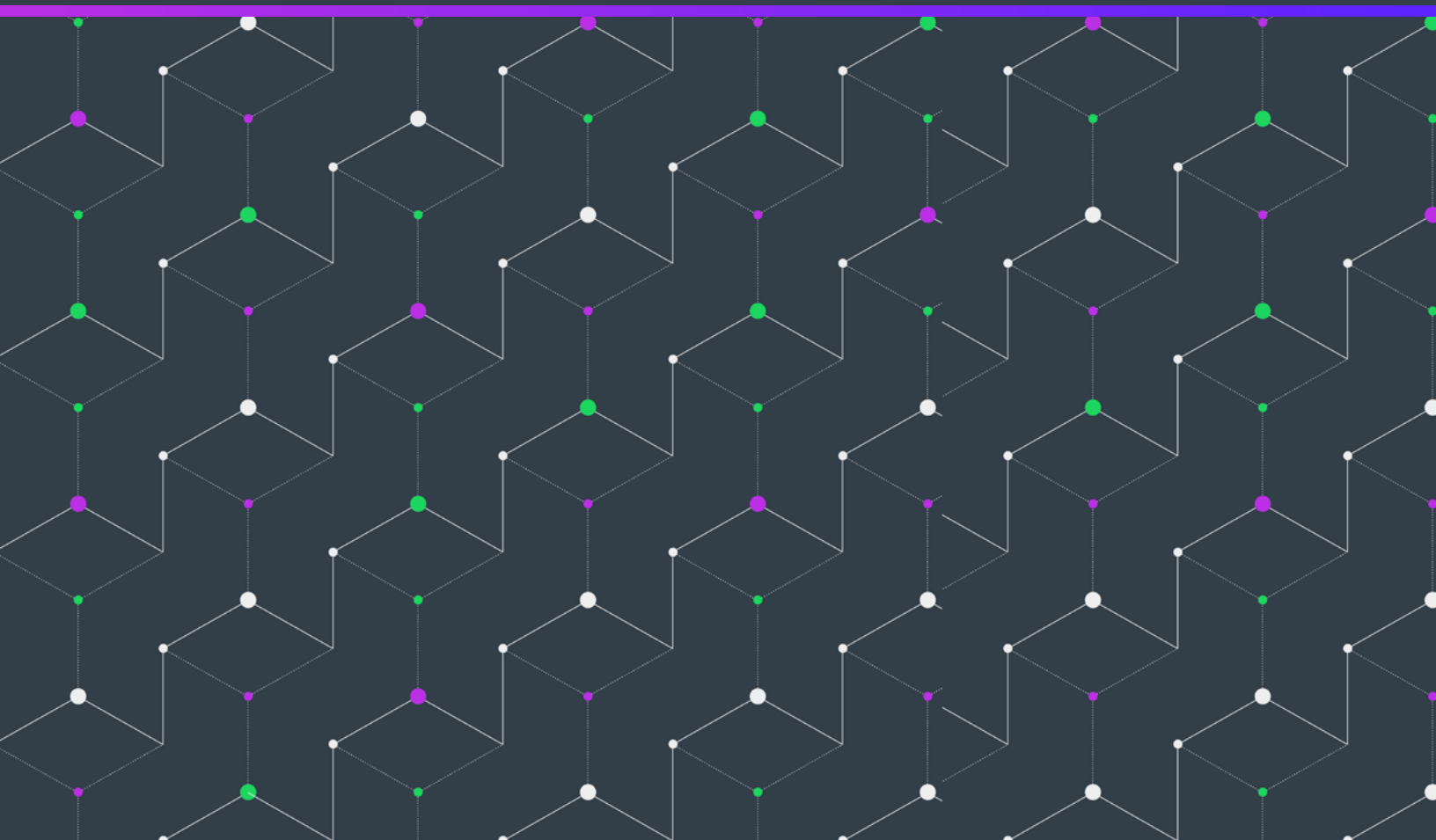
WHITE PAPER

revenera

Profiting through Software Intelligence:

A Layered Approach to License Compliance



Executive Summary

Since the emergence of the commercial software industry, software vendors have struggled to overcome piracy. Software theft has cost developers billions of dollars, sometimes making the difference between sustainable profit and unsustainable loss.

