



KEYnote 43

THE WIBU - MAGAZINE

The Many Opportunities and Few Risks of Software Subscriptions

Highlights

- Creating and Delivering Cloud Licenses Made Easy
- CodeMeter Protection Suite – The Multitool for Software Protection
- Protecting Standalone MATLAB Applications



Content

SECURITY

Geoblocking - Limiting Access by Geographies 4

PROTECTION

Protecting and Monetizing IP in Additive Manufacturing 5

LICENSING

Creating and Delivering Cloud Licenses Made Easy 7



LICENSING

The Many Opportunities and Few Risks of Software Subscriptions 9

PROTECTION

CodeMeter Protection Suite – The Multitool for Software Protection 11



PROTECTION

Protecting Standalone MATLAB Applications 13



SECURITY

Professional Response to Security Incidents 15

HIGHLIGHTS

News in Brief 17

INFORMATION

Wibu-Systems Training 18

Dear Clients and Partners!



Our IT Security Club has become the place to meet and mingle with likeminded professionals, spark interesting conversations, and share in the innovation network with other companies, start-ups, and researchers active in the field. If you want to know more about membership opportunities, come and visit us at: www.wibu.com/itsc.

And remember to use CodeMeter and our Protection Suite to protect your know-how and create new license-driven business models to make your software and devices more secure in today's world! With CodeMeter, updating software and configuration files becomes as safe and secure as it ought to be, and would-be attackers have a much harder time – at no additional cost for you.

Read this issue of KEYnote to find out how to protect MATLAB applications, create software subscriptions, secure 3D printing data, use the many tools and capabilities of our Protection Suite, create and distribute cloud licenses, or limit licenses by regions.

I always love hearing about your current needs, plans, and wishes for the future. Reach out to me or come and visit us at one of the upcoming trade fairs – there is nothing better than meeting people who care about the same issues that I care about.

Kind regards,

Oliver Winzenried

CEO

Our CERT team is tasked with responding to security incidents and analyzing and removing vulnerabilities. The team is also there for our customers, providing them with information and advisories to help them understand possible vulnerabilities and find workarounds until an update is ready to fix the issue.

ALERT

One idea at the right time
can change everything.

Subscribe to our blog





Geoblocking – Limiting Access by Geographies

Depending on the type of product they are selling, software vendors often have to contend with different legal requirements and access restrictions in different countries. Some things simply cannot or must not be sold in some countries. But how to comply with these restrictions? One solution is geoblocking.

Geofiltering and geoblocking sound dramatic, but the terms refer to something that virtually everybody has experienced at some point. We all have a favorite streaming service or Internet radio, but if we try to catch up on our local news on holiday, we often encounter a familiar error message: “This function is not available in your region.” This is particularly common in TV streaming services: We cannot watch our usual shows, because they are not licensed in the country from where we are accessing them. Or we are trying to watch our favorite team’s latest match, but we suddenly find that the match is only carried on pay TV in this country. What gives, and is there a way we can get around such restrictions?

These restrictions can be applied because, in theory, every time anything is accessed via the Internet, the IP address of the Internet location can be identified and linked to a real-world location. IP addresses are assigned to telecommunications services providers, which helps understand which country the user is based in or, more specifically, from where they have accessed the Internet.

This points to one of the essential weaknesses of the method: Technologies like virtual private networks can establish a tunnel to access the Internet from a completely different geographic location. It would appear to the world that the user is located at the end of that virtual tunnel. Still, not everybody has such a VPN connection.


IP addresses do not necessarily translate directly into exact geographic locations. There will be cases in which data is assigned to a country that the user is not actually located in, and the allocation of IP addresses to regions is constantly being changed by different providers and projects.

Despite these two reservations, geoblocking is one of several powerful means to restrict access to content or services. If access is restricted in this manner, it can safely be assumed that any user circumventing the restrictions does so consciously and deliberately. Medical technology is an interesting case in hand: Devices and software often need to pass separate certification and approval procedures in every country. To make sure that the certified prod-

ucts are only used in the countries they were certified for, vendors can either take certain precautions in their sales process, e.g. with separate online shops, or they can use CodeMeter licenses and take the right measures to allow their activation only in specific geographies. Whatever the user tries to do to circumvent these restrictions, the vendor has done everything in their power to prevent this.

Many software developers rely on Wibu-Systems’ Operating Services to handle their license management via CodeMeter License Central. The system works through certain user-facing interfaces, WebDepot or Gateways, which can be restricted for selected countries to prevent CodeMeter licenses from being activated in regions where they should not be.

The same restrictions work with CmCloudContainers: Software vendors can restrict access to their licenses for defined regions.

If you are interested in geoblocking, please visit our support services at <https://support.wibu.com>. 



Protecting and Monetizing IP in Additive Manufacturing

Additive manufacturing has truly arrived. When the first 3D printer was introduced back in 1987, it was the start of a long and often arduous journey until we learned how to print 3D objects at the required quality and at a competitive price. In all this time, one issue was often and undeservedly pushed to the sidelines: What about protecting 3D printing data from piracy? And how can print jobs be tracked and billed correctly and securely for everybody involved?

The Rise of Additive Manufacturing

As so often happens when highly complex technology is concerned, the story is not one of a single solution or one-time eureka moment, but of long and patient work on countless individual problems and issues that needed lots of time and experience to solve. People had already begun thinking about 3D printing in the 1970s, but it would take until 1987 for the physicist Chuck Hull to come up with the first working model. A generation later, it has become normal for objects to be designed on one side and created on the other side of the world, even combining different materials. What started as rapid prototyping, i.e. the ability to quickly produce prototypes of an object, has turned into a means to produce individual parts, custom products, or even entire production runs. Now, manufacturers are working hard on integrating additive manufacturing even deeper in their production processes. And why should they not? The benefits are obvious: Complex and unwieldy supply chains can be trimmed back, the carbon footprint of each product suddenly shrinks sig-

nificantly, and on-demand production without slow and complex tool engineering means a faster time to market and the ability to roll out new business models.

This is not to say that there are no challenges remaining in the field. But one key aspect that is an essential element of any viable additive manufacturing business models keeps getting overlooked. The designs and data for additive manufacturing need to be protected at every link in the chain, and there needs to be a transparent and tamper-proof way to count, track, and bill the number of printed objects.

