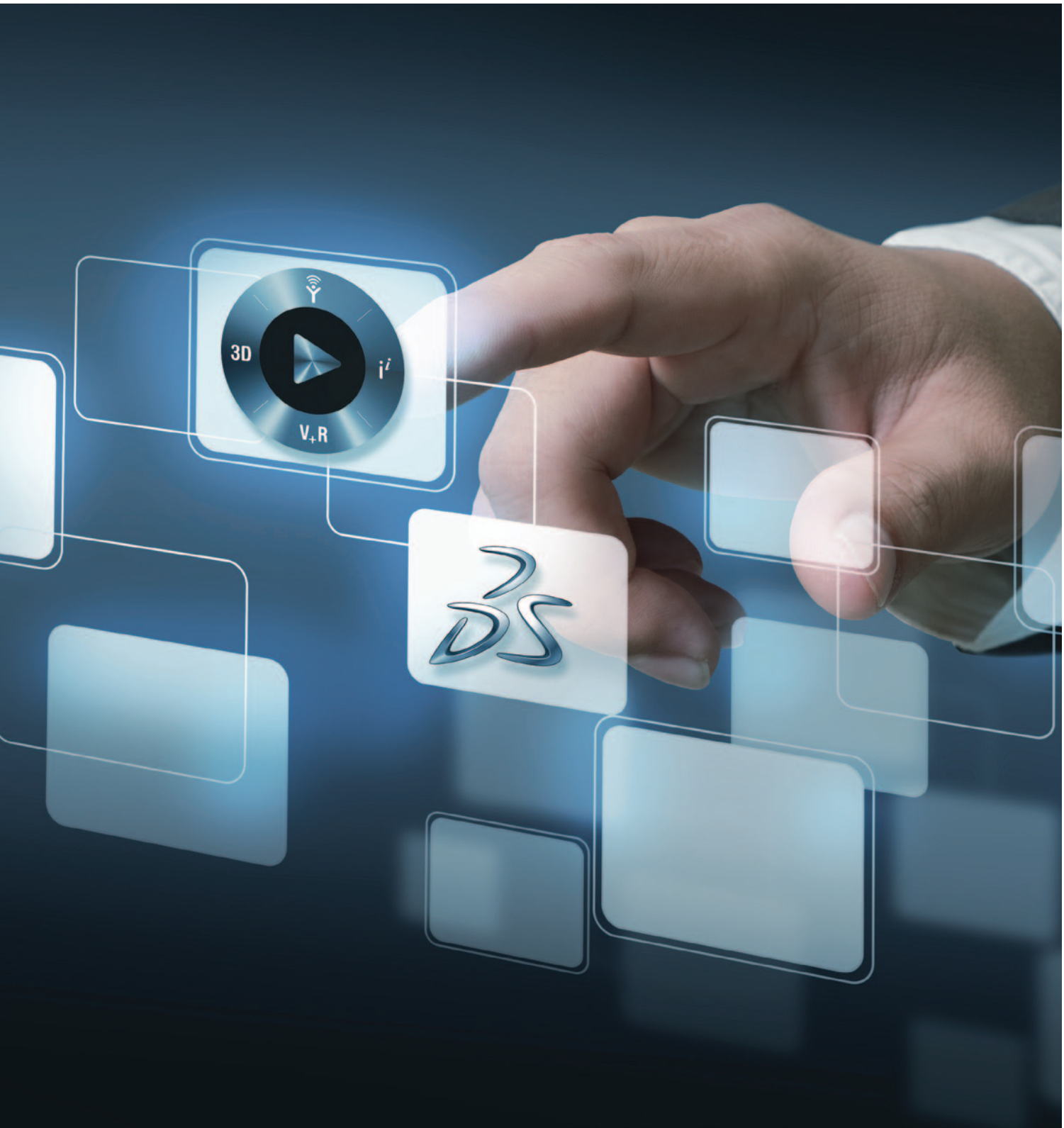
DASSAULT SYSTEMES

TAKE CONTROL

Protect Your Intellectual Property



Contents

Executive Summary

Organizations seek a way for employees to collaborate freely within the company and with business partners across the globe without worrying about sensitive product information or trade secrets ending up in the wrong hands. How do companies strike the right balance between sharing information and securing it?