To protect their intellectual property, software vendors have evolved four common approaches to piracy: licensing systems, software protection, internal compliance, and legal action. Each approach has strengths and weaknesses, separately and in combination. Even so, for most software vendors, piracy remains a costly and unsolved business problem.

In this white paper, we demonstrate how the use of software intelligence can significantly strengthen your overall license compliance strategy, and improve its effectiveness. You'll learn how layering software intelligence with your current techniques can add value to each of them, helping you transform surprisingly large numbers of pirates into paying customers.

What Existing Methods Can and Cannot Accomplish

When software vendors apply conventional approaches to countering piracy, they often assume that they've addressed the problem as well as possible. Often, they haven't. To understand why, it is important to clarify what each method can and cannot achieve on its own.

Limitations of Software Licensing Tools

Most packaged software vendors rely on licensing tools as a foundational strategy. Whether homegrown or purchased from a third party, these tools help keep customers honest, and may help vendors track entitlements. However, a higher level of protection is achieved when licensing tools are augmented by a dedicated compliance analytics solution.

Licensing software varies, and may provide few (or no) tools for tracking unlicensed usage or identifying overuse. While it's sometimes possible to capture very basic data—for example, by pulling logs—this data is cumbersome to work with. Worse, the data is often insufficient for making a reliable business decision about a customer's compliance status.

Moreover, one primary piracy attack vector is to disable or bypass licensing altogether. If this occurs, a software vendor gets no information about how its application is being used, or by whom.

Limitations of Software Protection Strategies

Software protection is more directly aimed at preventing piracy. However, most software vendors have discovered that standard techniques only delay piracy—often, only briefly.

Software vendors often struggle to balance the advantages and costs of advanced protection. What's more, since application software runs on top of an operating system that they don't control, even these protection measures rarely prevent piracy for long.

Limitations of Internal Compliance Methods

"Internal compliance" usually means auditing. Audits are a useful component of any license compliance strategy, but the way companies identify infringing customers and conduct audits is usually far from optimal.

Internal compliance specialists typically profile customers to identify and target those at high risk for overuse, even if there's no solid proof of infringement.

For example, an audit might be triggered if salespeople complain that a fast-growing company has just rejected a proposal for additional licenses, if customer support reports calls from users not in the customer database, or if a whistleblower exposes a former employer's infringements. Either way, audit triggers are often anecdotal. The resulting audits can be time-consuming and injurious to the customer relationship.

Ideally, audits should be carefully targeted at clients where infringement is significant and already essentially proven, with incontrovertible data. But internal compliance programs rarely know enough to be this confident in advance.

There's one more major problem with audits. They rarely involve noncustomers, who may or may not have agreed to a license agreement containing audit rights.

Limitations of Legal Action

Many software companies invest heavily in monitoring piracy channels and issuing takedown notices. While large developers such as Adobe and Microsoft have made it less likely that purchasers will inadvertently pay for pirated software through channels that appear legitimate, pirate channels are resilient: the pirate community typically creates new ways to deliver their cracked wares.

For all but the very largest companies, the cost and complexity of pursuing legal action against pirate sites and channels often exceeds the benefits, which—if they occur at all—may be only temporary.

Poor Data + Poor Analytics = Minimal Revenue Recovery

None of the solutions we've discussed, either separately or in combination, offer adequate insight into how your product is being used, or by whom. This means, at the very best, they might be able to temporarily and modestly reduce piracy. But they do little or nothing to help you recover revenue and generate new opportunities.

All four approaches are hobbled by a common problem: software vendors don't have the right data or analysis tools. Adding software intelligence solves this problem.

Software intelligence comprises a set of technical and business solutions for detecting, collecting and analyzing application usage, so you can:

- Detect true unlicensed use
- Validate infringements and identify infringers
- Gain accurate and complete data about unlicensed use, so you can provide actionable follow-up opportunities to your compliance teams

Adding software intelligence helps you discover the many infringers who will pay. Many software vendors have used it to earn millions of dollars or euros in incremental revenue—all without compromising valued relationships.