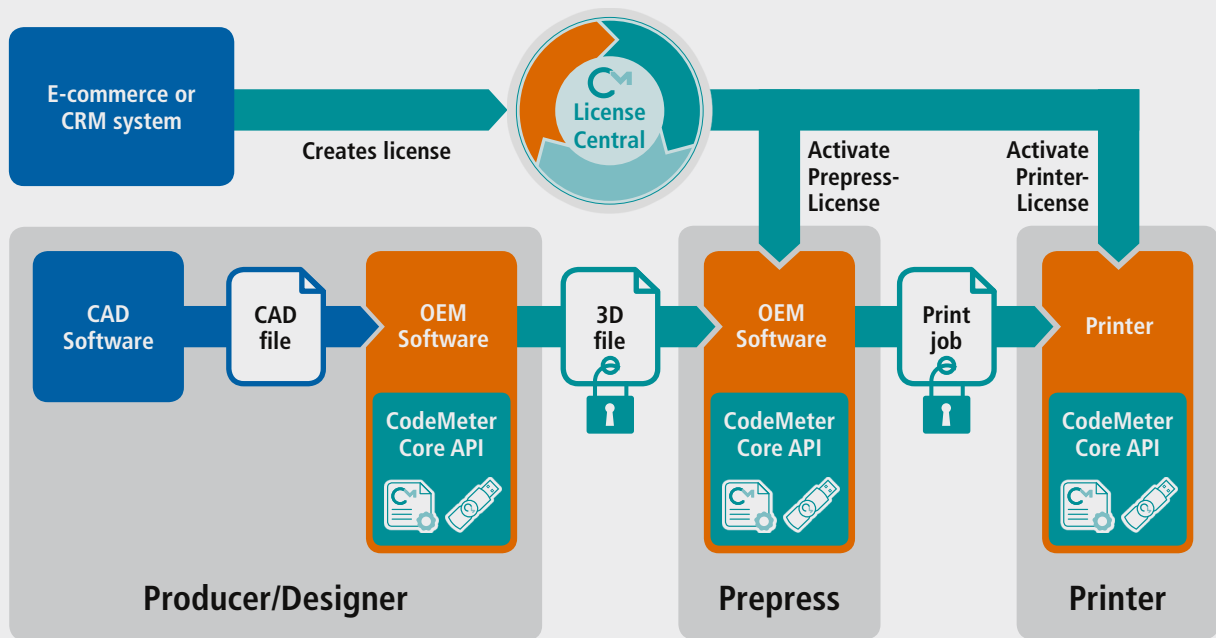
The Additive Manufacturing Process

To understand why this matters, we need to understand how a 3D design becomes a printed object and who is involved in that process. It all starts with the development of a digital object, which contains or represents a crucial piece of intellectual property. This asset needs to be protected, because only protected IP can be marketed in any sensible way. This should not be a problem if the holder of

that IP is actually the same person or business doing the processing and printing as well. But the 3D printing market is moving in another direction: In many cases, the digital object will be only one component of a whole array of pieces that an integrator would assemble into a finished product, and the printing happens outside of the direct control of the IP's owner. Commercial concerns mean that the actual printing business will be dominated more and more by specialized 3D service providers. In essence: there has to be a way to protect a digital object, but also to legitimately guide it through an entire process chain with many different actors involved.

Prepress and Printer: Different Licenses for Different Purposes

At first sight, this seems to be an unsolvable proposition, but the same situation has long been solved in the software business, where software protection and license management are (or should be) commonplace. The CodeMeter technology by Wibu-Systems uses tough cryptographic standards to encrypt digi-



The entire process chain for additive manufacturing combined with protection and monetization

tal IP, while also making it easy to distribute the necessary keys to handle it in the form of licenses – securely, around the world and around the clock, and fully integrated in existing process chains.

A concrete example can illustrate how this works. Imagine an automotive enterprise that is taking its B2B parts business into the digital realm. It already has a shop system in place where registered commercial clients can order parts. This system is integrated seamlessly with the company’s order management system to make the entire process as smooth and automated as possible. Today, the spare parts are physically delivered through a well-oiled, but complex logistics machine. But tomorrow, they will be sent as encrypted files, ready for download.

The buyer would receive a specific processing license to prepare the printing process. Another order-specific printing license then defines how many copies the customer can create of the object he has bought. The illustration captures this process in a nutshell.

CodeMeter technology provides the protection and license management link between each piece in the process. The 3D designs and print jobs are encrypted with standard technology that is available as libraries for many target platforms and programming languages, including support for embedded systems thanks to Wibu-Systems’ long-standing experience in the industrial sphere. The makers of prepress software and 3D printing systems have finished libraries available to integrate IP protection in their additive manufacturing portfolio. Depending on the


conditions on the ground or the desired level of protection, the cryptographic keys can be stored on a physical CmDongle, a software container (CmActLicense), or in the CmCloud.

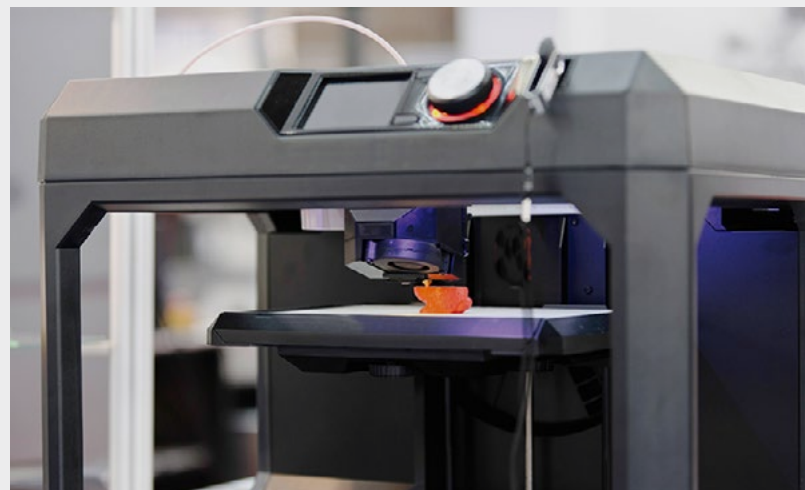
The encrypted 3D data can only be accessed if the right prepress license is available, and a printer can only create physical pieces if a printing license with sufficient print jobs is present. Both license types include the necessary cryptographic keys; in the case of the printing license, there is also a secure unit counter to keep track of how many copies of an object have actually been printed.

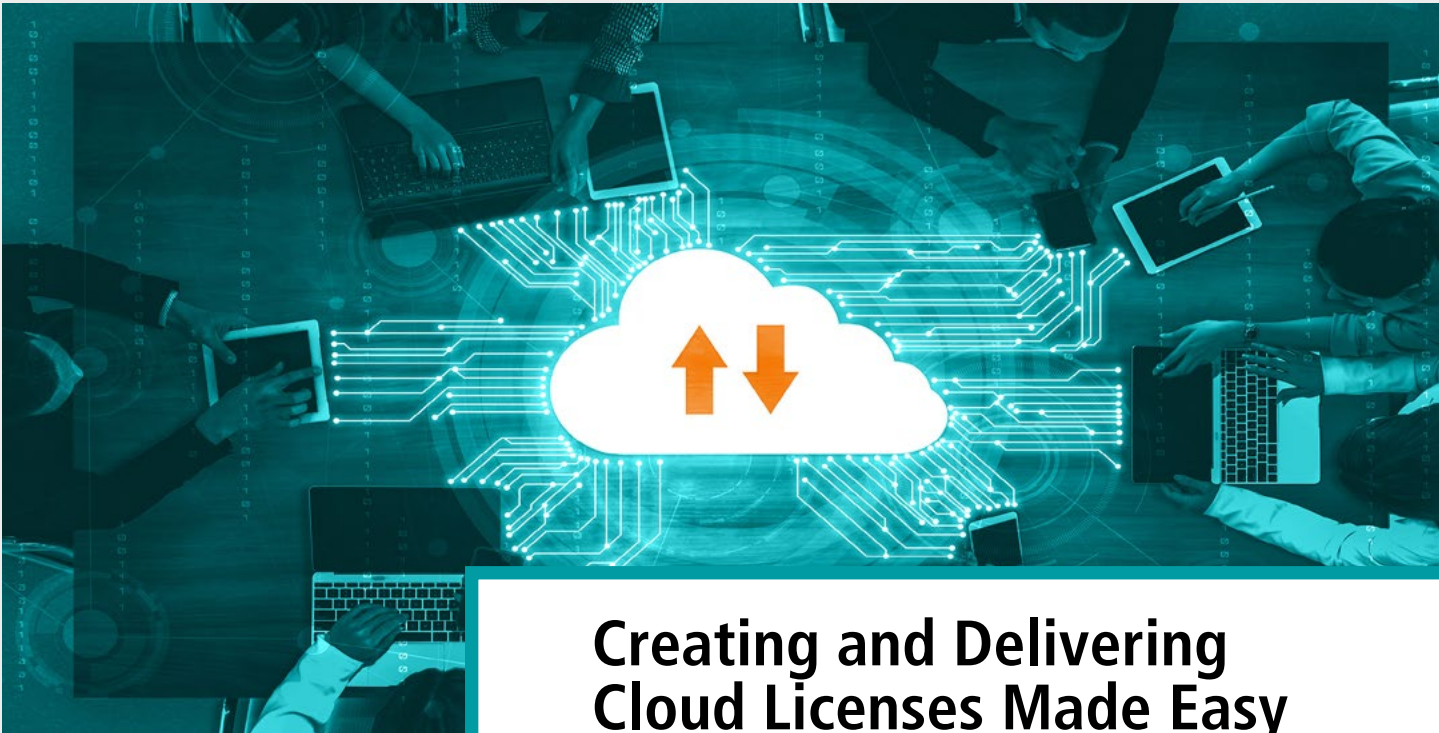
The popular CodeMeter License Central management system is available for managing and distributing both licenses. It can be readily integrated into existing e-commerce or order management systems with its set of webservice

interfaces. In the ideal case, the licenses would be delivered simply by online activation, but file transfer options are also possible for offline or otherwise separated workstations or printers.