Running a business—whether it's a one-person auto repair shop or a multibillion dollar aircraft manufacturing company—has always involved a certain amount of risk. In recent years, however, the steady shift to what is now a global economy has pushed the risk quotient associated with running a business to stratospheric levels.

For manufacturing companies, this new economy requires managing extended supply chains in which outside partners and suppliers perform critical functions—from product design to manufacturing, and even post-sales product support—from various points around the globe.

Manufacturers increasingly are turning to outsourcing and off-shoring for one simple reason: it has proven to make economic sense. But those economic benefits can quickly be mitigated—if not completely wiped out—if a company doesn't have a sound strategy for managing critical supply chain risk.

In the current economy, the possibility of having intellectual property (IP) stolen or otherwise compromised is among the greatest—and potentially most harmful—risks manufacturers face. It's also a risk that far too many manufacturers are ill prepared to manage.

IP typically is lost or compromised in one of two ways:

Outright theft by an unscrupulous party; or

A phenomenon often referred to as "leakage," which is unintentional disclosure that occurs in the course of sharing information with individuals from various departments within the company or with outside supply chain partners.

Regardless of how the loss of IP occurs, it can have a devastating impact on the corporate bottom line. IP theft often results in counterfeit versions of a company's products being manufactured and sold on the black market. Using pilfered design data, unprincipled individuals are making products that resemble authentic items—many of them bearing the original manufacturer's logo—to unsuspecting customers.

A Flood of Fake Products

Fake products have become a far too-common occurrence for companies that make high-tech products, and the impact of these incidents reverberates throughout the broader economy because high-tech manufacturers supply goods to so many other industries.

In the defense industry alone, the number of counterfeit electronic products uncovered more than doubled—going from 3,868 to 9,356 in the three-year period from 2005 to 2008, according to a U.S. Commerce Department report released in January 2010.[1]

The economic impact of this activity is tremendous. For instance, fake products cost the information technology industry roughly $100 billion each year, according to the national Electronic Distributors association.[2]

Counterfeit products also pose a major public safety risk, as fake products are more likely to fail without notice because they are neither manufactured nor tested in accordance with the original design specifications.

Though not safety related, a 2007 incident at Los Angeles International Airport points to the potential problems counterfeit electronics can cause. according to the U.S. Department of Homeland Security, a malfunctioning router shut down the computer network that the U.S. Customs and Border Protection Service relies on when screening passengers, causing long delays for more than 17,000 passengers. an investigation of this incident led to a counterfeit version of a component that was designed to aid communication with the network.

The U.S. General accountability office (GAO) recently noted that the risk of IP theft is growing as U.S.-based companies integrate further into the global economy by moving more sophisticated business processes to regions that don't have strong track records for enforcing IP rights.

"Initially, U.S. firms invested in overseas manufacturing facilities in countries such as China and India to perform labor-intensive assembly of semiconductors for export to the U.S.," the recent GAO report stated. "However, as the technological and manufacturing capability in Asia has increased, more sophisticated parts of the process have been sourced in India and China. This shift to having more advanced technology used abroad creates a greater risk for those firms involved by making advanced technologies protected by IP laws more readily available to those who might want to copy them illegally. The severity of these risks has been intensified by weak enforcement in some countries, particularly China, whose enforcement challenges have persisted despite U.S. efforts."[3]

In other words, companies that rely heavily on offshore supply chain partners— which is now the case for most manufacturers—need to develop their own strategies for preventing the theft of their IP.

Those strategies also need to protect against IP leakage, which can pose an additional set of problems. as stated previously, leakage is the loss of IP during the process of sharing information among groups of people who are collaborating to design or build a product.

While IP can be stolen in this manner, leakage most often leads to the unintentional release of information that violates government export regulations or non-disclosure agreements with business partners.

