NEXTLABS

CASE STUDY

Marvin Engineering

"Marvin Group established a design joint venture with one of its competitors. Both companies were utilizing Siemens Teamcenter for PLM, but needed to find a way to protect our IP from being accessed by our competitor. Our IP is the most valuable asset we own. NextLabs Enterprise Digital Rights Management (EDRM) solution provides the security enforcement we need and is tightly integrated with Teamcenter. NextLabs is the only EDRM product integrated with Teamcenter and it provides a granular level of access control to ensure that our partners are only able to view authorized information."

Director of Engineering, Marvin Engineering

Marvin Engineering, based in Inglewood, California, is a privately-owned business engaged in the development, delivery and support of world leading aerospace and defense equipment. Specializing in Airborne Armament Equipment (AAE), Marvin Engineering is one of the major defense suppliers of ejector racks, missile launchers, aircraft pylons and other associated equipment such as test sets.

Marvin Engineering is the flagship company of The Marvin Group and a worldwide leader in Alternate Mission, Auxiliary Aircraft and Role Equipment. The company supports both in-service and emerging platforms including F-15, F-16, F-18, F-22, F-35, and rotary-wing applications such as Blackhawk, Cobra and Apache. Marvin Engineering also provides equipment to support unmanned aerial systems such as Predator, Reaper and Gray Eagle, as well as ground launch systems including SLAMRAAM and NASAMS.

Marvin Engineering's products and services are offered both domestically and internationally and are currently being provided through the Department of Defense (DoD), Foreign Military Sales (FMS), Prime Contractors and via Direct Commercial Sales (DCS).

Marvin's Challenges and Use Cases

As a supplier to the US and foreign governments, Marvin Engineering is subject to strict regulations regarding who can access confidential information about their products and services. They are required to share this information with their partners and suppliers but must do so in a very controlled manner. When Marvin Engineering needs to share critical information from their Flyer Defense Group with large subcontractors, who may compete with them for other government projects, they must ensure that only the necessary data is shared.

To avoid penalties and fines, Marvin needs to ensure that access to data subject to export compliance is strictly controlled and sharing is restricted to authorized parties only. Compliance with ITAR, EAR and other export regulations needs to be enforced across the organization.

Another objective for Marvin is to prevent data leakage and misuse. They want to implement a solution that allows them to protect sensitive data and continually monitor and track who is using what data and how. Business policies and regulatory mandates require data usage and audit capabilities.

NextLabs Solution: Enterprise Digital Rights Management (EDRM) for Teamcenter

To gain the level of controls necessary to assign specific rights to certain individuals on a need to know basis, Marvin selected Enterprise Digital Rights Management (EDRM) for Teamcenter, a rights protection solution based on dynamic authorization and Attribute Based Access Control (ABAC) by NextLabs. Enterprise Digital Rights Management is natively integrated with Teamcenter, so it is seamless to the end user. It allows the organization to make access decisions based on real-time contextual information about the user, the data and the environment at the time of request to prevent unauthorized access.

This advanced method ensures that the most up-to-date and relevant information is used to determine whether to allow or deny access. For example, if certain data can only be accessed by a US citizen located in the US, the system checks the user's nationality and location at the time of the request. Location, as well as time, network, device, classification, project, user position, among many other variables, provide the context to make the right decision in real-time.

A unique differentiator of the NextLabs EDRM solution is that it is built to secure any data type – particularly more complex files, such as 2 & 3D CAD models and other proprietary PLM data. It also provides a variety of viewing options, so partners and suppliers do not have to download special software to view protected files. They can simply access the files through a web browser or mobile app. This allows secure sharing among all of the partners and suppliers in a very scalable manner.

The solution automatically encrypts sensitive data according to the business rules and policies that apply. End users are not required to take any action. The protection persists throughout the sharing process, regardless of where the data goes. You can use the solution to impose time limits on access to certain data which prevents access by contractors or suppliers who are no longer associated with the project or company.

The Benefits

Marvin's critical data is continually protected throughout the extended enterprise, even when it is being shared with partners outside of their organization. Only authorized users can view the information and permissions are granted for view, edit, print on an individual basis. This prevents unauthorized users from accessing sensitive project information.

Another benefit of the solution is the centralized management capability. Policies are centrally managed, so all enforcement is consistent throughout the enterprise. As the business requirements change, policies can be amended quickly and updated across all applications. This is particularly beneficial to ensure that as regulations change, the company can quickly and easily update policies to reflect the new requirements. These new policies are then automatically enforced throughout the extended enterprise.

Organizations subject to export controls and secure data sharing mandates must audit and report on data usage. NextLabs offers comprehensive tracking, monitoring and audit capabilities so Marvin can see who is accessing which documents in real time. Marvin can proactively monitor compliance with ITAR and other export regulations. Alerts notify users of any anomalies in data activity to prevent major violations and data leakage.

The NextLabs' solution for Marvin Engineering is now implemented and is protecting 1,000 users. The next step is to implement internal controls across a wider audience to eliminate internal misuse of critical information.

ABOUT NEXTLABS

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premise.

The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM.

For more information on NextLabs, please visit

http://www.nextlabs.com.