customers and new prospects

SOLUTION

- Deploy Compliance Intelligence in two key PLM products, then expanded to 17 products worldwide
- Track leads and performance through Salesforce.com integrated dashboard

BENEFITS

- Earned $5.6 million in new revenue in the first year
- Built its compliance program to $24 million within four years
- Consistently achieved 60-90% close rates on actionable data, depending on region

No reliable data to quantify losses to piracy or inform compliance strategy

Our customer offers a comprehensive suite of mid-range and high-end PLM products for efficiently designing, analyzing, and manufacturing products, and managing enormous amounts of design-related data.

Serving more than 70,000 customers, the company sells its high-end products directly in most regions, including EMEA, the Americas, and the Asia-Pacific region. For some mid-range products and some geographies, it leverages indirect channels.

Like many software developers in its space, it manages licensing certificates through Revenera's FLEXnet Publisher. Its specific licensing arrangements vary by product: for technical desktop applications, it uses floating and/or node-locked licenses; for high-performance computing products, it licenses based on server or CPU; and for client-server applications, it licenses by named user, offering floating licenses in certain cases.

While our customer already had a sizable compliance organization, it still faced large and growing piracy-related revenue losses.

Like many developers, it began by largely ignoring piracy, because it couldn't find reliable data to quantify losses or inform strategy. Increasingly, it was receiving support calls from non-customers; and receiving complaints from account teams, third-party distributors, and whistleblowers. Ignoring the problem became untenable.

Simple web searches quickly found illegal download sites, demonstrating that the company's products had been targeted by organized piracy groups. Cracked products were routinely available within 30 days of release. Thousands of downloads were being reported on Cyberlocker sites, and on portals such as Rutracker, Lavteam, and Hao007.

The company considered several strategies for addressing the issue:

- It considered auditing, but rarely had rock-solid proof of piracy, didn't have the internal skill sets to run audits, and realized that its targets were often strategic customers. Maintaining strong relationships with these customers was critical, and audits were often viewed as hostile. Software contracts were often complex, making full compliance difficult or debatable. Auditing would inconvenience customers, and audit requests gave intentional pirates time to cover their tracks.
- The development team's first instincts were to further harden their software. But this presented technical challenges, and might impact properly licensed customers. Moreover, crackers were exceptionally sophisticated, and knew licensing management systems inside and out. Certain best practices might help a bit, but cracks were now appearing in days, not months. Prevention was a losing strategy.
- Could the company sue pirate sites? Perhaps, but most were run from locations where enforcement was difficult—and pirates could easily move elsewhere.

Choosing the best solution

To capture the piracy data its compliance and sales organizations wanted, the company selected Compliance Intelligence based on several key criteria:

- Compliance Intelligence is transparent to the end user, and won't impact application performance
- Compliance Intelligence is configurable to detect piracy whether caused by tampering or counterfeit license files
- Compliance Intelligence is easy to integrate with the company's existing software build processes
- Compliance Intelligence is fully compatible with the company's existing licensing system and enforcement technology
- Compliance Intelligence offers strong capabilities for detecting, transporting, and reporting on data from multiple sources and networks

"We've realized that piracy cannot be addressed by licensing and DRM alone. Viewing it as a marketing opportunity has enabled us to implement a license revenue recovery program that's adding millions of dollars to our bottom line."

—VP OF LICENSE ENFORCEMENT

If these strategies wouldn't work, what would? The company's compliance and sales organizations realized they could transform piracy into a revenue opportunity, if they could reliably detect it.

Many infringing organizations were either current or prospective customers. Some were accidentally overusing software; some weren't aware of abusive individuals; some temporarily overused software on specific projects. At many of these companies, leadership was committed to paying what they owed. Elsewhere, cracked software was in use simply because a company needed a solution. If handled properly, some of them might pay, too. Sales increasingly viewed piracy data as a valuable new source of leads, and viewed detection-based compliance efforts as marketing support.

Given this customer's large and sophisticated sales organization, it chose to host its own gateway servers and Salesforce.com dashboard, which links tightly to its own enterprise CRM system. (Other customers choose to rely on Revenera for hosting the middle layer and back end of their Compliance Intelligence deployments.)

Through the Compliance Intelligence dashboard, the sales and compliance teams can securely track a wide variety of piracy-related leads, both individually and in the aggregate. As with any lead management system, they have up-to-the-minute information about:

- Leads created, current quarter and year to date
- Unique machines and infringements, per month and application
- Closed won opportunities, by month and current quarter

The company is also beginning to discover new ways to use software usage analytics to add value and increase profitability. For example, it can gather information on feature usage that can help shape development programs, refocusing programmer resources in areas that customers are most interested in.

Generating new license revenue and growing a successful compliance program

Our customer began by deploying Compliance Intelligence into two key PLM products. Within just three months of deployment, it had identified 271 actionable non-compliant organizations, and successfully settled with 21 of them.

Based on these early successes, within six months, our customer integrated Compliance Intelligence into two more products. Since then, it expanded its use to five products, then 14, and now 17. Starting with deployments throughout Europe, it has expanded its use of Compliance Intelligence worldwide.

Using Compliance Intelligence data, the company has discovered that roughly half of its piracy comes from existing customers, and half represents entirely new customers. Within one year of deployment, both streams of leads had generated approximately $5.6 million in new license revenue.

But that was just the beginning. Within four years, the company had built its compliance revenue streams to $24 million. Equally impressive, it consistently achieves close rates of 60-90% of actionable data, depending on region.

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**