Exposing a business partners' proprietary information to unauthorized individuals—even within your company—can do irreparable harm to business relationships, in addition to exposing your company to potential lawsuits.

Aerospace and Defense (A&D) manufacturers—and particularly the prime contractors in this sector—face a special set of risks when it comes to protecting IP. The increasing pressure to reduce both the time and costs associated with developing complex products such

as aircraft and weapons systems, has forced prime contractors to place more responsibility for designing and integrating major subsystems in the hands of their Tier 1 and Tier 2 suppliers. That means these suppliers now have access to the prime contractors' most valuable data, and that data must not be allowed to leak into competitors' hands. This is no small task given the fact that a Tier 1 supplier on one A&D program could very well be a competitor on another program.

National security considerations also must be top of mind for A&D manufacturers when it comes to the handling of IP, with governments across the globe wanting to keep their military secrets from falling into enemy hands. The need to comply with national security protocols is obvious when the data in question pertains to products made specifically for military use, but these protocols also must be honored for "dual-use" components or materials that can be used in both consumer goods and military products. Companies that violate national security regulations related to the disclosure of IP are subject to both civil and criminal penalties.

In the U.S., the following sets of regulations govern the disclosure of most IP:

- ITAR—International Traffic in Arms Regulations, which dictate that information pertaining to military technologies may not be shared with citizens of another country without prior authorization from the U.S. State Department; and
- EAR—Export Administration Regulations, administered by the U.S. Department of Commerce, which outline specific commodities that may not be exported to certain countries.

The U.S. and the European Union (EU) have been working to develop common rules governing the export of military-related technology, but that process is taking time. So, for the foreseeable future, companies doing business in the EU must be aware of—and adhere to—the IP protection laws of each individual country.

Severe Penalties for Non-Compliance

In the UK, for instance, licenses for exporting military technology are granted by the Export Control organization, and the type of license required differs according to the exact nature of the product being moved out of the country, its ultimate destination, and its actual end use. Individuals found in violation of the UK's export control laws can face up to 14 years in prison.

Penalties for running afoul of ITAR regulations in the U.S. can be as high as $1 million per violation, in addition to a 10-year prison sentence. and ignorance of the law is no excuse. Companies have been penalized for what could be perceived as innocent business transactions.

In 2008, for instance, a veterinary supply wholesaler based in Iowa, was assessed a $250,000 civil penalty for an EAR violation. Its transgression: shipping a total of 16 electric cattle prods to customers in Mexico, Chile, South Africa, the Dominican Republic, Columbia and El Salvador.

The items are on the U.S. Commerce Department's export control list because they are known to be used by authorities in those countries to interrogate prisoners—an action the U.S. government considers a violation of human rights. Because the wholesaler was unaware it had committed a violation, the Commerce Department agreed to waive $150,000 of the original penalty, still leaving the company with a hefty bill.

Large manufacturers in similar situations—and especially those in sensitive industries such as high-tech and aerospace and defense—typically are treated even more harshly. Consider these situations:

- In 2008, a well-known military aircraft manufacturer was found in violation of ITAR regulations and assessed a $4 million fine for providing technical data—some classified and some not—about Hellfire missiles to the government of the United Arab Emirates. In ruling on the case, the State Department noted that this manufacturer believed the UAE was cleared to receive this information because it already possessed the missiles. The State Department also noted that the manufacturer attempted to recover the information after learning it had acted in error, yet the fine was still imposed.
- Also in 2008, a second large defense contractor reported to the State Department that a company it recently acquired had modified a series of commercial inertial navigation systems to make them suitable for military use and exported them to several countries. While citing the "mitigating circumstances" of the contractor self-reporting violations that occurred before it acquired this company, the State Department still charged the contractor with 110 ITAR violations and imposed a $20 million fine.
- In 2007, a leading supplier of night vision equipment to the U.S. Department of Defense was hit with a $100 million penalty after admitting to sending classified technical information to China, Singapore and Britain without receiving prior authorization from the U. S. Government.

These situations illustrate the importance of having a solid strategy for managing and protecting IP. What they don't illustrate is how today's global supply chains can complicate the task developing and executing that strategy.

