

Bajaj Auto Group

Automotive Manufacturer



The Bajaj Group is one of the top ten business houses in India, with a footprint that spans a wide range of industries including automobiles, home appliances, lighting, iron and steel, insurance, travel, and finance.

The group's flagship company, Bajaj Auto, manufactures and sells motorcycles, scooters, and auto rickshaws. The division is ranked as the world's sixth largest manufacturer of motorcycles and the second largest in India. Bajaj Auto is the world's largest three-wheeler manufacturer. The Auto Group has a market cap of \$9.5 billion and employs more than 9,000 people.

THE CHALLENGE AND USE CASE

Like most major manufacturers, Bajaj shares critical engineering information with multi-tiered suppliers and partners. Protecting the confidentiality of intellectual property (IP) including product designs, processes, and manufacturing specifications is a challenge. Bajaj's information is secure when they use it within Siemens Teamcenter, however, it is vulnerable and unprotected when it leaves the application. Bajaj needs to ensure that their IP can only be accessed by authorized users when it is shared with partners and suppliers that are part of their extended enterprise.

The issue is further complicated by what people are authorized to do once they get access to sensitive data. When partners, customers, or suppliers request access, they are often limited by certain rights or privileges associated with their profile, including the right to view, edit, copy, save, or print. These rights must be enforced as data is shared across multiple environments.

THE SOLUTION: ENTERPRISE SKYDRM FOR TEAMCENTER

Bajaj needed a solution that could handle all types of engineering data and files, including 2D and 3D CAD, and the ability to manipulate and specify parts of the file to be viewed and edited. After evaluating various solutions, Bajaj chose NextLabs' SkyDRM for Teamcenter. The NextLabs solution utilizes Dynamic Authorization with Attribute Based Access Control (ABAC) to provide fine-grained access and usage controls. Attribute-based policies leverage detailed characteristics of the user, the data, and the environment at the time of access to determine what rights a user has to the document and if authorization should be granted.

Dynamic Authorization uses the most up-to-date information to make decisions, taking into account attributes of the user, such as title, job function, program assignment, and location; attributes of the data, such as classification, revision, and associated product; information about the network and device where the access request is coming from; as well as any attribute that the organization deems relevant. To safeguard intellectual property and increase data protection, the most up-to-date information is considered before granting access to intellectual property.

Centralized policy management with enforcement at the point of access provides consistent application of data governance and safeguards information sharing across the enterprise. Comprehensive audit and reporting capabilities allow Bajaj to easily monitor abnormal activity and track data usage in real time. Bajaj can now safeguard product data distribution among multi-tiered suppliers so that their IP remains secure throughout the manufacturing process regardless of where it goes. Only the information that is necessary to transact business is shared — on a “need to know” basis without risk of data loss.

NextLabs provided the complete enterprise digital rights management solution Bajaj needed to consistently protect all of their files with one solution and the ability to access protected information from any device without installing any software. Critical product and engineering data in Teamcenter is protected throughout the data lifecycle regardless of where it goes and with whom it is shared.

THE BENEFITS FOR BAJAJ

After implementing NextLabs' SkyDRM, Bajaj was able to provide a secure method for sharing their critical engineering and product information with complete visibility into all data access and usage activity. This gave them the ability to amend policies and processes quickly to respond to changes in the business environment. Some of the specific benefits include:

Dynamic and Fine-Grained Access Decisions

Bajaj can make fine-grained access decisions dynamically which result in improved data governance and fewer policy violations.

Centralized Policy Management

Central administration allows changes in policies to be made quickly and easily with consistent enforcement across the organization, regardless of system or location.

Enhanced Visibility and Reporting

Monitoring capabilities and alerts enable Bajaj to detect anomalies quickly and prevent violations. Centralized reporting and forensic analysis also facilitates and streamlines the audit process.

Automated Controls

Automated controls ensure that appropriate protection is applied automatically, and policies are always enforced without reliance on the end user to apply protection or manual processes.

Protection Anytime, Anywhere

Critical product and engineering data in Teamcenter is protected throughout the data lifecycle — regardless of where it goes and with whom it is shared.

Ease of Use and Transparency to the End User

End users do not have to change the way they do business — protection is seamless and is applied automatically based on policy

THE RESULT

Now that Bajaj Auto has implemented NextLabs' SkyDRM solution, they have the assurance they need that their data is always secure. Their sensitive data is automatically protected so that only authorized users have access. Key stakeholders can now feel comfortable sharing confidential documents with external suppliers without the risk of data loss and sharing violations. Bajaj management now receives real-time alerts about anomalies in end-user behavior. They also receive reports on data access and usage to ensure compliance with company policies.

NEXTLABS® | **Zero Trust
Data-Centric Security**

ABOUT NEXTLABS

NextLabs®, Inc. provides zero trust data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based zero trust 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 premises. 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, AWS, Accenture, Deloitte, Infosys, and IBM. For more information on NextLabs, please visit: <http://www.nextlabs.com>.