Vision Meets Reality

Does this sound like science fiction that will never work in the hard reality of industrial manufacturing? Nothing could be further from the truth: Our automotive example is taken from real life. Working with a popular 3D printer maker and using the technology made by Wibu-Systems, the company is going live with this novel business model in 2022. It is the first tentative step into the digital future of additive manufacturing. Confucius knew: Even the longest journey starts with a single step. And we are excited about what we will experience along the road. 





Creating and Delivering Cloud Licenses Made Easy

The License Portal gives software developers a simple and flexible way to allow users to create and manage their CmCloudContainers and activate or deactivate licenses themselves. But this degree of freedom and trust does not fit in with every software project. In such cases, these abilities should be handled by a dedicated portal or separate software, where the entire license portal, including user registration, is completely hidden from viewers. This is why the CodeMeter License Portal comes with a special REST-API for the purpose. This article takes a closer look at this API, called Gateways.

The Credential File

The License Portal and REST-API represent a simple means to communicate with CodeMeter License Central and the CodeMeter Cloud. Users are given credential files with the details they need to access their CmCloudContainers. CodeMeter Cloud creates these files, but it does not store them. This is where the License Portal enters the picture: it maintains a direct one-to-one connection between a user on the Portal and a CmCloudContainer and, by implication, a credential file. Whenever a user decides to change their password, the old credential file is invalidated and a new one created. Everything happens in the background, without the user having to know what the credential file is doing for the application or the Portal. The reasons for this are psychological in nature: Users are less likely to share their passwords than their files. For even greater security, the credential file is encrypted with the user's password.

User Accounts Required

This unbreakable link between a credential file and a user account demonstrates that License Portals and CodeMeter Cloud together can only function with user accounts. There are three options for integrating this with existing solutions:

- Using the Portal's own user admin capabilities
- Creating dummy accounts for all users
- Integrating with a Single-Sign-On (SSO) system

The latter option is currently handled by Wibusystems' Professional Services, but is scheduled for release as a standard feature from version 22.11.

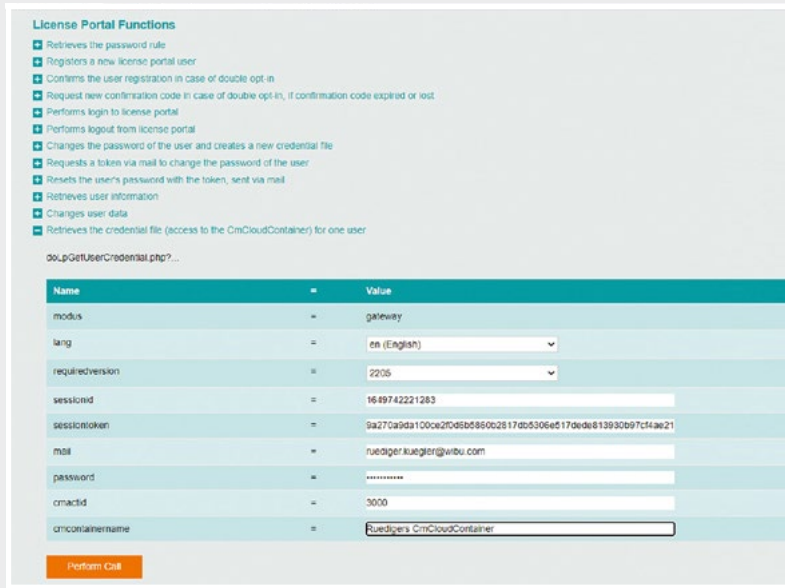
Creating Accounts

The first step in using the password is creating a user account, achieved with four parameters: "mail", "password", "data", and "ticket". The

email address ("mail") functions as a unique identifier of the user in question, which has many benefits that may outweigh the potential downsides of using email accounts for this purpose: For most users, the License Portal is something they rarely encounter, and it is unfair to expect them to remember the random name they chose for the purpose. Their email address, on the other hand, should be something they remember.

The password ("password") should be checked in a separate client before registration, i.e. the user should have to enter it twice to double-check it. Specific rules and restrictions for passwords can also be put in place, and the system can check whether the password is compliant with those rules before the proper registration starts.

The "data" field accepts entries in any format. Its purpose is to capture additional details in the form of a Json string about the users, such



as their name, age, address, shoe size etc.: Anything you want to have recorded, with only the EU GDPR regulations limiting your flexibility. The API offers an option to change or delete these entries to be fully GDPR-compliant.

The final and most interesting field is "ticket". The License Portal can define whether a ticket from CodeMeter License Central should act as a Captcha to prevent automatic bots from creating countless spam accounts. Tickets have to be fresh by the time of registration, i.e. not yet been assigned to any other user or group. To make things easier, the ticket is automatically assigned to the user in question after the finished registration process. The captcha field can also be replaced with your own anti-spam mechanism or left out entirely.

The Session

The "register" command should ideally get the user up and running immediately. It would return a "sessionid", the "mail", and a "sessiiontoken", which are then used for later API calls.

The system also informs you whether the user has to confirm with a Double-Opt-In option. This can be configured for the License Portal and would require the user to confirm a code that they are sent by email. A separate API call is used for this purpose, and the process would not continue until the user has confirmed the code.

The same "sessionid", "mail", and "sessiontoken" values would naturally also be returned if you connect the user by a later "login" API process. "logout" is used to end the session.

Dummy Users

One quite popular option is for user accounts

to be created automatically without the actual user having to bother with the process. This is a valid choice, but should still be handled with care to make sure that the automatically created profile is compliant with the EU GDPR data protection standards.

To create such dummy accounts, a mail address is created from the internal user ID, such as a virtual mail address on your own server; alternatively, the ticket ID could be used if users do not have an ID given to them.

A much more interesting question is the automatic creation of a password. Ideally, the system starting the registration process should be able to store a random value for each user, which could take the form of an entry in the user database, or some value on a local machine. This random value is defined, appended to the user ID, and hashed to get an automatic password.

Assigned Credential Files

A separate API call is used to get the credential file, which needs the "sessionid", "sessiontoken", and "mail" from the user logging in.

The password also has to be included for this purpose. Asking users again for their passwords in this manner is a good means, albeit better used sparingly to avoid irritation, to protect important functions from unauthorized use. For the License Portal, it is technically required, since the credential file is encrypted with the password.

The name of the CmCloudContainer in question can be included in this first call. This would be the name that is visible to the user in CodeMeter's Control Center. However often it is called, this refers to the same file, even if a

new name is given. To refer to the CmCloud-Container the CmActID should use the standard fixed value "3000", which is reserved for all future purposes.

