THE OEM'S DILEMMA: ENABLING IP-SECURE SUPPLIER COLLABORATION

Securing intellectual property (IP) is a crucial concern in engineering. As hacks of personal data and product specifications proliferate in the news cycle, the risk of data loss looms. At the same time, manufacturers are transitioning from traditional mechanical products to increasingly complex "smart" ones. As a result, they are outsourcing work to an increasing number of suppliers in ever-evolving, discipline-specific areas. The need to develop competitive solutions drives such outsourcing. Working with an expert supplier of technologies that are not among an organization's competencies—for example, integrated circuitry—allows deadlines to be met and products to be delivered on time.

Manufacturers can't afford to let such outsourcing slow down development. They must remove friction from collaboration. At the same time, they must be careful to not expose trade secrets and product designs. These constraints are not simple to manage. Suppliers need access to specific information for limited amounts of time, and security is critical. Manufacturers must have easy-to-use, scalable systems that keep data secure while allowing all project partners efficient access to the information

they need. And companies must not only secure their own data from vendors but also suppliers' data from each other.

Manufacturers must employ new technology-led initiatives to address these requirements. Indeed, enabling IP-secure collaboration with suppliers requires a digital transformation initiative. Several kinds of systems for secure collaboration are available. This brief explores those options.

AN ILLUSTRATIVE EXAMPLE

Imagine a company that produces walk-behind lawn mowers. Offering a new self-driven lawn mower that operates independently would help it maintain, or even boost, its market share.

A smart, connected mower—unlike a walk-behind mower—requires sensors, software code, and other components as part of a safety system. Because the manufacturer does not have these competencies, it must collaborate with numerous suppliers to develop the new system. For example, it might work with a lidar sensor specialist company along with an embedded software developer.

Everyone must move fast to meet deadlines. The suppliers should be exposed to only the specific IP they must have to do their job. The manufacturer must be able to onboard suppliers easily and, once the project is complete, offboard them and shut down their access to the project.

ACCESS MODELS

Collaboration can be accomplished in various ways, and manufacturers must evaluate the advantages and disadvantages of each option to determine which best meets their needs.

The no-cost way to share data is to send emails with files attached. Since such files are snapshots of a product's current design, they don't update when changes are made by the file owner. This is the least secure option because the manufacturer has no control over how the data is shared after emailing it.

A manufacturer can give suppliers access to its product lifecycle management (PLM) system through a VPN or similar connection. Drawbacks include difficulties in supplier onboarding and offboarding and the necessity of local installation and configuration of software clients. This option gives the manufacturer more control over its data because the data is accessible by those who require it but never leaves the manufacturer's system.

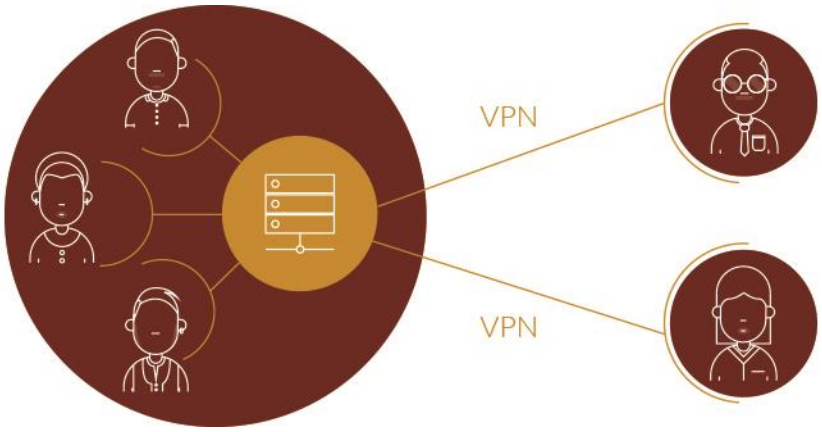

Figure 1: Direct supplier access to an OEM's PLM system.

Another option involves setting up a separate PLM system in the demilitarized zone (DMZ)—the commonly accessible portion of the internet. The PLM system in the DMZ synchronizes a subset of information with the internal PLM system behind the manufacturer's firewall. Suppliers access the DMZ PLM system to get the information they need to complete their portion of the project. The shortcoming of this access control approach is that technical knowledge is required to set up paired syncing between the PLM systems.

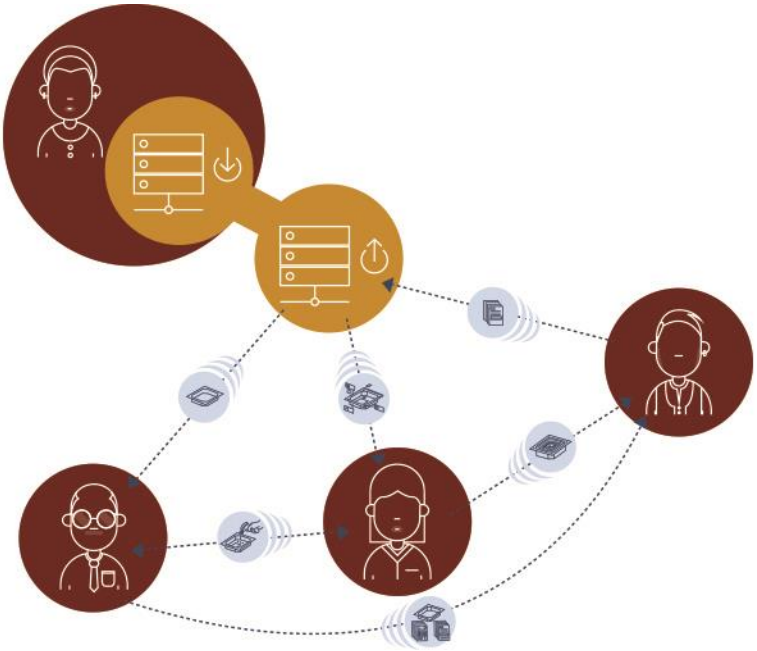

Figure 2: Supplier access using paired PLM systems. One sits in the internet demilitarized zone (DMZ).