In the following sections, *we'll show you how*, drawing on examples from the industry's best-in-class solution for delivering software intelligence: Revenera Compliance Intelligence.

How Compliance Intelligence Enhances All Your Anti-piracy Strategies

The best-in-class Compliance Intelligence solution adds value to all four core strategies for addressing piracy:

Enhancing licensing strategies. Compliance Intelligence gives you complete visibility on the use of your pirated software, even when licensing has been disabled. It delivers far more information than even a properly working activation system ever could: everything from the number of pirating users on each device to accurate identification of your pirate's true location.

What's more, Compliance Intelligence enriches this data to help you analyze the full scope of an organization's piracy, infringement, and overuse, as well as trends over time. For the first time, you can accurately compare true usage to entitlements, and understand exactly what you're owed.

Enhancing software protection. Compliance Intelligence alerts vendors when a new version of point release has been cracked, and provides missing information for identifying users, so these can be converted into paying customers.

This gives you highly-granular information about the effectiveness of your software protection methods. You can use this new knowledge to make better decisions about which protections to apply in each product and market, optimizing tradeoffs between protection and cost.

Enhancing internal compliance (auditing). Compliance Intelligence replaces "suspicions" with specific, reliable, and detailed forensic evidence of overuse and piracy.

By utilizing Data Optimizer to enrich captured data, vendors can discover the full extent of a company's infringement across divisions and locations worldwide, in real-time. This highly efficient "data-driven auditing" can tell you who is abusing your software right now, and how long they've been doing so. This information is delivered in ways that are fully consistent with your contract rights, and without the infringer's awareness.

You now have crucial knowledge for prioritizing compliance efforts. Instead of relying on "profiling" or guesswork, you can confidently target proven infringers whose piracy crosses a threshold that translates into meaningful revenue.

When physical audits are necessary, they are consistently fruitful: costly and counterproductive "fishing expeditions" are eliminated. You can simply exercise your routine contractual auditing rights, *but you already know what you'll find, and where you'll find it.*

You've also reduced internal friction among functional areas within your organization. Without real proof, sales and compliance are often reticent to approach a possibly non-compliant customer and risk the relationship. With proof in hand, sales and compliance teams become more comfortable doing so.

Enhancing legal response. Using Compliance Intelligence, you can learn more about piracy distribution channels, more quickly. In certain cases, you may be able to execute takedowns. Based on experience, this will not always be possible: piracy distribution channels are resilient, and takedowns are resource intensive. But, with detailed information about who is using your pirated software, you can start viewing pirate sites as yet another distribution channel to manage for profit.

Experience consistently shows that a significant number of pirates in many markets—even those using obviously illicit sites—can be converted to customers. Moreover, you can encourage conversion through in-app messaging campaigns and by gradually degrading software features—options that were previously unavailable to you.

Layering, Not Replacement: A More Powerful Approach

Traditional approaches to countering piracy are still necessary. However, adding software intelligence helps you drive more value from all of them.

Software vendors of all sizes have repeatedly proven this. For example, using Compliance Intelligence:

- A leading Product Lifecycle Management software vendor built a $20M annual compliance program, averaging one new 7-figure deal per quarter
- A top engineering simulation software provider generated 130 settlements in its first year, widened its compliance program to EMEA, and earned $3M there in eight months
- A leading provider of prosumer creative tools is using in-app messaging to convert 3%+ of its enormous global base of pirates to paying customers

You can also achieve results like this—without complicating development, management, or your customer's experience. To do so, you need a software intelligence solution purpose-built to capture full and accurate infringement information, and make it actionable. You need partners to help you make the most of what you're learning about infringement, and optimize your response for every product, market, and customer.

If you're ready to maximize revenue recovery and build profitable relationships where only pirates existed before, Compliance Intelligence is your bestin- class solution—and Revenera is your best-in-class partner.

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**