When the Portal's user admin features are used, the client should require the password again before this API call or calculate the value accordingly in the case of dummy accounts.

Changing Passwords

A call to change the passwords needs the old and new passwords on top of the session parameters. Again, a simple precaution against accidental typos is asking the user to enter the new password twice.

This call invalidates the old credential file. When licenses in the CmCloudContainer are accessed next, they are flagged as "red" and cannot be used anymore. The user should then receive and import a new credential file with the new password.

Resetting Passwords

The API is, naturally, also ready for the inevitable case that a user forgets their passwords. The process uses two specific calls: The first returns a reset token, which only needs the user's email address and does not initiate any internal actions in the system. The reset token needs to be used in a time that you can set to your liking.

Usually, the token is sent to the email address stored in the system. It could alternatively be delivered via the API, but this calls for special attention to make sure that the API function in question can only be used by authorized applications.

The token then allows a new password to be created in a second call. This would invalidate the old credential file, which would have to be recreated and delivered with the new password.

Activating Licenses

Licenses are activated in the same manner as they are on CmDongles or in CmActLicenses: A context file is created for the CmCloudContainer by the local copy of CodeMeter and used for activation via the standard Gateway function. The update file produced in return is then uploaded again via the local CodeMeter copy, and if CodeMeter is not installed locally because the system is arranged as a SaaS solution, the License Portal API can step in as the middle man to retrieve the context file and return the update file (limited to CmCloudContainers).



The Many Opportunities and Few Risks of Software Subscriptions

My first version of MS Office still came on discs in a box and was paid for with Deutschmarks. It served me well for a long time, until my mail provider decided to change the security standards and my old and dear MS Outlook stopped working. This meant that I had to buy a new version of MS Office. I was very upset about having to pay good money for new versions of a software that I had been using for such a long time. In all other walks of life, nobody bats an eyelid at having to buy new versions of old products. The average European buys more than 10 cars over their lifetime. And we keep buying our favorite albums again and again, first on vinyl, then on cassettes, then on CDs, as downloads, and now streams.

The key to solving this conundrum is a subscription service: The subscriber pays only a fraction of the cost of a software package in exchange for the ability to use the software – always in its latest version – for a defined period of time. No need to pay full-retail every few years, and the subscriber still gets the newest security and safety standards guaranteed. On the other side of that relationship, the provider gets a dependable revenue stream and the certainty needed to plan and budget for future developments and new products.

Which models are there?

In the software scene, maintenance subscriptions and software subscriptions (and any combination thereof) have established themselves as the typical models on offer. With maintenance subscriptions, the user would buy the software outright in the first place and then enter a maintenance contract for access

to regular updates and, frequently, exclusive services. As long as the maintenance contract is active, the user will always get the latest version of the software, and when it ends or is cancelled, that latest version will be the one the user is stuck with (but that they can still use).

With software subscriptions, the user enters into a regular subscription contract without having to buy the software first. However, the right to use the software would be lost as soon as the subscription ends; even older versions are not available anymore. This means that the threshold for becoming a user is far lower, but the threshold for cancelling the subscription is far higher than with a maintenance subscription.

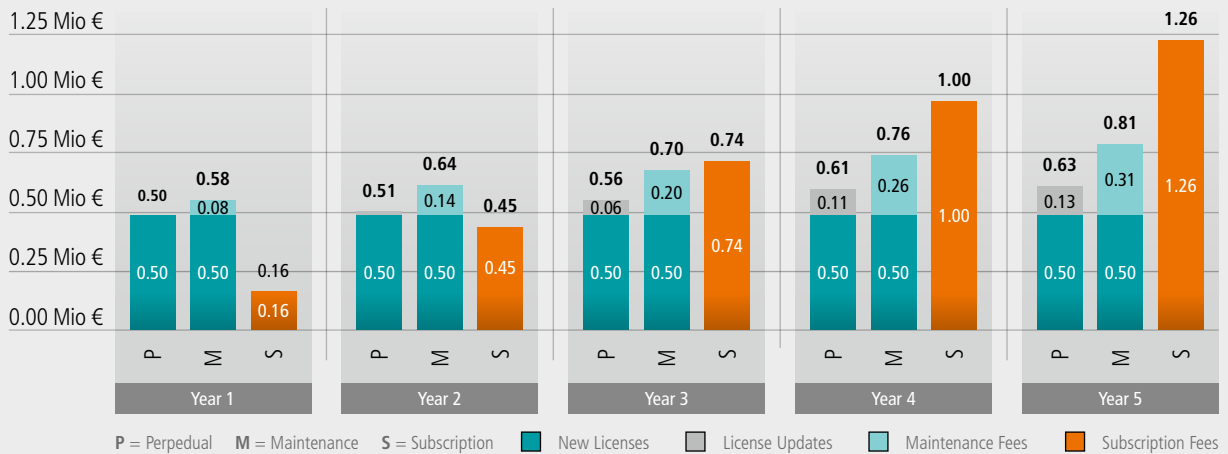
The technology behind both options is identical: Upon ordering the subscription, the user

will get a license that is regularly refreshed as long as the contract is active. With maintenance subscriptions, the period of access to maintenance services is extended (Maintenance Period); with software subscriptions, it is the license for the software itself (Expiration Time). When the contract is cancelled, the licenses will not be refreshed anymore, or the Expiration Time is set to the end of the contract.

Which pricing policy will work?

In recent issues of this magazine, we took a closer look at the technical niceties of subscription licenses. Now we need to take a closer look at the commercial considerations: Pricing and revenue. Take a concrete example: A software product that is sold for €5000.00.

Without a subscription option, the user can buy updates to the software, usually at a 50%



discount for the first two to three years from the original purchase. In our case, this would be a price point of €2500.00. If a user skips too many updates or exceeds the three-year period, they would have to buy again the entire package at full cost.

For maintenance subscriptions, the annual maintenance fee would be 12% to 25% of the purchase price, i.e. the user would pay an addition of €600.00 to €1250.00 for maintenance services on top of the original €5000.00 product license.

Monthly maintenance subscriptions would usually range between 2% and 5% of the purchase price, i.e. €100.00 to €250.00 per month in our example. Depending on the contract, payment can be per month, quarter, six months, or year.

Which opportunities and risks should be expected?

Consider the opportunities and risks for this specific example. We assume that our business gets a hundred new customers purchasing the product in the first year and that we will be able to increase these numbers by 5% year on year. We also assume that updates are offered for half of the purchase price and that half of our current customers will take us up on that offer. This immediately shows one of the typical risks of a purchase model: Without exciting new “killer” features, very few users will be tempted to buy every single update.

For a comparison with maintenance subscriptions, let us assume that 75% of our users buy a maintenance contract at 20% of the purchase price and that 10% of these will exit their contracts every year.

For a subscription license, we can assume a monthly fee of 4% of the purchase price, only 5% churn per year, and 25% more customers attracted by the more appealing payment option. Since users who cancel their software

subscription cannot enjoy their product anymore (compared to maintenance subscribers), far fewer of them will take this drastic decision and stop using the software altogether.

The comparison shows how subscription licenses outperform conventional purchases in the long run – even if only 25% more new customers can be sold on the new model. The data does reveal that a revenue slump needs to be expected in the first years, especially if an established product needs to be transitioned to a subscription service. Introducing subscriptions needs persistence and perseverance. A good compromise is to introduce new products or new markets under the subscription model and to let older products slowly run their course.

Maintenance subscriptions, by comparison, are essentially risk-free, while also promising attractive revenues over the long haul, especially if customers can be kept on board. It is not unheard of for established companies to get substantially more revenue from maintenance subscriptions than from new licenses.