Some companies choose to allow collaboration partners access through a web service powered portal. This involves using a PLM system's web services to allow access through a firewall. This approach is simpler and safer than the last two, requires only a browser, and can be used from any location. It has the drawback that implementation requires technical skills.

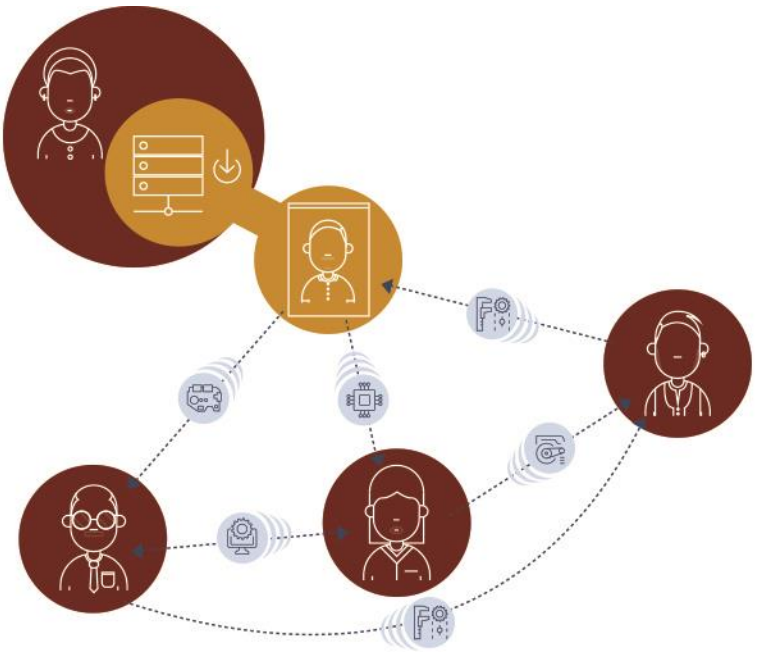

Figure 3: Supplier access granted through a supplier portal built on the web services of many enterprise systems, including PLM.

ACCESS CONTROL

Access models offers one layer of control during supplier collaboration. Access control is a second, supplementary, layer, and many different, complementary methods of access control exist.

Role-based access to IP is an uncomplicated control method. Specific people and groups, including suppliers' personnel, are given access rights to specific containers, projects, and objects. This option is simple but effective when used properly during a collaborative project.

Another path is allowing people and groups access rights based on values of an object's metadata. The visibility in the sharing system can be determined by lifecycle state, security clearance, or other properties applied to that object.

Figure 4: Access control rules defined based on location.

In contrast, environment-based access rights use the location of the person attempting to access information to determine their retrieval permissions. If an employee or an outside supplier is traveling outside of a geographical region, their access can be limited and controlled, even hiding the item completely from their view.

The most complete option is domain access control. Access rules are established with controls inherited through relationships of connected objects like projects, organizations, and more. Many existing solutions track and report on data usage to ensure that no IP is inadvertently exposed. This multifaceted protection approach allows large amounts of critical data to be safeguarded and shared effectively. While the advantages of this method are great, implementing and monitoring it can complex.

These access control options are not mutually exclusive. One collaboration partner may require a specific file-sharing option due to regulations governing its industry, while another may not be able to connect because of a physical location restriction on its geographic location. Companies must develop a system tailored to their needs that provides dynamic data protection. A combined approach suits many companies.

RECOMMENDATIONS

The shift to smart, connected products is driving companies to collaborate with more suppliers to ensure that their products remain competitive in an ecosystem rich with innovation. They still must protect their IP. Secure collaboration is achievable, and many options exist for protecting IP from prototype to production. Implementing a scalable system that safeguards

data from loss—due to negligence or theft—encourages beneficial relationships with all tiers of the supply chain.

Lifecycle Insights suggests the following:

- Analyze the amount and complexity of work outsourced to suppliers, taking CAD and other metadata into account. An increase in either is a sign of new opportunities for IP-secure collaboration with suppliers.
- Assess technology enablers currently used for collaboration with supply chain partners. Manifestations of the issues highlighted in this brief signify that new solutions are needed to help leverage global talent without compromising IP.
- Identify the company's need to protect IP, which drives what safeguards must be put in place before collaborating with suppliers. Timed file access and controlled edit permissions allow companies to track compliance and ensure dynamic control of collaboration policies.
- Explore the current PLM system's capability to securely share IP. If it suffers from any of the faults identified in this brief, look at augmenting or replacing the system.

Chad Jackson leads Lifecycle Insights' research and thought leadership programs, attends and speaks at industry events, and reviews emerging technology solutions.

Lifecycle Insights is a research and advisory publishing firm. Our mission is to help executive reap more value from tech-led initiatives without disruption.

EMAIL - contact@lifecycleinsights.com

SITE - www.lifecycleinsights.com