Taking Responsibility for IP Protection

Let's look at it from the perspective of a large OEM who is the prime contractor on an aerospace and defense program. as the prime contractor, the OEM typically will engage with a number of other large organizations—known as Tier 1 suppliers—to handle major aspects of the program.

These engagements require the OEM to share detailed information about its products with its Tier 1 suppliers—some of whom might be competitors on other programs. That means the OEM must have a way of keeping detailed records on all of its IP to ensure that only the information necessary to fulfill the current contract—and nothing else—is passed to the Tier 1 suppliers. and the need for protecting IP—like the supply chain—doesn't stop at this level.

The Tier 1 suppliers have their own network of subcontractors with whom they must share sensitive product information, and the process continues until ultimately the OEM finds itself needing to keep track of information that's traveling across a far flung network of contractors and suppliers spread out all over the globe.

Each time information moves down a level in the supply chain, the potential for IP theft or leakage grows, but the OEM's responsibility for protecting its own IP never diminishes.

In an ideal world, each member of an extended supply chain would be fully committed to protecting IP—their own as well as their supply chain partners — and they would demonstrate that commitment by implementing proven tools and techniques for safeguarding that property.

As the brisk trafficking in black market goods proves, however, a lot of suppliers appear to have a vested interest in not protecting their supply chain partners' IP. That means the larger companies—the OEMs and their top-tier suppliers—must assume that responsibility.

Currently, most companies that are attempting to protect IP are taking one of two approaches:

- Manual, ad-hoc processes in which a small group of people in a document control department are assigned to track the usage and movement of data in much the same way books are checked out of and back into a library; or
- IT-based processes that call for segregating data into multiple systems—often by location—and only giving certain individuals access to those systems.

Both approaches have major shortcomings. The first one offers no real IP protection, since manual processes are easily circumvented.

The second approach, in effect, puts the company's IT staff in charge of controlling access to IP, rather than the people who actually use it and ultimately are responsible for its protection. This approach also makes it difficult for people to get information when they need it, which can stifle the type of free flowing collaboration that needs to take place within supply chains in order to design, develop and manufacture products in the timely, cost-effective manner that customers now demand. Managing IP in this manner also can lead to unnecessary IT costs, as multiple applications and the associated infrastructure continue to be maintained for the sole purpose of keeping data segregated.

A New Approach to IP Protection

Fortunately for manufacturers, another approach is now available—one that makes it easy to strike the right balance between the increasing need for seamless supply chain collaboration and the ongoing requirement for maintaining tight controls on IP.

This approach centers around the deployment of a next-generation product lifecycle management (PLM) software platform that can federate data from multiple systems across an extended global supply chain, in effect creating a central repository for all data associated with a particular project or program regardless of where—or on what system—the data was created.

With this type of system place, all requests for access to IP—no matter where they originate within the supply chain—are managed by this single system, which can determine within a matter of seconds whether any individual is authorized to access the information they are seeking.

A PLM platform is the perfect tool to support the twin goals of streamlining product development and protecting IP, because the PLM system is where product designs—which are the core piece of any company's IP—are created. PLM systems also are increasingly being relied on as the primary platforms for sharing product design data with everyone involved in building, selling and servicing products.

For that reason alone it makes more sense for a PLM platform—as opposed to an ERP or supply chain management system—to take on the primary role of protecting the company's IP. It becomes an even easier decision when the company can deploy a next-generation PLM platform like the ENOVIA® IP and Export Classification and Enforcement solution from Dassault Systémes.

This system enables manufacturers to maintain strict control over data—while also ensuring that those who need specific pieces of information can get it without delay—because it has separate application components that focus on what have proven to be the two most critical aspects of IP protection:

- IP Classification: Establish a system of classification of data in order to define and apply security rules to each category
- IP Enforcement: Enforcing rules to ensure that all data remains secure as it's accessed and shared across the supply chain

These functions are becoming increasingly critical as global economic pressures force manufacturers to constantly search for new methods of getting products to market faster at ever lower costs.