The eventual business plan for a new subscription service has to take the market and customer preferences into account in every case, and any sample calculation or projection can only serve as a general point of reference for decision makers.

Everybody Wins?

The advantages for providers are plain as day: With maintenance subscriptions, but even more so with software subscriptions, they win new, lasting, and predictable revenue streams at lower commercial risk. But the users also benefit, again especially with software subscriptions. The most immediate gain for them is the far lower entry cost. Instead of spending €200 to €300 for the full suite of MS Office products, they only need to pay €10 a month for the subscription. Another advantage may not be as obvious at first, but will soon make

itself felt: Subscriptions usually mean constant access to the most recent software versions with the most recent security standards. No need to buy a new software version again when the next update rolls around.

A greater feature set is another typical advantage. The typical buyer will only spend for the applications and features that they need at that moment, whereas a subscriber can get access to a larger, often complete set of features and functions. This can be as simple as certain functions in Excel that most would have never noticed if they had not been included in the subscription – but which quickly become a favorite choice if one has them available.

Subscriptions have become the norm in the music industry, and they are becoming normal in the car industry. Who still buys CDs? Most people subscribe to a streaming service to get all the freshest beats without spending a penny extra. True, most people will not listen to all of the music library. Who in the world would be an avid fan of Brazilian metal, Euro-pop, and 80s one-hit wonders at the same time? As these examples and the success of video streaming sites have shown: The subscription age is here to stay. 📺



CodeMeter Protection Suite – The Multitool for Software Protection

Every software vendor knows: To monetize your software, you use licenses. But what about protecting the invaluable know-how that is invested in the software? Algorithms, parameters, and data do not grow on trees. They are paid for with hard cash and lots of effort. Let's see how CodeMeter Protection Suite helps you as the go-to tool for all your software protection and licensing needs.

Been Hacked Yet?

For many businesses, it happens like a bolt out of the blue: Suddenly, their software sales slump in select niches or across all of their markets. Or users might be contacting them for support even though evidently they never bought the software. This is a bad sign: Pirates have been at work and either released a clone of the software with similar capabilities or started selling the original software without the legitimate licenses. In whichever form it comes, the situation will definitely be catastrophic for the original vendor. And the long arm of the law is often not long enough to reach the culprits everywhere on our planet.

The Way to Go: Encrypt and Sign

Control is what CodeMeter Protection Suite excels at. In essence, it is an encryption and licensing tool for a range of platforms that makes integrating protections and licensing easy. It achieves exceptional levels of protection by combining its specific encryption capabilities with cutting-edge anti-debugging and anti-reverse-engineering measures, right in the protected application.

CodeMeter Protection Suite also uses signatures to check whether code has been tampered with (code integrity).

Dynamic Decryption for Maximum Security

To achieve the optimum in protection against typical types of attacks like memory dumping, applications protected with CodeMeter Protection Suite have their functions and methods decrypted dynamically during runtime. Depending on the programming language in question, this can happen automatically (with .NET, Java, JavaScript, or Python), or the methods that need to be dynamically decrypted are flagged as such in the code.

Protection and Licensing in Harmony

In most cases, protection and licensing will go hand in hand. This is what CodeMeter Protection Suite does best, because the cryptographic keys used to encrypt the software are already securely built into the licenses defined with a Firm Code and Product Code: When encrypting an application (executables and libraries), you enter these two codes and receive an ap-

plication protected with the right cryptographic keys in return. There is usually no need for any changes to the source code.

The end user needs the right license to access the protected application, stored for each user in a container of your choice, either a portable CmDongle, an encrypted license file (CmActLicense), or in a cloud container bound to the user (CmCloudContainer).

Finding the Right AxProtector

AxProtector is available for a wide selection of programming languages, including the popular choices in the table on the following page.

AxProtector and Available Expansion Modules

All versions of AxProtector come with a standard set of features to encrypt and license applications, even if the protected application consists of multiple executables and libraries.

Modular Licensing

Applications can be sold in one package or "by the feature". For the latter case, modular licensing is the way to go. For this purpose,

Language	AxProtector Version	
Python	AxProtector Python	
JavaScript, TypeScript	AxProtector JavaScript	
Java	AxProtector Java	
C#, Visual Basic .NET, other .NET languages	AxProtector .NET	
Visual Basic 6, Delphi, FORTRAN, Visual Fox Pro	AxProtector Windows	
Tools creating machine code for Windows, e.g MATLAB	AxProtector Windows	
C/C++	AxProtector Windows	AxProtector Linux
	AxProtector Android	AxProtector macOS
C++/CLI, Managed C++	AxProtector .NET	

separate licenses (Product Codes) are created to go with each separate feature or function. Depending on the licensed feature set, the user will receive a combination of different Product Codes.

In the application, the software protection API (WUPI) checks for the licenses' presence and can hide features for which the license is missing. Dynamic decryption during runtime means that you can assign separate licenses to these parts of the application, giving each its own cryptographic key based on each additional Product Code. No attacker could decrypt these locked-off parts of the application without these keys.

IP Protection

Are you planning to distribute free versions of your software? Are you thinking about a free-mium option, with individual features requiring the user to purchase a license? Or do you want to give the user a bit more leeway even

if a license might be missing, which can be important in machine operating software in industry? In any case, you still want your know-how protected.

By contrast to the standard approach, the encryption for the IP Protection mode is not bound to a CodeMeter license. Instead, the decryption keys are securely hidden away in the application itself. This means that the application would start even without a license container present. This is a clever choice for combining with modular licensing to keep the paid features especially protected e.g. in free-mium models.

CodeMoving

For optimum security, machine code can be executed in a CmDongle or CmCloudContainer. This is made possible by turning the particularly critical code into a C source file that is compiled and placed as a binary, encrypted blob in the application during the protection process.

During runtime, the code is called up by a special API, transferred onto the CmDongle or the CmCloudContainer, decrypted, and executed with the relevant input parameters in that secure environment. The output is then fed back as a response to the API call.

File Encryption

This module is used for the quick and easy protection of data files. The file in question would be protected by CodeMeter Protection Suite and can then only be opened and accessed by applications encrypted with the same parameters, and only if the right license is present.

Supported Platforms

The typical platforms for use with standard PCs are already covered by the basic version of AxProtector.

If you are developing software for embedded devices, an additional AxProtector license will be required for each target platform, i.e. for a combination of operating system, processor type, and (in the case of Linux) the chosen standard library.


The table below helps you find your way around the different options.

Supported Development Environments

All AxProtectors can be used in Windows and Linux-based development environments, and AxProtector macOS is available for direct use on macOS.

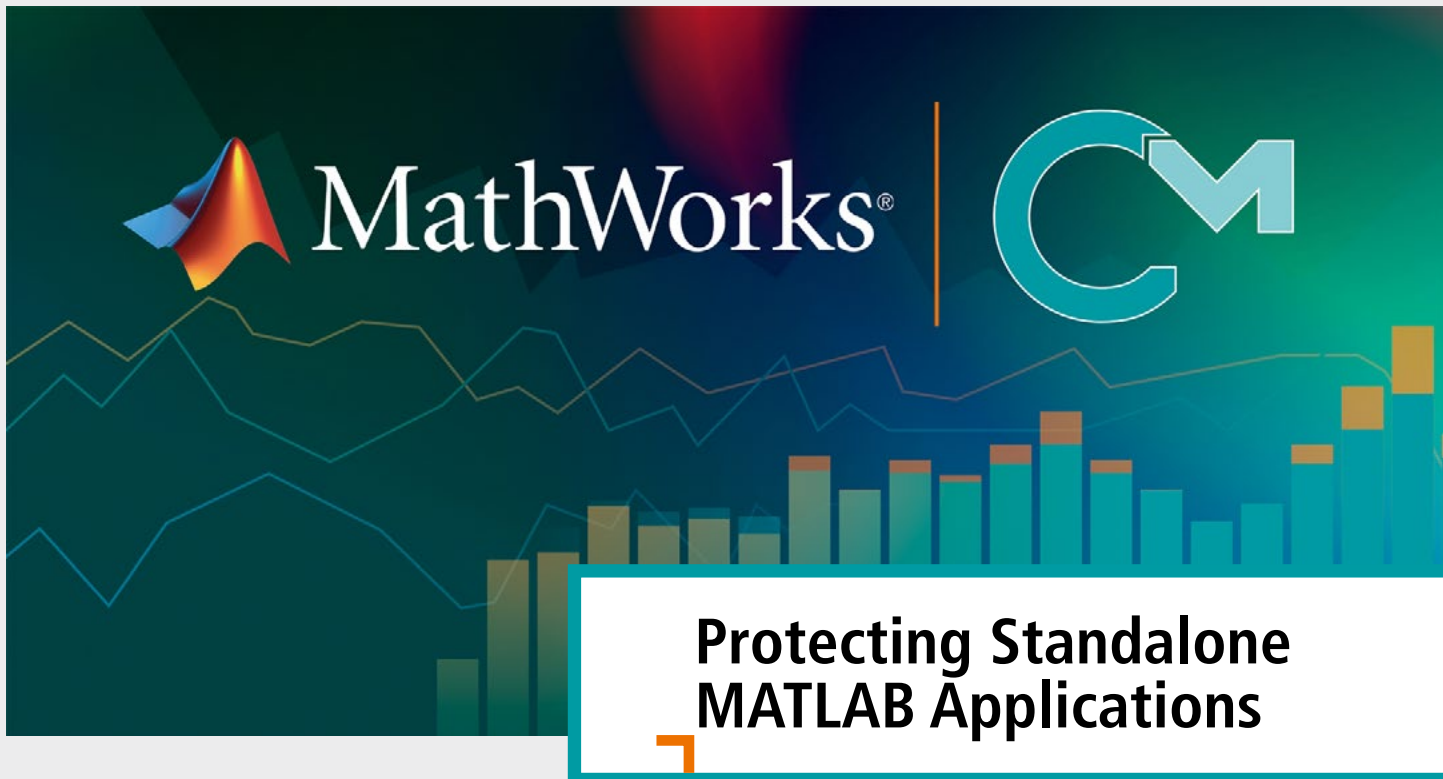
Stay Up to Date with an AxProtector Subscription

Since early 2022, AxProtectors have been available by subscription to help you be sure that you are always using the most recent version and benefitting from the latest state-of-the-art security functions.

The subscriptions are timed to go for one year, renewing automatically unless you cancel your subscription. With your automatic renewal, the updated licenses for your AxProtectors and options are immediately available for you to pick from the license portal. 

Target platforms	AxProtector Windows	AxProtector macOS	AxProtector Linux	AxProtector .NET	AxProtector Python	AxProtector JavaScript	AxProtector Java	AxProtector Android
Windows x86	✓	–	–	✓	✓	✓	✓	–
Windows x86_64	✓	–	–	✓	✓	✓	✓	–
macOS x86_64	–	✓	–	✓	✓	✓	✓	–
macOS ARM	–	✓	–	✓	✓	✓	✓	–
Linux x86 glibc	–	–	✓	–	✓	–	✓	–
Linux x86_64 glibc	–	–	✓	✓	✓	✓	✓	–
Linux ARMhf glibc	–	–	✓	✓	✓	✓	✓	–
Linux AArch64 glibc	–	–	✓	✓	✓	✓	✓	–
Linux x86_64 musl	–	–	optional	optional	optional	optional	optional	–
Linux ARMhf musl	–	–	optional	optional	optional	optional	optional	–
Linux AArch64 musl	–	–	optional	optional	optional	optional	optional	–
Linux MIPS glibc	–	–	optional	optional	optional	optional	optional	–
Android ARMhf	–	–	–	optional	optional	optional	optional	✓
Android AArch64	–	–	–	optional	optional	optional	optional	✓

■ Included target
 ■ Planned target
 ■ Optional target
 ■ Planned optional target



Protecting Standalone MATLAB Applications

Engineers, scientists, economists, and the mathematically inclined everywhere swear by it: MATLAB by Mathworks Inc., the numeric computing solution of choice for millions of users. Born as a research project in the 1960s, MATLAB, short for MATrix LABoratory, soon developed into a firm favorite among science and engineering students and was eventually commercialized in the mid-1980s. Even after decades in the field, MATLAB remains the go-to solution for numeric calculation purposes like those common in scientific computation, which can, by their nature, become unwieldy for the symbolic computation of regular computer algebra. Many of the algorithms used by professionals in many industries, from aeronautical engineers to stock market whiz-kids, are made possible by MATLAB.

It's a MATLAB World

From its humble beginnings, MATLAB has evolved into a wide array of tools built around its unique programming language and libraries. Its toolbox has grown to cover a fast range of applications, from financial mathematics to rocket science, and the versatility of its proprietary programming language means that there is virtually no limit to the mathematical operations and use cases that can be realized with MATLAB. With the ability to turn these into standalone applications with MATLAB Compiler, MATLAB is an expression par excellence of how intellectual property is born: A smart developer tackles a numerical computation or other data manipulation problem, invents a solution for it with MATLAB, and turns it into a ready-made application that can be sold to people who may not have the same

mathematical programming expertise. Especially with MATLAB's cult following among STEM students and researchers, this makes for a great opportunity for enterprising engineering talent. The growing presence of AI and machine learning on its home-turf disciplines like financial mathematics has only reinforced MATLAB's prominence in the field.

But every opportunity will attract unwanted attention, and MATLAB tools and applications are no exception. IP theft and the threat of manipulation are constant concerns, especially as the stakes are particularly high here. Invaluable and exceedingly expensive intellectual resources are invested in most applied MATLAB technology and may be at risk of theft. Even worse, potentially incalculable financial or material damage is likely if an attacker managed

to sabotage the mathematical software that makes algorithmic trading, space flight, or power grid management possible.

This is the essence of CodeMeter's mission: To protect not just what is dear to us, but also what lets us excel, as professionals, companies, or entire communities. With Wibu-Systems' IT security, protection, and licensing expertise and just a few tiny tweaks to the regular CodeMeter workflow, it becomes easy to secure standalone applications made with MATLAB compiler and monetize them with the full power and comfort of CodeMeter.

A Case Study in Simplicity: Protecting MATLAB Applications

Applying CodeMeter protections to a MATLAB standalone application could not be simpler:

All that is needed is a version of AxProtector, a Firm Code, a Product Code, and just a few minutes of the developer's time.

The Firm Code is a seven-figure code assigned by Wibu-Systems to a user of AxProtector along with the developer's master dongle, the Firm Security Box. It is needed to create unique licenses with CodeMeter. Whether it is older Firm Codes issued specifically for use with hardware CmDongles or software CmActLicenses, with numbers of 100,000 and higher, or the new Universal Firm Code for all types of license containers, starting at 6,000,000, every Firm Code is fit for purpose for protecting and preparing the licensing for MATLAB standalone applications.

The Product Code is chosen by the developer for each item to be protected, using a simple integer format. This can be entire applications or individual functions and features. With the Firm Security Box capable of handling 4 billion options, this leaves enough freedom to organize the portfolio of protected and licensed applications on offer to match virtually any business model.