Rules for Classification and Control

Advances in communications and collaboration technology are making it easier for manufacturers to locate new business partners with innovative ideas for designing and building products, but those partners must be vetted carefully, particularly if they're located in countries that don't have strong IP protection laws. That's why it's important to have an IT system that enables the easy classification of both personnel and data. It simplifies the task of establishing— and enforcing—rules to ensure that no information ever makes it into the wrong hands.

These rules can come into play in a variety of processes common to all manufacturers, such as:

- Collaborating with potential partners on requests for proposals;
- Collaborating on new product designs;
- Managing changes to existing designs;
- Transmitting manufacturing work instructions to contract manufacturers; or
- Sharing engineering documents with MRO partners.

In any of these situations, an IP protection system should identify each person involved in a transaction according to one or more classifications—such as the location in which they normally work, the location from which they are attempting to access data at that moment, and the country or countries in which they hold citizenship. This type of information is vital to maintaining compliance with the U.S. government's ITAR and EAR regulations, as well as the import-export rules of other governments.

Once an individual's classification has been established, whenever they try to retrieve data from the system, it should run a check to determine if they are allowed to have access to the data they are requesting. Dassault Systémes' ENOVIA IP and Export Classification and Enforcement system does this, and more. It also allows for establishing rules for what all individuals on a project are allowed to do with any data they retrieve.

For instance, some data may be restricted to only certain uses due to export control regulations, while other data may be subject to rules governing its disclosure to competitors or potential competitors. and finally, some information may only be accessible to people with the proper government-issued security clearance.

With a system like this in place, multinational project teams can collaborate effectively while obeying the export control regulations, commercial IP laws and security protocols of all countries involved. This is possible because even though the system federates data from across the supply chain, it also has the ability to compartmentalize and segregate data when necessary to keep it from being accessed by the wrong individuals.

The company that deploys the system—which is likely to be an OEM or top-tier contractor—establishes its own system for classifying both people and data, and then sets the rules for who is allowed access to specific pieces of data. Once the rules for managing and protecting data have been established within the ENOVIA IP and Export Classification and Enforcement solution those rules can be reused— and modified as needed—to fit the needs of future programs.

Reusing rules is extremely easy, thanks to the inheritance properties built into the system. Under these properties, rules are applied to each piece of data at the class level, and those rules remain associated with that data whenever it's accessed throughout its lifecycle. For instance, if a specific piece of data is placed under access restrictions mandated by ITAR , those restrictions are enforced whenever anyone tries to access that information. If that data is used with a new program, the original ITAR restrictions will remain in place. The restrictions can be lifted by granting exceptions to specific individuals under specific circumstances. Even in those cases, however, the original restrictions will apply to that data anywhere else it is used throughout its entire lifecycle. The inheritance feature of the ENO VIA IP and Export Classification and Enforcement solution allows companies to move quickly in setting up data-sharing procedures for new programs without having to worry about IP being compromised.

Managed by IP Control Specialists

The ENOVIA IP and Export Classification and Enforcement solution also is designed to be managed by people with job titles such as project manager, compliance officer or export control administrator rather than IT personnel. These are the people who specialize in making sure the company complies with all legal agreements, regulations and security protocols in every country in which it does business. Therefore, they are the most qualified to set rules for controlling IP, as well as managing the system that enforces those rules.

The ENOVIA IP and Export Classification and Enforcement solution comes with a pre-defined set of security classes for both personnel and data, and companies can modify those classes or add new ones to meet their specific needs. The companion Export Control system acts as a network security officer, ensuring rules for accessing data that were established in the classification system are enforced each time someone attempts to access information. The system is extremely thorough in carrying out this task, even being able to track the physical location of the person requesting data, and denying access based on that information if the company controlling the data deems that appropriate. Such controls might be in place, for instance, if regulations governing certain data say it can only be accessed by citizens of the country in which it was created, and only when those citizens are physically located in that country.