To encrypt the application in practice, AxProtector first asks for the source file and a destination for the protected file. The magic hap-

pens with the next important entry in the Licensing Systems tab: Among other licensing options, the developer's Firm Code and a Product Code are entered here. Together, they are used to create the cryptographic underpinnings of the MATLAB application's license.


As a final step in the CodeMeter protection process, dynamic code modification, which normally modifies the source code of the protected application during runtime, needs to be switched off for the system to work with MATLAB: Since this is not compatible with MATLAB Compiler, the option needs to be unchecked in the Security options tab. Once the application is protected, it is impossible to run it without the right license, using the same Product Code as the one used during protection.

CodeMeter has many more tricks and capabilities up its sleeve that give the developer free rein to design the protection and licensing for every business model or use case. But the simple steps laid out here are more than enough to protect any MATLAB standalone application with unbeaten encryptions and be ready to create licenses and distribute the application with confidence.

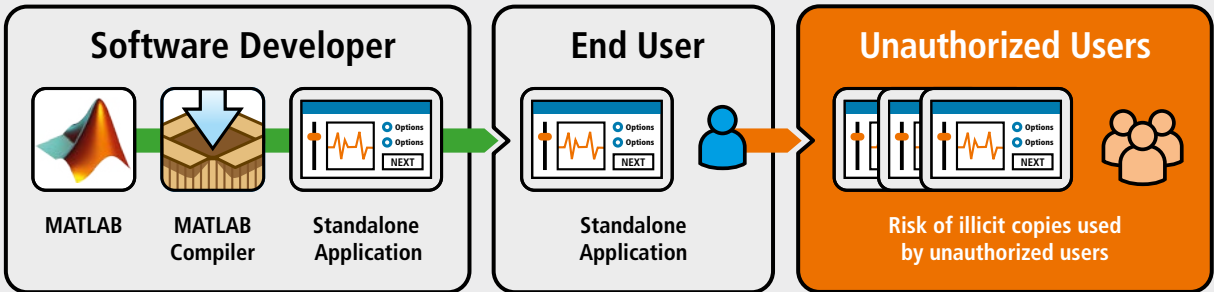
And CodeMeter makes the developer's life even easier with its excellent automation and

integration capabilities. The license creation and management process can be facilitated with many self-service options or integration with existing CRM and e-commerce systems. This leaves enough choice for MATLAB applications of every type and scale, from highly specialized solutions for a limited user group that need strong protection for the sophisticated IP that went into them to commercial applications for engineering clients that are sold through regular large-scale software distribution systems.

Made for Each Other and Made to Work

CodeMeter and MATLAB make for a perfect pairing and proof that protection, licensing, and monetization do not have to be complicated, even when the most intricate mathematical solutions are protected with the toughest and most sophisticated encryption technology. Just add AxProtector encryption and CodeMeter licensing, and any MATLAB application can be safe from hackers and thieves, be it in an engineering lab, on Wall Street, or on its way to the Moon. 

Standalone Applications without License Protections



Standalone Applications with CodeMeter Licensing

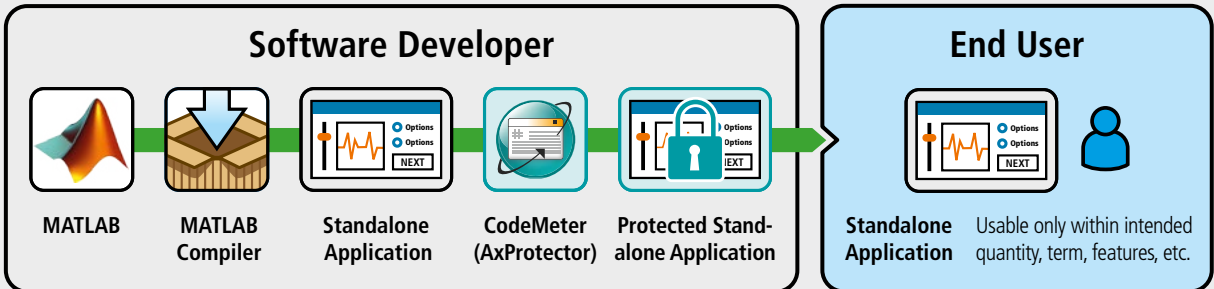


Figure 1: Comparing use cases with and without CodeMeter licensing



Professional Response to Security Incidents

In December 2021, there was a much-publicized security incident. Known as “Log4Shell”, it is a good lesson in how important it is to respond to such problems with readiness, but also with care and structure.

Log4Shell was a vulnerability so critical that it received the greatest severity rating (CVSS 10.0). It affected the Log4j library of the Apache Software Foundation, which is used by countless companies around the world.

The main products of Wibu-Systems (CodeMeter Runtime and SDK, CodeMeter Protection Suite, CodeMeter License Central, CmCloud, WibuKey) were not affected, and CodeMeter Keyring for TIA Portal and CodeMeter Cloud Lite only needed a minor update.

But what happened behind the scenes? How does Wibu-Systems respond to such vulnerabilities in third-party components? What if there is an issue with our own software?

A look at our security incident response process:

1. Incident Report

Vulnerabilities and incidents are reported in either of two ways:

- External report: Information about a possible vulnerability is sent by email to cert@wibu.com or via the Incident Management System located at <https://support.wibu.com>.

- Internal report: Findings from internal scans, automated code reviews, or other security checks are flagged directly in our internal tracking system.

2. Analysis

The information is sent to our dedicated Product Security Incident Response Team (PSIRT), also called Wibu-CERT (Computer Emergency Response Team) for analysis, where four security specialists take care of coordinating the response and supporting the vulnerability analysis by the Product Security Board (a group of specialists assigned to the job by our developer teams). A score is given to each affected product in line with the accepted industry standard CVSS (Common Vulnerability Scoring System) to understand how severe the issue is.

3. Countermeasures

Two important tasks are covered in this phase:

- Treatment: Once the analysis confirms the severity of the incident, the issue is flagged in our development tracking system. The tag tells our developers how urgent a response is needed: Either, the vulnerability is addressed in a planned release or an immediate bugfix has to be released.
- Coordinated communication: The evaluation is provided to the reporter and

further coordinated with him, if necessary. The CERT mailing list makes sure that clients are told in good time about vulnerability and necessary bugfixes. This gives them a vital head start to e.g. prepare their own security advisories and test necessary fixes before the vulnerability becomes public knowledge.

4. Publication

Security advisories are produced for publication on <https://wibu.com/security-advisories>, and a “Tech News Flash” email is sent to our clients, users, distributors, and the relevant authorities with more information about the vulnerability and available security fixes.

This simple, but critical process enables Wibu-Systems to respond immediately and prepare solutions for all clients and users affected, true to our guideline for all security incidents: Be open and be honest!



ALERT


Do you want to receive more frequent updates from our WIBU world?

Subscribe to our newsletter




News in Brief


Firm Security Box (FSB) in the Cloud

As of April 2022, Firm Security Boxes (FSB) are available as CmCloudContainers to move the entire build and deploy process (e.g. Azure pipelines) into the cloud. CodeMeter SDK 7.40a or newer required. 

Extended Windows 7 Support

CodeMeter 7.21c is available for download for clients with extended support for Windows 7 since February 2022. The release includes fixes for vulnerabilities published since the last full version. 


Improved Support for Microsoft Azure

The bugfix release 7.40a of CodeMeter Runtime improves the detection and automatic binding of CmActLicenses for Microsoft Azure. 


Support for Alpine

Since AxProtector version 11.00 was recently distributed, you can protect applications, libraries, and .NET assemblies built for the Alpine Linux distribution that uses musl instead of glibc as their C library. Encryptions for Alpine systems require an additional AxProtector license. 


Licensing CodeMeter Protection Suite

Our popular CodeMeter Protection Suite, the go-to tool for protecting software against reverse engineering and unauthorized use, was given a new licensing model in January 2022. The new licenses distinguish between target platforms and protection targets. All basic licenses come with automatic encryption, automatic license checks, integrity protection, and anti-debugging capabilities as well as support for a choice of license containers (CmDongles, CmActLicenses, CmCloudContainers). 

Writing License Data Dynamically to Embedded Devices

CodeMeter Embedded 2.53 introduces the ability to write license data like Extended Protected Data into CmActLicenses during runtime by means of generic programming sequences. 

Contributing to the Platform Industry 4.0

Professor Andreas Schaad and Dr. Carmen Kempka are representing Wibu-Systems in a high-profile network of politicians and researchers dedicated to powering the digital transformation of Germany's manufacturing sector. 



Journal of Innovation


Get up to speed with the why and how of protecting the entire machine learning lifecycle in our article in the Journal of Innovation: <https://bit.ly/Jol-ML>.  

IT Security Club


An "Innovation Membership" in our IT Security Club offers exclusive access to pioneering thinkers and inspiring partnerships as well as attractive funding opportunities for collaborative projects. Register today: <https://www.wibu.com/itsc>  




CodeMeter Cloud 2.2

The new Personal CmCloudContainer is introduced with CodeMeter Cloud 2.2. This type of CmContainer is intended for use by a single user on a maximum of three devices at once. 


CodeMeter Cloud Lite 2.3

A new support function has been added to CodeMeter Cloud Lite 2.3 that allows all CmContainers and users to be displayed. 


CodeMeter License Central Extensions 21.04b

Release 21.04b uses a new approach to retrieving automatic updates in the background and improves support for values that are only set by the Extensions upon activation. 

CodeMeter License Central 4.01d

Version 4.01d brings a marked improvement in performance when listing all licenses on a ticket, increasing the number of licenses that can be used per ticket in real-world conditions. 

SmartShelter|PDF 22.04

Our solution for protecting pdf files has been updated with SmartShelter|PDF 22.04. This new version includes native support for Acrobat Reader on 64-bit systems. 

Subscribe to our Podcast

Our Wibu-Systems podcast offers a lot of exclusive material, including talks and presentations from popular conferences and expos, interviews with our team, premium customers, international industry associations, and academia experts. The episodes provide details on success stories, product launches, industry insights, and behind-the-scenes details to keep you on top of the latest trends in the protection, licensing, and security of your digital assets.  



VE-ASCOT

Greater security for industrial Chains of Trust: That is the mission of the VE-ASCOT research project, coordinated by Wibu-Systems and supported by the Federal Ministry of Education and Research. VE-ASCOT is promoting digital security and sovereignty with a secure electronics value chain with the active contributions of Siemens, Infineon, Schoelly, RevOne, FhG SIT, KASTEL at the KIT, and the University of Bielefeld.  



Wibu-Systems Training

Wibu-Systems offers custom training to get you off to a running start with CodeMeter software protection and licensing. The training is offered in the form of company courses, typically hosted as in-house classes on your premises. The standard training program includes three days of courses, which can be adjusted to your needs and level of expertise. You can pick and choose the contents you need and shorten the program to 1 or 2 days. Alternatively, you can add a hands-on workshop to allow your participants to try out their own practice cases.



www.wibu.com/tr

Available Courses

CodeMeter Core Features

- CodeMeter at a glance
- Configuring licenses
- The components of CodeMeter Runtime
- Use as a network server

Software Integration for .NET Assemblies with AxProtector .NET and API

- Encrypting .NET assemblies
- Encrypting individual classes and methods
- Integrating Wibu Universal Protection Interface (WUPI)
- Using CodeMeter Core API

Back Office Integration with CodeMeter License Central

- Configuring products
- Creating licenses
- Integrating license activation in applications
- Setting up and configuring license portals

Contact our local representatives for training courses on site

WIBU-SYSTEMS AG
Germany
+49 721 931720
info@wibu.com

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 5566 1790
Beijing: +86 10 8296 1560/61
info@wibu.com.cn

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.systems

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS BV/NV
The Netherlands: +31 74 750 14 95
Belgium: +32 2 808 6739
sales@wibu.systems

WIBU-SYSTEMS
Spain | Portugal
+34 91 123 0762
sales@wibu.systems

WIBU-SYSTEMS K.K.
Japan
+81 45 565 9710
info-jp@wibu.jp

WIBU-SYSTEMS sarl
France
+33 1 86 26 61 29
sales@wibu.systems

WIBU-SYSTEMS
Scandinavia | Baltics
+46 8 5250 7048
sales@wibu.systems

Join Wibu-Systems and its subsidiaries at the following events:

 **MedtecLIVE with T4M**
3-5 May 2022
Stuttgart, Germany
Hall 10, Booth 124a

 **Hannover Messe**
30 May – 2 June 2022
Hannover, Germany
Hall 5, Booth B43

 **Karlsruher Entwicklertag**
17-18 May 2022
Karlsruhe, Germany

For an up-to-date overview of our workshops, visit mycodemeter.com/workshop/.

Also, our monthly fully immersive masterclasses focus on unique content and are designed for beginner, intermediate, or advanced users of our CodeMeter technology. The 2022 season will cover areas such as Machine Learning, Features-on-Demand, Salesforce integration, authentication, cloud licensing, and license monitoring. Watch out for our forthcoming announcements either on our website or via newsletter and get ready to register for the sessions that are most helpful to you.

Imprint
KEYnote 43
Spring-Summer Edition 2022

Publisher
WIBU-SYSTEMS AG
Zimmerstrasse 5
76137 Karlsruhe, Germany
Tel. +49 721 93172-0
Fax +49 721 93172-22
info@wibu.com
www.wibu.com

Responsible for the content
Oliver Winzenried

Editors
Stefan Bamberg
Alvaro Forero
Joerg Jans
Ruediger Kuegler
Daniela Previtali
Wolfgang Voelker
Oliver Winzenried

Design
Eugen Olchin

Print
Stober Medien GmbH, Eggenstein, Germany

Letters are always welcome. We will protect the confidentiality of sources. Third party articles do not necessarily reflect the opinion of the editorial office. Write us at team@wibu.com

Wibu-Systems expressly reserves the right to change its programs or this documentation without prior notice.

Wibu-Systems®, CodeMeter®, SmartShelter®, SmartBind®, and Blurry Box® are registered trademarks of WIBU-SYSTEMS AG. All other brand names and product names used in this documentation are trade names, service marks, trademarks, or registered trademarks of their respective owners.

Copyright ©2022 Wibu-Systems. All rights reserved.

Picture credits:
Cover: [istockphoto.com/R&A-Studio](https://www.istockphoto.com/R&A-Studio)
Page 4: [istockphoto.com/Blue Planet Studio](https://www.istockphoto.com/Blue Planet Studio)
Page 5: [123rf.com/3dmentat](https://www.123rf.com/3dmentat)
Page 7: [istockphoto.com/Blue Planet Studio](https://www.istockphoto.com/Blue Planet Studio)
Page 9: [istockphoto.com/R&A-Studio](https://www.istockphoto.com/R&A-Studio)
Page 11: [istockphoto.com/razhusin](https://www.istockphoto.com/razhusin)
Page 13: [MATLAB+unsplash.com/Gradients](https://www.MATLAB+unsplash.com/Gradients)
Page 15: [istockphoto.com/Andrej Popov](https://www.istockphoto.com/Andrej Popov)

All remaining images are copyrighted by their owner

**SECURITY
LICENSING
PERFECTION IN PROTECTION**