While the system is extremely diligent in protecting data, it also gives users the flexibility to set exceptions for access to data for individuals who have a legitimate reason for viewing data that is not typically linked to their specific classification. This can be the case, for instance, if two companies enter a new partnership and a non-disclosure agreement (NDA) suddenly grants one partner temporary access to data they had not been allowed to see when the original IP classification and export control rules were established.

The specific reason for making an exception to the regular data-access rules— whether it's due to a special export license, an NDA, a technical assistance agreement, or any other circumstance—can be documented in the system. an audit trail also is created for each exception, giving compliance officers the ability to know—at all times, and with absolute certainty—whether anyone accessing data is following normal procedures or operating under an authorized exception to the normal procedures. This is not the case in companies that rely on the IT department to manage their IT protection systems. Those companies generally follow security rules designed for IT systems, not IP protection solutions.

With the ENOVIA IP and Export Classification and Enforcement solution, any exception to the original data-access rules also can be set to expire after a certain time period, ensuring that all data is being afforded the appropriate levels of protection at all times.

Industry best practices dictate that exceptions to data-access rules only be applied to situations that don't involve bypassing a government security clearance. It's one thing to grant an exception to an export control regulation or a non-disclosure agreement. But it's completely different—and far more risky—to grant exceptions to rules designed to protect military secrets.

The ENOVIA IP and Export Classification and Enforcement solution comes with a pre-defined list of clearance levels from multiple countries and international organizations, such as the U.S. military, NATO, and more. That allows user companies to easily set the precise clearance level—military secret, top secret, etc.—that should be granted to each individual who will be using the system.

The Human Element

The system's method of establishing standard security classes and exceptions— and basing them on things like NDAs between business partners or special export licenses granted to specific businesses—makes it easy to maintain a record of exactly who is accessing what data, even when normal rules are not being followed. This capability proves especially useful when a company needs to demonstrate its ability to protect IP to government auditors or potential new business partners.

Examples of the system's audit capabilities include the ability to create a dynamic record of all data accessed by a given user. That record also can differentiate between access governed by normal rules and access governed by exceptions such as an NDA. It's also possible to generate lists of users who are authorized—or not authorized—to access specific classes of data. These lists can be created in real time if the need to verify users' credentials arises.

While the ENOVIA IP and Export Classification and Enforcement solution sets a new standard for IP protection technology, it's important to note that even the best systems can't perform their designated functions if people refuse to use them. That means companies must take time to educate their employees on the importance of protecting IP—as well as the importance of using the systems the company has invested in to do so.

The risk of having IP stolen or compromised is a huge issue for manufacturers, but one that can be managed with the proper amount of diligence from both an organizational and technology standpoint. With the right people, processes and systems in place, manufacturers can meet the challenges of doing business in the 21st century without fear of having their most valuable assets—the ideas that eventually become profitable products—stolen or devalued.

To learn how the Dassault Systémes ENOVIA IP and Export Classification and Enforcement solution can meet your company's specific IP protection needs, visit www.3ds.com

DASSAULT SYSTEMES

Delivering Best-in-Class Products

CATIA
Virtual Product

EXALEAD
Information Intelligence

SOLIDWORKS
3D Design

GEOVIA
Virtual Planet

SIMULIA
Realistic Simulation

NETVIBES
Dashboard Intelligence

DELMIA
Digital Manufacturing

3DSWYM
Social Innovation

ENOVIA
Collaborative Innovation

3DVIA
3D Communication

Dassault Systèmes, the **3D**EXPERIENCE Company, provides business and people with virtual universes to imagine sustainable innovations. Its world-leading solutions transform the way products are designed, produced, and supported. Dassault Systèmes' collaborative solutions foster social innovation, expanding possibilities for the virtual world to improve the real world. The group brings value to over 150,000 customers of all sizes, in all industries, in more than 80 countries. For more information, visit www.3ds.com.

Europe/Middle East/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific
Dassault Systèmes
Pier City Shibaura Bldg 10F
3-18-1 Kaigan, Minato-Ku
Tokyo 108-002
Japan

Americas
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

Visit us at
3DS.COM

WI-TC 12-1212